COUNCIL OF THE EUROPEAN UNION

Brussels, 8 April 2011

8795/11

Interinstitutional File: 2010/0273 (COD)

DROIPEN 27
TELECOM 43
CODEC 609

NOTE

from:	Presidency
to:	Council
No. prev. doc.:	8508/11 DROIPEN 24 TELECOM 39 CODEC 561
Subject:	Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA - Orientation debate and state of play

I. GENERAL INFORMATION

On 30 September 2010 the Commission submitted to the European Parliament and to the Council a proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, repealing Council Framework Decision 2005/222/JHA.

In accordance with Article 3(1) of Protocol (No 21) to the Treaties, both the United Kingdom and Ireland notified the Council that they would wish to take part in the adoption and application of the Directive. Denmark does not take part in the adoption of this instrument in accordance with Protocol (No 22) to the Treaties.

UK has a Parliamentary scrutiny reservation. DE, SI, FR and SE have a general scrutiny reservation on the proposal.

The proposal was presented to the Working Party on General Matters, including Evaluations (GENVAL) on 13 October 2010 and to the Council at its meeting on 8-9 November 2010. Council took note of the state of play of the discussions on 25 February 2011.

CATS was requested on three occasions to provide strategic guidance for the discussions in the Working Party on Substantive Criminal Law (hereinafter DROIPEN). On 13 December 2010, at the outset of the negotiations, some general issues were addressed. On 11 February 2011, CATS examined Article 10 (3) of the Commission proposal, which would introduce a new aggravating circumstance of cyber attacks committed by misusing the identity data of the rightful owner. Lastly, on 22 March CATS was consulted on four outstanding issues concerning minor cases, the scope of criminalisation in Art. 3, the level of penalties and jurisdiction based on nationality.

DROIPEN discussed the proposal during its meetings on 13-14 and 28 January 2011 and on 2-3 and 29 March 2011. At its meeting on 29 March 2011 DROIPEN concluded a third reading of the text and examined the drafting suggestions put forward by the Presidency in order to bring the discussions forward.

The proposal was further examined by the JHA Counsellors on 4 April 2011.

II. ISSUES ON WHICH MINISTERS ARE INVITED TO GIVE POLITICAL GUIDANCE

Throughout the discussions, a number of adjustments of the initial Commission proposal were made in order to accommodate as far as possible the concerns expressed by delegations. The Presidency has also taken note of the positions of the delegations, which were in favour of maintaining a level of ambition in the text. In the view of the Presidency, a possible compromise has emerged and a proposal to that end was submitted to COREPER on 7 April 2011 (found in Annex I).

The discussions of COREPER demonstrated, however, that there are some policy issues which would need further guidance from the Council in order to define the political framework in which the Working Party shall continue its deliberations. In this respect, the Presidency would like to submit the following issues to the attention of the Council:

1. Level of Penalties (Art. 9 (2)) in relation to the scope of criminalisation (Articles 3-7)

Compared to the initial Commission proposal, some important compromises affecting the scope of criminalisation were introduced as a result of the discussions in the Working Party. These changes were intended to address the specific concerns of some Member States as follows:

- The reference to "minor cases" has been extended to all offences referred to in the Directive (Article 3 to Article 7). Therefore, minor cases are entirely excluded from the scope of the Directive.
- The scope of Article 3 "Illegal access to information systems" has been limited to cases in which the infringement of a security measure is a constituent element of the offence. The possibility for this is provided by the Budapest Convention as an option, but was not included in the original Commission proposal.
- The possession of tools used for committing cyber attacks has been excluded from the scope of Article 7.

In the view of the Presidency, this limited scope of criminalisation justifies the retention of the initial Commission proposal in relation to the level of penalties for the basic offences (see Article 9 (2)), i.e. maximum of at least two years of imprisonment. It should also be noted that the scope of the provision has been further limited to Articles 3 to 6, thus excluding Article 7 from the obligation to provide for this specific penalty level.

There is still, however, a group of Member States, which consistently expressed their opposition to this, maintaining that the level of penalty should be lowered to one year. As an alternative to one year, this aim could also be achieved by maintaining the solution in the Framework Decision 2005/222/JHA of a maximum of at least one to three years of imprisonment, since in practice it means an obligation for the Member States to provide for at least one year of a maximum penalty.

The Presidency would like to underline that the solution on the level of penalties is related to the scope of the proposal, and therefore in the latter case certain elements of the compromise package presented to the COREPER on 7 April will have to be revisited.

