



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 19.04.2002  
COM(2002) 173 final

2002/0086 (CNS)

Proposal for a

**COUNCIL FRAMEWORK DECISION**

**on attacks against information systems**

(presented by the Commission)

## EXPLANATORY MEMORANDUM

### 1. INTRODUCTION

Electronic communication networks and information systems are now an essential part of the daily lives of EU citizens and are fundamental to the success of the EU economy. Networks and information systems are converging and becoming increasingly interconnected. Despite the many and obvious benefits of this development, it has also brought with it the worrying threat of intentional attacks against information systems. These attacks can take a wide variety of forms including illegal access, spread of malicious code and denial of service attacks. It is possible to launch an attack from anywhere in the world, to anywhere in the world, at any time. New, unexpected forms of attacks could occur in the future.

Attacks against information systems constitute a threat to the achievement of a safer Information Society and an Area of Freedom, Security and Justice, and therefore require a response at the level of the European Union. Part of the Commission's contribution to this response is this proposal for a Framework Decision on approximation of criminal law in the area of attacks against information systems.

#### 1.1. Types of attacks against information systems

The phrase "information system" is deliberately used here in its broadest sense in recognition of the convergence between electronic communication networks and the various systems they connect. For the purpose of this proposal, information systems therefore include "stand-alone" personal computers, personal digital organisers, mobile telephones, intranets, extranets and, of course, the networks, servers and other infrastructure of the Internet.

In its Communication "Network and Information security - A European Policy Approach"<sup>1</sup>, the Commission has proposed the following description of threats against computer systems:

- (a) **Unauthorised access to information systems.** This includes the notion of "**hacking**". Hacking is gaining unauthorised access to a computer or network of computers. It can be undertaken in a variety of ways from simply exploiting inside information to brute force attacks and password interception. It is often – though not always - with malicious intent to either copy, modify or destroy data. Intentional corruption of web-sites or access to services protected by conditional access without payment can be one of the aims of unauthorised access.
  
- (b) **Disruption of information systems.** Different ways exist to disrupt information systems through malicious attacks. One of the best known ways to deny or degrade the services offered by the Internet is a "**denial of service**" attack (DoS). In a way this attack is similar to fax machines being flooded with long and repeated messages. Denial of service attacks attempt to overload web servers or Internet Service Providers (ISPs) with automatically generated messages. Other types of attacks can include disrupting servers operating the domain name system (DNS) and attacks directed at "routers". Attacks aimed at disrupting systems have been damaging for certain high profile web-sites like portals. Some studies have calculated that a recent

---

<sup>1</sup> Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "Network and Information Security: Proposal for a European Policy Approach" of 6.6.2001. COM (2001) 298 final.

attack caused damage worth several hundred million Euros, in addition to the intangible damage to reputation. Increasingly, companies rely on the availability of their web-sites for their business and those companies which depend on it for “just in time” supply are particularly vulnerable.

- (c) **Execution of malicious software that modifies or destroys data.** The most well known type of malicious software is the virus. Infamous examples include the “I Love You”, “Melissa” and “Kournikova” viruses. About 11 % of European users have caught a virus on their home personal computer (PC). There are other types of malicious software. Some damage the PC itself, whereas others use the PC to attack other networked components. Some programs (often called ‘logic bombs’) can lie dormant until triggered by some event such as a specific date, at which point they can cause major damage by altering or deleting data. Other programs appear to be benign, but when opened release a malicious attack (often called ‘Trojan Horses’). Another variant is a program (often called a worm) that does not infect other programs as a virus, but instead creates copies of itself, which in turn create even more copies and eventually swamp the system.
- (d) **Interception of communications.** Malicious interception of communications compromises the confidentiality and integrity requirements of users. It is often called “sniffing”.
- (e) **Malicious misrepresentation.** Information systems offer new opportunities for misrepresentation and fraud. The taking of someone else’s identity on the Internet, and using this for malicious purposes, is often called “spoofing”.

## 1.2. The nature of the threat

There is a clear need to gather reliable information on the scale and nature of attacks against information systems.

Some of the most serious incidents of attacks against information systems are directed against electronic communications network operators and service providers or against electronic commerce companies. More traditional areas can also be severely affected given the ever-increasing amount of inter-connectivity in the modern communications environment: manufacturing industries; service industries; hospitals; other public sector organisations and governments themselves. But victims of attacks are not only organisations; there can be very direct, serious and damaging effects on individuals as well. The economic burden imposed by certain of these attacks on public bodies, companies and individuals alike is considerable and threatens to make information systems more costly and less affordable to users.

The type of attacks described above are often carried out by individuals acting on their own, sometimes by minors who perhaps do not fully appreciate the seriousness of their actions. However, the level of sophistication and ambition of the attack could grow. There is growing and worrying concern of organised criminals using communication networks to launch attacks against information systems for their own purposes. Organised hacking groups specialised in hacking and defacement of web-sites are more and more active at world-wide level. Examples include the Brazilian Silver Lords and the Pakistan Gforce, which try to extort money from their victims by offering them specialised assistance after hacking into their information systems. The arrest of large groups of hackers suggest that hacking could increasingly be an organised crime phenomenon. There have recently been sophisticated,

organised attacks against intellectual property as well as attempts to steal substantial funds from banking services<sup>2</sup>.

Security breaches at e-commerce merchant databases where access is gained to customers' information, including credit card numbers, are also a cause for concern. These attacks result in increased opportunities for payment fraud and in any case force the banking industry to cancel and re-issue thousands of cards. A further consequence is the intangible damage to the merchant's reputation and to consumer confidence in e-commerce. Preventive measures, such as minimum security requirements for online merchants accepting payment cards, are being discussed under the Action Plan to prevent fraud and counterfeiting of non-cash payments<sup>3</sup>.

This proposal also forms part of the Commission's contribution to the response to the threat of a terrorist attack against vital information systems within the European Union. It supplements the Commission's proposals to replace extradition within the European Union with a European Arrest Warrant<sup>4</sup> and to approximate laws on terrorism<sup>5</sup>, on which political agreement was reached at the Laeken European Council on 14/15 December 2001. . Taken together, these instruments will ensure that Member States of the European Union have effective criminal laws in place to tackle cyber-terrorism, and will enhance international co-operation against terrorism.

