EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2010/0273(COD)

27.1.2012

AMENDMENTS
34 - 128

Draft report
Monika Hohlmeier
(PE476.089v01-00)

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_LegReport

Amendment 34
Alexander Alvaro

Proposal for a directive
Citation 2

Text proposed by the Commission	*Amendment*
Article 83(1) thereof,	Article ***16 and Article*** 83(1) thereof,

Or. en

Amendment 35
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 and other specialised law enforcement services of the Member States***, the Commission, Eurojust, Europol and the European Network and Information Security Agency (ENISA), to enable a common and comprehensive EU approach***.

Or. ro

Amendment 36
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 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***.

Or. ro

Amendment 37
Marie-Christine Vergiat, Kyriacos Triantaphyllides

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, ***at least those linked to*** organised crime, are a growing menace, and there is increasing concern about the potential for terrorist 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.

Or. fr

Amendment 38
Ioan Enciu

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 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***, such as 'botnet' networks, in which a large number of information systems are infected via a computer program so that they can be controlled and used to commit large-scale cyber attacks***.

Or. ro

Amendment 39
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 for ***response and prevention mechanisms and*** penalties in respect of attacks against information systems. The penalties provided for should be effective, proportionate and dissuasive.

Or. ro

Amendment 40
Jan Mulder

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. The penalties provided for should be effective, proportionate and dissuasive ***and could include imprisonment and/or financial penalties***.

Or. en

Amendment 41
Marie-Christine Vergiat, Kyriacos Triantaphyllides

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. The penalties provided for should be proportionate.

Or. fr

Amendment 42
Marian-Jean Marinescu

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(6) Member States should provide for penalties in respect of attacks against	(6) Member States should provide for ***effective measures to prevent attacks***

information systems. ***The penalties provided for*** should ***be effective***, ***proportionate and dissuasive***.	***against information systems and*** penalties in respect of attacks against information systems. ***Member States and the Union*** should ***ensure a comprehensive framework dealing with prevention***, ***teaching of personal cyber security to citizens as part of all digital literacy curriculum***. ***The penalties provided for should be effective, proportionate and dissuasive.***

Or. en

Amendment 43
Axel Voss

Proposal for a directive
Recital 7 a (new)

Text proposed by the Commission	*Amendment*
	(7a) There should be no mandatory requirement to impose a penalty in cases deemed to be 'minor'. A case may be considered as '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 an information system or computer data, or to a person's integrity, rights and other interests, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary;

Or. de

Justification

The definition of 'minor' cases should be included in Article 2. However, since a 'minor case' is such an imprecise legal concept, further elucidation is also required in the recitals, and can give some indication of the scope of the directive for legal purposes.

Amendment 44
Ioan Enciu

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, ***such as via a 'botnet' network,*** 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 ***critical infrastructure or*** essential interests.

Or. ro

Amendment 45
Jan Philipp Albrecht

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 intend to impose criminal liability where the offences are committed without criminal intent, such as for testing or protection of information systems***, provided that the operator or vendor of the system is fully informed of the vulnerability in a timely manner, or where the withholding of an authorisation for access to a system constitutes an abuse of rights by itself***.

Or. en

Justification

This AM ensures whistleblower protection, which according to the IT security experts is a vital function of how the global IT immune system works. The rapporteur proposes to de-criminalise access 'in accordance with law' instead of 'authorised', which goes into the right direction but this directive is the law that should clearly spell out what is allowed and what not. The last part of the sentence is based on the rapporteur's AM 7

Amendment 46
Marie-Christine Vergiat

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, e.g. the ability of an information system to resist criminal acts as defined in this Directive, or to make available tools used or intended to be used to enhance that ability***. ***It also does not seek to impose criminal liability if the objective criteria used to define the crimes listed in this Directive have been met, but the act was committed without criminal intent.***

Or. fr

Amendment 47
Monika Hohlmeier

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	(10) This Directive does not intend to impose criminal liability where the ***objective criteria of the crimes listed in***

intent, such as for ***authorised*** testing or protection of information systems.	***this Directive are met but the*** offences are committed without criminal intent, such as for testing ***in accordance with law*** or protection of information systems***, or where the withholding of an authorisation for access to a system constitutes an abuse of rights by itself***.

Or. en

Amendment 48
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 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, ***including as regards restoring information system functionality,*** the preservation of data ***in conformity with personal data protection principles***, the collection of evidence, the provision of legal information, and the locating ***and identification*** of suspects.

Or. ro

Amendment 49
Rolandas Paksas

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. ***Because not all the Member States collect information concerning attacks against information systems, little is known about such attacks. Because the methods used to collect statistics differ, the Member States which do collect them cannot compare them.*** 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.

