COUNCIL OF THE EUROPEAN UNION

Brussels, 15 June 2011

Interinstitutional File: 2010/0273 (COD)

11566/11

DROIPEN 62
TELECOM 95
CODEC 1025

OUTCOME OF PROCEEDINGS

of:	Council ("Justice and Home affairs") on 10 June 2011
Com. initiative:	14436/10 DROIPEN 107 TELECOM 100 CODEC 952 + ADD 1 + ADD 2
No. prev. doc.:	10751/11 DROIPEN 47 TELECOM 82 CODEC 915
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 - General approach

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.

At its meeting on 10 June 2011, the Council reached a general approach on the compromise text of the proposal, as laid out in the Annex. This text will form the basis for the incoming discussions with the European Parliament pursuant to Art. 294, TFEU.

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 and FR have a Parliamentary scrutiny reservation. ES and EL maintain reservations in relation to the level of penalties envisaged in the general approach.

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 the criminal legislation in the Member States in the area of attacks against information systems, by establishing minimum rules concerning the definition of criminal offences and the sanctions in this area, and to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States.

(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.

[1] OJ C […], […], p. […].

(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 often can be critical to states or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of the so called "botnets". The latter is characterised by subsequent stages of the criminal act, where each stage alone could pose serious danger to public interests. In this respect, the Directive aims, inter alia, to introduce criminal sanctions for the stage where the "botnet" is created, namely, where remote control over a significant number of computers is established by infecting them with malicious software, through targeted cyber attacks. At a later stage, the infected network of computers, constituting the "botnet", could be activated without the computer users' knowledge in order to launch a large scale cyber attacks, which usually would have the capacity to cause serious damage, as referred to in this Directive. Member States may determine what constitutes serious damage according to their national law and practice, which may include disrupted system services of significant public importance, or major financial cost or loss of personal data.

(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 to the integrity of a computer 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.

(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] or when the attack is conducted on a large scale, thus affecting a significant number of information systems or causing serious damage, including when the attack has been intended to create a "botnet" or was carried out through a "botnet", thus resulting in serious damage.

(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.

(9) Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive refers to ’tools’ that can be used in order to commit the crimes listed in this Directive. Tools refer to, for example, malicious software, including those able to create botnets, used to commit cyber attacks. Since this Directive sets up minimum rules, Member States may provide for criminal sanctions for other types of offences in relation to the tools used for committing offences, such as the possession of such tools or the production, sale, procurement for use, import, distribution or otherwise making available of any other devices, including hardware, designed or adapted primarily for the purpose of committing any of the offences referred to in the Directive.

---

[2] OJ L 300, 11.11.2008, p. 42.

(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 exercise jurisdiction over any of the offences referred to in Art. 3 to 8, 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 committed.

(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.

(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.

(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.

(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[3] 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[4].

[3] OJ L 350, 30.12.2008, p.60.
[4] OJ L 8, 12.1.2001, p. 1.

(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 Article 3 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.

(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 Inter-institutional Agreement on better law-making[5], 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.

[5] OJ C 321, 31.12.2003, p. 1.

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.

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 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.

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, when committed intentionally, are punishable by a maximum penalty of at least three years of imprisonment when a significant number of information systems have been affected through the use of a tool, referred to in Article 7 (1), designed or adapted primarily for this purpose.

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

(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.

[…]

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

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:

   (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 on the 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.

(…)

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*