In view of the limited scope of criminalisation, ministers are requested to give their guidance as to whether

- *they accept the two year as a level of penalty for the basic offences in Article 9 (2), as set out in the Commission proposal,*
- *or they support the position expressed by some delegations to lower the level of penalty to a maximum of at least one year of imprisonment.*

2. Aggravating circumstances (Article 9 (3), (4) and (5))

The Commission proposal aimed to tackle two emerging threats in the cyberworld, by introducing two aggravating circumstances to the basic offences. The two new aggravating circumstances addressed are:

- large scale cyber-attacks, committed trough the so called "botnets" (currently found in Art. 9 (3)), and
- misuse of personal data of another person in order to gain trust of a third party, which facilitates in practice the commitment of the cyber-attack (currently found in Art. 9 (5))

Throughout the discussions, although they were core elements of the Commission's ambitions, these provisions were substantially amended in order to take on board the concerns of delegations, while at the same time maintaining the substance of the Commission proposal on these issues.

As to the level of penalties for aggravating circumstances, the text currently offers more flexibility than in the original Commission proposal. It provides for two different thresholds: a maximum term of imprisonment of at least three and at least five years, depending on the gravity of the offence, while introducing new circumstances where the highest penalty would apply. Thus, when the attack has caused serious damage or when it has affected a critical infrastructure information system, the proposed level of maximum imprisonment is at least five years.

The misuse of identity data of a third person is included in Article 9 (5) as a pure aggravating circumstance, without envisaging a specific level of penalty, while the method to achieve this result is left to the Member States. It was repeatedly stated in the course of the discussions that this element should be distinguished from an identity theft, which is a complex phenomenon of a partially different nature. At the same time, as far as cyber attacks were concerned, the modus operandi is frequently used to commit serious computer crime.

Some delegations still maintain their preference for taking out this element from the Directive, since it should be addressed in a separate instrument, dealing with identity theft in general. As regards the other new element of the Commission proposal concerning the use of a tool for launching large scale attacks (art. 9(3)), this issue was met with some resistance from delegations.

Ministers are requested to give guidance as to whether the concept of a crime being committed by botnets should be kept as an aggravating circumstance, or it should be deleted from the draft.

Ministers are requested to give guidance on as to whether the concept of misuse of identification data should be kept as an aggravating circumstance, or it should be deleted from the draft.

Should the answer be positive, the drafting will be adapted further at expert level.

3. Jurisdiction (Article 13)

The issue of jurisdiction has been subject of detailed discussions in the Working Party. The compromise text in Art. 13 differs from the initial proposal of the Commission, building on the approach found in this respect in the THB Directive. It also introduces as a minimum standard the requirement for a positive double criminality check, in particular in relation to nationals when the offence has been committed outside the territory of the Member State concerned (Article 13 (1) (b)). The conditions for exercising national jurisdiction are not subject to the provisions of the Directive as established in the newly introduced recital 10a.

Minsters are requested to confirm that the jurisdiction in relation to nationals shall be retained in the scope of the proposal.

4. Tools used for committing offences - criminalisation of device (Art. 7)

The Working Party confirmed the interpretation of the scope of Art. 7 of the draft proposal in conformity with Art. 6 of the Budapest Convention on Cybercrime.

Art. 6 (3) of the Convention, however, provides for a possibility for each party to the Convention not to apply this provision in some parts, including when a device, "designed or adapted primarily" for the purpose of committing cyber attacks is in question. The lack of possibility for such an exception in the Commission proposal proved difficult for one delegation.

In this respect the Presidency suggests the following compromise wording:

Article 7

Tools used for committing offences

(1) 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, with the intent that it be used for the purpose of committing any of the offences referred to in Articles 3 to 6 at least for cases which are not minor:

(a) (…) 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.

(2) Member States may also take the necessary measures to ensure that the production, sale, procurement for use, import, distribution or otherwise making available of any other devices, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence when committed intentionally and without right, with the intent that it be used for the purpose of committing any of the offences referred to in Articles 3 to 6 at least for cases which are not minor.

Ministers are invited to confirm the compromise proposal of the Presidency in relation to Art. 7.

III. STATE OF PLAY

The Presidency is of the opinion that there are a certain number of provisions, where a provisional agreement has been reached. These provisions are as follows: Art. 1 to Art. 6, and Art. 11 to Art 19.

In view of the above, Council is invited to take note that the text of Art. 1 to Art. 6, and Art. 11 to Art 19 as set out in Annex II, is subject to a provisional agreement , on the understanding that further discussions may show that there is a need to revisit any of those provisions.

