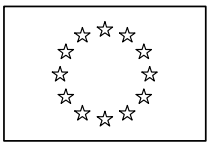

EUROPEAN COMMISSION

Brussels, 30.9.2010
COM(2010) 517 final

2010/0273 (COD)

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

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

EXPLANATORY MEMORANDUM

1. GROUNDS FOR AND OBJECTIVES OF THE PROPOSAL

The purpose of the proposal is to replace Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[1]. The Framework Decision responded, as stated in its recitals, to the objective of improving cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, by approximating the rules of the criminal law in the Member States in relation to attacks against information systems. It introduced EU legislation to deal with offences such as illegal access to information systems, illegal system interference and illegal data interference, as well as specific rules on the liability of legal persons, jurisdiction and exchange of information. Member States were required to take the necessary measures to comply with the provisions of the Framework Decision by 16 March 2007.

On 14 July 2008, the Commission published a report on the implementation of the Framework Decision[2]. In the conclusions to the report, it was noted that significant progress had been made in most Member States and that the level of implementation was relatively good, but that implementation in some Member States was not yet complete. Further on in the report, it was stated that several "emerging threats have been highlighted by recent attacks across Europe since adoption of the Framework Decision, in particular the emergence of large-scale simultaneous attacks against information systems and increased criminal use of so-called 'botnets'." These attacks were not the centre of attention when the Framework Decision was adopted. In response to these developments, the Commission will consider actions aimed at devising better responses to the threat (see next section for the explanation of a botnet).

The importance of taking further action to step up the fight against cybercrime was underlined in the 2004 Hague Programme on strengthening freedom, security and justice in the European Union as well as the 2009 Stockholm Programme and its respective action plan[3]. Furthermore, the recently presented Digital Agenda for Europe[4], the first flagship initiative adopted under the Europe 2020 strategy, recognised the need to address the rise of new forms of crime, in particular cybercrime, at European level. In the action area focused on trust and security the Commission is committed to measures to combat cyber attacks against information systems.

On the international level, the Council of Europe Convention on Cybercrime ("Cybercrime Convention"), signed on 23 November 2001, is regarded as the most complete international standard to date, since it provides a comprehensive and coherent framework embracing the various aspects relating to cybercrime.[5] So far, the Convention has been signed by all 27 Member States, but it has been ratified by only 15 Member States.[6] The Convention entered into force on 1 July 2004. The EU is not a signatory to the Convention. Given the importance of this instrument, the Commission actively encourages the remaining EU member states to ratify the Convention as soon as possible.

---

1 OJ L 69, 16.3.2005, p. 68.

2 Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems - COM(2008) 448.

3 OJ C 198, 12.8.2005, OJ C 115, 4.5.2010, COM(2010) 171, 20.4.2010.

4 Commission Communication - COM(2010) 245, 19.5.2010.

5 Council of Europe Convention on Cybercrime, Budapest 23.11.2001, CETS n° 185.

6 For an overview of the ratifications of the Convention (CETS n° 185), see: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

- **General context**

With regard to cybercrime, the main cause of this phenomenon is vulnerability resulting from a variety of factors. Insufficient response by law enforcement mechanisms contributes to the prevalence of these phenomena, and exacerbates the difficulties, as certain types of offences go beyond national borders. Reporting of this type of crime is often inadequate, partly because some crimes go unnoticed, and partly because the victims (economic operators and companies) do not report crimes for fear of getting a bad reputation and of their future business prospects being affected by public exposure of their vulnerabilities.

Furthermore, variations in national criminal law and procedure may give rise to differences in investigation and prosecution, leading to differences in how these crimes are dealt with. Developments in information technology have exacerbated these problems by making it easier to produce and distribute tools ('malware' and 'botnets'), while offering offenders anonymity and dispersing responsibility across jurisdictions. Given the difficulties of bringing a prosecution, organised crime is able to make considerable profits with little risk.

This proposal takes into account the new methods of committing cybercrimes, especially the use of botnets. The term 'botnet' indicates a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'. The persons who control this centre are among the offenders, as they use the compromised computers to launch attacks against information systems. It is very difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack may be in a different location from the offender himself.

Attacks carried out by a botnet are often executed on a large scale. Large-scale attacks are those attacks that can either be carried out with the use of tools affecting significant numbers of information systems (computers), or attacks that cause considerable damage, e.g. in terms of disrupted system services, financial cost, loss of personal data, etc. The damage caused by large-scale attacks has a major impact on the functioning of the target itself, and/or affects its working environment. In this context, a 'big botnet' is understood to have the capacity to cause serious damage. It is difficult to define botnets in terms of size, but the biggest botnets witnessed have been estimated to have between 40,000 and 100,000 connections (i.e. infected computers) per period of 24 hours.[7]

[7] Number of connections per 24 hours is the commonly used measuring unit to estimate the size of botnets.

