



EUROPEAN PARLIAMENT

2009 - 2014

Committee on Foreign Affairs

2010/0273(COD)

28.11.2011

OPINION

of the Committee on Foreign Affairs

for the Committee on Civil Liberties, Justice and Home Affairs

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

Rapporteur: Kristiina Ojuland

PA_Legam

SHORT JUSTIFICATION

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

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

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

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

AMENDMENTS

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

Amendment 1

Proposal for a directive

Recital 1

Text proposed by the Commission

(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.

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 ***and of the Union. That this objective forms part of the Union's general strategy to combat organised crime, secure information***

networks more effectively, protect critical information infrastructures and safeguard data.

Amendment 2

Proposal for a directive Recital 1 a (new)

Text proposed by the Commission

Amendment

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

Amendment 3

Proposal for a directive Recital 2

Text proposed by the Commission

Amendment

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

(2) Attacks against information systems are a growing menace. *They may arise from terrorism or organised crime and they may be perpetrated by states or individuals.* There is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. *The cross-border nature of certain infringements and the relatively low risks and costs to perpetrators, coupled with the potentially high returns and resulting damage inflicted, seriously increases the risk of such attacks.* This

constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response *not only* at the level of the European Union *but also the international community*.

Amendment 4

Proposal for a directive Recital 3

Text proposed by the Commission

(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.

Amendment

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

Amendment 5

Proposal for a directive Recital 4 a (new)

Text proposed by the Commission

Amendment

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

Amendment 6

**Proposal for a directive
Recital 4 b (new)**

Text proposed by the Commission

Amendment

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

Amendment 7

**Proposal for a directive
Recital 6**

Text proposed by the Commission

Amendment

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

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

Amendment 8

**Proposal for a directive
Recital 8 a (new)**

Text proposed by the Commission

Amendment

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

Amendment 9

**Proposal for a directive
Recital 11 a (new)**

Text proposed by the Commission

Amendment

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

Amendment 10

**Proposal for a directive
Recital 11b (new)**

Text proposed by the Commission

Amendment

(11b) Recent initiatives and projects relating to cyberdefence, such as within the European Defence Agency (EDA), should be encouraged to support the cyberdefence capabilities of Member States. Closer cooperation should be envisaged both with the EDA and with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), in particular in the field of capacity building and training.

Amendment 11

**Proposal for a directive
Recital 12**

Text proposed by the Commission

Amendment

(12) There is a need to collect data on offences under this Directive, in order to gain a more complete picture of the

(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.

problem at Union level and thereby contribute to formulating more effective responses. ***Member States should step up exchanges of information regarding cyber attacks with the support of the Commission and the European Network and Information Security Agency.*** The data will moreover help specialised agencies such as Europol and the European Network and Information Security Agency to better assess the extent ***and impact*** of cybercrime and the state of network and information security in Europe. ***Improved knowledge of present and future risks will make it possible to take decisions which are more effective in deterring and combating cyber attacks or reducing the resulting damage.***

Amendment 12

Proposal for a directive Recital 12 a (new)

Text proposed by the Commission

Amendment

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

Amendment 13

Proposal for a directive Recital 13

Text proposed by the Commission

(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.

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 ***at Union level. The Union should also seek greater international cooperation in the field of data network security by collaborating closely with other organisations with the relevant terms of reference, such as the United Nations, NATO, the Council of Europe, or the OSCE and involving other international stakeholders.*** Besides that, the coordination of prosecution of cases of attacks against information systems should be facilitated by the adoption of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings.

Amendment 14

Proposal for a directive Recital 16

Text proposed by the Commission

(16) This Directive ***respects*** the fundamental rights and ***observes*** the principles recognised in particular by the Charter of Fundamental Rights of the European Union, including the protection of personal data, freedom of expression and information, the right to a fair trial, presumption of innocence and the rights of the defence, as well as the principles of

Amendment

(16) This Directive ***and any practical application thereof respect*** the fundamental rights, ***in particular the right to privacy***, and ***observe*** the principles recognised in particular by the Charter of Fundamental Rights of the European Union, including the protection of personal data, freedom of expression and information, the right to a fair trial,

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.

presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. In particular, this Directive seeks to ensure full respect for these rights and principles and must be implemented accordingly. ***The free and open nature of the internet is not adversely affected by this Directive.***

Amendment 15

Proposal for a directive Recital 16 a (new)

Text proposed by the Commission

Amendment

(16a) The Council and the Commission should insist, in negotiations and in the course of their cooperation with third countries, on minimum requirements for preventing and fighting cybercrime and cyber attacks as well as on minimum standards for information system security.

Amendment 16

Proposal for a directive Recital 16 b (new)

Text proposed by the Commission

Amendment

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

Amendment 17

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

Text proposed by the Commission

Amendment

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

Amendment 18

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

Text proposed by the Commission

Amendment

2b. The Council shall clarify the role of the Political and Security Committee and its other bodies in the context of dealing with potential cyberattacks.

Amendment 19

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

Text proposed by the Commission

Amendment

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

Amendment 20

**Proposal for a directive
Article 15 – paragraph 3**

Text proposed by the Commission

Amendment

3. Member States shall transmit the data collected according to this Article to the

3. Member States shall transmit the data collected according to this Article to the

Commission. They shall also ensure that a consolidated review of these statistical reports is published.

Commission. They shall also ensure that a consolidated review of these statistical reports is *submitted to the European Parliament and* published.

Amendment 21

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

Text proposed by the Commission

Amendment

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

PROCEDURE

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