ANNEX I

2010/0273 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 83(1) thereof,
Having regard to the proposal from the European Commission[1],
After transmission of the draft legislative act to the national Parliaments,
Having regard to the opinion of the European Economic and Social Committee,
Having regard to the opinion of the Committee of the Regions,
Acting in accordance with the ordinary legislative procedure,
Whereas:

(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 **(…)** competent authorities, including the police and other specialised law enforcement services of the Member States.

[1] OJ C […], […], p. […].

(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.

(2a) "There are a certain number of critical infrastructures in the Union, the disruption or destruction of which would have significant cross-border impacts. It emerges from the need to increase the critical infrastructure protection capability in Europe that the fight against the attacks against information systems should be complemented by serious criminal sanctions reflecting the gravity of such attacks. Critical infrastructure may be understood as an asset, system or part thereof located in Member States which is essential for instance for the maintenance of vital societal functions, health, safety, security, economic or social well-being 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."

(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.

(4) Common definitions in this area, particularly of information systems and computer data, are important in order to ensure a consistent approach in the Member States to the application of this Directive.

(5) There is a need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal access to an information system, illegal system interference, illegal data interference, and illegal interception.

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

(6a) The directive provides for criminal sanctions at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. The case may be considered minor, for example, (…) when the damage and/or the risk it carries to public or private interests, such as the integrity of a computer system or computer data, or 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.

(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[2], when the attack is conducted on a large scale, or has caused a seriouse damage or when the offence is committed (…) by misusisng personal data related to a person other than the perpetrator with the aim to gain trust of a third party. [3]

(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.

[2] OJ L 300, 11.11.2008, p. 42.
[3] The text has been adjusted to the current wording of the proposal.

(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.[4]

(10) This Directive does not intend to impose criminal liability where the acts are committed without criminal intent, such as for authorised testing or protection of information systems, or when the person did not know that the access was unauthorised (…).

(10a) This Directive does not govern the conditions that should be met in order to initiate a prosecution of any of the offences referred to in Art. 3 to 8 when committed outside the territory of the Member State concerned, such as a report made by the victim in the place where the offence was commited, or a denunciation from the State of the place where the offence was commited, or when the principle of *non bis in idem* applies.

(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 (…) available relevant information for the purpose of investigations or proceedings concerning criminal offences related to information systems and data involving the requesting Member State (…). 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. In such cases, it may be expedient that the request for (…) information is accompanied by a telephone contact, in order to ensure that it will be processed swiftly by the requested state and that feedback will be provided within the limit of 8 hours, acknowledging receipt of the requests and indicating whether and when it is likely to be answered.

[4] LT entered scrutiny reservation pending an agreement on Art. 9.

(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[5].

(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.

(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 subsidarity 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.

---

[5] NL entered a scrutiny reservation pending the agreement on Art. 15.

(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[6] 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[7].

(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 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.

(17) In accordance with Articles 1, 2, 3 and 4 of the Protocol on the position of United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland have notified their wish to participate in the adoption and application of this Directive.

---

6 OJ L 350, 30.12.2008, p.60.
7 OJ L 8, 12.1.2001, p. 1.

(18) In accordance with Articles 1 and 2 of Protocol on the position of Denmark annexed to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is therefore not bound by it or subject to its application.

(19) This Directive aims to amend and expand the provisions of Framework Decision 2005/222/JHA. Since the amendments to be made are of substantial number and nature, the Framework Decision should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive.

(20) In accordance with point 34 of the Interinstitutional Agreement on better law-making[8], Member States are encouraged to draw up, for themselves and in the interest of the Union, their own tables which will, as far as possible, illustrate the correlation between this Directive and the transposition measures, and to make them public[9].

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter

This Directive establishes minimum rules concerning the definition of criminal offences and the sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities[10].

[8] OJ C 321, 31.12.2003, p. 1.
[9] DE entered a scrutiny reservation.
[10] ES maintains a scrutiny reservation.

Article 2

Definitions

For the purposes of this Directive, the following definitions shall apply:

(a) "information system" means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

(b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function;

(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;

(d) "without right" means access, interference, interception, or any other (…) conduct referred to in this Directive, not authorised by the owner, other right holder of the system or of part of it, or not permitted under national legislation.

Article 3

Illegal access to information systems[11]

Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right to the whole or any part of an information system is punishable as a criminal offence, at least when the offence is committed by infringing a security measure and for cases which are not minor.

Article 4

Illegal system interference

Member States shall take the necessary measures to ensure that the 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 intentionally and without right, at least for cases which are not minor.