- **Existing provisions in the area of the proposal**

At EU level, the Framework Decision introduces a minimum level of approximation of Member States' legislation to criminalise a number of cybercrimes, including illegal access to information systems, illegal system interference, illegal data interference, and instigation, aiding and abetting and attempting to do so.

Although the provisions of the Framework Decision have generally been implemented by the Member States, the Decision has a number of shortcomings due to the trend in the size and number of the offences (cyber attacks). It approximates legislation only on a limited number of offences, but does not fully address the potential threat posed to society by large scale attacks. Nor does it take sufficient account of the gravity of the crimes and sanctions against them.

Other EU initiatives and programmes in force or planned go some way to addressing problems related to cyber attacks or issues, such as network security and the safety of Internet users. They include actions supported by the programme 'Prevention of and Fight against Crime'[8], 'Criminal Justice'[9] programme, the 'Safer Internet'[10] programme and the 'Critical Information Infrastructure Initiative'[11]. In addition to the Framework Decision, another relevant legal instrument in force is Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography.

At administrative level, the practice of infecting computers, turning them into 'botnets', is already prohibited under EU privacy and data protection rules[12]. Notably national administrative agencies are already cooperating under the European Contact Network of Spam Authorities. Under those rules, Member States are required to prohibit the interception of communications on public communications networks and publicly available electronic communications services without the consent of the users concerned or legal authorisation.

This proposal is compliant with those rules. Member States should pay attention to improving the cooperation between administrative and law enforcement authorities for cases subject to both administrative and criminal sanctions.

- **Consistency with other policies and objectives of the Union**

The objectives are consistent with EU policies on combating organised crime, increasing the resilience of computer networks, protecting critical information infrastructure and data protection. The objectives are also consistent with the Safer Internet Programme which was set up to promote safer use of the Internet and new online technologies, and to combat illegal content.

This proposal was subjected to in-depth scrutiny to ensure that its provisions were fully compatible with fundamental rights and, in particular, with the protection of personal data, freedom of expression and information, the right to a fair trial, presumption of innocence and

---

8 See: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 See: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm

10 See: http://ec.europa.eu/information_society/activities/sip/index_en.htm

11 See: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12 Directive on privacy and electronic communications (OJ L 201, 31.7.2002), as amended by Directive 2009/136/EC (OJ L 337, 18.12.2009).

the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

A broad range of experts in the field have been consulted in a number of different meetings dealing with various aspects of the fight against cybercrime, including the judicial follow-up (prosecution) of these crimes. They included, in particular, representatives of Member States' Governments and the private sector, specialised judges and prosecutors, international organisations, European agencies and expert bodies. A number of experts and organisations have subsequently sent in submissions and provided information.

Key messages resulting from the consultation are:

– the need for the EU to act in this field;

– the need to criminalise forms of offences not included in the current Framework Decision, in particular new forms of cyber attacks (botnets);

– the need to eliminate obstacles to investigation and prosecution in cross-border cases.

The input received during the consultation has been taken into account in the Impact Assessment.

Collection and use of expertise

External expertise has been obtained during various meetings with stakeholders.

Impact Assessment

Various policy options have been examined as a means of achieving the objective.

- Policy option (1): Status Quo / No new EU action

This option means that the EU will not take any further action to combat this particular type of cybercrime, i.e. attacks against information systems. Ongoing actions are due to be continued, in particular the programmes to strengthen critical information infrastructure protection and improve public-private cooperation against cybercrime.

- Policy option (2): Development of a programme to strengthen the efforts to counter attacks against information systems by means of non-legislative measures

Non-legislative measures would, in addition to the programme for critical information infrastructure protection, focus on cross-border law enforcement and public-private cooperation. These soft-law instruments should aim to promote further coordinated action at EU level, including strengthening of the existing 24/7 network of contact points for law enforcement agencies; establishment of an EU network of public-private contact points involving cybercrime experts and law enforcement agencies; elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators; and

support for the organisation of training programmes for law enforcement agencies on the investigation of cybercrime.

- Policy option (3): Targeted update of the rules of the Framework Decision (new Directive replacing the current Framework Decision) to address the threat from large-scale attacks against information systems (botnets) and, when committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner, the efficiency of Member States' law enforcement contact points, and the lack of statistical data on cyber attacks.

This option provides for the introduction of specific targeted (i.e. limited) legislation to prevent large-scale attacks against information systems. Such strengthened legislation would be accompanied by non-legislative measures to strengthen operational cross-border cooperation against such attacks, which would facilitate the implementation of the legislative measures. The aim of these measures would be to enhance the preparedness, security and resilience of critical information infrastructure and exchange best practice.

