EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2010/0273(COD)

24.11.2011

***I
DRAFT REPORT

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

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Monika Hohlmeier

Symbols for procedures

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

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

Amendments to a draft act

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

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

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

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

(Ordinary legislative procedure: first reading)

The European Parliament,

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

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

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

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

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

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Foreign Affairs and the Committee on Industry, Research and Energy (A7-0000/2010),

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

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

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

Amendment 1

Proposal for a directive
Recital 1

Text proposed by the Commission	*Amendment*
(1) The objective of this Directive is to approximate rules on criminal law in the Member States in the area of attacks against information systems, and improve cooperation between judicial and other	(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

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

competent authorities, including the police and other specialised law enforcement services of the Member States.	competent authorities, including the police and other specialised law enforcement services of the Member States***, and specialised agencies of the Union***.

Or. en

Justification

Given the transnational nature of attacks against information systems, it is essential to improve the cooperation between judicial and police authorities of both the Member States and the European Union.

Amendment 2

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, 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. ***Attacks on critical infrastructures may have significant cross-border impacts and disrupt or destroy services which are absolutely vital for the security, safety, health, mobility, social and economic well-being of Union citizens and the good functioning of public administrations, such as power plants, transport networks and government networks.*** 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. en

Justification

It is necessary to outline the possible effects and the magnitude of cyber attacks particularly when committed against critical infrastructures.

Amendment 3

Proposal for a directive
Recital 7 a (new)

Text proposed by the Commission	*Amendment*
	(7a) While the concealment of the real identity of the perpetrator and the prejudice caused thereby to the rightful identity owner is an important element for the determination of penalties within the scope of this Directive, the Union should nevertheless develop a horizontal instrument which covers those and related offences in a more comprehensive form, addressing, inter alia, identity theft, the link to law on persons' names and consumer protection .

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 4

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	(8) The Council Conclusions of 27-28 November 2008 indicated that a new strategy should be developed with the Member States and the Commission, taking into account the content of the 2001 Council of Europe Convention on

Cybercrime. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive builds on that Convention.	Cybercrime. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive builds on that Convention. ***Therefore, it is essential that Member States which have not yet ratified the Council of Europe Convention on Cybercrime do so as soon as possible.***

Or. en

Justification

As the Convention on Cybercrime is the central instrument of international law to fight cybercrime, Member States who have not yet ratified the Convention should be encouraged to do so both for reasons of coherence and as a political sign.

Amendment 5

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive shall refer to 'tools' that can be used in order to commit the crimes listed in this Directive. Tools refer to, for example, malicious software, including botnets, used to commit cyber attacks.	(9) Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive shall refer to 'tools' that can be used in order to commit the crimes listed in this Directive. Tools refer to, for example, malicious software, including botnets, used to commit cyber attacks. ***These tools represent only a few among many possibilities of attacking information systems. Against this background, the work on a Union strategy on IT architecture, in particular cloud computing, including a technical standardisation and a common legal framework, should be continued and intensified.***

Or. en

Justification

In view of the current technical developments, a reference to cloud computing is essential. We need further technical standardization and a common European legal framework for cloud computing. This would also enhance the EU's role as supplier and user of state-of-the-art and secure IT structures.

Amendment 6

Proposal for a directive
Recital 9 a (new)

Text proposed by the Commission	*Amendment*
	(9a) The intentional use without right of a computer programme designed to remove evidence of the offences referred to in this Directive should be regarded either as a form of aiding and abetting or as a separate criminal offence.

Or. en

Justification

Whilst a computer programme designed to remove evidence is not a tool in the sense of Article 7 of this Directive, its deployment is nevertheless in support of cyber attacks. Therefore, Member States need to make sure that the use of such a programme is either considered as aiding and abetting or as an offence on its own (such as the obstruction of criminal investigations).