Or. lt

Amendment 50
Ioan Enciu

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) It is also necessary to foster and improve cooperation between service providers, producers, law enforcement authorities and judicial authorities, while fully respecting the rule of law, especially as regards legal certainty and foreseeability, as well as the rights of

suspected and accused persons such as the presumption of innocence and judicial redress. That cooperation should include, for example, providing support to service providers for shutting down, completely or partially, illegal systems or functions, in accordance with the legislation in force.

Or. ro

Amendment 51
Jan Philipp Albrecht

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) In order to fight cybercrime effectively, it is also necessary to increase the resilience of information systems by protecting them more effectively against attacks and setting the right incentives for this. In this respect, the establishment of minimum standards and of liability for vendors and operators for the adequate protection of information systems should play a central role. Therefore, the Union and the Member States' fight against cybercrime will have an impact, only if this Directive is accompanied by preventive measures against such offences adopted in accordance with Article 67(3) and Article 84 of the Treaty of the Functioning of the European Union.

Or. en

Justification

This is AM 9 from the rapporteur with incentives and liabilities added. If there is only work on standards without any enforcement and incentives, we will be in the same situation as before. Vendors and operators of IT systems who grossly violate state of the art security techniques or refuse fixing known vulnerabilities should be held liable for this, including

criminal liability in severe cases.

Amendment 52
Marie-Christine Vergiat

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) Member States should regard the protection of their information systems and the data they contain as part of their duty of care. Reasonable levels of protection should be provided against reasonably identifiable threats and areas of vulnerability. The costs and charges linked to this protection should reflect the harm which a cyber attack would cause to the persons concerned.

Or. fr

Justification

This amendment is based on Amendment 10 by Ms Hohlmeier, with certain changes.

Amendment 53
Monika Hohlmeier

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) Member States should consider the protection of their information systems and associated data as part of their respective duty of care. Appropriate levels of protection should be provided against reasonably identifiable threats. The cost and burden of such protection should be proportionate to the likely damage to

those affected.

Or. en

Amendment 54
Ioan Enciu

Proposal for a directive
Recital 12 b (new)

Text proposed by the Commission	*Amendment*
	(12b) The European Union and Member States should pay due regard to the protection of their information systems and associated data and provide a high level of protection against identifiable threats and vulnerabilities. The cost and burden of such protection should be proportionate to the potential damage to those affected by cyber attacks.

Or. ro

Amendment 55
Jan Philipp Albrecht

Proposal for a directive
Recital 12 b (new)

Text proposed by the Commission	*Amendment*
	(12b) Member States should consider the protection of their information systems and associated data. Reasonable levels of protection should be provided against reasonably identifiable threats and vulnerabilities. The cost and burden of such protection should be proportionate to the likely damage to those affected.

Or. en

Justification

This is AM 10 from the rapporteur with 'duty of care' deleted and vulnerabilities added. Threats are very difficult to identify and could come from anywhere, therefore protection has to focus on vulnerabilities.

Amendment 56
Marie-Christine Vergiat

Proposal for a directive
Recital 12 b (new)

Text proposed by the Commission	*Amendment*
	(12b) Member States should also take appropriate steps to oblige legal persons who operate of supply information systems on their territory to protect personal data in their care against offences referred to in this Directive. Legal persons should provide reasonable levels of protection against reasonably identifiable threats and areas of vulnerability. Member States should ensure that a legal person who has failed to provide a reasonable level of protection is liable to criminal prosecution for negligence and to severe penalties if the damage suffered as a result of that failure is considerable.

Or. fr

Justification

This amendment is based on Amendment 11 by Ms Hohlmeier, with certain changes.

Amendment 57
Monika Hohlmeier

Proposal for a directive
Recital 12 b (new)

Text proposed by the Commission	*Amendment*
	(12b) Member States should also take appropriate steps to oblige legal persons within their jurisdictions to protect personal data in their care from offences referred to in this Directive, as already envisaged by EU law on telecommunications and data protection. Appropriate levels of protection should be provided by legal persons against reasonably identifiable threats 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 to those affected. Where a legal person has clearly failed to provide an appropriate level of protection, and where the damage caused as a result of such failure is considerable, Member States should ensure that it is possible to prosecute that legal person.

Or. en

Justification

By dealing with personal data legal persons carry the responsibility of protecting this data at an adequate level in view of reasonably identifiable threats. This is already envisaged in Directive 2002/58/ EC on e-privacy, in Directive 95/46/EC on data protection and the proposal on a General Data Protection Regulation COM(2012) 11 final (among others, art. 22, 30). If they fail to provide this level of protection, Member States should ensure that it is possible to prosecute this legal person.

Amendment 58
Ioan Enciu

Proposal for a directive
Recital 12 c (new)

Text proposed by the Commission	*Amendment*
	(12c) The European Network and Information Security Agency (ENISA) should play a key role in providing the Member States and EU institutions and bodies with technical expertise in the field of preventing and combating cyber attacks, in line with its mandate. In this connection, ENISA should advise the Member States on the establishing and operation of national contact points and Computer Emergency Response Teams (CERTs). ENISA should also be forwarded statistical data by the Member States on offences under this Directive and, on the basis of this and other relevant information, should draw up reports and recommendations on the state of information system and computer data security.