This proposal does not relate only to acts directed at Member States. It also applies to conduct on the territory of the European Union which is directed against information systems on the territory of third countries. This reflects the Commission's commitment to tackle attacks against information systems at a global as well as European Union level.

In fact, there have already been several recent occasions where tensions in international relations have led to a spate of attacks against information systems, often involving attacks against web-sites. More serious attacks could not only lead to serious financial damage but, in some cases, could even lead to loss of life (e.g. hospital systems, air traffic control systems etc). The importance attached to it by Member States is demonstrated in the priority attached to various Critical Infrastructure Protection initiatives. For example, the EU Information Society Technologies (IST) Programme<sup>6</sup> has established, in collaboration with the US Department of State, a Joint EU/US Task Force on Critical Infrastructure Protection.<sup>7</sup>

### **1.3. The need for accurate information and statistics**

There are few reliable statistics available on the full scale of the computer-related crime phenomenon. The number of intrusions detected and reported up to now probably under-

---

<sup>2</sup> According to a survey published by the Communications Management Association (CMA), there have been hacking attacks against a third of UK's big companies and public sector organisations, including government offices, causing damage ranging from infiltrating corporate bank accounts to information theft. See the survey at <http://www.cma.org>.

<sup>3</sup> Communication from the Commission "Preventing fraud and counterfeiting of non-cash means of payment", COM (2001) 11 final. Adopted by the Commission on 9.2.2001.

<sup>4</sup> Proposal for a Council Framework Decision on the European arrest warrant and the surrender procedures between the Member States. COM(2001) 522 final. Adopted by the Commission on 19.9.2001.

<sup>5</sup> Proposal for a Council Framework Decision on combating terrorism. COM(2001) 521 final. Adopted by the Commission on 19.9.2001

<sup>6</sup> The IST Programme is managed by the European Commission. It is part of the 5th Framework Programme, which runs from 1998 to 2002. More information is available at <http://www.cordis.lu/ist>.

<sup>7</sup> Under the auspices of the Joint Consultative Group of the EC/US Science and Technology Co-operation Agreement.

represent the scope of the problem. According to a US survey<sup>8</sup>, in 1999 only 32% of respondents who have suffered a computer intrusion in the previous year reported it to law enforcement. And this was an improvement on previous years when only 17% had reported. Numerous reasons have been given for non-reporting. Because of limited awareness and experience of system administrators and users, many intrusions are not detected. In addition, many companies are not willing to report cases of computer abuse, to avoid bad publicity and exposure to future attacks. Many police forces do not yet keep statistics on the use of computers and communication systems involved in these and other crimes<sup>9</sup>. Law enforcement authorities lack adequate training to detect, identify and investigate computer related offences. However, the European Union has started to address this issue by collecting some figures on attacks against information systems. In one Member State, it was estimated that there were between 30 000 and 40 000 attacks in 1999 on information systems, whereas no more than 105 official complaints were recorded in this field. Indeed, in 1999, seven Member States recorded a total of only 1844 official reports of crimes against information systems and computer data. Nevertheless, this is twice the figure reported in 1998, when only 972 cases were officially recorded in the seven Member States<sup>10</sup>.

In addition, a recent survey<sup>11</sup> reported that 13 per cent of companies that had been victim to economic crime stated one of the crimes was cybercrime. The survey also reported increasing concern about cybercrime, with 43 per cent of respondents believing cybercrime would be a future risk. Another study concluded that hackers and viruses now pose the main cybercrime threat to organisations, with the main perpetrators being hackers (45 per cent), former employees (13 per cent), organised crime (13 per cent) and current employees (11 per cent)<sup>12</sup>. Such figures can be expected to continue to grow as the use of information systems and interconnectivity increases, and the willingness to report attacks improves. But it is clear that urgent measures are needed to produce a statistical tool for use by all Member States so that computer-related crime within the European Union can be measured both quantitatively and qualitatively. The starting point for such an analysis is a common definition at the level of the European Union of the offences involved in attacks against information systems.

#### **1.4. European Union policy background**

Against this background, at the Lisbon European Council of March 2000, the European Council stressed the importance of the transition to a competitive, dynamic and knowledge-based economy, and invited the Council and the Commission to draw up an eEurope Action plan to make the most of this opportunity.<sup>13</sup> This Action Plan, prepared by the Commission and the Council, adopted by the Feira Summit of the European Council in June 2000, includes actions to enhance network security and the establishment of a co-ordinated and coherent approach to cybercrime by the end of 2002.

---

<sup>8</sup> The Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) produce an annual "Computer Crime and Security Survey" published early in each year. CSI's website and further details about the survey may be found at [www.gocsi.com](http://www.gocsi.com)

<sup>9</sup> The Italian Ministry of Interior recently published statistics on its operational activities against computer-related crime in 1999 and 2000 (see at [http://www.mininterno.it/dip\\_ps/dcpsffp/index.htm](http://www.mininterno.it/dip_ps/dcpsffp/index.htm)). Official reports of hacking cases in 2000 are 98, four times the figure reported in 1999, when only 21 cases were officially recorded.

<sup>10</sup> Council doc. 8123/01 ENFOPOL 38. Available from the Council website <http://db.consilium.eu.int/jai>  
<sup>11</sup> European Economic Crime Survey 2001, PricewaterhouseCoopers 2001 ( <http://www.pwcglobal.com> )

<sup>12</sup> The Cybercrime Survey 2001, Confederation of British Industry (see <http://www.cbi.org.uk> )

<sup>13</sup> Presidency Conclusions of the Lisbon European Council of 23 and 24 March 2000, available at <http://ue.eu.int/en/Info/eurocouncil/index.htm>.

As part of the Commission's contribution to this mandate on cybercrime, the Commission published a Communication entitled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime"<sup>14</sup>. This proposed a balanced approach to tackling the problems of cybercrime, by taking full account of the views of all the interested parties including law enforcement agencies, service providers, network operators, other industry groups, consumer groups, data protection authorities and privacy groups. The Communication proposed a number of legislative and non-legislative initiatives.

An important example of an ongoing action is within the IDA Programme, where Member States and the Commission are already working on a common security policy and implementing a secure network for exchange of administrative information.

One of the key issues addressed by the Communication was the need for effective action to deal with threats to the authenticity, integrity, confidentiality and availability of information systems and networks. Much has already been achieved in the field of Community law. There are already several legal measures in place at Community level with specific implications for network and information security.

This Framework Decision supplements what has already been achieved in the field of Community law to protect information systems, such as under Directives 95/46/EC, Directive 97/66/EC and Directive 98/84/EC on the legal protection of services based on, or consisting of, conditional access. In particular, the European telecommunication and data protection framework (Directives 95/46/EC and 97/66/EC<sup>15</sup>) contains provisions to ensure that providers of publicly available telecommunications services must take appropriate technical and organisational measures to safeguard the security and confidentiality of their services, and that these measures must ensure a level of security appropriate to the risk presented.

One of the most important and effective ways to address these problems is through prevention and education. The Communication underlined the importance of the availability, development, deployment and effective use of preventive technologies. It highlighted that there was a need to raise public awareness on the risks posed by computer-related crime, promote best practices for IT security, develop effective tools and procedures to combat computer-related crime as well as encourage further development of early warning and crisis management mechanisms. The EU Information Society Technologies (IST) Programme<sup>16</sup> provides a framework to develop capability and technologies to understand and tackle emerging challenges related to computer crime.

More recently, the Stockholm European Council on 23-24 March recognised the need for further action in the area of network and information security and concluded "*the Council together with the Commission will develop a comprehensive strategy on security of electronic networks including practical implementing action. This should be presented in time for the Göteborg European Council.*" The Commission responded to this call with its Communication on "Network and Information Security: A European Policy approach"<sup>17</sup>. This analysed the current problems in network security, and provided a strategic outline for action in this area. It was followed by a Council Resolution of 6 December 2001 on a

---

<sup>14</sup> COM (2000) 890 final

<sup>15</sup> OJ L. 281, 23.11.1995, p. 0031-0050, OJ L. 024, 30.01.1998, p. 0001-0008

<sup>16</sup> The IST Programme is managed by the European Commission. It is part of the 5th Framework Programme, which runs from 1998 to 2002. More information is available at <http://www.cordis.lu/ist>.

<sup>17</sup> COM (2001) 298 final. 6.6.2001.

common approach and specific actions in the area of network and information security. These initiatives are not in themselves sufficient to provide all the necessary responses to serious attacks against information systems. Both Commission Communications also recognised that there was an urgent need for approximation of substantive criminal law within the European Union in the area of attacks against information systems. This reflected the conclusions of the Tampere Summit of the European Council in October 1999<sup>18</sup> which include high-tech crime in a limited list of areas where efforts should be made to agree on common definitions, incriminations and sanctions, and was included in Recommendation 7 of the European Union strategy for the new Millennium on the prevention and control of organised crime adopted by the JHA Council in March 2000.<sup>19</sup> This proposal for a Framework Decision is also part of the Commission Work Programme for the Year 2001<sup>20</sup> and the Scoreboard for the establishment of an area of Freedom, Security and Justice, produced by the Commission on 30 October 2001<sup>21</sup>.

### **1.5. The need for approximation of criminal law**

Member States' laws in this area contain some significant gaps and differences which could hamper the fight against organised crime and terrorism, as well as serious attacks against information systems by individuals. Approximation of substantive law in the area of high tech crime will ensure that national legislation is sufficiently comprehensive so that all forms of serious attacks against information systems can be investigated using the techniques and methods available under the criminal law. Perpetrators of these offences need to be identified, brought to justice, and the courts need to have appropriate and proportionate penalties at their disposal. This will send a strong deterrent message to those contemplating attacks against information systems.

In addition, these gaps and differences could act as a barrier to effective police and judicial co-operation in the area of attacks against information systems. Attacks against information systems could often be trans-national in nature, and would require international police and judicial co-operation. Approximation of laws will therefore improve this co-operation by ensuring that the dual criminality requirement is fulfilled (in which an activity must be an offence in both countries before mutual legal assistance can usually be provided to assist a criminal investigation). This will benefit EU Member States in co-operation between themselves, as well as improving co-operation between EU Member States and third countries (provided that an appropriate mutual legal assistance agreement exists).

There is also a need to supplement existing instruments at European Union level. The Framework Decision on the European Arrest Warrant<sup>22</sup>, the Annex to the Europol Convention<sup>23</sup> and the Council Decision setting up Eurojust<sup>24</sup> contain references to computer-related crime which need to be defined more precisely. For the purposes of such instruments,

---

<sup>18</sup> <http://db.consilium.eu.int/en/Info/eurocouncil/index.htm>.

<sup>19</sup> The Prevention and control of organised crime: A European Union strategy for the beginning of the new Millennium (OJ 2000 C124, 3.5.2000).

<sup>20</sup> [http://europa.eu.int/comm/off/work\\_programme/index\\_en.htm](http://europa.eu.int/comm/off/work_programme/index_en.htm)

<sup>21</sup> [http://europa.eu.int/comm/dgs/justice\\_home](http://europa.eu.int/comm/dgs/justice_home).COM (2001) 628 final, 30.10.2001

<sup>22</sup> OJ C . . p

<sup>23</sup> Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention)  
OJ C 316 , 27.11.1995 p. 0001 - 0001

<sup>24</sup> OJ C . . p

computer-related crime should be understood as including attacks against information systems as defined in this Framework Decision, which will provide a much greater level of approximation of the constituent elements of such offences. This Framework Decision also complements the Framework Decision on combating terrorism<sup>25</sup> which covers terrorist actions causing extensive destruction of an infrastructure facility, including an information system, likely to endanger human life or result in major economic loss.

## **1.6. Scope and purpose of the proposed Framework Decision**

The objectives of this Council Framework Decision are therefore to approximate criminal law in the area of attacks against information systems and to ensure the greatest possible police and judicial co-operation in the area of criminal offences related to attacks against information systems. Moreover, this proposal contributes to the efforts of the European Union in the fight against organised crime and terrorism. It is not intended to require Member States to criminalise minor or trivial conduct.

It is clear from Article 47 of the Treaty on European Union that this Framework Decision is without prejudice to Community law. In particular, it does not affect privacy or data protection rights and obligations provided for under Community law such as in Directives 95/46 and 97/66. It is not intended to require Member States to criminalise breaches of rules on access to / disclosure of personal data, secrecy of communications, security of processing of personal data, electronic signatures<sup>26</sup> or intellectual property violations and it does not prejudice the Directive 98/84/EC on the legal protection of services based on, or consisting of, conditional access<sup>27</sup>. These are important issues, but they are already covered by existing Community legislation. Any approximation of criminal law in these areas to meet Community law objectives, such as the protection of personal data, the remuneration of service providers using conditional access or intellectual property, therefore needs to be considered using the framework of Community law rather than Title VI of the TEU. For these reasons, this Framework Decision limits itself to addressing the conduct described in points (a)-(c) in section 1.1.

Legislative action at the level of the European Union also needs to take into account developments in other international fora. In the context of approximation of substantive criminal law on attacks against information systems, the Council of Europe (C.o.E.) is currently the most far-advanced. The Council of Europe started preparing an international Convention on cyber-crime in February 1997, and the Convention was formally adopted and opened for signature in November 2001.<sup>28</sup> The Convention seeks to approximate a range of criminal offences including offences against the confidentiality, integrity and availability of computer systems and data. This Framework Decision is intended to be consistent with the approach adopted in the Council of Europe Convention for these offences.

In G8 discussions on high tech crime, two major categories of threats have been identified. First, threats to computer infrastructures, which concern operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computer and

---

<sup>25</sup> OJ C . . p

<sup>26</sup> Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L. 13 of 19/01/2000

<sup>27</sup> OJ L320, 28.11.1998, p. 54-57

<sup>28</sup> The text is available on the web, in two languages, in French : <http://conventions.coe.int/treaty/fr/projets/cybercrime.htm>. and in English: <http://conventions.coe.int/treaty/en/projets/cybercrime.htm>.

networks themselves. Secondly, computer-assisted threats, which concern malicious activities, such as fraud, money laundering, child pornography, infringement to intellectual property rights and drug trafficking, which are facilitated by the use of a computer. This proposal deals with the first category of threats.

Approximation at the level of the EU should take into account developments in international fora and should be consistent with current Community policies. This proposal also seeks to provide greater approximation within the EU than has been possible in other international fora.

## **2. LEGAL BASIS**

The objective of the establishment of an area of freedom, security and justice must be achieved by preventing and combating crime, organised or otherwise, including terrorism, through closer co-operation between law enforcement and judicial authorities in the Member States and approximation of rules in criminal matters of the Member States. This proposal for a Framework Decision is therefore aimed at approximating laws and regulations of the Member States in the area of police and judicial co-operation in criminal matters. It concerns "minimum rules relating to the constituent elements of criminal acts", in particular, to a substantial degree, in the fields of organised crime and terrorism. It also involves "ensuring compatibility in rules applicable in the Member States" in order to facilitate and accelerate co-operation between judicial authorities. The legal basis indicated in the preamble of the proposal is therefore Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. The proposal will not entail financial implications for the budget of the European Communities.

## **3. THE FRAMEWORK DECISION: ARTICLES**

### **Article 1 - Scope and purpose of the Framework Decision**

This Article explicitly states that the objectives of this Framework Decision are to approximate criminal law in the area of serious attacks against information systems, in particular to contribute to the fight against organised crime and terrorism, and by doing so to ensure the greatest possible judicial co-operation in the area of criminal offences related to attacks against information systems. In accordance with Article 47 of the Treaty on European Union, this Framework Decision is also without prejudice to Community law. In particular this includes privacy or data protection rights and obligations provided for under the Directives 95/46 and 97/66. It is not intended to require Member States to criminalise breaches of rules on access to / disclosure of personal data, secrecy of communications, security of processing of personal data, electronic signatures<sup>29</sup> or intellectual property violations and it does not prejudice the Directive 98/84/EC on the legal protection of services based on, or consisting of, conditional access<sup>30</sup>.

This Framework Decision is not intended to require Member States to criminalise minor or trivial conduct. Articles 3 and 4 define the criteria which need to be met in order for the

---

<sup>29</sup> Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L. 13 of 19/01/2000

<sup>30</sup> OJ L320, 28.11.1998, p. 54-57

action to be criminalised. These criteria are consistent with the derogation and reservation possibilities in the draft Council of Europe Cybercrime Convention.

All the criminal offences covered in the framework decision need to be committed with intent. The term “intentional” is used explicitly in Articles 3, 4 and 5. This should be interpreted in accordance with the normal criminal law principles in Member States governing intent. Thus, this Framework Decision does not require criminalisation of actions where there is gross negligence or other recklessness, but no intent as such. An intent to unlawfully access or interfere with information systems in general should also be sufficient, rather than it being necessary to prove that the intent was directed at a specific information system.

## Article 2 - Definitions

The proposed Council Framework Decision contains the following definitions:

- (a) “*Electronic communications network*”. This definition is the same as that adopted by the Council and European Parliament on 14 February 2002 in the Directive on a common regulatory framework for electronic communications networks and services<sup>31</sup>.
- (b) “*Computer*”. This definition is based on Article 1 of the draft Council of Europe Convention on Cybercrime. The definition also includes for example “stand-alone” personal computers, personal digital organisers, digital set-top boxes, personal video recorders and mobile telephones (provided they have some data processing functions, e.g. WAP and third generation), which would not be covered solely by the definition of electronic communication networks.
- (c) “*Computer data*”. This definition is built upon the ISO<sup>32</sup> definition of data. It is not intended to include physical items such as books. However, it does include a book stored in the form of computer data (e.g. saved in electronic form as a word processing file) or turned into computer data by means of scanning. For this reason, the definition makes clear that computer data needs to have been “created or put into a form” suitable for processing in an information system or suitable for causing a function of an information system.
- (d) “*Information System*”. The definition of information systems is originally drawn from that adopted by the OECD in 1992 in its Guidelines for the Security of Information Systems and the previous definitions by referring to electronic communications networks, computers and computer data. The term has also been used in previous community law instruments, such as the Council Decision of 31 March 1992 “in the field of security of information systems” and the Council Recommendation of 7 April 1995 “on common information technology security evaluation criteria”. It is intended to be technology neutral, and to reflect accurately the concept of interconnected networks and systems containing data. It covers both the hardware and the software of the system, though not the content of the information itself. It also covers stand-alone systems. In the Commission’s view, it

---

<sup>31</sup> For final text see [http://europa.eu.int/information\\_society/topics/telecoms/regulatory/new\\_rf/index\\_en.htm#reg](http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg)

<sup>32</sup> The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from some 100 countries.

is desirable to extend the protection afforded by the criminal law to stand-alone computers as well and not to limit it only to systems that are inter-connected.

- (e) “*Legal person*”. This is a standard definition from previous Council Framework Decisions.
- (f) “*Authorised person*”. This means any person who has the right, by contract or by law, or the lawful permission, to use, manage, control, test, conduct legitimate scientific research or otherwise operate an information system and who is acting in accordance with that right or permission. This includes persons acting in accordance with the lawful consent of someone given such an explicit authorisation. It is particularly important that the following categories of persons and legitimate activities (within the limits of the person’s rights, permissions and responsibilities, and in accordance with Community laws on data protection and secrecy of communications) should not be criminalised when this Framework Decision is transposed into domestic law:
  - actions of ordinary users, whether private or business users, including their use of encryption to protect their own communications and data;
  - reverse engineering, within the limits provided by Directive 91/250 of 14 May 1991 “on the legal protection of computer programs”<sup>33</sup>
  - actions of managers, controllers and operators of networks and systems;
  - actions of authorised persons testing a system, whether within the company or person appointed externally and given permission to test the security of a system;
  - legitimate scientific research.
- (g) “*Without right*”. This is a broad notion, and leaves some flexibility to Member States to decide the precise scope of the offence. Nevertheless, to assist in the implementation of the Council Framework Decision in domestic laws, the Commission believes that it is necessary to indicate that certain activities should not fall within the scope of the offence. It is not possible, and probably not desirable, to draw up a comprehensive, exclusive list of exemptions at the level of the European Union. But the phrase “without right” builds on the previous definitions so as to exclude conduct by authorised persons. It also excludes any other conduct recognised as lawful under domestic law, including standard legal defences and other types of authority recognised in domestic law.

### **Article 3 – Attack through illegal access to Information Systems**

This offence is intended to cover the offence of illegal access to information systems. This includes the notion of “hacking” an information system. Member States are free to exclude minor or trivial cases from the scope of the offence when transposing the Framework Decision into domestic law.

---

<sup>33</sup> OJ L 122 , 17/05/1991 P. 0042 - 0046

The offence is required to be established in Member States' laws only to the extent that the offence is committed:

- (i) against any part of an information system which is subject to specific protection measures; or
- (ii) with the intent to cause damage to a natural or legal person; or
- (iii) with the intent to result in an economic benefit.

The Commission does not wish to undermine in any way the importance it attached to the use of effective technical measures to protect information systems. Nevertheless, it is an unfortunate fact that a high proportion of users leave themselves exposed to attacks by not having adequate (or even any) technical protection. To deter attacks against these users, it is necessary that criminal law covers unauthorised access to their systems even though there may not be adequate technical protection for their systems. For this reason, and provided that there is either an intent to cause damage or an intent to result in an economic benefit, there is no requirement that security measures must have been overcome for the offence to have been committed.

#### **Article 4 – Illegal interference with Information Systems**

This offence covers the intentional conduct, without right, of one of the following actions:

- (a) the serious hindering or interruption, without right, of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. The elements of inputting or transmitting computer data specifically address the problem of so-called “denial of service attacks” where there is a deliberate attempt to overwhelm an information system. The offence also covers the “interruption” of the functioning of an information system, which could be inferred from the phrase “hindering” but is included here explicitly for the sake of clarity. The other elements in the offence (damaging, deleting, deteriorating, altering or suppressing computer data) specifically address the problem of viruses, and other types of attacks, which are directed at hindering or interrupting the functions of the information system itself.
- (b) the deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person. This covers virus attacks aimed at the content (or computer data) on the information system, as well as corruption of web-sites.

Subparagraph (a) uses the word “serious hindering or interruption” as a constituent element of the offence in order to describe the effects of such an attack. The meaning of the word “serious hindering” is not defined, as hindering could take different forms and its level could vary depending upon the type of the attack and the technical capacities of the information system being attacked. Each Member State shall determine for itself what criteria must be fulfilled in order for an information system to be considered as “seriously hindered”. However, minor nuisances or disruptions in the functioning of the services should not be considered as fulfilling the threshold of seriousness.

As above, Member States are free to exclude minor or trivial cases from the scope of the offence when transposing the Framework Decision into domestic law.

### **Article 5 - Instigation, aiding, abetting and attempt**

Article 5(1) puts an obligation on Member States to ensure that the intentional instigation of, aiding or abetting offences against information systems as described in Articles 3 and 4 are punishable.

Article 5(2) specifically concerns attempt. It puts an obligation on Member States to ensure that attempt to commit any of the offences against information systems described in Articles 3 and 4 is punishable.

### **Article 6 – Penalties**

Paragraph 1 requires Member States to take the necessary measures to ensure that the offences defined in Articles 3-5 are punishable by effective, proportionate and dissuasive penalties<sup>34</sup>. By virtue of this paragraph, Member States are required to lay down penalties commensurate with the gravity of the offence, which includes custodial sentences with a maximum term of imprisonment of no less than one year in serious cases. Serious cases shall be understood as excluding cases where the conduct resulted in no damage or economic benefit.

The maximum penalty of at least one year imprisonment in serious cases brings these offences within the scope of the European Arrest Warrant as well as other instruments such as the Council Framework Decision of 26 June 2001<sup>35</sup> on money laundering, the identification, tracing, freezing, seizing and confiscation of the instrumentalities and the proceeds from crime.

In keeping with the nature of all framework decisions, which are binding on the Member States as regards the result to be achieved, but leave the choice of form and means to their discretion, the Member States retain some degree of flexibility to adapt their legislation to these rules and to determine the severity of the penalties that apply, within the limits imposed by the Framework Decision, particularly the aggravating circumstances in Article 7. The Commission would stress that it is for the Member States to decide the criteria for determining the gravity of an offence, on the basis of their respective legal systems.

Punishment need not always take the form of imprisonment. Paragraph 2 provides the possibility for Member States to impose fines in addition to or as an alternative to custodial sentences, in line with their respective traditions and legal systems.

### **Article 7 - Aggravating circumstances**

This Article provides for Member States to increase the penalties defined in Article 6 under certain circumstances. The Commission would stress that the list of aggravating circumstances provided in this Article is without prejudice to any other circumstances regarded as aggravating in Member States' legislation. This list takes into account the

---

<sup>34</sup> The phrase is taken from the Judgment given by the Court of Justice on 21 September 1989 in Case 68/88 [1989] ECR 2965.

<sup>35</sup> OJ L 182, 5.7.2001, p.1

aggravating circumstances described in the national provisions in Member States and as laid down in previous Commission proposals for Framework Decisions.

If one of the following conditions listed in paragraph 1 is fulfilled then the maximum term of imprisonment may not be less than four years:

- (a) the offence has been committed within the framework of a criminal organisation as defined by Joint Action 98/733 JHA, apart from the penalty level referred to therein;
- (b) the offence caused, or resulted in, substantial direct or indirect economic loss, physical harm to a natural person or substantial damage to part of the critical infrastructure of the Member State; or
- (c) the offence resulted in substantial proceeds.

Member States are also required to ensure that the offences referred to in Articles 3, 4 and 5 are punishable by custodial sentences greater than those foreseen under Article 6, when the offender has been convicted of such an offence by a final judgement in a Member State.

#### **Article 8 - Particular circumstances**

This article provides for circumstances in which a Member State may decide to reduce the penalties referred to in Articles 6 and 7 where, in the opinion of the competent judicial authority, the offender caused only minor damage.

#### **Article 9 - Liability of legal persons**

In line with the approach taken in a number of legal instruments adopted at EU level to combat different types of criminality, it is necessary also to cover the situation in which legal persons are involved in attacks against information systems. Article 9 therefore contains provisions for holding a legal person liable for the offences envisaged by Articles 3, 4 and 5, committed for their benefit by any person with certain leading positions, acting either individually or as a part of the organ of the legal person. The term liability should be construed so as to include either criminal or civil liability.

In addition, according to standard practice, paragraph 2 provides that a legal person can also be held liable when the lack of supervision or control by a person in a position to exercise control, has rendered possible the commission of the offences for its benefit. Paragraph 3 indicates that legal proceedings against a legal person do not preclude parallel legal proceedings against a natural person.

#### **Article 10 - Sanctions on legal persons**

Article 10 sets out a requirement for sanctions for legal persons held liable for the offences referred to in Articles 3, 4 and 5. It requires effective, proportionate and dissuasive sanctions, where the minimum obligation is to impose criminal or non-criminal fines. Other sanctions that could typically apply to legal persons are also indicated.

#### **Article 11 - Jurisdiction**

The international nature of offences involving attacks against information systems means that an effective legal response requires procedural provisions on jurisdiction and extradition

which should be clear and far-reaching at the European Union level, to ensure that offenders cannot escape prosecution.

Paragraph 1 sets out a series of criteria for conferring jurisdiction on national judicial authorities to prosecute and investigate cases involving the offences referred to in this framework decision. A Member State will establish its jurisdiction in three situations:

- (a) where the offence is committed in whole or in part on its territory, irrespective of the status of the legal person or the nationality of the natural person involved (territoriality principle);
- (b) where the offender is a national of that Member State (active personality principle) and the act affects individuals or groups of that State. Member States that make no provision for extradition are responsible for prosecuting their own nationals who have committed offences abroad;
- (c) where the offence is committed for the benefit of a legal person established in the territory of that Member State.

Paragraph 2 is intended to ensure that when establishing its jurisdiction over the offences based on the territoriality principle in paragraph 1(a), each Member State ensures that its jurisdiction includes cases where:

- (a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory. For example, a person obtaining illegal access to (hacking) an information system in a third country from the territory of the Member State; or
- (b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory. For example, a person obtaining illegal access to (hacking) an information system on the territory of the Member State from the territory of a third country.

Given that not all Member States' legal traditions recognise extraterritorial jurisdiction for all types of criminal offence, paragraph 3 allows them not to apply the rules on jurisdiction set out in paragraph 1 as regards the situations covered by paragraph 1(b) and (c).

Paragraph 4 requires each Member State to take the necessary measures also to establish its jurisdiction over the offences referred to in Articles 3 to 5 in cases where it refuses to hand over or extradite a person suspected or convicted of such an offence to another Member State or to a third country.

Paragraph 5 covers multi-jurisdictional cases, and aims to ensure full co-operation between the Member States in order to centralise, if possible, proceedings in a single Member State. To this end, it is recalled that Member States may have recourse to any body or mechanism established within the European Union in order to facilitate co-operation between their judicial authorities and the co-ordination of their action. This would include Eurojust and the European Judicial Network.

Paragraph 6 states that the Member States shall inform the General Secretariat of the Council and the Commission where they decide to apply paragraph 3.

## **Article 12 – Exchange of Information**

The purpose of Article 12 is to facilitate the exchange of information by ensuring that there are operational points of contact. This is important for effective police co-operation. In particular, the need for all Member States to join the G8 network of points of contact was recognised by the Justice and Home Affairs Council on 19 March 1998 and more recently when it adopted a Council Recommendation on contact points maintaining a 24-hour service for combating high-tech crime<sup>36</sup>.

## **Article 13 - Implementation**

Article 13 concerns the implementation and follow-up of this Framework Decision. Member States are required to take the necessary measures to comply with this Framework Decision not later than 31 December 2003.

Member States shall transmit by that date to the General Secretariat of the Council and to the Commission the provisions transposing the obligations imposed on them under this Framework Decision into national law. The Council shall assess within one year, on the basis of that information and a Commission's written report, the extent to which Member States have complied with the obligations imposed by the Framework Decision.

## **Article 14 – Entry into force**

Article 14 states that the Framework Decision will enter into force on the twentieth day following that of its publication in the *Official Journal of the European Communities*.

---

<sup>36</sup> OJ C 187, 3.7.2001, p. 5

Proposal for a

**COUNCIL FRAMEWORK DECISION**

**on attacks against information systems**

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 29, 30(1)(a), 31 and 34(2)(b) thereof,

Having regard to the proposal of the Commission<sup>1</sup>,

Having regard to the opinion of the European Parliament<sup>2</sup>,

Whereas:

(1) There is evidence of attacks against information systems, in particular as a result of the threat from organised crime, and increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States. This constitutes a threat to the achievement of a safer Information Society and an Area of Freedom, Security and Justice, and therefore requires a response at the level of the European Union.

(2) An effective response to those threats requires a comprehensive approach to network and information security, as underlined in the eEurope Action Plan, in the Communication by the Commission “Network and Information Security: Proposal for a European Policy Approach”<sup>3</sup> and in the Council Resolution of 6 December 2001 on a common approach and specific actions in the area of network and information security.

(3) The need to further increase awareness of the problems related to information security and provide practical assistance has also been stressed in the European Parliament Resolution of 5<sup>th</sup> September 2001<sup>4</sup>.

(4) Significant gaps and differences in Member States’ laws in this area hamper the fight against organised crime and terrorism, and act as a barrier to effective police and judicial co-operation in the area of attacks against information systems. The trans-national and borderless character of modern electronic communication networks means that attacks against information systems are often international in nature, thus underlining the urgent need for further action to approximate criminal laws in this area.

---

<sup>1</sup> OJ C . . p .

<sup>2</sup> OJ C . . p

<sup>3</sup> COM (2001) 298

<sup>4</sup> [2001/2098(INI)]

(5) The Action Plan of the Council and the Commission on how to best implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice<sup>5</sup>, the Tampere European Council on 15-16 October 1999, the Santa Maria da Feira European Council on 19-20 June 2000, the Commission in the Scoreboard<sup>6</sup> and the European Parliament in its Resolution of 19 May 2000<sup>7</sup> indicate or call for legislative action against high technology crime, including common definitions, incriminations and sanctions.

(6) It is necessary to complement the work performed by international organisations, in particular the Council of Europe's work on approximating criminal law and the G8's work on transnational co-operation in the area of high tech crime, by providing a common approach in the European Union in this area. This call was further elaborated by the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime"<sup>8</sup>.

(7) Criminal law in the area of attacks against information systems should be approximated in order to ensure the greatest possible police and judicial co-operation in the area of criminal offences related to attacks against information systems, and to contribute to the fight against organised crime and terrorism.

(8) The Framework Decision on the European Arrest Warrant<sup>9</sup>, the Annex to the Europol Convention and the Council Decision setting up Eurojust contain references to computer-related crime which needs to be defined more precisely. For the purposes of such instruments, computer-related crime should be understood as including attacks against information systems as defined in this Framework Decision which provides a much greater level of approximation of the constituent elements of such offences. This Framework Decision also complements the Framework Decision on combating terrorism<sup>10</sup> which covers terrorist actions causing extensive destruction of an infrastructure facility, including an information system, likely to endanger human life or result in major economic loss.

(9) All Member States have ratified the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. The personal data processed in the context of the implementation of this Framework Decision will be protected in accordance with the principles of the said Convention.

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

---

<sup>5</sup> OJ C 19, 23.1.1999

<sup>6</sup> COM (2001) 278 final

<sup>7</sup> A5-0127/2000

<sup>8</sup> COM (2000) 890

<sup>9</sup> OJ C . . p

<sup>10</sup> OJ C . . p

(11) There is a need to achieve a common approach to the constituent elements of criminal offences by providing for a common offence of illegal access to an information system, and illegal interference with an information system.

(12) There is a need to avoid over-criminalisation, particularly of trivial or minor conduct, as well as the need to avoid criminalising right-holders and authorised persons such as legitimate private or business users, managers, controllers and operators of networks and systems, legitimate scientific researchers, and authorised persons testing a system, whether a person within the company or a person appointed externally and given permission to test the security of a system.

(13) There is a need for Member States to provide penalties for attacks against information systems which are effective, proportionate and dissuasive, including custodial sentences in serious cases;

(14) It is necessary to provide for more severe penalties when certain circumstances accompanying an attack against an information system make it an even greater threat to society. In such cases, sanctions on perpetrators should be sufficient to allow for attacks against information systems to be included within the scope of instruments already adopted for the purpose of combating organised crime such as the 98/733/JHA Joint Action of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union<sup>11</sup>.

(15) Measures should be taken to enable legal persons to be held liable for the criminal offences referred to by this act which are committed for their benefit, and to ensure that each Member State has jurisdiction over offences committed against information systems in situations where the offender is physically present on its territory or where the information system is on its territory.

(16) Measures should also be foreseen for the purposes of co-operation between Member States with a view to ensuring effective action against attacks against information systems. Operational contact points should be established for the exchange of information.

(17) Since the objectives of ensuring that attacks against information systems be sanctioned in all Member States by effective, proportionate and dissuasive criminal penalties and improving and encouraging judicial co-operation by removing potential obstacles, cannot be sufficiently achieved by the Member States individually, 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 referred to in Article 2 of the EU Treaty and as set out in Article 5 of the EC Treaty. In accordance with the principle of proportionality, as set out in the latter Article, this Framework Decision does not go beyond what is necessary in order to achieve those objectives.

(18) This Framework Decision is without prejudice to the powers of the European Community.

---

<sup>11</sup> OJ L 351, 29.12.1998, p. 1

(19) This Framework Decision respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, and notably Chapters II and VI thereof.

HAS ADOPTED THIS FRAMEWORK DECISION:

### *Article 1*

#### **Scope and objective of the Framework Decision**

The objective of this Framework Decision is to improve co-operation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems.

### *Article 2*

#### **Definitions**

For the purposes of this Framework Decision, the following definitions shall apply:

- (a) “*Electronic communications network*” means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed
- (b) “*Computer*” 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.
- (c) “*Computer data*” means any representation of facts, information or concepts which has been created or put into a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function.
- (d) “*Information System*” means computers and electronic communication networks, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.
- (e) “*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.
- (f) “*Authorised person*” means any natural or legal person who has the right, by contract or by law, or the lawful permission, to use, manage, control, test, conduct legitimate scientific research or otherwise operate an information system and who is acting in accordance with that right or permission.

- (g) “*Without right*” means that conduct by authorised persons or other conduct recognised as lawful under domestic law is excluded.

### *Article 3*

#### **Illegal access to Information Systems**

Member States shall ensure that the intentional access, without right, to the whole or any part of an information system is punishable as a criminal offence where it is committed:

- (i) against any part of an information system which is subject to specific protection measures; or
- (ii) with the intent to cause damage to a natural or legal person; or
- (iii) with the intent to result in an economic benefit.

### *Article 4*

#### **Illegal interference with Information Systems**

Member States shall ensure that the following intentional conduct, without right, is punishable as a criminal offence:

- (a) 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;
- (b) the deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person.

### *Article 5*

#### **Instigation, aiding, abetting and attempt**

1. Member States shall ensure that the intentional instigation of, aiding or abetting an offence referred to in Articles 3 and 4 is punishable.
2. Member State shall ensure that attempt to commit the offences referred to in Articles 3 and 4 is punishable.

### *Article 6*

#### **Penalties**

1. Member States shall ensure that offences referred to in Articles 3, 4 and 5 are punishable by effective, proportionate and dissuasive penalties including a custodial sentence with a maximum term of imprisonment of no less than one year in serious cases. Serious cases shall be understood as excluding cases where the conduct resulted in no damage or economic benefit

2. Member States shall provide for the possibility of imposing fines in addition to or as an alternative to custodial sentences.

#### *Article 7*

#### **Aggravating circumstances**

1. Member States shall ensure that the offences referred to in Articles 3, 4 and 5 are punishable by a custodial sentence with a maximum term of imprisonment of no less than four years when they are committed under the following circumstances:
  - (a) the offence has been committed within the framework of a criminal organisation as defined in Joint Action 98/733/ JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union, apart from the penalty level referred to therein;
  - (b) the offence caused, or resulted in, substantial direct or indirect economic loss, physical harm to a natural person or substantial damage to part of the critical infrastructure of the Member State;
  - (c) the offence resulted in substantial proceeds; or
2. Member States shall ensure that the offences referred to in Articles 3 and 4 are punishable by custodial sentences greater than those foreseen under Article 6, when the offender has been convicted of such an offence by a final judgement in a Member State.

#### *Article 8*

#### **Particular circumstances**

Notwithstanding Articles 6 and 7, Member States shall ensure the penalties referred to in Articles 6 and 7 can be reduced, where, in the opinion of the competent judicial authority, the offender caused only minor damage.

#### *Article 9*

#### **Liability of legal persons**

1. Member States shall ensure that legal persons can be held liable for conducts referred to in Articles 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:
  - (a) a power of representation of the legal person, or
  - (b) an authority to take decisions on behalf of the legal person, or
  - (c) an authority to exercise control within the legal person.

2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 3, 4 and 5 for the benefit of that legal person by a person under its authority.
3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who commit offences or engage in the conduct referred to in Articles 3, 4 and 5.

#### *Article 10*

#### **Sanctions for legal persons**

1. Member States shall ensure that a legal person held liable pursuant to Article 9(1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and may include other sanctions, such as:
  - 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; or
  - d) a judicial winding-up order.
2. Member States shall ensure that a legal person held liable pursuant to Article 9(2) is punishable by effective, proportionate and dissuasive sanctions or measures.

#### *Article 11*

#### **Jurisdiction**

1. Each Member State shall establish its jurisdiction with regard to the offences referred to in Articles 3, 4 and 5 where the offence has been committed:
  - (a) in whole or in part within its territory; or
  - (b) by one of its nationals and the act affects individuals or groups of that State; or
  - (c) for the benefit of a legal person that has its head office in the territory of that Member State.
2. When establishing jurisdiction in accordance with paragraph (1)(a), each Member State shall ensure that it includes cases where:
  - (a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or
  - (b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State may decide not to apply, or to apply only in specific cases or circumstances, the jurisdiction rule set out in paragraphs 1(b) and 1(c).
4. Each Member State shall take the necessary measures also to establish its jurisdiction over the offences referred to in Articles 3 to 5 in cases where it refuses to hand over or extradite a person suspected or convicted of such an offence to another Member State or to a third country.
5. Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall co-operate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate co-operation between their judicial authorities and the co-ordination of their action.
6. Member States shall inform the General Secretariat of the Council and the Commission accordingly where they decide to apply paragraph 3, where appropriate with an indication of the specific cases or circumstances in which the decision applies.

#### *Article 12*

#### **Exchange of information**

1. For the purpose of exchange of information relating to the offences referred to in Articles 3, 4 and 5, and in accordance with data protection rules, Member States shall ensure that they establish operational points of contact available twenty four hours a day and seven days a week.
2. Each Member State shall inform the General Secretariat of the Council and the Commission of its appointed point of contact for the purpose of exchanging information on offences relating to attacks against information systems. The General Secretariat shall notify that information to the other Member States.

#### *Article 13*

#### **Implementation**

1. Member States shall bring into force the measures necessary to comply with this Framework Decision by 31 December 2003.
2. They shall communicate to the General Secretariat of the Council and to the Commission the text of any provisions they adopt and information on any other measures taken to comply with this Framework Decision.
3. On that basis, the Commission shall, by 31 December 2004, submit a report to the European Parliament and to the Council on the operation of this Framework Decision, accompanied where necessary by legislative proposals.
4. The Council shall assess the extent to which Member States have complied with this Framework Decision.

*Article 14*

**Entry into force**

This Framework Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Communities*.

Done at Brussels,

*For the Council*  
*The President*