- Policy option (4): Introduction of comprehensive EU legislation against cybercrime

This option would entail new comprehensive EU legislation. In addition to introducing the soft-law measures in policy option 2 and the update in policy option 3, it would also tackle other legal problems related to Internet use. Such measures would cover not only attacks against information systems, but also issues such as financial cybercrime, illegal Internet content, the collection/storage/transfer of electronic evidence, and more detailed jurisdiction rules. The legislation would operate in parallel with the Council of Europe Convention on Cybercrime, and would include the accompanying, non-legislative measures mentioned above

- Policy option (5): Update of the Council of Europe Convention on Cybercrime

This option would require substantial renegotiation of the current Convention, which is a lengthy process and is at odds with the time frame for action that is proposed in the Impact Assessment. There seems to be no international willingness to renegotiate the Convention. Updating of the Convention therefore cannot be considered a feasible option, as it falls outside the required time frame for action.

Preferred policy option: combination of non-legislative measures (option 2) with a targeted update of the Framework Decision (option 3)

Following the analysis of the economic impact, social impacts, and impacts on fundamental rights, options 2 and 3 represent the best approach to deal with the problem and achieve the objectives of the proposal.

In preparing this proposal, the Commission carried out an Impact Assessment.

3. LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed action**

The Directive, while repealing Framework Decision 2005/222/JHA, will retain its current provisions and include the following new elements:

– On substantive criminal law in general, the Directive:

A. Penalises the production, sale, procurement for use, import, distribution or otherwise making available of devices/tools used for committing the offences.

B. Includes aggravating circumstances:

- the large-scale aspect of the attacks - botnets or similar tools would be addressed by introducing a new aggravating circumstance, in the sense that the act of putting in place a botnet or a similar tool would be an aggravating factor when crimes listed in the existing Framework Decision are committed;

- when such attacks are committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner. Any such rules would need to comply with the principles of legality and proportionality of criminal offences and penalties and be consistent with existing legislation on the protection of personal data[13].

C. Introduces 'illegal interception' as a criminal offence.

D. Introduces measures to improve European criminal justice cooperation by strengthening the existing structure of 24/7 contact points[14]:

- an obligation to comply with a request for assistance by the operational contact points (set out in Article 14 of the Directive) within a certain time limit is proposed. The Cybercrime Convention does not specify a binding provision of this kind. The aim of this measure is to ensure that the contact points indicate within a specified time whether they are able to provide a solution to the request for assistance, and by when the requesting point of contact can expect such a solution to be found. The actual content of the solutions is not specified.

E. Addresses the need to provide statistical data on cybercrimes by making it obligatory for the Member States to ensure that an adequate system is in place for the recording, production and provision of statistical data on the offences referred to in the existing Framework Decision and the newly added 'illegal interception'.

The Directive contains in the definitions of criminal offences listed in articles 3, 4, 5 (illegal access to information systems, illegal systems interference and illegal interference) a provision allowing to criminalise only 'cases which are not minor' in the process of transposition of the directive into national law. This element of flexibility is intended to allow Member States not to cover cases that would *in abstracto* be covered by the basic definition but are considered not to harm the protected legal interest, e.g. in particular acts by young people who attempt to prove their expertise in information technology. This possibility to limit the scope of criminalisation should not however lead to the introduction of additional constitutive elements of offences beyond those that are already included in the Directive,

---

13 Such as the Directive 2002/58/EC of the European Parliament and of the Council of 12.7.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37) (currently under revision), and such as the general data protection Directive 95/46/EC.

14 Introduced by the Convention, and FD 2005/222/JHA on Attacks against Information Systems

because this would lead to the situation that only offences committed with the presence of aggravating circumstances are covered. In the process of transposition, Member States should refrain in particular from adding additional constitutive elements to the basic offences such as e.g. a special intention to derive illicit proceeds from crime or the presence of a specific effect such as causing a considerable damage.

- **Legal basis**

Article 83(1) of the Treaty on the Functioning of the European Union[15].

- **Subsidiarity principle**

The subsidiarity principle applies to the actions of the European Union. The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reasons:

Cybercrime and, more specifically, attacks against information systems have a considerable cross-border dimension, which is most obvious in large scale attacks, as the connecting elements of an attack are often situated in different locations and in different countries. This requires EU action, in particular to keep abreast of the current trend towards large scale attacks in Europe and in the world. Action at EU level and an update of the Framework Decision 2005/222/JHA have also been called for in the Council Conclusions of November 2008[16], as the objective of effectively protecting citizens from cybercrimes cannot be sufficiently achieved by Member States alone.