Or. ro

Amendment 59
Marie-Christine Vergiat

Proposal for a directive
Recital 12 c (new)

Text proposed by the Commission	*Amendment*
	(12c) It is also necessary to foster and improve cooperation between service providers, producers and law-enforcement bodies, whilst fully respecting the rule of law, especially as regards legal certainty and the rights of suspects and accused persons, such as the presumption of innocence and the right to seek legal redress. It is also necessary that in a constitutional state the persons responsible for enforcing the law should respect the rule of law.

Or. fr

Justification

This amendment is based on Amendment 12 by Ms Hohlmeier, with changes at the end. It also reiterates certain principles.

Amendment 60
Jan Philipp Albrecht

Proposal for a directive
Recital 12 c (new)

Text proposed by the Commission	*Amendment*
	(12c) Member States should also take appropriate steps to oblige legal persons within their jurisdictions who operate or provide IT systems to protect from offences referred to in this Directive. Reasonable levels of protection should be provided by legal persons against reasonably identifiable threats and vulnerabilities. Such protection should be proportionate to the likely damage to those affected. Where a legal person has clearly failed to provide a reasonable level of protection, and where the damage caused as a result of such failure is considerable, Member States should ensure that it is possible to impose deterrent sanctions and to prosecute this legal person for negligence.

Or. en

Justification

This AM adds vulnerabilities and replaces 'data in their care', which would only address operators, with 'who operate or provide IT systems' in order to also address vendors. It deletes 'personal', because for this directive, it is not just personal data that should be protected, but all data and adds 'negligence' and 'deterrent sanctions' for cases where a failure to provide reasonable protection has caused considerable damage. This would overcome the current 'as is' software licenses that free the vendor from all liabilities.

Amendment 61
Monika Hohlmeier

Proposal for a directive
Recital 12 c (new)

Text proposed by the Commission	*Amendment*
	(12c) It is also necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law, especially as regards legal certainty and foreseeability, as well as the rights of suspected and accused persons such as the presumption of innocence and judicial redress. This should include, for example, support by service providers in helping to preserve potential evidence, in providing elements helping to identify perpetrators and, as last resort, to shut down illegal systems or functions.

Or. en

Justification

The cooperation between service the private and the public sector is essential in order to effectively fight against cyber attacks.

Amendment 62
Marie-Christine Vergiat

Proposal for a directive
Recital 12 d (new)

Text proposed by the Commission	*Amendment*
	(12d) Without prejudice to voluntary cooperation between legal persons, such as service providers and producers, on the one hand, and law-enforcement bodies and judicial authorities, on the other,

Member States should define the cases in which the failure to act can in itself constitute criminal behaviour.

Or. fr

Justification

This amendment is based on Amendment 13 by Ms Hohlmeier, with changes at the end to make the new provision more binding.

Amendment 63
Jan Philipp Albrecht

Proposal for a directive
Recital 12 d (new)

Text proposed by the Commission	*Amendment*
	(12d) It is also necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law, especially as regards legal certainty and foreseeability, as well as the rights of suspected and accused persons such as the presumption of innocence and judicial redress.

Or. en

Justification

This is AM 12 from the rapporteur with the last sentence deleted. Shutting down of (allegedly) 'illegal systems' is a very risky business that currently very often is done without proper rule of law procedures and therefore introduces 'privatised policing'. This aspect should be addressed in the context of the upcoming initiative from the Commission on notice & takedown (announced for 2012 in the Commission work programme).

Amendment 64
Marie-Christine Vergiat

Proposal for a directive
Recital 12 e (new)

Text proposed by the Commission	*Amendment*
	(12e) In order to fight cybercrime effectively, it is also necessary to increase the resilience of information systems by taking appropriate measures to protect them more effectively against attacks. In that connection, the introduction of minimum standards and of the principle of the criminal liability of operators and producers in respect of the appropriate protection of information systems is fundamental. For this reason, the Union's and the Member State' fight against cybercrime will be effective only if this Directive is accompanied by preventive measures to combat such offences adopted in accordance with Articles 67(3) and 84 of the Treaty on the Functioning of the European Union.

Or. fr

Amendment 65
Ioan Enciu

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 *cross*-border dimension, thus underlining the urgent need for further action to approximate criminal legislation	(13) Significant gaps and differences in Member States' laws 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

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.	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. ***The European Union should also seek to improve international cooperation on information system, computer network and computer data security, and ensure that consideration is given, in any international agreement involving the exchange of data, to the security of data transfer and storage.***

Or. ro

Amendment 66
Tiziano Motti

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. 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. ***There is, moreover, an urgent need to carry into effect the***

European Parliament declaration of 23 June 2010 on setting up a European early warning system (EWS) for paedophiles and sex offenders[1];

---

[1] ***OJ C 236 E, 12.8.2011, p.152***

Or. it

Amendment 67
Rolandas Paksas

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 ***and criminal law procedures and systems*** in the area of attacks against information systems area may hamper the fight against organised crime and terrorism, and may complicate effective ***international*** police and judicial cooperation in this area***, since widely differing measures may be employed to combat such crimes***. 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.