Amendment 7

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 ***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

Justification

The term "authorised testing" can be interpreted in a way that would require a formal authorization before the security testing of own information systems. This would entirely undermine the effectiveness and practicality of selftests without criminal intent. Further, there should be no criminal liability when the limitation of access to a system is illegal by itself.

Amendment 8

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) Against the backdrop of establishing a Union policy for the fight against cybercrime, the Council Conclusions of 24 October 2008, the Council Conclusions of 27-28 November 2008 and the Council Conclusions of 26 April 2010 allocated a specific role to Europol to contribute to this objective. To that end, Europol should establish and host a European platform which will be the point of convergence of national platforms and will have as its purpose, inter alia, to collect and centralise information about offences noted on the internet. This should include information about perpetrators and their modus operandi. In accordance with the Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol)[1], and specifically the rules on personal data protection in Chapter V, as well as in accordance with 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[2], this Directive takes account of the tasks designated to Europol.

[1] OJ L 121, 15.5.2009, p. 37.

[2] OJ L 350, 30.12.2008, p. 60.

Or. en

Justification

Given the transnational nature of attacks against information systems as well as the coordinating role of Europol, it is necessary to outline the Agency's role in the field of cyber attacks. For this purpose, the European Council has already given valuable guidance that should be taken into consideration in this Directive.

Amendment 9

Proposal for a directive
Recital 12 b (new)

Text proposed by the Commission	*Amendment*
	(12b) In order to fight cybercrime effectively, it is also necessary to increase the resilience of information systems by protecting them more effectively against attacks. In this respect, the establishment of minimum standards 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

Whilst criminal law is an important element in fighting cybercrime, it is nevertheless the very last step after an attack has occurred. Therefore, the EU should step up is efforts in better protecting their systems in the first place, for example with minimum standards for the adequate protection of information systems.

Amendment 10

Proposal for a directive
Recital 12 c (new)

Text proposed by the Commission	*Amendment*
	(12c) Member States should 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 threats. The cost and burden of such protection should be proportionate to the likely damage to those affected.

Or. en

Justification

Member States deal themselves with important and sensitive data, such as tax or health insurance information. Therefore, it is in their duty of care to adequately protect those data against attacks.

Amendment 11

Proposal for a directive
Recital 12 d (new)

Text proposed by the Commission	*Amendment*
	(12d) 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. Reasonable levels of protection should be provided by legal persons against reasonably identifiable threats. 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 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 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. If they fail to provide this level of protection, Member States should ensure that it is possible to prosecute this legal person.

Amendment 12

Proposal for a directive
Recital 12 e (new)

Text proposed by the Commission	*Amendment*
	(12e) 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 includes, for example, support by service providers 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 13

Proposal for a directive
Recital 12 f (new)

Text proposed by the Commission	*Amendment*
	(12f) Notwithstanding 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 could constitute a criminal behaviour by itself.

Or. en

Justification

The non-cooperation or obstruction of criminal investigations by legal persons is highly critical and could be seen as aiding and abetting to the offences outlined in this Directive, for example.

Amendment 14

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 ***adequate implementation and application*** of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings.

Or. en

Justification

Linguistic correction.

Amendment 15

Proposal for a directive
Recital 13 a (new)

Text proposed by the Commission	*Amendment*
	(13a) Improved cooperation between law enforcement bodies and between judicial authorities across the Union is essential in fighting effectively against cybercrime. In this context, the Commission and the Member States should step up their efforts, as regards adequate training of law enforcement bodies and judicial authorities, in order to raise the understanding of cybercrime and its impact, and foster cooperation and exchange of best practices, for example through the European Judicial Network, with the assistance of Europol, Eurojust and the European Network and Information Security Agency.

Or. en

Justification

Adequate training of the actors concerned with prosecuting cyber criminals is vital in the fight against cybercrime. Further, at EU level we already have instruments to enhance this cooperation and training. This is all the more important as police and judicial bodies are faced with legal systems that qualify and define offences differently. Mutual understanding is hence pivotal.