Action by the European Union will better achieve the objectives of the proposal for the following reasons:

The proposal will further approximate the substantive criminal law of Member States and the rules on procedure, which will have a positive impact on the fight against these crimes. Firstly, it is a way of preventing offenders from moving to Member States in which legislation against cyber attacks is more lenient. Secondly, shared definitions make it possible to exchange information and collect and compare relevant data. Thirdly, the effectiveness of prevention measures across the EU and international cooperation are also enhanced.

The proposal therefore complies with the subsidiarity principle.

- **Proportionality principle**

The proposal complies with the proportionality principle for the following reason:.

This Directive confines itself to the minimum required in order to achieve those objectives at European level and does not go beyond what is necessary for that purpose, taking into account the need for accuracy of criminal legislation.

- **Choice of instruments**

Proposed instrument: Directive.

---

15 OJ C 83, 30.3.2010, p. 49.

16 'Concerted Work Strategy and Practical Measures Against Cybercrime', 2987th JUSTICE and HOME AFFAIRS Council meeting, Brussels, 27-28 November 2008.

Other means would not be adequate for the following reason:

The legal basis requires a Directive.

Non-legislative measures and self-regulation would improve the situation in certain areas where implementation is crucial. However, in other areas where new legislation is essential, the benefits would be modest.

4. BUDGETARY IMPLICATION

The implications of the proposal for the Union budget are small. More than 90% of the estimated cost of EUR 5,913,000 would be borne by the Member States and there is the possibility of applying for EU funding to reduce the cost.

5. ADDITIONAL INFORMATION

- **Repeal of existing legislation**

The adoption of the proposal will lead to the repeal of the existing legislation.

- **Territorial scope**

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

2010/0273 (COD)

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

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[17],

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 judicial and other 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.

(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.

[17] OJ C […], […], p. […].

(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.

(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[18], when the attack is conducted on a large scale, or when an offence is committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner. It is also appropriate to provide for more severe penalties where such an attack has caused serious damage or has affected essential interests.

(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 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.

(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.

(11) This Directive strengthens the importance of networks, such as the G8 or the Council of Europe's network of points of contact available on a twenty-four hour, seven-day-a-week basis to exchange information in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to information systems and data, or for the collection of evidence in electronic form of a criminal offence. Given the speed with which large-scale attacks can be carried out, Member States should be able to respond promptly to urgent requests from this network of contact points. Such assistance should include facilitating, or directly carrying out, measures such as: the provision of technical advice, the preservation of data, the collection of evidence, the provision of legal information, and the locating of suspects.

(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

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

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 subsidiarity as set out in Article 5 of the Treaty on European Union. This Directive does not go beyond what is necessary in order to achieve those objectives.

(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[19] 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[20].

(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] OR [Without prejudice to Article 4 of Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, the United Kingdom and Ireland will not participate in the adoption of this Directive and will not be bound by or be subject to its application].

---

19 OJ L 350, 30.12.2008, p.60.

20 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

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Subject matter

This Directive defines criminal offences in the area of attacks against information systems and establishes minimum rules concerning penalties for such offences. It also aims to introduce common provisions to prevent such attacks and improve European criminal justice cooperation in this field.

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 or interference 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 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.

Article 4
Illegal system interference

Member States shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible

computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 5
Illegal data interference

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

Article 6
Illegal interception

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.

Article 7
Tools used for committing offences

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

(a) device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Article 8
Instigation, aiding, abetting and attempt

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

2. Member States shall ensure that the attempt to commit the offences referred to in Articles 3 to 6 is punishable as a criminal offence.

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, proportional and dissuasive criminal penalties.

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

Article 10
Aggravating circumstances

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

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6 are punishable by criminal penalties of a maximum term of imprisonment of at least five years when committed through the use of a tool designed to launch attacks affecting a significant number of information systems, or attacks causing considerable damage, such as disrupted system services, financial cost or loss of personal data.

3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6 are punishable by criminal penalties of a maximum term of imprisonment of at least five years when committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner.

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, 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 or a person with habitual residence in the territory of the Member State concerned; or

   (c) for the benefit of a legal person that has its head office in the territory of the Member State concerned.

2. When establishing jurisdiction in accordance with paragraph 1(a), Member States 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.

Article 14
Exchange of information

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.

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 8.

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover the number of offences referred to in Articles 3 to 8 reported to the Member States and the follow-up given to these reports, and shall indicate on an annual basis the number of reported cases investigated, the number of persons prosecuted, and the number of persons convicted for the offences referred to in Articles 3 to 8.

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.

Article 16
Repeal of Framework Decision 2005/222/JHA

Framework Decision 2005/222/JHA is hereby repealed, without prejudice to the obligations of the Member States relating to the time limits for transposition into national law.

References to the repealed Framework Decision 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] at

the latest. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive. When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 18
Reporting

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.

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 twentieth day following 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*