Or. lt

Amendment 68
Marie-Christine Vergiat

Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(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 subsidiarity 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.	(14) Since the objectives of this Directive, i.e. ensuring that attacks against information systems***, at least when they are perpetrated with criminal intent,*** are punished in all Member States by proportionate criminal penalties and improving and encouraging judicial cooperation, 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 subsidiarity 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.

Or. fr

Amendment 69
Marie-Christine Vergiat, Kyriacos Triantaphyllides

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) Any personal data processed in the context of the implementation of this Directive should be protected in accordance with the rules laid down in the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters with regard to those processing activities which fall	(15) Any personal data processed in the context of the implementation of this Directive should be protected in accordance with the rules laid down in the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters with regard to those processing activities which fall

within its scope and Regulation (EC) No. 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.	within its scope and Regulation (EC) No. 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. ***This Directive should also be consistent with Directive 95/46/EC[1] and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981; it should also take account of two recommendations of the Committee of Ministers of the Council of Europe, No R(87)15 regulating the use of personal data in the police sector and No R(95)4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services.***
	[1]Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
	Or. fr

Amendment 70
Marie-Christine Vergiat, Kyriacos Triantaphyllides

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	(16) This Directive ***should respect*** fundamental ***freedoms and*** rights and ***observe*** the principles recognised in particular by the Charter of Fundamental Rights of the European Union ***and the***

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.	***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. This Directive ***must*** ensure full respect for these rights and principles and ***should*** be implemented accordingly.

Or. fr

Amendment 71
Marie-Christine Vergiat

Proposal for a directive
Recital 16 a (new)

Text proposed by the Commission	*Amendment*
	(16a) This Directive is not intended to be applied by the Member States in a manner which is not consistent with Articles 2 and 3(1) and (2) of the Treaty on European Union, which lay down principles which must apply to cyberspace and the fight against cybercrime. Its application must not undermine the principle of internet neutrality.

Or. fr

Amendment 72
Ioan Enciu

Proposal for a directive
Article 1

Text proposed by the Commission	*Amendment*
This Directive defines criminal offences in	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.	the area of attacks against information systems and establishes 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 73
Marie-Christine Vergiat, Kyriacos Triantaphyllides

Proposal for a directive
Article 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 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. ***It also aims to encourage the production of ever more secure IT tools and the installation of ever more secure IT systems.***

Or. fr

Amendment 74
Ioan Enciu

Proposal for a directive
Article 2 – point c

Text proposed by the Commission	*Amendment*
(c) "legal person" means any entity having such status under the applicable law***, except for States or other public bodies in***	(c) "legal person" means any entity having such status under the applicable law;

the exercise of State authority and for public international organisations;

Or. ro

Amendment 75
Alexander Alvaro

Proposal for a directive
Article 2 – point c

Text proposed by the Commission	*Amendment*
(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;***	(c) 'legal person' means any entity having such status under the applicable law

Or. en

Amendment 76
Jan Philipp Albrecht

Proposal for a directive
Article 2 – point c

Text proposed by the Commission	*Amendment*
(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***;***	(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***, which does not imply that States or other public bodies should be able to attack information systems without a legal basis and full respect for fundamental rights.***

Or. en

Justification

We don't want state hacking be legalised, as it would violate the 'basic right to the integrity and confidentiality of information technical systems' as determined by the German Constitutional Court.

Amendment 77
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***, use*** 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 78
Jan Philipp Albrecht

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 ***unless the withholding of such authorisation constitutes an abuse of rights by itself***, or ***unless such access or interference is*** permitted under national legislation***;***

Or. en

Justification

This is based on AM 17 from the rapporteur, with 'use' deleted (too broad, includes anything).

We also propose to clarify 'or not permitted under national legislation', to make sure it is read as an exception clause, not as an option for member states to widen the scope of the directive.

Amendment 79
Monika Hohlmeier

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***, use,*** or interference not authorised by the owner, other right holder of the system or of part of it, or not permitted under national legislation.

Or. en

Amendment 80
Marie-Christine Vergiat

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, ***unless the denial of such authorisation in itself constitutes an abuse of the law*** or ***unless such access or interference is*** permitted under national legislation.

Or. fr

Amendment 81
Axel Voss

Proposal for a directive
Article 2 – point d a (new)

Text proposed by the Commission	*Amendment*
	(da) 'minor case' means a case where the offence itself is deemed to be minor, there is no pressing need to prosecute in the public interest and the consequences of the offence are negligible;

Or. de

Justification

Since 'minor' cases are an integral part of this directive, Article 2 should contain a reasonably precise definition of such cases.