Article 5

Illegal data interference

Member States shall take the necessary measures to ensure that the deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed intentionally and without right, at least for cases which are not minor.

[11] Scrutiny reservation by UK.

Article 6

Illegal interception

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 are not minor.

Article 7

Tools used for committing offences[12]

(1) 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, with the intent that it be used for the purpose of committing any of the offences referred to in Articles 3 to 6 at least for cases which are not minor:

(a) device, including [13] 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.

(…)

[12] UK maintains its scrutiny reservation.
[13] DE suggests deletion of the following: "device, including a".

Article 8

Incitement, aiding and abetting and attempt

1. Member States shall ensure that the incitement, aiding and abetting to commit 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 an offence referred to in Articles 4 to 5 is punishable as a criminal offence.

Article 9

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.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6 are punishable by a maximum penalty of at least two years of imprisonment.

3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 to 5 are punishable by a maximum penalty of at least three years of imprisonment when committed intentionally through the use of a tool designed primarily (…) to launch attacks affecting a significant number of information systems, or attacks causing serious damage.

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 to 5 are punishable by a maximum penalty of at least five years of imprisonment when[14]

(a) committed within the framework of a criminal organisation, as defined in Framework Decision 2008/814/JHA irrespective of the penalty level referred to therein, or

(b) causing serious damage, or

(c) committed against a critical infrastructure information system.

5. In so far as the following circumstances do not already form part of the constituent elements of the offences referred to in Articles 3 to 5, Member States shall take the necessary measures to ensure that when these offences are committed by misusing personal data related to a person other than the perpetrator with the aim of gaining trust of a third party, they may be regarded as an aggravating circumstance (…).

(…)

Article 11

Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person, based on one of the following:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person.

[14] RO has a scrutiny reservation on Art. 9 (4) (b) and (c).

2. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.

3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators of, inciters, or accessories to, any of the offences referred to in Articles 3 to 8.

Article 12

Penalties on legal persons

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:
   (a) exclusion from entitlement to public benefits or aid;
   (b) temporary or permanent disqualification from the practice of commercial activities;
   (c) placing under judicial supervision;
   (d) judicial winding-up;
   (e) temporary or permanent closure of establishments which have been used for committing the offence.
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.

Article 13

Jurisdiction[15]

1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:

[15] UK and ES maintain a scrutiny reservation on this article.

(a) in whole or in part within the territory of the Member State concerned; or

(b) by one of their nationals, at least in cases when the act is a criminal offence at the place where it was performed.

(…)[16]

2. When establishing jurisdiction in accordance with paragraph 1(a), a Member State shall ensure that the jurisdiction includes cases where:

(a) the offender commits the offence when physically present on the territory of the Member State concerned, whether or not the offence is against an information system on its territory; or

(b) the offence is against an information system on the territory of the Member State concerned, whether or not the offender commits the offence when physically present on its territory.

3. A Member State shall inform the Commission where it decides to establish further jurisdiction over an offence referred to in Articles 3 to 8 committed outside of their territory e.g. where:

(a) the offender has his or her habitual residence in the territory of that Member State; or

(b) the offence is committed for the benefit of a legal person established in the territory of that Member State.

[16] Following a request of several delegations Art. 13 (1a) has been moved to the Preamble - new recital 10a.

Article 14

Exchange of information[17]

1. For the purpose of exchange of information relating to the offences referred to in Articles 3 to 8, 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 in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered, as well as the form and the estimated time of this answer.

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.

Article 15

Monitoring and statistics[18]

1. Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 to 7.

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover existing data onthe number of offences referred to in Articles 3 to 7 registered by the Member States and the number of persons, prosecuted and convicted for the offences referred to in Articles 3 to 7.

3. Member States shall transmit the data collected according to this Article to the Commission. The Commission shall ensure that a consolidated review of these statistical reports is published.

---

17 Scrutiny reservation of ES.
18 Scrutiny reservation of ES.

Article 16

Replacement of Framework Decision 2005/222/JHA[19]

Framework Decision 2005/222/JHA is hereby replaced in relation to Member States participating in the adoption of this Directive,without prejudice to the obligations of the Member States relating to the time-limit for transposition of the Framework Decision into national law.

In relation to Member States participating in the adoption of this Directive, references to the Framework Decision 2005/222/JHA shall be construed as references to this Directive.

Article 17

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [two years from adoption]

2. Member States shall transmit to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Directive.

3. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

[19] UK maintains a scrutiny reservation.