Amendment 16

Proposal for a directive
Recital 13 b (new)

Text proposed by the Commission	*Amendment*
	(13b) Such training and exchange of information should raise awareness of

differences in national legal systems and of the problems faced in criminal prosecutions as a result of having different national provisions on the seriousness of the offence, such as the level of damage, and the distribution of competences between national law enforcement bodies.

Or. en

Justification

When prosecuting cyber attacks, police and judicial bodies are faced with legal systems that qualify and define offences differently. Mutual understanding is hence pivotal.

Amendment 17

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, ***in as much as the withholding of such authorisation does not constitute an abuse of rights by itself,*** or not permitted under national legislation;

Or. en

Justification

The free flow of information must not be restricted in such a way that the withholding of an authorisation actually infringes other rights, such as the right to freedom of information, for instance. Withholding an authorisation can therefore constitute an abuse of rights by itself.

Amendment 18

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

Text proposed by the Commission	*Amendment*
	(da) "minor cases" may be considered as such, for example, when the damage 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 nature, that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary;

Or. en

Justification

"Minor cases" are an essential element of this Directive when qualifying an offence. For reasons of legal certainty, we therefore have to give a definition of this term.

Amendment 19

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

Text proposed by the Commission	*Amendment*
	(db) "critical infrastructure information systems" are information systems of infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

Or. en

Justification

For reasons of legal certainty, the term "critical infrastructure information systems" shall be clarified. The Commission Green Paper COM(2005) 576 as well as the Communications COM(2011)163 and COM(2009)149 on the protection of critical infrastructures provide valuable input for this.

Amendment 20

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 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

Justification

For reasons of legal certainty, "access" needs to be defined. Further, illegal access should presuppose the infringement of security measures. Otherwise, the unauthorised access to an open wifi network could for example qualify as an offence.

Amendment 21

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,	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.	including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed without right***, at least for cases which are not minor***. ***Interception by technical means relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the information system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording.*** ***Technical means includes 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. en

Justification

In coherence with Articles 3 to 5, also this Article should not include minor cases as an offence. Further, a definition of "interception" is necessary. The explanatory report of the Convention on Cybercrime offers valuable input for this in para. 53. For reasons of legal certainty, the term "technical means" shall be clarified. The explanatory report on the Convention of Cyber Crime provides a useful definition in paragraph 53, second part.

Amendment 22

Proposal for a directive
Article 7

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	Member States shall take the necessary *measures* to ensure that the production, sale, procurement for use, import, distribution or otherwise making available of the following is punishable as a criminal offence when committed intentionally and without right for the ***clear*** purpose of committing any of the offences referred to in Articles 3 to 6:

to 6:

Or. en

Justification

Given the possibility to use programmes in dual forms, i.e. for legal as well as criminal purposes, the possession of a tool should as such not be punishable. In addition, the purpose of the actions described in this article should only be punishable when it is clearly aimed at committing an offence.

Amendment 23

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) a computer *programme*, ***clearly*** designed or adapted for the purpose of committing any of the offences referred to in Articles 3 to 6;

Or. en

Justification

The term "device" creates legal uncertainty and could be interpreted for example as a simple hardware product, such as a computer or a camera. Therefore, it should be deleted. In addition, the term "primarily" is not sufficiently clear and could be specified by "clearly".

Amendment 24

Proposal for a directive
Article 8 – title

Text proposed by the Commission	*Amendment*
Instigation, aiding**,** abetting and attempt	***Incitement***, aiding ***and*** abetting and attempt

Or. en

Justification

Linguistic correction

Amendment 25

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

Or. en

Justification

Linguistic corrections

Amendment 26

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, ***proportionate*** and dissuasive criminal penalties.

Or. en

Justification

Linguistic correction.

Amendment 27

Proposal for a directive
Article 10 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall take the necessary	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.	measures to ensure that the offences referred to in ***Articles 4 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 *organisation* as defined in Framework Decision 2008/841/JHA. ***In these cases, the penalties as laid down in that Framework Decision shall not apply.***

Or. en

Justification

Article 3 of Framework Decision 2008/841/JHA foresees penalties of two to 5 years of imprisonment for offences committed in the framework of a criminal organisation, while Article 10 of this proposal foresees a maximum term of at least 5 years of imprisonment. For reasons of legal certainty, it must therefore be clarified which level of penalty is to be applied for cyber crime committed within the framework of a criminal organisation.

Amendment 28

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 4 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 ***serious*** damage, such as disrupted system services, financial cost or loss of personal data***, or when committed against a critical infrastructure information system***.

Or. en

Justification

Article 4 to 6 represent particularly heavy offences when committed at large scale and causing serious damage or when committed against critical infrastructure information

systems.

Amendment 29

Proposal for a directive
Article 14 – title

Text proposed by the Commission	*Amendment*
Exchange of information	Exchange of information ***and cooperation***

Or. en

Justification

In accordance with the following amendments, the scope of this article shall also include cooperation. For this purpose, the title of this article needs to be adapted

Amendment 30

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, ***by indicating*** whether and in what form the request for help will be answered and when. ***Such an exchange of information shall not affect Member States' national rules in relation to the gathering or admissibility of evidence as regards the use of such information in subsequent criminal proceedings.***

Or. en

Justification

While the rapid exchange of information and mutual help is an essential tool of fighting jointly against cross-border cyber attacks, these rules do no affect the admissibility of evidence in possible subsequent criminal procedures.

Amendment 31

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

Text proposed by the Commission	*Amendment*
	2a. For the exchange of information in relation to the offences referred to in Articles 3 to 8, Member States shall, in accordance with data protection rules, establish cooperation and partnership networks with service providers and producers.

Or. en

Justification

Besides the cooperation between the authorities, it is vital to increase the cooperation between the private sector and public authorities in order to effectively fight against cyber attacks and increase the resilience of both public and private networks.

Amendment 32

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 statistical data collected according to this Article to the Commission ***and to the European Network and Information Security Agency for the purpose of assessing the state of network and information security in accordance with Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information***

Security Agency*[1]*.

Member States shall also transmit the statistical data and other available data on the modus operandi used by the perpetrators to Europol for the purpose of conducting threat assessment and strategic analyses of cybercrime in accordance with the Council Decision 2009/371/JHA.

The Commission together with the Member States shall also ensure that a consolidated review of these statistical reports is published.

---

[1] OJ L 77, 13.3.2004, p. 1.

Or. en

Justification

Given the transnational nature of attacks against information systems and the possible effects across the Union, it is necessary to involve both the European Network and Information Security Agency and Europol more in the assessment of the relevant data. In line with the guidance given by the European Council, for the fulfilment of its tasks Europol shall in particular receive data on the modus operandi used by the perpetrators.

Amendment 33

Proposal for a directive
Article 18 - paragraph 1

Text proposed by the Commission	*Amendment*
1. By [FOUR YEARS FROM ADOPTION] and every three years thereafter, the Commission shall submit a report to the European Parliament and the Council on the application of this Directive in the Member States including any necessary proposal.	1. By [FOUR YEARS FROM ADOPTION] and every three years thereafter, the Commission shall submit a report to the European Parliament and the Council on the application of this Directive in the Member States including any necessary proposal. ***When reviewing, the Commission shall also take into account the technical and legal developments in the field of cyber crime, particularly with regard to the scope of this Directive.***

Or. en

Justification

Given the fast developments in cyber technologies, it is necessary to regularly review whether the regulatory content of this Directive is apt to cover the current technical possibilities and whether changes in the legal framework also at EU level affect the scope of this Directive, for example with regard to a future EU policy on Cloud Computing.