Amendment 82
Axel Voss

Proposal for a directive
Article 2 – point d b (new)

Text proposed by the Commission	*Amendment*
	(db) 'interception' means listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly or indirectly through the use of electronic eavesdropping or tapping devices by technical means.

Or. de

Justification

The meaning of 'interception' should be precisely defined.

Amendment 83
Alexander Alvaro

Proposal for a directive
Article 2 a (new)

Text proposed by the Commission	*Amendment*
	Article 2a
	Preventive measures
	1. Member States shall in cooperation with the European Network and Information Security Agency promote good practices in relation to security of data processing and support cooperation between public and private stakeholders by facilitating information sharing, awareness raising and dialogue on network and information security, including aspects of the fight against cybercrime.
	2. Member States shall ensure that in the case of a personal data breach, the data controller and the data processor notify without undue delay and, as a rule, not later than 24 hours after the personal data breach has been established, the personal data breach to the competent national authority in line with Article 4 of Directive 2002/58/EC as amended by Directives 2006/24/EC and 2009/136/EC (e-privacy Directive).
	3. Member States shall take the necessary measures to protect critical infrastructure from cyber attacks and provide for means to hermetically cut off access to a critical infrastructure in case a direct cyber attack severely threatens its proper functioning.

Or. en

Amendment 84
Alexander Alvaro

Proposal for a directive
Article 3

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional access without right ***to*** the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.	Member States shall take the necessary measures to ensure that the intentional access without right – ***meaning entering*** the whole or any part of an information system – is punishable as a criminal offence, at least for cases which are not minor. ***Each Member State shall decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing an effective security measure.***

Or. en

Amendment 85
Marie-Christine Vergiat

Proposal for a directive
Article 3

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which ***are not minor***.	Member States shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which ***involve criminal intent and which have serious and damaging consequences for the existence and functioning of the information system or systems concerned***. ***The actions referred to in the first subparagraph shall only be regarded as a criminal offence if a security measure has been breached and if the operator or provider of the system was not informed comprehensively and in good time of the vulnerability of the information system.***

Or. fr

Amendment 86
Jan Philipp Albrecht

Proposal for a directive
Article 3

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information ***system*** is punishable as a criminal offence, at least for cases which are not minor.	Member States shall take the necessary measures to ensure that the intentional access without right ***-meaning entering*** to the whole or any part of an information ***system-*** is punishable as a criminal offence, at least for cases which are not minor. ***The conduct referred to in paragraph 1 shall be incriminated only where the offence is committed by infringing a security measure and provided that the operator or vendor of the system is not fully informed of the vulnerability in a timely manner.***

Or. en

Justification

This is based on AM 20 from the rapporteur, with two changes: 1) It does not leave it to the member states to introduce the threshold of infringing a security measure, which ensures that e.g. using your neighbour's public and open wifi does not constitute a crime. 2) It adds 'provided that the operator or vendor of the system is not informed of the vulnerability afterwards'. This is taken from our AM on whistleblower protection.

Amendment 87
Monika Hohlmeier

Proposal for a directive
Article 3

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional access ***without right to*** the whole or any part of an information system is punishable as a criminal offence, at least for cases	Member States shall take the necessary measures to ensure that the intentional access **–** ***meaning entering*** the whole or any part of an information system **–** ***without right*** is punishable as a criminal

which are not minor.	offence, at least for cases which are not minor. ***Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.***

Or. en

Amendment 88
Marie-Christine Vergiat, Kyriacos Triantaphyllides

Proposal for a directive
Article 4

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional 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 without right, at least for cases which ***are not minor***.	Member States shall take the necessary measures to ensure that the intentional 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 without right, at least for cases which ***involve criminal intent and which have serious and damaging consequences for the existence and functioning of the information system or systems concerned***.

Or. fr

Amendment 89
Marie-Christine Vergiat

Proposal for a directive
Article 5

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional	Member States shall take the necessary measures to ensure that the intentional

deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which ***are not minor***.	deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which ***involve criminal intent and which have serious and damaging consequences for the existence and functioning of the information system or systems concerned***.

Or. fr

Amendment 90
Axel Voss

Proposal for a directive
Article 6

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional 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 without right.	Member States shall take the necessary measures to ensure that the intentional 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 without right, ***at least in cases which are not minor***. ***Interception may also involve recording. Data transmissions comprise the period taken to transfer the data, by cable or by wireless, between the time it is transmitted by the sender and the time it reaches the recipient. Technical means include technical devices fixed to transmission lines as well as devices to collect and record wireless communications, including the use of software, passwords and codes.***

Or. de

Amendment 91
Marie-Christine Vergiat

Proposal for a directive
Article 6

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional 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 without right.	***In accordance with Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and with the Charter of Fundamental Rights,*** 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 involve criminal intent and which have serious and damaging consequences for the existence and functioning of the information system or systems concerned***.

Or. fr

Amendment 92
Jan Philipp Albrecht

Proposal for a directive
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measures to ensure that the intentional 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	Member States shall take the necessary measures to ensure that the intentional 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 without right.	computer data, is punishable as a criminal offence when committed without right***, at least for cases which are not minor***.

Or. en

Amendment 93
Jan Philipp Albrecht

Proposal for a directive
Article 7 – introductory part

Text proposed by the Commission	*Amendment*
Member States shall take the necessary measure to ensure that the production, sale, procurement for use, import, possession, distribution or otherwise making available of the following is punishable as a criminal offence when committed intentionally and without right for the purpose of committing any of the offences referred to in Articles 3 to 6:	***deleted***
(a) device, including 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.	

Or. en

Justification

So-called 'hacker tools' are inherently dual-use, and they are crucially needed for security testing. If we want to have the whistleblower protection, we also have to legalise their possession and distribution. Passwords and access codes should not be regarded as hacker tools. If they get lost, the operator should immediately improve his security measures and set up new passwords, just as people do when they lose their keys.

Amendment 94
Marie-Christine Vergiat

Proposal for a directive
Article 7 – point a

Text proposed by the Commission	*Amendment*
(a) device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;	(a) device, including a computer program ***but excluding a computer itself***, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

Or. fr

Amendment 95
Marie-Christine Vergiat

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.	***deleted***

Or. fr

Amendment 96
Jan Philipp Albrecht

Proposal for a directive
Article 8

Text proposed by the Commission	*Amendment*
Instigation, aiding, abetting and attempt	***deleted***
1. Member States shall ensure that the instigation, aiding and abetting of 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 the offences referred to in Articles 3 to 6 is punishable as a criminal offence.

Or. en

Justification

We risk criminalising whistleblowers if publication of vulnerabilities (in cases where vendors or operators do not react) is considered as instigation, aiding or abetting. The paragraph also would move criminalisation far into the area before a crime is actually committed. It would be especially unproportionate to do this considering the safeguards we propose for minor offences etc.

Amendment 97
Marie-Christine Vergiat

Proposal for a directive
Article 8 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that the instigation, aiding and abetting of an offence referred to in Articles 3 to 7 is punishable as a criminal offence.	***deleted***

Or. fr

Amendment 98
Marie-Christine Vergiat

Proposal for a directive
Article 8 a (new)

Text proposed by the Commission	*Amendment*
	Article 8a
	Manufacturers' liability
	Member States shall take the measures

required to ensure that manufacturers are held criminally liable in connection with the production, placing on the market, marketing, operation and non-compliance with security standards of products and systems which are defective or which have proven security problems, thus making cyber attacks or data loss more likely.

Or. fr

Amendment 99
Jan Mulder

Proposal for a directive
Article 9 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, proportional and dissuasive criminal 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, proportional and dissuasive criminal penalties***, including the imposition of adequate fines***.

Or. en

Amendment 100
Marie-Christine Vergiat, Kyriacos Triantaphyllides

Proposal for a directive
Article 9 – paragraph 1

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

Or. fr

Justification

Some terms should be deleted, since they relate to the enforcement, and not the substance, of the law.

Amendment 101
Jan Philipp Albrecht

Proposal for a directive
Article 9 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to ***8*** are punishable by effective, proportional and dissuasive criminal penalties.	1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to ***6*** are punishable by effective, proportional and dissuasive criminal penalties.

Or. en

Justification

Logical consequence of deletion of articles 7 and 8

Amendment 102
Jan Mulder

Proposal for a directive
Article 9 – 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 7 are punishable by criminal penalties of a maximum term of imprisonment of at least two years.	2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by criminal penalties of a maximum term of imprisonment of at least two years ***including the imposition of an adequate fine***.

Or. en

Amendment 103
Marie-Christine Vergiat

Proposal for a directive
Article 9 – 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 7 are punishable by criminal penalties of a maximum term of imprisonment of ***at least*** two years.	2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by criminal penalties of a maximum term of imprisonment of two years.

Or. fr

Justification

The original wording is contradictory, and that contradiction should be done away with. Attention should be drawn to the principle that the punishment must fit the crime, something which can only be determined in a court of law, on the basis of an assessment of the facts of the case.

Amendment 104
Jan Philipp Albrecht

Proposal for a directive
Article 9 – 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 7 are punishable by criminal penalties of a maximum term of imprisonment of at least ***two*** years.	2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by criminal penalties of a maximum term of imprisonment of at least ***between one and three*** years ***of imprisonment***.

Or. en

Justification

A deviation from the penalty level contained in articles 6 and 7 of framework decision 2005/222/JHA on attacks against information systems has not been substantiated.

Amendment 105
Alexander Alvaro

Proposal for a directive
Article 10

Text proposed by the Commission	*Amendment*
Aggravating circumstances	***deleted***
1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by criminal penalties of a maximum term of imprisonment of at least five years when committed within the framework of a criminal organization as defined in Framework Decision 2008/841/JHA.	
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.	
3. 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 by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner.	

Or. en

Amendment 106
Marie-Christine Vergiat

Proposal for a directive
Article 10 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by criminal penalties of a maximum term of imprisonment of ***at least*** five years when committed within the framework of a criminal organization as defined in Framework Decision 2008/841/JHA.	1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by criminal penalties of a maximum term of imprisonment of five years when committed within the framework of a criminal organisation as defined in Framework Decision 2008/841/JHA.

Or. fr

Justification

The original wording is contradictory, and that contradiction should be done away with. Attention should be drawn to the principle that the punishment must fit the crime, something which can only be determined in a court of law, on the basis of an assessment of the facts of the case.

Amendment 107
Jan Philipp Albrecht

Proposal for a directive
Article 10 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by criminal penalties of a maximum term of imprisonment of at least five years when committed within the framework of a criminal organization as defined in Framework Decision 2008/841/JHA.	1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by criminal penalties of a maximum term of imprisonment of at least ***between two and*** five years when committed within the framework of a criminal organization as defined in Framework Decision 2008/841/JHA.

Or. en

Justification

A deviation from the penalty level contained in articles 6 and 7 of framework decision 2005/222/JHA on attacks against information systems has not been substantiated.

Amendment 108
Ioan Enciu

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 affecting critical infrastructure information systems***.

Or. ro

Amendment 109
Marie-Christine Vergiat

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	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 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.	significant number of information systems, or attacks causing considerable damage, such as disrupted system services, financial cost or loss of personal data.

Or. fr

Justification

The original wording is contradictory, and that contradiction should be done away with. Attention should be drawn to the principle that the punishment must fit the crime, something which can only be determined in a court of law, on the basis of an assessment of the facts of the case.

Amendment 110
Jan Philipp Albrecht

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 ***between two and*** 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. en

Justification

A deviation from the penalty level contained in articles 6 and 7 of framework decision 2005/222/JHA on attacks against information systems has not been substantiated.

Amendment 111
Jan Philipp Albrecht

Proposal for a directive
Article 10 – paragraph 3

Text proposed by the Commission	*Amendment*
3. 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 by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner.	***deleted***

Or. en

Justification

The concealment of the real identities of the perpetrator and the damage caused to the rightful identity owners are not only important for the punishment of offences within the scope of this Directive. Rather, on the long run this and related offences should be addressed by a horizontal instrument going beyond the attacks against information systems.

Amendment 112
Marie-Christine Vergiat

Proposal for a directive
Article 10 – paragraph 3

Text proposed by the Commission	*Amendment*
3. 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 by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner.	***deleted***

Or. fr

Amendment 113
Jan Philipp Albrecht, Marie-Christine Vergiat

Proposal for a directive
Article 10 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Member States shall ensure that the penalties referred to Article 9 will not apply to offences referred to in Articles 3 to 7 when the offences are clearly not committed for criminal intent, such as during the testing or the immediate protection of information systems, or if the operator or vendor of the system is fully informed of the vulnerability in a timely manner.

Or. en

Amendment 114
Jan Philipp Albrecht, Marie-Christine Vergiat

Proposal for a directive
Article 10 – paragraph 3 b (new)

Text proposed by the Commission	*Amendment*
	3b. Member States shall consider the protection of their information systems and associated data. Reasonable levels of protection should be provided against reasonably identifiable levels of threats and vulnerabilities, with the protection proportionate to the probable damage to the parties concerned.

Or. en

Justification

The rapporteur has already included incentives for better security in AMs 3 and 4 (recitals). We should put this into a real article.

Amendment 115
Jan Philipp Albrecht, Marie-Christine Vergiat

Proposal for a directive
Article 10 – paragraph 3 c (new)

Text proposed by the Commission	*Amendment*
	3c. Member States shall take appropriate steps to oblige legal persons under their jurisdictions to protect information systems from offences detailed in Articles 3 to 7. Reasonable levels of protection should be provided against reasonably identifiable levels of threats and vulnerabilities, with the protection proportionate to the probable damage to the parties concerned.

Or. en

Justification

The rapporteur has already included incentives for better security in AMs 3 and 4 (recitals). We should put this into a real article.

Amendment 116
Jan Philipp Albrecht, Marie-Christine Vergiat

Proposal for a directive
Article 10 – paragraph 3 d (new)

Text proposed by the Commission	*Amendment*
	3d. Where legal persons are considered to have failed to provide a reasonable level of protection as detailed in paragraph 3b and 3c against offenses detailed in Articles 3 to 7, and where these offenses

are considered to have been carried out with clear criminal intent, then these offenses will be considered to have been carried out under alleviating circumstances when applying criminal penalties.

Or. en

Justification

The rapporteur has already included incentives for better security in AMs 3 and 4 (recitals). We should put this into a real article. Paragraph 3d introduces alleviating circumstances for attackers who only had to overcome unreasonably weak security measures.

Amendment 117
Jan Philipp Albrecht, Marie-Christine Vergiat

Proposal for a directive
Article 10 – paragraph 3 e (new)

Text proposed by the Commission	*Amendment*
	3e. Where legal persons have clearly failed to provide a reasonable level of protection and in cases where the damage caused as a result of this failure is considerable, then Member States shall ensure that is possible to impose deterrent sanctions and to prosecute this legal person for negligence.

Or. en

Justification

The rapporteur has already included incentives for better security in AMs 3 and 4 (recitals). We should put this into a real article. Paragraph 3e introduces criminal liability (negligence) for clearly failing to provide reasonable security in cases where an attack has caused considerable damage.

Amendment 118
Alexander Alvaro

Proposal for a directive
Article 10 a (new)

Text proposed by the Commission	*Amendment*
	Article 10a
	Extenuating circumstances
	1. Member States shall ensure that the penalties referred to in Article 9 will not apply to offences referred to in Articles 3 to 7 when the offences are clearly not committed for criminal intent, such as during the mandated testing or the immediate protection of information systems.
	2. Member States shall consider the protection of their information systems and associated data as part of their respective duty of care. Reasonable levels of protection should be provided against reasonably identifiable levels of threats.
	3. Member States shall take the necessary measures to oblige data controllers and data processors within their jurisdiction to protect data from offences referred to in Articles 3 to 6 and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
	4. Where a data controller or a data processor is considered to have failed to provide a reasonable level of protection against offences referred to in Articles 3 to 6, these offences shall be considered to have been carried out under alleviating circumstances when applying criminal penalties.
	5. Where a data controller or a data processor has clearly failed to provide a reasonable level of protection and

consequently damage is caused, Member States shall ensure that it is possible to prosecute this data controller or data processor.

Or. en

Amendment 119
Marie-Christine Vergiat, Kyriacos Triantaphyllides

Proposal for a directive
Article 12 – paragraph 1 – introductory part

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

Or. fr

Justification

See justification for the amendment to Article 9.

Amendment 120
Ioan Enciu

Proposal for a directive
Article 12 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) exclusion from entitlement to public benefits or aid;	(a) ***temporary or permanent*** exclusion from entitlement to public benefits or aid;

Or. ro

Amendment 121
Marie-Christine Vergiat

Proposal for a directive
Article 12 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	2. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 11(2) is punishable by proportionate penalties or measures.

Or. fr

Justification

See justification for the amendment to Article 9.

Amendment 122
Axel Voss

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

Text proposed by the Commission	*Amendment*
(b) by one of their nationals ***or a person with habitual residence in the territory of the Member State concerned; or***	***(b) by one of their nationals; or***

Or. de

Justification

Any extension of the jurisdiction of foreign States over people who merely habitually reside in another Member State should be rejected on principle.

Amendment 123
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 conformity 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 124
Marian-Jean Marinescu

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,	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.	Member States shall make use of ***operational national points of contact and*** 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. en

Amendment 125
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***, Europol, Eurojust and the European Network and Information Security Agency (ENISA)*** 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 126
Marian-Jean Marinescu

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,	1. Member States shall ensure ***the operability of national contact points and***

production and provision of statistical data on the offences referred to in Articles 3 to 8.	***provide for*** a system for the recording, production and provision of statistical data on the offences referred to in Articles 3 to 8***; national contact points shall deal with requests for assistance and facilitate the following measures: provision of technical advice and legal information as well as establishing programs on prevention and fight against cybercrime***.

Or. en

Amendment 127
Marie-Christine Vergiat, Kyriacos Triantaphyllides

Proposal for a directive
Article 15 a (new)

Text proposed by the Commission	*Amendment*
	Article 15a
	Training
	1. Member States shall encourage the organisation and contribute to the funding of training courses for members of the public so that the latter are aware of the possibility of attacks intended to undermine the freedom and security of cyberspace and are able to protect themselves against such attacks.
	2. Member States shall incorporate into their school curricula lessons which teach pupils about IT tools, the dangers they pose and how to protect themselves.

Or. fr

Amendment 128
Marie-Christine Vergiat

Proposal for a directive
Article 15 b (new)

Text proposed by the Commission	*Amendment*
	Article 15b
	Conformity with levels of security
	1. Member States shall lay down in their national law criteria regarding the conformity of all IT tools with minimum levels of security.
	2. No more than two years after the adoption of this Directive, the Commission shall submit a proposal for a directive which lays down minimum security criteria for all IT tools sold on the internal market.

Or. fr