Article 18

Reporting

1. The Commission shall by [FOUR YEARS FROM ADOPTION], submit a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals.

2. Member States shall send to the Commission all the information that is appropriate for drawing up the report referred to in paragraph 1. The information shall include a detailed description of legislative and non-legislative measures adopted in implementing this Directive[20].

Article 19

Entry into force

This Directive shall enter into force on the day of its publication in the *Official Journal of the European Union*.

Article 20

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

---

[20] ES expressed reservations in relation to para 2, since it is not an element of the THB Directive.

ANNEX II

2010/0273 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Article 1

Subject matter

This Directive establishes minimum rules concerning the definition of criminal offences and the sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.

Article 2

Definitions

For the purposes of this Directive, the following definitions shall apply:

(a) "information system" means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

(b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function;

(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;

(d) "without right" means access, interference, interception, or any other conduct referred to in this Directive, not authorised by the owner, other right holder of the system or of part of it, or not permitted under national legislation.

Article 3

Illegal access to information systems

Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right to the whole or any part of an information system is punishable as a criminal offence, at least when the offence is committed by infringing a security measure and for cases which are not minor.

Article 4

Illegal system interference

Member States shall take the necessary measures to ensure that the 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 intentionally and without right, at least for cases which are not minor.

Article 5

Illegal data interference

Member States shall take the necessary measures to ensure that the deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed intentionally and without right, at least for cases which are not minor.

Article 6

Illegal interception

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 are not minor.

Article 11

Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person, based on one of the following:

   (a) a power of representation of the legal person;

   (b) an authority to take decisions on behalf of the legal person;

   (c) an authority to exercise control within the legal person.

2. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.

3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators of, inciters, or accessories to, any of the offences referred to in Articles 3 to 8.

Article 12

Penalties on legal persons

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:
   (a) exclusion from entitlement to public benefits or aid;
   (b) temporary or permanent disqualification from the practice of commercial activities;
   (c) placing under judicial supervision;
   (d) judicial winding-up;
   (e) temporary or permanent closure of establishments which have been used for committing the offence.
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.

Article 13
Jurisdiction[21]

1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:

[21] The following accompanying recital is included in the partial general approach:
"This Directive does not govern the conditions that should be met in order to initiate a prosecution of any of the offences referred to in Art. 3 to 8 when committed outside the territory of the Member State concerned, such as a report made by the victim in the place where the offence was commited, or a denunciation from the State of the place where the offence was commited, or the fact that the offender has not been prosecuted in the place where the offence was commited."

(a) in whole or in part within the territory of the Member State concerned; or

(b) by one of their nationals, at least in cases when the act is a criminal offence at the place where it was performed.

2. When establishing jurisdiction in accordance with paragraph 1(a), a Member State shall ensure that the jurisdiction includes cases where:

(a) the offender commits the offence when physically present on the territory of the Member State concerned, whether or not the offence is against an information system on its territory; or

(b) the offence is against an information system on the territory of the Member State concerned, whether or not the offender commits the offence when physically present on its territory.

3. A Member State shall inform the Commission where it decides to establish further jurisdiction over an offence referred to in Articles 3 to 8 committed outside of their territory e.g. where:

(a) the offender has his or her habitual residence in the territory of that Member State; or

(b) the offence is committed for the benefit of a legal person established in the territory of that Member State.

Article 14

Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 3 to 8, 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 in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered, as well as the form and the estimated time of this answer.

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.

Article 15

Monitoring and statistics

1. Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 to 7.

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover existing data onthe number of offences referred to in Articles 3 to 7 registered by the Member States and the number of persons, prosecuted and convicted for the offences referred to in Articles 3 to 7.

3. Member States shall transmit the data collected according to this Article to the Commission. The Commission shall ensure that a consolidated review of these statistical reports is published.

Article 16

Replacement of Framework Decision 2005/222/JHA

Framework Decision 2005/222/JHA is hereby replaced in relation to Member States participating in the adoption of this Directive,without prejudice to the obligations of the Member States relating to the time-limit for transposition of the Framework Decision into national law.

In relation to Member States participating in the adoption of this Directive, references to the Framework Decision 2005/222/JHA shall be construed as references to this Directive.

Article 17

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [two years from adoption]

2. Member States shall transmit to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Directive.

3. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

Article 18

Reporting

1. The Commission shall by [FOUR YEARS FROM ADOPTION], submit a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals.

2. Member States shall send to the Commission all the information that is appropriate for drawing up the report referred to in paragraph 1. The information shall include a detailed description of legislative and non-legislative measures adopted in implementing this Directive.

Article 19

Entry into force

This Directive shall enter into force on the day of its publication in the *Official Journal of the European Union*.

Article 20

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels,