

EN

EN

EN



EUROPEAN COMMISSION

Brussels, 30.9.2010  
SEC(2010) 1122 final

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying document to the*

Proposal for a

**DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on attacks against information systems, and repealing Council Framework Decision  
2005/222/JHA**

{COM(2010) 517 final}

{SEC(2010) 1123 final}

## Terms of Reference - Definition of basic concepts for the purposes of this Impact Assessment

**Botnet** – indicates a network of computers that have been infected by malicious software (computer virus). Such network of compromised computers ('zombies') may be activated to perform specific actions such as attacks against 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, might be located elsewhere than the offender himself.

**Bot capacity** – the number of computers in a given botnet.

**Contact Point** – two relevant definitions exist. Firstly, in the context of the G8 network of contact points, Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime (2001/C 187/02), stipulates: "A desirable common standard would be that the unit designated as a national contact point really is a specialist unit that applies recommended international practice to investigations of high-tech crime, and that the unit is prepared to take any possible action, with due regard, of course, to national legislation." (OJ C 187/5, 3/7/2001)

Secondly, the Council of Europe's Cybercrime Convention defines a contact point as: "Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence [...]"

Both definitions are applicable. For the purpose of this Impact Assessment, the essential function required from a contact point is to react swiftly to requests for assistance.

**Critical Information Infrastructure (CII)** – Information and Communication Technologies (ICT) systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).<sup>1</sup>

**Critical Information Infrastructure Protection (CIIP)** – the programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.<sup>2</sup>

**Denial-of-Service (DoS) attack** – a denial of service attack is an act to make a computer resource (for example a website or Internet service) unavailable to its intended users. The contacted server or webpage will show itself as "unavailable" to its users. The result of such an attack could, for example, render online payment systems non-operational, causing losses for its users.

---

<sup>1</sup> COM(2005) 576 final, Annex 1, p. 19.

<sup>2</sup> Idem.

**Information System** is any device or group of interconnected or related devices, one or more of which, pursuant to a programme, 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.<sup>3</sup> An example of this is a computer or a server.

**Illegal System Interference** is 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, which is punishable as a criminal offence when committed without right, at least for cases which are not minor (as defined in Framework Decision 2005/222/JHA).

**Illegal data interference** is the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system, which is punishable as a criminal offence when committed without right, at least for cases which are not minor (as defined in Framework Decision 2005/222/JHA).

**Large-scale** attacks are the attacks that can either be carried out by big botnets, 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 the attack can have a major impact on the functioning of the target itself, and/or affect its working environment. In this context, a 'big' botnet will be understood to have the capacity to cause serious damage. It is difficult to define botnets in terms of size, but the biggest botnets witnessed were estimated to have between 40,000 to 100,000 connections (i.e. infected computers) per time span of 24 hours.<sup>4</sup>

**Malware** is computer software designed to infiltrate or damage a computer system without the owner's consent. It is distributed through a variety of means (emails, computer viruses, botnets). Intention is to obtain data (passwords, codes) in a fraudulent way, or to integrate this computer in a computer network destined to be used for criminal actions.

**Phishing** is an electronic mail that convinces end users to reveal confidential data via websites that imitate the sites of bona fide companies (e.g. websites of banks).

**Spam** is electronic messages sent in large numbers to internet users without their consent. These unsolicited electronic messages are usually of a commercial nature. Spam is the electronic equivalent of stuffing letter boxes with advertising materials that have not been requested by their recipients.

**Spyware** is software that is installed on a user's computer without his knowledge. Such software transmits information on the user and his habits once connected to the internet. The information gathered this way is usually intended for use by advertisers.

---

<sup>3</sup> Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69 of 16.3.2005, p. 67.

<sup>4</sup> Number of connections per 24 hours is the commonly used measuring unit to estimate the size of botnets.

## IMPACT ASSESSMENT

### On a proposal for a Directive repealing Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

#### 1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

##### 1.1 Background

###### 1.1.1. Policy context

The Commission's Work Programme for 2009<sup>5</sup> included a proposal to amend Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems<sup>6</sup> (hereafter: "FD on attacks"). The FD on attacks responded, as stated in its recitals, to the objective to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of EU Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems. It introduced EU legislation against the offences such as illegal access to information systems, illegal system interference and illegal data interference<sup>7</sup>, as well as particular rules on the liability of legal persons, jurisdiction and exchange of information. Member States were obliged to take the necessary measures to comply with the provisions of the FD on attacks by 16 March 2007.

On 14 July 2008, the Commission published a report on the implementation of the FD on attacks<sup>8</sup>. In the conclusive part of the report, it was noted that significant progress was made in most Member States and that the level of implementation was relatively good, but that implementation was still ongoing in some Member States. Further on, it was stated that "[s]everal emerging threats have been highlighted by recent attacks across Europe since adoption of the FD, 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 focus when the FD was adopted. In response to these developments, the Commission will consider actions aiming at finding better responses to the threat [...]."

The importance of taking further actions to strengthen the fight against cybercrime was underlined in the Hague Programme on strengthening freedom, security and justice in the European Union, and in its successor, the Stockholm programme and the Action Plan implementing the Stockholm Programme.<sup>9</sup>

At the international level, the Council of Europe Convention on Cybercrime (CETS N° 185)<sup>10</sup>, signed on 23 November 2001, is regarded by experts as constituting the highest international standard to date, since it provides a comprehensive and coherent framework on the different aspects relating to cybercrime. To date, the Convention has been signed by 25

---

<sup>5</sup> COM(2008) 712.

<sup>6</sup> OJ L 69 of 16.03.2005, pp. 67-71.

<sup>7</sup> See Definitions provided in the terms of reference of this report.

<sup>8</sup> 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)0448 final.

<sup>9</sup> OJ C 236 of 24.9.2005; OJ C 155 of 4.5.2010, pp.1-38.

<sup>10</sup> Council of Europe Convention on Cybercrime, Budapest 23.XI.2001, CETS n° 185. See also the Terms of Reference - Definition of Basic Concepts.

out of 27 Member States, and has been ratified by 15 Member States.<sup>11</sup> The Convention entered into force on 1 July 2004. The European Union (EU) is not a signatory to the Convention.

This impact assessment discusses possible actions in this sense from a primarily criminal law and police cooperation perspective. Any such EU action has to be developed with consideration given to related EU policies, in particular on critical information infrastructure protection, but also to international instruments, such as the Council of Europe convention on Cybercrime, in order to avoid duplication of efforts.

Following the entry into force of the Treaty of Lisbon, the possibility of amending the FD does not exist anymore. According to the new legislative framework in place, the existing FD can only be repealed via a Directive, which is foreseen in the Commission's Work Programme 2010.

## 1.2 Consultation and expertise

The issue of cyber attacks has been discussed intensively in Europe during the last few years. This led to extensive consultations at EU-level, in particular within the framework of the policy on network and information security. These consultations have been of fundamental importance for the policy initiative discussed in this report, and a full presentation of these consultations and the conclusions of them is given in the recent Communication from the Commission on Critical Information Infrastructure Protection (CIIP): 'Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience' and the Impact Assessment report linked to that Communication.<sup>12</sup> The present Impact Assessment report generally refers to the documents mentioned, and therefore limits itself to a description of a number of specific consultations targeted at criminal law and police cooperation issues.

On 22 May 2007, the Communication from the Commission 'Towards a general policy on the fight against cybercrime' was adopted.<sup>13</sup> This Communication was preceded by extensive consultations with stakeholders and an impact assessment.<sup>14</sup> Among other things, these consultations touched upon the issues discussed in the present report and should be regarded as a first step in the preparation towards a further development of EU legislation and other actions to combat attacks against information systems.

These initial consultations induced the Commission to start analysing different policy options in detail, in view of both an update the EU legislation on cybercrime and potential non-legislative actions. In this context, an Inter-service steering group was set up, including DG INFSO, MARKT, HR (formerly ADMIN) and DIGIT, in addition to the General Secretariat and the Legal Service. The steering group met on 27 November 2008 and on 18 February 2009.

---

<sup>11</sup> An overview of the ratifications of the Convention (CETS n° 185) can be seen at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>

<sup>12</sup> "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM (2009) 149/1

<sup>13</sup> Communication from the Commission to the European Parliament, the Council and the Committee of the regions "Towards a general policy on the fight against cyber crime", COM(2007) 267 final

<sup>14</sup> As presented in the accompanying Impact assessment report, SEC (2007) 0642.

Informal consultations have been carried out continuously since at least 2006.<sup>15</sup> In particular, specific issues concerning attacks against information systems were addressed in the context of a number of expert meetings in 2007 and 2008. The main events where stakeholders have been consulted can be summarised in the following non-exhaustive way:

- In preparation of the expert meeting held on 15-16 November 2007, a questionnaire was sent to the Member States on EU needs in the area of fight against cybercrime
- 15-16 November 2007: EU expert meeting on cybercrime in Brussels, with the participation of experts from almost all Member States, both from public and private sector
- 25-26 September 2008: EU expert meeting on cybercrime in Brussels, with participation of experts from the almost all Member States and the private sector
- 30-31 October 2008: OSCE member states' experts at annual OSCE Police Experts meeting on "Fighting the Threat of Cybercrime" in Vienna (Austria)
- 25-29 November 2008: EU seminar for the fight against cybercrime for judges and prosecutors in Durbuy (Belgium)
- 2-3 December 2008: EU Member States' experts at annual Europol High Tech Crime Expert meeting in The Hague (The Netherlands)
- 10 December 2008: Consultation of important third country partners to the EU at the G 8 Roma-Lyon High Tech Crime Group meeting in Kyoto (Japan)
- 16 December 2008: Consultation meeting with representatives of EU business and industry federations in the area of information and network security in Brussels

During most of the meetings mentioned above, different concrete options – presented orally or in the form of non-papers - for further EU legislative and other actions were presented and discussed in detail. A short discussion on future plans was also held at the occasion of the presentation of the report on the implementation of the FD on attacks at the Council Working Group DROIPEN meeting on 21 January 2009.

The general principles for consultations laid down by the Commission have been followed, as a wide range of stakeholders, including governments, NGOs, the private sector and independent experts have taken part in the preliminary discussions. The outcome of these consultations and discussions will be outlined below, but it should already be underlined that a high degree of consensus regarding the needs and possible actions has been observed among both governments and private sector experts.

### **1.3 Impact Assessment Board**

The Impact Assessment was revised to take into account the opinion issued by the Impact Assessment Board (IAB) on 2 June 2009. All comments made by the IAB were taken into consideration in the present, revised Impact Assessment. It was explained why enhanced penalisation and approximation of criminal laws against cybercrime is an effective, but not

---

<sup>15</sup> When the preparations for the Communication "Towards a general policy on the Fight against cyber crime" were started.

the only measure to combat cybercrime, the content of the preferred policy option was clarified, and the option was presented and assessed up-front. The issue of the appropriate level of action was elaborated further, and the level of penalties was better explained.

The issue of the interaction between the EU's action and wider international cooperation was broadly discussed, the impacts on third countries were included and a new policy option on updating the Council of Europe Convention was added.

The exception for the legitimate use of IT-tools such as botnets in order to develop Internet security applications was explained.

Following these modifications, the Impact Assessment Board on 31 August 2009 issued a favourable opinion on the Report. The Board however also asked for further explanations on certain issues related to the level of penalties, the appropriateness of setting penalty levels at EU level instead of the national level as well as regarding the need for the proposed level of penalties of five years imprisonment to be included in the Report. These requests have been taken into account through additional explanations that have been introduced in section 2.4 of this report dealing with the underlying drivers of the problem, section 2.7 concerning the right to act, subsidiarity and fundamental rights and section 5.6 proposing the preferred policy choice.

## **2 PROBLEM DEFINITION**

For a better understanding of the problem, the most important concepts are defined in the Terms of Reference - Definition of basic concepts (see above).

### **2.1 What is the problem?**

The number of attacks against information systems has increased significantly since the adoption of the FD on attacks. One of the leading Internet Security firms reported that threats to confidential information (as opposed to publicly available information, and not protected by a password) increased considerably in 2008, rising from 624,267 to 1,656,227 identified new threats in 2008.<sup>16</sup> Moreover, a number of attacks of previously unknown large and dangerous scale have been observed, such as those in Estonia and Lithuania in 2007 and 2008 respectively (the consequences of these attacks are detailed in section 2.1.1). In March 2009, computer systems of government and private organizations of 103 countries (including a number of Member States, such as Cyprus, Germany, Latvia, Malta, Portugal and Romania) were attacked by malware installed to extract sensitive and classified documents. Finally, at the time of writing this assessment, the world witnessed the spread of a botnet called 'Conficker' (also known as Downup, Downadup and Kido), which has propagated and acted in an unprecedented scale and scope since November 2008, affecting millions of computers worldwide.<sup>17</sup> Although it is impossible to determine exactly how many were infected in the EU due to the lack of reporting and the density of the ICT infrastructure, the number is deemed to be considerable as demonstrated by the increasing number of threats.

---

<sup>16</sup> [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_internet\\_security\\_threat\\_report\\_xiv\\_04-2009.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf), p.10.

<sup>17</sup> [http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril\\_1174916\\_651865.html](http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html)

Secondly, insufficient co-operation between the Member States, and specifically law enforcement agencies and judicial authorities within the EU make a coordinated and effective response to these attacks difficult. Whilst the implementation report on the FD on attacks shows that a majority of Member States have put in place permanent contact points as required by Article 11 of the FD on attacks, problems persist as to their responsiveness and their capacity to react to urgent requests for cooperation.<sup>18</sup>

In line with the Council of Europe Cybercrime Convention, the role of a permanent contact point is to ensure the provision of immediate assistance for the purpose of investigations concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying measures, such as the provision of technical advice, the preservation of data, the collection of evidence or locating of suspects. Each contact point shall have the capacity to carry out communications with the point of contact of another party on an expedited basis.<sup>19</sup>

Indeed the existence of a contact point is not a guarantee for its proper functioning. In their notifications to the Commission, a number of Member States indicated that their respective contact points were in place, but not operating 24 hours a day as required by the FD on attacks. This indicates that they cannot respond to urgent requests outside the office hours. Public-private cooperation is often hampered by the low efficiency/availability of contact points or their inability to deal with private sector requests for cooperation.

Thirdly, there is still little data available concerning the follow-up given by the police and the judiciary to such attacks. Not all Member States collect statistical data relating to cybercrime, such as fraud through the use of the internet. Moreover, available statistics are often not comparable due to varying statistical methodologies among the Member States. For example, Luxemburg does not collect statistical data specifically on cybercrime, however the crimes categorized elsewhere sometimes involve the use of the Internet and a computer. Italy does collect data concerning attacks against information systems, but sub-divides these attacks according to 6 different classifications.

### *2.1.1 Types of attacks*

A number of ways to carry out an attack have been observed. However, most important and threatening are botnets (see terms of reference). Botnets have become an increasingly significant part of the cybercrime landscape, and are used to send spam and phishing e-mails, as well as to launch large-scale denial of service attacks, or similar (i.e. any attack that disables an information network to fulfil its normal function).

The underlying objectives can be of different character. Attacks can have criminal objectives, but they sometimes are used as one of the means in a larger campaign to exert pressure. Attacks often include one or more of the following elements:

---

<sup>18</sup> 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)0448 final.

<sup>19</sup> See: <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

- Extortion: criminals only unlock the computers after the victims pay a certain amount of money to the controllers of the botnet;<sup>20</sup>
- Sabotage purposes: disabling (critical) infrastructure, such as a security system, either to commit another crime, or in relation to a terrorist act;
- Exerting illicit pressure on a state or an organization.<sup>21</sup> This pressure can have various objectives. In some cases, pressure is exerted through illegal means: there are a number of documented cases where viruses attacked sites related to certain political movements,<sup>22</sup> or attempted to take out the sites and servers of governments.<sup>23</sup> Economic pressure on a company can be exerted through for example, the use of emails containing malware. These can also be used to undermine the reputation of a competitor.
- Illegal information gathering / spying activities. Information and Communication Technologies (ICT) are increasingly used for purposes of information gathering, setting up surveillance networks by breaking into computer systems of economic competitors, or political opponents.<sup>24</sup>

A strong tendency towards a stronger implication of organized crime in the attacks has been observed; organized crime groups may, for instance hire hackers or other computer specialists to conduct a specific attack.<sup>25</sup>

A large-scale attack may be launched against a critical information infrastructure of for example a financial institution, followed by a message that the financial institution has to pay a ransom in order for the attack to cease.<sup>26</sup> Networks of more than a million computers linked together by a command-and-control centre have been observed, and the damages caused by a coordinated attack through the use of such network can be considerable.<sup>27</sup>

Attacks from such botnets can be very dangerous for the affected country as a whole, and can also be used by terrorists or others as a tool to put political pressure on a state. This became clear in Estonia in April-May 2007, where important parts of the critical information

---

<sup>20</sup> See: [http://www.cpni.gov.uk/docs/botnet\\_11a.pdf](http://www.cpni.gov.uk/docs/botnet_11a.pdf) , p11, indent 30;  
[http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns441/networking\\_solutions\\_whitewater0900aecd8072a537.pdf](http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns441/networking_solutions_whitewater0900aecd8072a537.pdf)

<sup>21</sup> Jennifer A. Chandler, University of Ottawa, "Liability for Botnet Attacks", p. 16 Conference Paper, presented at the Oxford Internet Institute's Conference "Safety and Security in a Networked World", September 8–10, 2005. Paper available at: [http://cjlt.dal.ca/vol5\\_no1/pdfarticles/chandler.pdf](http://cjlt.dal.ca/vol5_no1/pdfarticles/chandler.pdf), footnotes 48-50

<sup>22</sup> [http://www.sophos.com/pressoffice/news/articles/2004/12/va\\_maslanc.html](http://www.sophos.com/pressoffice/news/articles/2004/12/va_maslanc.html)

<sup>23</sup> "Yaha Worm Takes Out Pakistan Government's Site" Security Focus (26 June 2002); available at: <http://online.securityfocus.com/news/501>

There are several other cases like this documented, where political opponents attack the websites of rival groups or the state they oppose. However, similar attacks have been seen targeted against commercial organisations and companies.

<sup>24</sup> An example of this is the so-called "Ghostnet" where 1295 computers in highly sensitive places were infiltrated: embassies, foreign ministries and a number of international organisations. The origins of the network have been traced back to China-based computers. The Economist, 4/4/2009.

<sup>25</sup> Chandler, "Liability for Botnet Attacks", p. 15

<sup>26</sup>

<http://www.pdesign.net/SED/SED%20Articles/Web%20of%20Crime%20Enter%20the%20Professionals.htm>

<sup>27</sup>

See:  
<http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=172303265>

infrastructure in government and the private sector were taken out for days due to large scale attacks against them. As a result, the Parliament was forced to close down its e-mail system for 12 hours. Due to extensive access attacks two major banks present in Estonia (Hansabank and SEB Eesti Unisbank) completely stopped their online business and blocked their contacts with foreign countries for a long time. There have also been reports of attacks on the Estonian telephone system stating that at least one public telephone exchange was put out of service.

A similar attack occurred in Lithuania on 28 June 2008 when more than 300 private and official sites were attacked from proxy servers located outside of Lithuania.<sup>28</sup>

Although the total financial cost of a large-scale attack, regardless of the criminal objectives behind it, cannot be estimated precisely, it is likely to be considerable. According to an estimate by the Estonian government, the cost of the cyber attack against Estonia amounted to EEK 300 to 400 Million – roughly between EUR 19 and 28 Million.<sup>29</sup>

The (especially indirect) damage caused by the attacks against Lithuania could not be estimated precisely. The Lithuanian authorities estimated that the direct damage caused by the cyber attacks to one of the companies affected by the attack amounted to EUR 3,000. It is assessed that interruption of Internet sites of several hundred companies and public institutions caused much higher indirect damage.<sup>30</sup>

The low figure for direct cost is identified as a very limited number of computers that were damaged or destroyed due to the attacks. It does not refer to damages caused due to interruption of services by companies and the government.

Another, more precise estimation has been given regarding the financial cost of fraud crimes (phishing) conducted via different tools for large scale attacks: about USD 3.2 billion a year in the USA<sup>31</sup> (2007 data).

## **2.2 Who is affected and how?**

The victims of large-scale attacks against information systems can be found in all parts of society. The general public, consisting of the users of modern information systems, suffers negative effects, such as intrusion in their private spaces on-line, loss of access to increasingly vital information functions and fraud crime attacks targeted at them directly. There is no trustworthy estimation available on how many persons have been affected by the offences in question or how great the financial impacts are, but it is clear that citizens are at risk due to different types of cyber attacks. According to the 2008 Annual Report on the number of Internet crime complaints received by the Internet Crime Complaint Center (IC3) in the US, complaints of online crime hit a record high in 2008. IC3 received a total of 275,284 complaints, a 33.1% increase over the previous year. The average individual loss amounted to USD 931.<sup>32</sup> No comparable data is yet available at EU-level.

---

<sup>28</sup> <http://www.irishtimes.com/newspaper/world/2008/0702/1214949259098.html>

<sup>29</sup> There were costs to the government organisations related to the restoration of information systems and compensations for caused disturbances. In addition to the estimated financial cost, the total cost of such attacks is difficult to compile, as this involves not only the direct economic costs due to the attack, but also extra measures that were required to prevent further damage. Source: e-mail exchange with the Estonian Ministry of Foreign Affairs.

<sup>30</sup> E-mail exchange with Lithuanian authorities, April 2009.

<sup>31</sup> <http://www.gartner.com/it/page.jsp?id=565125>

<sup>32</sup> [http://www.ic3.gov/media/annualreport/2008\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf)

Furthermore, critical information infrastructures of central and local government, international organisations and private entities are under threat. This affects the general security in our societies, and individual citizens. Industry and business are also affected by the problem, mainly as victims, but also as providers of security solutions.

Third countries – and relations between the EU and third countries - may also be affected, as attacks can be launched in third countries against targets within the EU, and the other way around.

### 2.3 The size and nature of the problem

Statistics on the size of the problem are rare and often only estimates, as offences related to cyberspace in many cases are not reported, and sometimes go unnoticed. It is necessary to point out that the current dimension of cybercrime has a remarkable negative economic impact. UK's National Hi-Tech Crime Unit (NHTCU) estimated the nation's cost of computer crime at GBP 2.45 billion in 2005.<sup>33</sup> According to the 2007 Computer Economics Malware Report, worldwide loss due to malware attacks was estimated at USD 13.3 billion in 2006.<sup>34</sup> The same report notes interestingly that the overall cost of direct damages fell for the second year in a row due to more widespread deployment of anti-malware technology.<sup>35</sup>

Another factor is that the goals of malware authors have shifted over the past several years. In fact, the report notes that it is the nature of attacks that changed. According to the report, "cyber-criminals today are motivated more by a desire to gain financially than to create havoc." Instead of releasing malware as a form of electronic vandalism, they design malicious code to quietly use infected machines to accomplish their objectives, such as sending spam, stealing credit card numbers, perpetuating click-fraud<sup>36</sup>, displaying advertisements, or providing a backdoor into the organization's network. The second factor [...] implies that although direct damages of malware may be declining, the indirect or secondary damages (e.g. loss of personal data and their use for other criminal activities) are likely increasing. For example, a spyware attack may cost a few thousand dollars in damages, mostly in terms of the labour cost required to remove it from desktop machines. But if the spyware allows the hacker to sniff a user's password, which he then uses to infiltrate the organization's network, the secondary damages resulting from the unauthorized access could be devastating.<sup>37</sup> Therefore, the report suggests that the increase in indirect and secondary damages, in spite of the slight decline in direct damages, is due to the finding that malware has become more sophisticated and more 'large-scale'. The threat is particularly linked to botnets due to the wide variety of activities for which they are increasingly used, such as to mount denial of service attacks, host 'phishing' websites for identity theft<sup>38</sup>, financial fraud, and distribute malware.<sup>39</sup>

---

<sup>33</sup> <http://www.crime-research.org/news/28.04.2005/1189/>

<sup>34</sup> <http://www.computereconomics.com/article.cfm?id=1225>

<sup>35</sup> DG INFSO Safer Internet Programme:  
[http://ec.europa.eu/information\\_society/activities/sip/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/index_en.htm)

<sup>36</sup> Click fraud is a type of Internet crime that occurs in pay per click online advertising when a person, automated script, or computer programme imitates a legitimate user of a web browser clicking on an ad for the purpose of generating a charge per click without having actual interest in the target of the ad's link. Click fraud is the subject of some controversy and increasing litigation due to the advertising networks being a key beneficiary of the fraud.

<sup>37</sup> <http://www.computereconomics.com/article.cfm?id=1225>

<sup>38</sup> In the case of phishing scams, the scammer (cyber criminal, the person attempting to steal the confidential information) is attempting to acquire sensitive information such as usernames, credit card

In addition, according to the Symantec's 2008 "Underground Economy"-report, the cost of phishing attacks – an important aspect of the tools used for large-scale attacks - reached USD 2.1 billion for U.S. consumers and businesses in 2007.<sup>40</sup> Symantec is one of the world's biggest anti-virus software companies.

In terms of the potential capacity of current botnets, the above-mentioned botnet 'Conficker', with an alleged bot capacity number of 12 million infected computers (February 2009 estimate<sup>41</sup>) and a capacity to send 10 billion of spam emails per day, is considered the biggest and fastest botnet currently affecting the world. It infected at a rate of more than a million computers worldwide per day.<sup>42</sup> Inside the EU, damages from this botnet were reported in France, the UK and Germany. French fighter planes were unable to take off after military computers were infected by Conficker in January 2009. The German army reported in February 2009 that parts of its computer network were infected by Conficker, making the websites of the German army, and the Defence ministry unreachable and preventing them from being updated by their administrators.<sup>43</sup> Certain IT services, including e-mails, were unavailable for weeks to the UK Ministry of Defence personnel in January/February 2009 after they were infected by the Conficker botnet.<sup>44</sup>

Although the origins of the attacks are still technically difficult to determine, Symantec enlists 4 EU Member States in its top 10 of countries from where attacks are launched. According to these calculations, 15% of all worldwide detected attacks in 2008 were launched from inside the EU. To put this share into perspective, Symantec detected 1,656,227 new pieces of malware in 2008. Symantec has detected, over time, in total approximately 2.6 million pieces of malware. The number of new threats detected in 2008 represents over 60% of this total number. Virtually all attacks have been large-scale, given that they used botnets with bot capacities averaging tens of thousands of infected computers. Symantec also notes that whereas the US, Europe and Asia are the most targeted regions for large-scale attacks, the technical capability of botnets also turns the targeted countries into the countries of origin of such attacks by infecting computers there. This also demonstrates the difficulty in determining exactly the source and target countries of botnets.<sup>45</sup>

As already defined above in the terms of reference, large scale attacks usually take place in various locations. In a preparatory step, a hacker (i.e. the cyber criminal) takes control over

---

numbers, or bank account credentials. Source: Symantec Report on the Underground Economy, July 07-June 08, p.82.

<sup>39</sup> Symantec Report on the Underground Economy, July 07–June 08, p. 19. See also footnotes 13 & 14.

<sup>40</sup> Consumer Reports.org source cited in Symantec Report on the Underground Economy July 07–June 08, p. 19; source: [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_underground\\_economy\\_report\\_11-2008-14525717.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf)

<sup>41</sup> Arbor Sert Security Engineering and Response Team, <http://asert.arbornetworks.com/2009/01/two-weeks-of-conflicker-data/>

<sup>42</sup> <http://www.f-secure.com/weblog/archives/00001584.html>

<sup>43</sup>

[http://www.bundeswehr.de/portal/a/bwde/kcxml/04\\_Sj9SPykssy0xPLMnMz0vM0Y\\_QjzKLd443DgwBSUGYAfqR6GIBIQix0JRUFw99X4\\_83FT9AP2C3NCIckdHRQAIYgRn/delta/base64xml/L2dJQSEvUUt3QS80SVVFLzZfQ18zUkU!?yw\\_contentURL=/C1256EF4002AED30/W27PED65714INFODE/content.jsp](http://www.bundeswehr.de/portal/a/bwde/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd443DgwBSUGYAfqR6GIBIQix0JRUFw99X4_83FT9AP2C3NCIckdHRQAIYgRn/delta/base64xml/L2dJQSEvUUt3QS80SVVFLzZfQ18zUkU!?yw_contentURL=/C1256EF4002AED30/W27PED65714INFODE/content.jsp)

<sup>44</sup> [http://www.theregister.co.uk/2009/01/20/mod\\_malware\\_still\\_going\\_strong/](http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/)

<sup>45</sup> Symantec Global Internet Security report, Trends for 2008, Volume XIV, Published April 2009. The report specifically mentions the Netherlands as 4th worldwide source of attacks with 8%, the UK, Latvia and France are also in the top-10. [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_internet\\_security\\_threat\\_report\\_xiv\\_04-2009.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf)

one computer (this computer becomes the 'command-and-control centre', or 'C&C'), and is set-up by the hacker to remotely control other computers through malware. These malware-infected computers are called 'zombies'. All 'zombies' together form a botnet. Attacks carried out through means of a botnet are large-scale attacks. The sequence for a botnet attack is the following: (1) computers are successfully attacked by malware; (2) they are integrated in a botnet; and (3) they can carry out attacks upon command of the hacker. Otherwise stated, the attacked (compromised) computer later becomes an attacking computer.

Cyber attacks can be committed across a number of countries: e.g. a cyber criminal can be in the Netherlands, his command-and-control centre can be in Germany, the compromised computers can be in Ukraine, and the attack can be directed against a bank in the UK. For that reason, it is incorrect to assume there is a dominant link between the level of penalties in one Member State and the number of attacks originating from this Member State. Certainly, the level of penalties is an important factor. However, other factors also play an important role in selecting targets for attacks:

Attacks are most directed at countries/organizations where:

- Economic and financial gains can be made
- There is lesser degree of protection of computer networks

### *2.3.1. The issue of the (non-)availability of data*

Obtaining data on cyber attacks is difficult for a number of reasons:

Computers are interconnected and data flows freely across borders. Malware can be launched in one continent to infect a computer, after which the infected computer may attack another information system in another country or even continent. It is therefore very difficult to make geographical delimitations of cyber attacks. However, security companies start from the presumption that targeted attacks (botnet attacks, fraud, phishing and the like) go where profits are to be made, i.e. in wealthy areas of the world, including the European Union.

The available data is collected mainly by those companies at the source of combating malware, i.e. internet security firms. They however collect data largely on a global scale. The available regionalised data are often aggregated data, or extrapolations of initial findings.

To determine how many computers are affected in a certain geographical area, such as the EU, one should also know that (infected) computers can also form a 'sleeping botnet', only to be activated (and thus become detectable) when the cyber criminal wants to commit the crime. In such instances, botnets are difficult to trace.

There is also the issue of openness of data: in the European Union, firms are less willing to share data on cyber attacks they experienced, for reasons of loss of reputation and potentially business opportunities. Most attacks are not reported or do not become public, because the private sector, particularly small-size enterprises, either does not record such data, or is reluctant to release such data not to draw attention to its system vulnerabilities. As an

example, the (UK) Federation of Small businesses found that one third of SMEs do not report fraud or online crime to the police or to their banks because of a lack of faith in the system.<sup>46</sup>

Furthermore, a great many firms dealing with internet security are US firms, as are their clients, leading to the fact that a majority of their first-hand data concerns the situation in the US market. These internet security firms regularly publish reports based on the data they receive from their clients, albeit after this data was rendered anonymous.

## 2.4 The underlying drivers of the problem

The main drivers of the problem are the ease with which damages can be caused by illicit activities on the internet, in particular through large-scale attacks against information systems. Indeed, the internet today is host to mechanisms and tools used or designed to infect computers with viruses capable of launching attacks (increasingly large-scale) against information systems.<sup>47</sup> New criminal tools are being constantly developed, but the institutional response to this problem in terms of penalisation of spreading such tools remains inadequate.

The example of a too low level of penalisation is provided by the follow-up to the 2007 cyber attacks on Estonia: the only person brought to justice was fined EEK 17500 (equivalent to EUR 1180), which was deemed by the Estonian authorities as inadequate and not dissuasive enough. As a reaction to this, Estonia has since increased penalties for large-scale cyber attacks to up to five years of imprisonment, or up to 25 years of imprisonment if considered to be an act of terrorism. Following a legislative change, Estonia also increased its spending on the fight against cybercrime, by establishing an international centre of excellence in Tallinn 2008.<sup>48</sup> In the case of large-scale attack in Lithuania in 2008, no person has been prosecuted to date (situation as of April 2009).

General experience shows that a higher level of penalties tends to have the quasi-automatic effect that more resources are earmarked for law enforcement and judicial authorities to fight the corresponding crime. This should in particular be the case when it is question of crime that requires considerable resources to investigate, such as sophisticated attacks against information systems. It can be assumed that law enforcement authorities will not - primarily for economic reasons - allocate the substantial resources needed to fully investigate a crime when the penalties foreseen are so low that the cost of a complicated investigation would appear not to be proportionate to the results of it<sup>49</sup>. Higher penalties would thus have the *de facto* effect that more resources will be allocated to fight the crime in question. This effect could be expected to be particularly important in the area discussed in this report, where

---

<sup>46</sup> <http://www.fsb.org.uk/news.aspx?REC=5038&re=policy/news.asp>

See also: CSI Computer Crime and Security Surveys, CSI 2008:22-23, according to this research, only 27 percent of victims report cybercrime, and 47 percent of those interrogated agreed with the statement that they do "not believe that Law enforcement can help the matter".

<sup>47</sup> See: <http://www.darkreading.com/security/management/showArticle.jhtml?articleID=208808174>

<sup>48</sup> See: <http://news.bbc.co.uk/2/hi/technology/7208511.stm>;

<http://www.baltictimes.com/news/articles/18815/>

<sup>49</sup> This has been repeatedly explained to the Commission to be a well know fact within European law enforcement by different authorities in Member States and European institutions, although it has not been possible to find a scientific source to confirm this.

available resources for law enforcement are deemed inadequate to the scale of the problem.<sup>50</sup> The following higher prioritisation of the investigations of cybercrime is likely to lead to increased international cooperation. The discrepancy between the high frequency of cross-border cybercrime indicated in this report and the low number of cross-border requests for assistance observed must be considered to indicate that the recourse to international cooperation instruments is too rare.

Further on, the currently low level of penalties for cyber attacks may prevent the use of special investigative techniques (e.g. covert operations and remote searches online) in countries concerned, which are indispensable for investigating this type of crime.

The penalties for cybercrime are currently not on par with its effects: the Estonian government considered the sentence given (approx. EUR 1180) for the cyber attack as inadequate for the damage caused (EUR 19-28 million). The call for more adequate (stricter) penalties for cyber attacks has been made by all MSs and the private sector in the consultation process, and has also been raised by international organisations, such as the G8.

Another factor which has a strong impact on the weaknesses in investigations and prosecution is insufficient cooperation at European and international level. The procedures and mechanisms for cross-border actions from law enforcement and other authorities - necessary in order to build up effective counter actions against the attacks - are not sufficiently developed. Indeed, the majority of Member States have put in place national contact points to respond to requests for assistance from other Member States, but their capacity to react swiftly and efficiently is still low, as there is no obligation for them to react. When a threat is detected by one Member State, it is important that this information is shared swiftly with other Member States, so that they can take measures to defend themselves against the threat or seek effective remedies. Given the potential of current tools, such as botnets, to spread large-scale attacks by infecting thousands computers a day, a rapid cooperation among the Member States is crucial to tackle the problem.<sup>51</sup>

As an example of the low level of cooperation: France sent 3 requests for information and cooperation, and received 8 requests. The Netherlands sent out 13 requests, and received 31.<sup>52</sup> France and the Netherlands are the two top EU countries mentioned by Symantec as countries of origin of cyber attacks in data collected between January 2007 and October 2008. Given the number of pieces of malware detected in 2008 (1,656,227), each capable of being exploited in a cyber attack, the number of actual attacks is in the range of hundreds of thousands.

Differences in national legislations on criminalising acts of cybercrime also complicate an efficient response to cybercrimes. This applies in some cases to the mere definition of cybercrime in the law, and the laws governing penalisation of internet-related crimes.<sup>53</sup> Also

---

<sup>50</sup> This has been confirmed to the Commission by law enforcement from different Member States and from Europol, for example, in a telephone conversation with the Europol High Tech Crime Centre on 29 January 2010.

<sup>51</sup> See Council of Europe paper "The functioning of 24/7 points of contact for cybercrime." 2 April 2009.

<sup>52</sup> Idem.

<sup>53</sup> See also point 2.1 Problem definition, see above in the text.

As an example of the differences in application of the law, we can look at the way "illegal system interference" is applied in Germany and France (FD 2005/222 JHA article 3, corresponding to the CoE Cybercrime Convention, article 5): this article implies the concept of serious hindering of the functioning of a computer system, which has, as such, been incorporated in French law (article 323-1 du code penal). In German law the hindering is not specified as dealing with a computer (or information technology)

concerning the applicable international law, differences exist: some Member States have ratified and incorporated the provisions of the Council of Europe Cybercrime Convention, whilst others have yet to do so. The reasons for non-ratifications vary from being political, structural or simply procedural or a combination of them. A number of EU stakeholders in the consultation process indicated that while their country is in favour of ratifying the Cybercrime Convention, the issue of ratification has not yet been put on the agenda of their Parliament. Similar reasons, compounded with insufficient or patchy awareness of risks related to cybercrime, have been evoked for failing to upgrade their legislation to EU standards.

As an example: although Estonia and Lithuania have upgraded their legislation, both Member States have asked the EU to take action also at the EU level to avoid situation, where countries without adequate penalties would become the weakest link, and targets for large-scale attacks. As shown in the time sequence of an attack, countries targeted by large-scale attacks can also become the 'source' of such attacks, as infected computers will be used as instruments in further attacks.<sup>54</sup>

## 2.5 Weakness of the current legal framework and policy

The current legal framework has two major weaknesses:<sup>55</sup>

- it does not foresee an adequate answer to large-scale attacks against information systems. This is due to the absence of specific legal provisions addressing botnets and similar tools used to prepare and conduct attacks against information systems; and due to the absence of dissuasive penalties associated with large-scale attacks.<sup>56</sup> This makes prosecution more difficult, as the formal criminal offence linked to a large-scale attack may not be regarded as severe enough to justify rapid cross-border law enforcement and judicial cooperation. Cybercrimes are prosecuted according to various national laws, some of which are not specifically geared to attacks through computer systems.
- it does not address the issue of cross-border cooperation against such attacks in a way which would ensure swift dealing with the problem.

The need to strengthen the exchange of urgent information on such offences was one of the main reasons why an obligation for Member States to use the existing network of operational points of contact 24 hours a day, seven days a week (24/7) was introduced in Article 11 of the FD on attacks. According to the FD's implementation report, the level of implementation of the contact points was relatively good, but that implementation was still ongoing in some Member States. However, as a result of the consultation process, concerns have been raised in terms of the contact points' effectiveness in providing a response. This position is also in line with the G8 JHA Ministerial Declaration (29-30 May 2009), where the issue of further cooperation between the Member States concerning cybercrime has been raised: "It is also essential for States to give a technologically advanced response, and to strengthen the existing

---

system, therefore allowing a subjective interpretation of the hindering. This might lead to a restriction of the criminalisation.

<sup>54</sup> See point 2.3 on the size and nature of the problem

<sup>55</sup> These areas of weakness have been identified as a result of consultations with Member States and stakeholders.

<sup>56</sup> 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)0448 final.

forms of international co-operation such as the G8 24/7 High Tech Crime Points of Contact."<sup>57</sup>

In addition, the consultation process and the above-mentioned recent large scale attacks against information systems of some Member States have shown that the mechanisms intended for the Member States to immediately engage in operational cooperation to counter ongoing attack, are not as effective as they could be, particularly in terms of their visibility and responsiveness to assistance requests by other law enforcement agencies and their openness to requests by the private sector and the possibility to exchange strategic information and share best practice with the private sector.<sup>58</sup>

To combat cybercrime effectively, cooperation beyond the EU is necessary. Weaknesses in the structures for international cooperation, and in the cooperation with governments and private sector, including independent experts, have been identified, in particular concerning the contact points.<sup>59</sup>

## **2.6 How would the problem evolve, all things being equal?**

In addition to the existing Framework Decision on attacks, the Council of Europe's Convention on Cybercrime addresses the problem of cyber attacks. Whereas the Convention remains the only international legal instrument to date, it shows certain weaknesses due to the fast-moving developments in cybercrime.

The Convention does not specifically address the above-highlighted weaknesses regarding large-scale attacks, and an update of the Convention is not on the agenda for the foreseeable future.

Furthermore, the existing structures for international cooperation tend to react too slowly to cyber attacks and other cybercrimes, principally due to the inefficient functioning of contact points.<sup>60</sup> The need for, and value added of an EU initiative to the Cybercrime Convention is outlined and discussed further down in this impact assessment.

Given the lack of comparable and reliable quantitative data, it is very difficult to foresee how this problem would evolve in the absence of further EU action. The activities of current botnets (see section 2.3 above) suggest that the problem will continue to rise in the future if no counteraction is taken.<sup>61</sup> Attacks have become an important field of activity for many

---

<sup>57</sup> Final Declaration, G8 ministerial meeting of Justice and Home Affairs, Rome, 29- 30 May 2009, [http://www.g8italia2009.it/static/G8\\_Allegato/declaration1giu2009.pdf](http://www.g8italia2009.it/static/G8_Allegato/declaration1giu2009.pdf)

<sup>58</sup> See Council of Europe paper "The functions of 24/7 points of contact for cybercrime", 2009; Report from the EU expert meeting on cybercrime of 15-16 November 2007 (internal DG JLS document).

<sup>59</sup> See Council of Europe paper "The functions of 24/7 points of contact for cybercrime", 2009. Still to be released.

<sup>60</sup> See Council of Europe paper "The functions of 24/7 points of contact for cybercrime", 2009. Still to be released. CETS 185, article 35 states that contact points shall ensure that they are able to coordinate with the responsible authority or authorities responsible for international mutual assistance or extradition. They thus act as liaison offices in cases of international requests.

<sup>61</sup> It should be kept in mind that the EU is not the only organisation that could take action to fight the problem. NATO and Council of Europe, are also very active in the efforts to strengthen the fight against attacks as well as to strengthen network and information security. In this context, NATO created a Cooperative Cyber Defence (CCD) Centre of Excellence (COE) in Tallinn, Estonia. However, NATO only deals with military infrastructure.

criminal networks at international level. Taking into account the recurrent dynamics of criminal markets, any lucrative activity attracts new criminal business. In addition, profits coming from the crime are re-invested in the same or other criminal activities. From this, we can conclude that the criminal phenomenon is expected to remain stable or even grow if no effective deterrents are put in place in the near future.

Finally, the risk that the confidence and trust in information systems in general would be seriously hampered if nothing is done needs to be highlighted. Such a drop in confidence and trust could have very serious consequences for the growing information technologies sector and thereby for the economy in general.

## **2.7 Right to act, subsidiarity and fundamental rights**

In accordance with Article 67 of the Treaty on the Functioning of the European Union, the Union's objective shall be to provide citizens with a high level of safety. This objective shall be achieved by preventing and combating crime.

Action of the Union in this field should be taken only if and in so far as this objective cannot be sufficiently achieved by the Member States and can be better achieved by the Union. Cybercrime is a truly international problem, which only rarely can be fought in a mere national context. It is generally accepted that EU and international actions are needed in order to prevent it. Most attacks cross also the borders of the EU. They affect all Member States, and there is evidence that a considerable proportion of it involves activities from one Member State to another. Information systems are often technically interconnected and interdependent across borders. The consensus among experts is therefore that international as well EU actions are needed, and that the objective of effectively combating such crime cannot be sufficiently achieved by Member States alone.

Experience also shows that Member States, who have not experienced large-scale attacks (or do not consider themselves to be 'interesting' targets – e.g. small countries) do not regard it as a political necessity to upgrade their legislation. However, reacting only after a large-scale attack has occurred is too late given that such an attack can paralyse the whole country and cause considerable damages. Damages in one country often have consequences in a number of other countries due to the interconnectedness of information networks and enterprises. There are clear indications that higher level of penalties in general will lead states and their authorities to give the fight against a specific crime higher priority (see section 2.4 above).

A number of other Member States (Malta, Portugal, Latvia), have considered to upgrade their laws, but argued that this is preferable at EU level, as most attacks cross their borders and those of the EU. A national approach to cybercrime runs the risk of producing a fragmentation and inefficiency across Europe. Differences in national approaches and the lack of systematic cross-border cooperation substantially reduce the effectiveness of domestic countermeasures, partly because the interconnectedness of information systems means that a low level of security in one country has the potential to increase vulnerabilities in other countries. It should also be kept in mind that attacks against information systems are phenomena which make it particularly easy for the criminal to choose the country from which he or she will conduct the attack. With regard to this, measures to decrease the fragmentation of criminal law and penalties would reduce the risk that the criminals will choose the location of their activities on the basis of the local criminal law ('forum shopping').

Finally, it can be argued that a lack of European coordination - including of penalties - would make it difficult for the EU to take a unified position in relation to third countries and in international fora. As explained in section 2.5 above, it is necessary to take the fight against cybercrime also beyond the borders of the Union.

In addition, any action of the EU in this field must respect fundamental rights and observe the principles recognised in particular by the Charter of Fundamental Rights of the European Union (EU Charter) and the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), and notably the protection of personal data and the right to freedom of expression, the right to a fair trial, presumption of innocence and the right of defence as well as the principles of legality and proportionality of criminal offences. Member States, when implementing Union law, must do so in accordance with these rights and principles.

The EU builds on the existing framework of the Council of Europe Convention on Cybercrime, and goes beyond to tackle those problems indicated as weaknesses in the current legal framework.

## **2.8 Views of stakeholders and Member States consulted**

The main outcome of the consultations was a wide consensus in favour of the Commission updating the existing legislation.<sup>62</sup> The general orientations of the Commission policy in this area has already been welcomed, as expressed in the Conclusions of the JHA Council 'Combating cyber crime' of 8 November 2007, and by the participants in the meetings of EU Member State experts on cybercrime organised by the Commission on 15-16 November 2007 and 25-26 September 2008.

The main remarks or suggestions expressed during the consultations can be summarized as follows:

- A large majority of Member States have, insofar as they have expressed an opinion (23 out of 27), agreed on the objectives and possible actions that the Commission has suggested in its 2007 Communication and, which were subsequently endorsed by the above-mentioned expert meetings in 2007 and 2008. Some Member States have underlined the importance of the Council of Europe Cybercrime Convention and made clear that they would be unlikely to give full support to an EU proposal which is not fully in line with the Convention. Overall, Member States have welcomed further development of the EU policy in this area, as efforts at European level would complement the Council of Europe Convention and different global international and national action programmes. None of the other Member States have voiced objections against the convention, but, as indicated above in section 2.4, it is unclear when ratification will happen. Only up to 5 Member States spoke in favour of comprehensive EU legislation against all forms of cybercrime.
- Private sector experts agreed on the problem description and objectives outlined by the Commission in this impact assessment, and have thereby underlined the need to formulate

---

<sup>62</sup> The consulted experts represented 27 EU member states law enforcement agencies, Switzerland, Norway and member countries of the Council of Europe, OSCE, G8, Interpol, Europol and Eurojust. Consultations with the private sector included industry federations, such as EuroISPA, Eco, the Irish Banking Federation, ECTA and a number of private companies including Symantec, eBay, Microsoft, MasterCard, Blueprint Partners, KPN, Telefonica, Bouygues Telecom, HP, CA, SAP, Business Software Alliance.

the legislation in a way, which ensures that private sector can develop security products and test them in all legality.<sup>63</sup> They have also pointed at the need to take action in this context against identity theft and fraud crimes, which are also committed at large scale. The need for a global legal instrument covering all types of cybercrime has also been highlighted in the long-term perspective.

- Third country experts declared that the problems described and policy objectives of the Commission are in principle identical to problems and objectives in other countries.

A number of experts from (mainly European) countries, which have not yet signed (e.g. Turkey) or ratified (12 EU countries) the Council of Europe Convention, were in favour of stronger measures to fight attacks, including large-scale, against information systems.<sup>64</sup> They recognized the scale of the problem – the increasing threat to societies from large-scale attacks – and the need to deal with it by introducing a specific measure at supranational level. They did not deem the non-signature or non-ratification by their respective countries of the Cybercrime Convention as an obstacle to reinforcing the fight against cyber attacks at EU level.

All the suggestions have been taken in due account while assessing the impacts of each policy option.

## **2.9 The EU's actions in the wider international framework.**

To deal effectively with cybercrime, cooperation is required on a technical level, dealing with the concrete instances of cybercrime. This technical, day-to-day cooperation is carried out through the 24/7 contact points. However, it is also of vital importance that different international organisations dealing with cybercrime work together. Besides the EU, the Council of Europe and the G8 currently work on cybercrime.

The Council of Europe Convention is the oldest and most comprehensive document on cybercrime. The EU's work on cybercrime feeds into our relations with other Council of Europe member states. The work undertaken by the EU on cybercrime, such as in the framework of the Commission Communication "Towards a general policy on the fight against cyber crime", Safer Internet programme and the protection of Critical Information Infrastructures (CIIP), serves as an inspiration for the other international organisations.

Dealing with the international aspects of cybercrime is also complicated by the current non-effectiveness of the existing Contact Points which has a negative effect on the whole network of G8 and Council of Europe contact points. The Contact points are the first interlocutors among Member States and when international cooperation is sought in cybercrime investigation. Their efficiency (rapidity) determines the efficiency of the whole investigation.

Furthermore, the Council of Europe's Global Project on Cybercrime, which aims to support countries worldwide in the implementation of the Cybercrime Convention, has called on Governments to provide for effective criminalisation of cyber offences. The project clearly

---

<sup>63</sup> The new framework decision must ensure that the private sector can still use botnets or similar tools for testing the effectiveness of anti-virus software or other security appliances.

<sup>64</sup> See: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>

states that "[t]he legislation of different countries should be as harmonized as possible to facilitate cooperation."<sup>65</sup>

Finally, there is no inconsistency of the proposed measures with other jurisdictions, such as the US. The proposed measures reinforce the Council of Europe Cybercrime Convention by making the EU contact points more efficient, and by strengthening the measures against large-scale attacks. The US are a signatory to the Convention, and have been favourable to the proposed measures in the consultation process. Similarly, the US, together with Japan, and partly also Russia (Russia does not wish to sign the Council of Europe Convention, but is in favour of implementing most of the measures it contains), have welcomed the proposed measures on number of occasions at the G8, considering them a step in the right direction in the global fight against cyber attacks and international cooperation.

### **3. OBJECTIVES**

#### **3.1 General, specific and operational objectives**

The overall goal is to **deter the occurrence of, and decrease the number of large-scale attacks** originating from and/or targeting the EU.

#### **A Specific objective: Prosecute and convict criminals responsible for large-scale attacks, through the approximation of criminal law dealing with attacks against information systems**

Operational objectives:

- A1 To ensure the criminalisation of large-scale attacks, through the criminalisation of the sale, use and putting at the disposal of tools;
- A2 To facilitate prosecution of cross-border cybercrime cases;
- A3 To impose effective, proportionate and dissuasive penalties.

#### **B Specific objective: Improve cross-border cooperation between Law Enforcement Agencies (LEA's)**

Operational objectives:

- B1 To introduce mechanisms for immediate international assistance in cases of urgency in a Member State;
- B2 To improve the exchange of information and best practices among the Member States.
- B3 To improve public-private cooperation through the establishment of contact points and cooperation agreements.

---

<sup>65</sup>

See:  
[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime%5Ccy%20Project%20global%20phase%202/2079adm\\_prosummary1d%20\\_9%20mar%202009.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime%5Ccy%20Project%20global%20phase%202/2079adm_prosummary1d%20_9%20mar%202009.pdf)

## **C Specific objective: To establish effective monitoring systems and data collection**

Operational objectives:

- C1 To record, produce and provide statistical data on the offences referred to in the Directive.

### **3.2 Consistency of the objectives with other EU policies and horizontal objectives**

Considering the global and borderless nature of cybercrime and cyber attacks, the policy in this area needs to be consistent not only with other EU policies, but also with the policies of international organisations and third countries.<sup>66</sup>

At the international level, the Council of Europe Cybercrime Convention is the only instrument.<sup>67</sup> It provides a comprehensive and coherent framework covering different aspects of criminal and procedural law, as well as of international law enforcement cooperation. The Convention is also open to countries that are not members of the Council of Europe and has already been ratified by *i.a.* the USA.<sup>68</sup> A truly global coordination of anti-cybercrime policies is necessary, as a policy limited to the EU alone would not be able to address all aspects of the problem. The European Commission has declared its full support for the Convention and its ratification by all Member States.<sup>69</sup>

The FD on attacks, and in particular the fundamental provisions of Articles 2 to 4, build on the Cybercrime Convention, and are in principle identical to the Convention's corresponding Articles. All potential new actions discussed in the present report will have to be defined in view of guaranteeing a good level of coherence with the Convention.

The objectives presented above have been defined in order to complement existing and prospective measures within the EU policies for a secure information society<sup>70</sup> and for Critical Information Infrastructure Protection. The Commission policy in this area has recently been presented in the Communication "Protecting Europe from large-scale cyber attacks and disruptions: enhancing preparedness, security and resilience".<sup>71</sup> The objectives have also been defined to be consistent with EU policies related to the fight against organised crime, terrorism and security in general.

The Impact Assessment is also consistent with the report on the implementation of the European Security strategy from 2003 (Implementation Report of the ESS, 4 February 2008), which for the first time mentions cyber security and internet-based crimes as one of the global challenges and key threats. The report requests more work to be done in this area, particularly

---

<sup>66</sup> In particular the United Nations, G 8 and NATO.

<sup>67</sup> Cybercrime Convention concluded in Budapest on 23 November 2001; See: <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

<sup>68</sup> List of signatories of the Cybercrime Convention (CETS 185): <http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=3/17/2009&CL=EG>

<sup>69</sup> COM(2007) 267 final

<sup>70</sup> COM(2006) 251 final

<sup>71</sup> "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" Communication from the Commission to the Council, the European Parliament, The European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM (2009) 149/1

when it comes to "attacks against private or government IT systems in EU Member States". The Impact Assessment responds to this challenge.

#### **4. POLICY OPTIONS**

Elements of the various policy options can be pursued independently of the overall option chosen.

##### **4.1 Policy option (1) Status quo / no new EU action**

This option implies that the EU will not take any further action to fight this particular type of cybercrime. Ongoing actions, in particular the programmes to strengthen critical information infrastructure protection and improve public-private cooperation against cybercrime, would be continued. This option does not exclude that existing global legislation is strengthened. This option might entail sustained political – and possibly financial – support for actions connected to the implementation of the Council of Europe Cybercrime Convention and its further development.

##### **4.2 Policy option (2) Development of a programme to strengthen efforts to counter attacks against information systems with 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 at favouring further coordinated action at EU level, including:

- strengthening of the existing 24/7 network of contact points for law enforcement authorities by establishing best practice recommendations;
- establishment of an EU network of public-private contact points of cybercrime experts and law enforcement. This network would take the form of a list containing contact details on both public and private contact points.
- elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators, as agreed by the Council of the EU in its conclusions in November 2008, when it invited the Council and the Commission to draft, in consultation with private operators, of a European agreement model for cooperation between law enforcement agencies and private operators.<sup>72</sup> The Conclusions stipulated that “the Member States are encouraged to set up standardized system for trusted operational and strategic information exchange between law enforcement and the private sector”. The EU service level agreement aims to create a trusted framework whereby companies and LE can exchange information on cybercrime and exchange best practice.
- supporting the organisation of training programmes for law enforcement agencies on cybercrime investigation. The Commission will be establishing, together with the Member States and the private sector, an EU cybercrime training platform.

---

<sup>72</sup> OJ C 62 of 17.3.2009, p. 17.

### **4.3. Policy option (3) Targeted update of FD on attacks to address the specific threat of large-scale attacks against information systems**

This option implies an introduction of specific targeted (*i.e.* limited) legislation against large-scale attacks against information systems that are particularly dangerous. Such targeted legislation would be linked to measures to strengthen operational cross-border cooperation against attacks on information systems and an increase of already foreseen minimum penalties. This option would have the form of an update of the existing FD on attacks, and would include the following specific measures identified in the consultation process with stakeholders:

- introduction of legislation against the tools used for attacks against information systems. This would entail the criminalisation of the production, sale, procurement for use, import, distribution or otherwise making available of a tool enabling large-scale attacks against information systems;
- introduction of new aggravating circumstances regarding large-scale attacks, such as the act of putting in place a botnet or a similar tool enabling committing offences mentioned in Article 2 of the current FD, and when committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner (so-called identity theft). For example, identity theft-related offence occurs when someone uses someone else's personal data, such as name or credit card number, without the permission of the identified person, to commit fraud or other criminal offences, such as attacks against information systems.
- introduction of an obligation for Member States to respond to an urgent request from both the public and the private sector via the 24/7 network of contact points within a certain time limit. The formulation should be based on Article 4 in the FD 2006/960/JHA<sup>73</sup> ("shall ensure that they have procedures in place so that they can respond within at most eight hours to urgent request..."), and should limit the time period of response.
- introduction of a monitoring obligation for Member States to facilitate the collection and provision of data about cyber attacks and cybercrime, including the number of prosecutions and criminal reports. As absence of accurate data is one of the key issues, there is a need for a provision introducing an obligation for Member States to collect and provide the Commission with statistical data regarding cybercrime. This obligation would also be consistent with the aim of EU Action Plan on criminal statistics, which is to develop statistics that will allow comparisons regarding the structure, levels and trends of crime as well as the various criminal justice measures between Member States and regions within Member States.<sup>74</sup>
- to limit the frequency of future changes, the proposed measures will be termed technologically neutral. An example of this is the use of the term 'tools' for attacks (instead of the currently used technical term 'botnets'). Moreover, the scope of the FD is geared

---

<sup>73</sup> Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

<sup>74</sup> Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 7 August 2006 - Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: an EU Action Plan 2006-2010, COM(2006) 437 final.

towards attacks only (and not other cybercrimes), which will reduce the likelihood of future changes.

#### 4.3.1. *Policy sub-options*

This policy option could have several sub-options.

(a) Three sub-options would be proposed when introducing aggravating circumstances. The purpose of these sub-options is to consider the most appropriate form of penalisation of the criminal activities. The sub-options are not mutually exclusive.

The first policy sub-option would require that Each Member State shall take the necessary measures to ensure that the offences related to large-scale attacks are punishable by criminal penalties of a maximum of at least five years of imprisonment when committed through the use of a mechanism conceived to launch an attack at a large-scale.

The second policy sub-option would require that Each Member State shall take the necessary measures to ensure that the offences related to large-scale attacks are punishable by financial penalties taking into account the estimated proceeds of the crime when committed through the use of a mechanism conceived to launch an attack at a large-scale.

The third policy sub-option would be a combination of the first two, and would require that Each Member State shall take the necessary measures to ensure that the offences related to large-scale attacks are punishable by criminal penalties of a maximum of at least five years of imprisonment and financial penalties taking into account the estimated proceeds of the crime when committed through the use of a mechanism conceived to launch an attack at a large-scale.

The current level of penalties is set between 1 to 3 years of imprisonment (3 years for aggravating circumstances). This level is perceived as not reflecting the gravity of the crime, besides the fact that this level excludes the use in some Member States of special investigative techniques indispensable to the investigations required for this type of crime, such as covert operations.

It is suggested to raise this level to 2, respectively 5 years (aggravating circumstances), which is in line with the legislation in countries that recently modified their legislation (Estonia, France, Germany), or that have a higher level of penalties (UK). Therefore, this sub-option is considered best suited for the aims of this Impact Assessment.

(b) Three sub-options would also be proposed when introducing the obligation on the 24/7 contact points to respond to requests for assistance.

The first policy sub-option would require that Member States shall ensure that they have procedures in place to respond to requests within the shortest delay possible.

The second policy sub-option would require that Member States shall ensure that they have procedures in place so that they can respond within at most eight hours to requests.

The third policy sub-option would require that Member States shall ensure that they have procedures in place so that they can respond within at most eight hours to urgent requests.<sup>75</sup> The qualification of 'urgent' should be agreed between law enforcement authorities and the private sector.

#### **4.4. Policy option (4) Introduction of comprehensive EU legislation against cybercrime**

This option would entail new and comprehensive EU legislation. In addition to the update set out in policy option 3, this option would add the soft-law measures of policy option 2, and go beyond these by tackling other legal problems related to Internet usage.

The identification of the use of botnets for a range of criminal activities including not only large-scale attacks, but also identity theft, hosting of illicit content online, fraud, etc., raises the question whether a new, broader EU legislation on cybercrime should be introduced. Such legislation would also necessitate measures addressing fraud committed online, illegal web content (e.g. by blocking or taking down web pages which sell/rent botnets), the collection/storage/transfer of electronic evidence, and the clarification of jurisdiction rules in cross border cyber incidents. The legislation would run in parallel to the Council of Europe Convention on cybercrime, and would include accompanying, non-legislative, measures mentioned above. The policy option would deal with other cybercrimes than merely large-scale attacks, which may however, facilitate the occurrence of large-scale attacks.

#### **4.5. 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 goes against the time frame for action that is proposed in this Impact Assessment. The renegotiation would have to focus in particular on those elements introduced in the policy option (3), i.e. the introduction of aggravating circumstances and penalties. At the time of negotiations of the current Convention (before 2001), no agreement could be reached on the issue of penalties, reason for which there is no mention of this in the convention. There is no indication that such consensus could be reached today.

There seems to be no international willingness to renegotiate. Furthermore, any efforts to reopen negotiations can be seen as efforts to undermine the ongoing, but not yet completed ratification process, and therefore be seen as an attempt to undermine the value of the convention.

The current convention entered into force on 1 July 2004, however 10 Member States have not yet ratified it.

**It is therefore outside the required time frame for action to consider an update of the Convention a feasible option. Consequently, this option will not be assessed in detail.**

---

<sup>75</sup> In line with Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

## 5. ANALYSIS OF IMPACTS

No significant environmental impacts are at stake in any of the considered policy options, and no particular difficulties in relation with third countries can be expected as a consequence of any of the policy options. The policy options are evaluated on the following categories:

- Economic impact, further subdivided in financial cost (including administrative costs for companies) of the option, and its economic benefit (savings, economic growth).
- Social impact
- Impact on fundamental rights
- Impact on third countries
- Relevance of the measure - contribution to the achievement of the objectives
- Consistency with international law
- Political Feasibility (without magnitudes)
- Proportionality (without magnitudes)

Member States' and stakeholders' views are also mentioned concerning all policy options.

### *Economic impact*

Measures that improve efficiency in fighting crime are likely to produce a general pattern of net positive economic impact. In the short term, there may be a moderate increase in administrative costs due to greater demands on the public system of criminal law (because a more efficient system to fight crime catches and processes more criminals), accompanied by a corresponding effect on the wider economy that must pay those costs. However, in the medium and long term, there should be a substantial reduction in such costs (because a more efficient system to fight and prevent crime deters more criminals and their rehabilitation leads to fewer offences, so that fewer criminals are 'processed'), bearing in mind that a baseline level of crime is probably unavoidable. At any rate, and especially in the case of crimes as fraud crimes committed via the internet, any possible short-term increase in administrative expenditure is largely compensated by the economic benefits of avoiding the economic costs of such offences listed above.

Inversely, measures that are inefficient in fighting crime will produce a general pattern of negative economic impact. In the long term, this includes inefficient State intervention due to lack of trust in public authorities, undermining trust to deploy or take part in economic activities on the Internet, inefficient use of resources due to individuals adopting self-protecting measures, and unfair distribution of wealth as criminals profit from their activities.

### *Social impacts*

Measures that improve efficiency in fighting crime are likely to produce positive social impacts, such as an increase in security and trust in authorities and interpersonal relations. They contribute to minimising the damage to values which matter to society, reinforce trust in public institutions and the authority of the State, help avoid trauma for victims and

widespread fear. In the case of cybercrime, these impacts affect both individuals and corporate citizens. The existence of trust is an essential component of the societal tissue.

A table of symbols is used to establish the magnitude of foreseen impact. It distinguishes "-" for negative impacts or costs and "+" positive impacts or savings. Symbols with both "-" and "+" mean that that both positive and negative impacts are expected.

Small magnitude - / +

Medium magnitude -- / ++

Significant magnitude --- / +++

No impact 0

## **5.1 Option (1) Status quo / no new EU action**

This option would not address the need for further strengthening the efforts to fight cybercrime.

The Council of Europe Convention on cybercrime is a very sound instrument (both contents wise and in implementation) in the area, but new events such as large-scale attacks necessitate EU action. In principle, all EU Member States should ratify the Convention. So far, however, only 15 Member States have done so.

In addition and beyond the Council of Europe Cybercrime Convention, all the considerations developed under paragraph 2.6 must be recalled here, with respect to the crime being expected to remain stable or even grow if no effective deterrence is put in place in the near future.

Taking into account that the fight against large-scale attacks against information systems is a high priority within EU policy, and a crosscutting issue affecting many fields of EU action, the option of not taking further action at the EU level would not provide adequate response to the identified problem.

### *5.1.1 Economic impact*

- *financial cost: 0*
- *economic benefit: 0*

No action will reinforce the existing weaknesses in the current legal set-up, leading eventually to legal uncertainty and the incapability to act following events such as large-scale cyber attacks. As a result, business and citizens will gradually lose trust in information technologies and the Internet, which will in turn hamper economic development. The effect particularly on SMEs, is likely to be significant, as their assets tend to be less protected against cybercrime due to their lower means to do so. Indeed, according to a report of the UK's Federation of Small Businesses, cybercrime is becoming an increasingly serious issue for SMEs which lose up to GBP 800 a year on average to cybercrime. According to the same report, 54 per cent of

UK SMEs reported being a victim of cybercrime in the last twelve months – 15 per cent falling foul of IT problems caused by viruses and hackers.<sup>76</sup>

***Magnitude of the economic impact: 0***

*5.1.2 Social impact*

Not acting (but continuing the ratification of the Council of Europe Convention) has the disadvantage that it is unclear by what time all Member States will have ratified and acceded to the Convention. The society will be increasingly affected by cybercrime and attacks against their information systems, creating the feeling of insecurity on the Internet.

***Magnitude of the social impact: 0***

*5.1.3 Fundamental rights impact*

In this option, interests and rights of individuals and businesses would be negatively affected due to the evolution of cybercrime, as further cases of misuse of personal data and/or stolen identity will occur.

***Magnitude of the fundamental rights impact: 0***

*5.1.4 Effects on third countries*

If no new measures are taken to combat cybercrime, the situation will become worse for the EU and third countries. This option also has as a consequence that no new legal, and practical expertise will be built in how to deal with large scale attacks. This expertise could eventually be used to assist third countries in their fight against cybercrime. The status quo can in this sense be considered to have negative effects for third countries in the medium to long term.

***Magnitude of the effects on third countries: -***

*5.1.5 Consistency with international law*

The relevance of the measure and consistence with international law as well as proportionality are also considered **null**, as there is no change in the policy. Therefore, the current difference between the existing FD on attacks and the Council of Europe Cybercrime Convention would remain, such as on the issue of criminalisation of putting at criminals' disposal of tools used to conduct criminal attacks, where the current FD on attacks is not as advanced as the Cybercrime Convention.

*5.1.6 Stakeholders' views*

This option was not deemed to be satisfactory by the stakeholders given the growing number of large-scale attacks against information systems, loss of personal data and fraud committed on the Internet.

---

<sup>76</sup> <http://www.smebusinessnews.co.uk/cyber-crime-costs-smes-800-each-year/160/>

### 5.1.7 *Political feasibility*

Given the dynamics of cybercrime and the need to take action, the political feasibility of non-action is low, as it would go against current EU policy and international developments.

## 5.2 **Option (2) Development of a programme to strengthen the efforts to counter attacks against information systems with non-legislative measures**

### 5.2.1 *Economic impact*

- *financial cost*: -
- *economic benefit*: +

The financial cost of this option is linked, first, to the strengthening of a law enforcement network of contact points by making them permanent and responding within a certain time limit to requests for cooperation and, second, to the establishment of a similar network including also the private sector. Given that the majority of Member States already have their law enforcement contact points and some private sector contact points in place, the additional cost by those lagging behind (about a third) is expected to be moderate.

The average cost related to the setting up of a permanent contact point is estimated at around EUR 219,000 per Member State (see Annex 1). The cost is low, as it is principally linked merely to making the existing contact points truly permanent and responsive within a defined time limit. Contact points that are not truly permanent cannot be expected to be able to react to assistance requests within a guaranteed time limit. The cost of the measure obliging a permanent contact point to respond within a time limit is expected to be negligible and covered under the overall cost, as the contact points are merely expected to reply whether a solution will be forthcoming from their side or not. The contact points are not expected to provide the actual solutions within the time limit, particularly when such solutions are complex and require the involvement of other authorities (e.g. only during working hours).

The cost of the establishment of an EU network of public-private contact points of cybercrime experts and law enforcement would be negligible, as it would consist essentially of a list containing contact details on both public and private contact points which already exist on both sides, but their existence is not known to the other side.

The cost of the elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators can be estimated at EUR 30,000 for the Commission, as was the case of the elaboration of the above-mentioned recommendations for public private partnership in Council Conclusions of November 2008.<sup>77</sup> This cost is related to the organisation by the Commission of consultations and an expert meeting with all stakeholders. The additional costs for the stakeholders are expected to be negligible, as they have already agreed to this measure in principle by supporting the recommendations in the Council Conclusions. Their agreement was based on the necessity of the measure and its low cost.

---

<sup>77</sup> OJ C 62 of 17.3.2009, pp. 17-18.

As a result, the impact on the economy is expected to be small, as benefits from the Internet (e.g. greater business opportunities in the IT sector, growth in employment and productivity of the economy) will be offset by financial losses caused by cybercrime, such as cyber attacks. These losses can be potentially very high, as according to a recent study, cost savings globally through business use of e-commerce reached more than a trillion euro a year.<sup>78</sup>

Therefore, all potentially positive impacts of these measures are diminished by the non-binding nature of the measures (i.e. permanent contact points for the private sector) and by the absence of an obligation to react swiftly to urgencies (for both law enforcement agencies and the private sector).

Concerning the financial cost of training programmes, the European Commission has, since 2001, lead efforts to develop standardised training programmes for law enforcement agencies and judicial authorities on cybercrime investigation and the admissibility of electronic evidence respectively. The cost of additional training foreseen in this policy option is estimated to reach almost EUR 4 million in the next two years, but the cost for the Member States is estimated at less than EUR 1 million (20%) in total, given the high level of co-funding by the Commission.<sup>79</sup> This measure is estimated independently of national training programmes run without the Commission's financial support, for which data are not available. Nevertheless, any Member State can apply for EU funding to cover for training costs which would arise from the application of the proposed non-legislative measures.

***Magnitude of the economic impact: -/+***

**5.2.2 Social impact**

The number of PCs attacked or perpetrators identified is not expected to decline significantly by a non-binding reinforcement of a network of contact points. Therefore, the social impact in terms of improving the security and trust of citizens by the actions of existing law enforcement contact points can be considered low without an obligation for the contact points to react to requests within a certain time limit. A similar situation exists within the private sector. Consultations on the above-mentioned recommendations on public-private partnership revealed that even though large private stakeholders currently operate their contact points, they are operational only during working hours. Without the guarantee of timely response by the contact points, the security and trust of citizens is not expected to be enhanced.

As for the elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators, the social impact could potentially be significant if all parties were fully committed to effective public-private cooperation in tackling cybercrime, including cyber attacks (e.g. in complying with the above-mentioned recommendations adopted by the JHA Council Conclusions). However, the voluntary nature of such an agreement is expected to produce a low impact in terms of security and trust. Similarly to the issue of permanent contact points, the non-legally binding nature of the agreement would not deliver the desired social impacts. Indeed, these measures will not impose effective, proportionate and dissuasive penalties on perpetrators of cyber attacks, as they will not reinforce the existing legislative measures.

---

<sup>78</sup> [http://www.businessweek.com/1999/99\\_40/b3649004.htm](http://www.businessweek.com/1999/99_40/b3649004.htm)

<sup>79</sup> These programmes have been financed by the financial programmes "Prevention of and fight against crime" and "Criminal Justice".

The organisation of training programmes for law enforcement agencies on cybercrime investigation, in order to improve best practice exchange and cooperation among law enforcement agencies, are also likely to have positive social impact. They provide opportunities to exchange experience and encourage operational cooperation, which in turns translates into more efficient investigation and prosecution of cybercrime and a more visible response by law enforcement agencies. The resulting personal contacts and trust are also essential for a more effective law enforcement cooperation and public-private partnership. The positive social impact of the EU cybercrime training platform will also reach beyond the EU, as the training material is currently being shared internationally (e.g. among Interpol members). The EU-funded material has become a global reference for cybercrime training.

The effect of EU support for cybercrime training is in its capacity to bring together the best cybercrime trainers and training material in Europe, and to share this expertise with countries, which would not otherwise be able to have access to such expertise. EU funding also serves to update the training material to keep abreast of the fast-evolving techniques used by cyber criminals. The EU is being assisted by Europol, Interpol and the Council of Europe, which all contribute to the development of cybercrime training platform in Europe, and consequently in the world. However, EU funding is used primarily to start up the process. It is expected that the private sector and universities will be able to sustain this process in the future.

***Magnitude of the social impact:*** ++

### 5.2.3 *Fundamental rights impact*

Public-private cooperation on cybercrime incidents and fighting against ID theft includes usually anonymous statistical, technical or economic data. However, in a significant number of cases it may also include the collection, storage and exchange of some personal data (such as IP-addresses, names, etc.). This is as such an interference with the fundamental rights to the protection of private life and protection of personal data (Articles 7 and 8 EU Charter). The processing of personal data, including the possible transborder exchange of information, must fully respect the applicable provisions in the EU and in EU Member States for the protection of personal data.

Any planned interference affecting these fundamental rights, in particular the protection of personal data, must demonstrably shown that this interference can be justified: the interference can only be justified, if it is in accordance with the law (this excludes taking non-legislative measures) and is necessary in a democratic society in the interests of a legitimate aim listed in Article 8 (2) ECHR, such as national security or public safety.

The fight against cybercrime will make some intrusions in the right of personal data protection which is strictly necessary in a democratic society. This interference applies both to the exchange of information among law enforcement agencies and between the public and the private sector when assistance requests are made through contact points or when standard EU service level agreements for law enforcement cooperation with private sector operators are established. This interference and the personal data processed for that purpose must however be clearly defined and be proportionate in relation to the purposes for which personal data are collected and/or further processed.

As a result, only the exchange of fully anonymous information has no negative fundamental rights impact in terms of the right to private life and the right to protection of personal data. However, depending on the concrete measures and the amount of personal data processed,

there will be a negative fundamental rights impact in terms of the right to private life and the right to protection of personal data. This concern was also raised by private sector stakeholders during consultations mentioned above in section 1.2. In any case, any interference with the fundamental rights to the protection of private life and protection of personal data in relation to law enforcement and public-private cooperation on cybercrime incidents has to be minimized by applying existing EU and national legislations particularly on personal data protection.

***Magnitude of the fundamental rights impact:*** -/+

#### *5.2.4 Effects on third countries*

The effect of this policy option and the programme will be to bring about the creation of networks and knowledge, which in turn will be helpful in combating cybercrime. Through its various programmes and relations with third countries, the EU could also put the newly-gained expertise at the disposal of countries, which would not otherwise be able to have access to such expertise.

Overall, impact on third countries is expected to be positive.

***Magnitude of the effects on third countries:*** ++

#### *5.2.5 Relevance of the measure*

This policy option contributes moderately to the achievement of objective B by introducing measures promoting international assistance in cases of urgency in a Member State and by improving the exchange of information and best practice (training) among Member States. The policy option's contribution is low to the achievement of objectives A and C

***Magnitude of the relevance:*** ++ (*objective B*)  
+ (*objectives A and C*)

#### *5.2.6 Consistency with international law*

This policy option has no impact on international law (the Cybercrime Convention), as it is a non-legislative option.

***Magnitude of the consistency:*** 0

#### *5.2.7 Proportionality*

This option is in line with the principle of proportionality since it does not introduce new obligations for Member States. The non-legislative measures such as recommendations and exchange of best practice would leave a large scope for national decision to Member States.

#### *5.2.8 Stakeholders' views*

Both law enforcement agencies and the private sector agreed on the necessity to create their respective permanent contact points by endorsing EU expert meeting recommendations, one of which stated: "Law enforcement permanent contact points – and private sector equivalents

– should be established in order to improve the clarity and efficiency of request and response processes. The private sector equivalent should also provide an 'out of hours' service in order to respond to urgent law enforcement requests. The qualification of 'urgent' should be agreed between law enforcement and the private sector." The cost of this measure was thoroughly discussed with the stakeholders and not deemed substantial. These recommendations were also agreed in form of Council Conclusions on 27-28 November 2008.<sup>80</sup>

Concerning the elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators, this is a measure that does not imply significant financial costs for both LEAs and the private sector, as this agreement would be voluntary. A comparison could be made again to the recommendations on public-private partnership against cybercrime adopted by JHA Council Conclusions of 27-28 November 2008. The Conclusions contain eight recommendations that were deemed necessary and not costly to implement by the stakeholders.<sup>81</sup>

### 5.2.9 *Political feasibility*

The political feasibility of this policy option is high, as it does not involve changes in the legislative framework.

## 5.3 **Option (3) Targeted update of FD on attacks to address the threat from large-scale attacks against information systems**

### 5.3.1 *Economic impact*

- *financial cost:* - -
- *economic benefit:* ++

An update of the current FD targeted at stronger penal measures against perpetrators of the most damaging manifestations of attacks – large-scale attacks against information systems – is likely to have positive financial and economic effects. This option is likely to reduce the financial cost caused by large-scale attacks coming from the European Union and third countries, which in turn will have a positive economic impact in terms of the continued growth of the Internet economy (estimated at more than EUR 300 billion in Europe) and the economy as a whole.

Moreover, the obligation for the contact points to react within a certain time frame would limit the possibility for attacks coming from outside the European Union to cause financial damage due to the lack of, or delayed response, by such contact points.

There would only be a limited cost related to the obligation on the Member States to ensure the permanency of their contact points, the time limit for the contact points' response to requests for assistance, and the collection and provision of statistics on attacks against

---

<sup>80</sup> OJ C 62 of 17.3.2009, p. 18.

<sup>81</sup> OJ C 62 of 17.3.2009, p. 18.

information systems. Such statistics will include security breaches, crime reports and prosecuted cases.<sup>82</sup>

The average cost related to the setting up of a permanent contact point is estimated at around EUR 219,000 per Member State (see Annex 1). The cost is low, as it is principally linked merely to making the existing contact points truly permanent and responsive within a defined time limit. Contact points that are not truly permanent cannot be expected to be able to react to assistance requests within a guaranteed time limit. The cost of the measure obliging a permanent contact point to respond within a time limit is expected to be negligible and covered under the overall cost, as the contact points are merely expected to reply whether a solution will be forthcoming from their side or not. The contact points are not expected to provide the actual solutions within the time limit, particularly when such solutions are complex and require the involvement of other authorities (e.g. only during working hours).

The cost of other measures, such as the introduction of legislation against the tools used for attacks against information systems and the introduction of new aggravating circumstances regarding large-scale attacks cannot be quantified since they are included in the general costs of the criminal justice system of each Member State. Similarly, although it can be expected that higher penalties will make at least some Member States willing or able to provide additional resources to investigate and prosecute cybercrime, these costs cannot be quantified at this stage. However, the Estonian example has shown that a legislative change has been followed by higher resources, such as in the establishment of an international centre of excellence in Tallinn in 2008.

The total administrative costs of this policy option would amount to approximately EUR 5,960,655 (see Annex 2)

***Magnitude of the economic impact: --/++***

### 5.3.2 Social impact

The scale of the social impact in terms of individuals' security and trust in cyberspace is expected to be positive and significant. Harsher criminal penalties for the production, sale, procurement for use, import, distribution or otherwise making available of a tool enabling large-scale attacks against information systems, and when committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner (so-called identity theft), are expected to reduce the number of such attacks originating in the European Union. Moreover, this measure will also provide a timely and visible response the public's current high concern about public security, including cybercrime. A survey has shown that a majority of EU citizens show concern about personal data protection issues.<sup>83</sup>

The obligation for Member States, not only to set up permanent contact points, but also to respond to information requests within a time limit in urgent cases is expected to speed up the authorities' reaction and consequently limit the extent of negative social impact – e.g. personal feeling of insecurity due to the possibility of personal data loss – a large-scale cyber attack

---

<sup>82</sup> Aspects of cybercrime often surface in other crimes, such as fraud through use of a computer. It is therefore essential that not only those crimes are recorded which "cyber crimes" are according to existing legislation, but also those where the cybercrime is a secondary crime in the prosecutor's file.

<sup>83</sup> Flash Eurobarometer, Data Protection in the European Union, Citizens' perceptions, Analytical Report, available at: [http://ec.europa.eu/public\\_opinion/flash/fl\\_225\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf)

may otherwise have. In addition, the actual implementation of the obligation by the Member States should facilitate cooperation among the permanent contact points also on non-urgent cases, and enhance citizens' trust in the capacity of the Member States and the EU as a whole to deal collectively with cyber attacks and cybercrime in general.

Finally, a non-legislative measure, including the organisation of training programmes for law enforcement agencies on cybercrime investigation in order to improve best practice exchange and cooperation among law enforcement agencies, are also likely to have positive social impact. They provide opportunities to exchange experience and encourage operational cooperation, which in turns translates into more efficient investigation and prosecution of cybercrime and a more visible response by law enforcement agencies. The resulting personal contacts and trust are also essential for a more effective law enforcement cooperation and public-private partnership

***Magnitude of the social impact:***   +++

### 5.3.3 *Fundamental rights impact*

In so far as this option suggests the introduction of new criminal provisions and harsher penalties, it must be ensured that these provisions are drafted in line with the principles of legality and proportionality of criminal offences and penalties, as foreseen in Article 49 of the EU Charter. Careful attention must furthermore be paid not to criminalise lawful behaviour in the efforts to legislate against the tools used for attacks. This could not only impede lawful business activities (see Article 16 EU Charter), but could also endanger the free exercise of political rights and activities, such as freedom of expression (Article 11 EU Charter). This potentially negative impact will be mitigated by a provision authorising the use of the tools, including botnets, not for the purpose of committing an offence, such as testing or protection of a computer system. An interference with the fundamental rights to the protection of private life and protection of personal data in relation to law enforcement and public-private cooperation on cybercrime incidents has to be minimized by applying existing EU and national legislation particularly for the protection of personal data.

Nevertheless, the impact on fundamental rights by the introduction of new criminal provisions and harsher penalties will mostly be positive in terms of the protection of private life and the protection of personal data as a result of more effective and deterring sanctions to be imposed in case of infringement of the provisions of existing EU and national legislation in particular for the protection of personal data.

***Magnitude of the fundamental rights impact:*** -/++

### 5.3.4 *Effects on third countries*

EU measures taken will have the effect of raising the standard for other countries. Based on the conducted consultations, the EU is looked upon as a standard setter. Therefore, an EU action will have a beneficial impact in the long run due to other countries following its lead. Stronger measures, such as more efficient contact points, will make the EU's action more effective, which in turn will translate into a more effective response worldwide given the interconnectedness of contact points worldwide, including third countries. The introduction of aggravating circumstances for committing large-scale attacks is not expected to 'export' the problem to third-countries, as large-scale attacks almost invariably target EU countries, and

their authors are therefore liable for prosecution. In addition, the majority of large-scale attacks already originates outside the EU.

***Magnitude of the effects on third countries: +++***

### 5.3.5 *Relevance of the measure*

As explained above on the analysis of impacts, this policy option contributes significantly to the achievement of all objectives, and they are expected to be met in the short-to-medium term.

***Magnitude of relevance: +++ (objectives A, B and C)***

### 5.3.6 *Consistency with international law*

As already discussed, above, this policy option is consistent with the Council of Europe Cybercrime Convention, as was also the requirement by the stakeholders during the consultation process. The new Directive on attacks would bring its use of terms and concepts in line with the Convention, and, similarly to Article 19 of the Convention, it introduces new procedural rules, such as those regarding search and seizure of computer data. However, it goes beyond the Convention in a number of aspects:

#### Substantive aspects:

The Directive will introduce measures allowing specifically tackling the large-scale aspect of attacks, which is in line with current tendencies witnessed in cybercrime.<sup>84</sup>

A. The Directive adds aggravating circumstances:

- the large-scale aspect of the attacks - the botnets or similar tools would be addressed through the introduction of a new aggravating circumstance, in the sense that the act of putting in place a botnet or a similar tool would be aggravating when crimes enumerated in the existing FD are committed.
- when concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner (e.g. identity theft). Any such rules would need to comply with the principles of legality and proportionality of criminal offences and penalties and be fully consistent with existing legislation on the protection of personal data<sup>85</sup>.

B. The Directive will also introduce measures to improve European criminal justice cooperation by strengthening the existing structure of 24/7 contact points<sup>86</sup>:

---

<sup>84</sup> the use of computer networks and botnets as tools in committing crimes.

<sup>85</sup> Such as the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 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 of 31.7.2002, p. 37–47 (currently under revision), and such as the general data protection Directive 95/46/EC.

<sup>86</sup> Introduced by the Convention, and FD 2005/222/JHA on Attacks against Information Systems

- An obligation to reply to assistance requests over the operational points of contact (foreseen in Article 11 of the FD) within a certain time limit could be proposed. . The Cybercrime Convention does not specify such binding provision;
- the Contact Points will also be accessible to private sector input and requests.

C. The Directive would also address the necessity to provide for statistical data on cybercrimes by imposing an obligation on 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 FD.

#### Formal aspects:

Due to the legal nature of the Convention, even if all Member States ratified, there are a number of advantages to taking action through means of a Directive, notably the:

- Faster adoption of national measures

In contrast with the lengthy procedures to sign and ratify international conventions that can last for many years, Directives have to be transposed to national legislation do, and set out a restricted period for implementation.

- Monitoring of implementation

Member States must notify the national measures implementing Directives to the Commission. The correct and full implementation by Member States is evaluated in an implementation report from the Commission, which is then sent to the European Parliament and the Council. In addition, the European Court of Justice is entitled to interpret Directives via preliminary rulings.

The Cybercrime Convention does not have the same binding nature as an EU-initiative, and it is not enforceable. This is a problematic aspect as an effective approach to large scale attacks can only be achieved if structures, such as the CP's are fully operational.

***Magnitude of consistency:*** ++

#### *5.3.7 Proportionality*

This option contributes substantially to the achievement of the objectives and, at the same time, results in a positive economic, social and fundamental rights impacts, which would not be possible to achieve applying simpler Community actions. The update would be limited only to large-scale attacks against information systems (targeted update). This problem can be tackled neither by the Member States alone nor merely by a non-legislative EU action. Well established national arrangements and legal systems applied in individual Member States would be respected. Medium financial costs would be necessary but would be kept on the minimal level to ensure the achievement of the objectives.

As already mentioned in relation to fundamental rights impact, the proposed measures would aim to prevent and combat large-scale attacks, a legitimate aim that, subject to the principle of proportionality, can justify limitations on the rights and freedoms recognised by the Charter, provided they are foreseen by law which contain, and respect, the essence of those rights. This is the case of policy option 3.

### 5.3.8 Stakeholders' views

The risk of non-compliance and low transposition is expected to be low due to broad agreement on this policy option that has been achieved in the consultation process and due to the low cost associated with the proposed measures. Indeed, as explained in section 5.2.1, the member States and the private sector agreed on the necessity to create permanent contact points to deal not only with the public, but also with the private sector.<sup>87</sup> The measure regarding data collection is also in line with JHA Council Conclusions of 24 October 2008, where Member States agreed to "compile statistics on alerts, showing the development of cybercrime at national level".<sup>88</sup>

### 5.3.9 Possible policy sub-options

#### (a) Aggravating circumstances:

These policy sub-options deal specifically with objective A. They have little to no impact on objectives B & C.

Policy options 1 and 2 aim at the establishing a system of dissuasive punishments as the legal response to cyber attacks. Policy option 2 aims at incorporating the proceeds of the illegal activities into the punishment. As these economic gains are the main reason for committing the crime, this might have a more dissuasive effect than option 1.

Option 3 (a combination of both) will of course have the biggest effect.

#### (b) The obligation on the 24/7 contact points to respond to assistance requests:

These policy sub-options deal specifically with objective B. They have little to no impact on objectives A & C.

Policy option 1 does not define a strict deadline for reaction, thus leaving a margin of interpretation. Opposed to this is policy option 2, where the deadline is fixed. Option 3 introduced the concept of 'urgency', whilst at the same time leaving the definition of this in the realm of the Member States. This, in ideal circumstances, could lead to a clear classification where Member States and the private sector have a clear understanding of cooperation. A risk lies in cross-border cases, where this solution leaves room for interpretation. However, the time limit, analogous with option 2, should offset this.

The sub-options under (b) are in line with the above-mentioned Council Conclusions of 27-28 November 2008, which stated that permanent contact points should facilitate the "clarity and efficiency of request and response processes" and that the "qualification of 'urgent' should be agreed between law enforcement and the private sector".<sup>89</sup> Moreover, the second and third policy sub-option takes into account Article 4 of the Council Framework Decision

---

<sup>87</sup> OJ C 62 of 17.3.2009, p. 18.

<sup>88</sup> Council Conclusions on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet, 2899th JUSTICE and HOME AFFAIRS Council meeting, Luxembourg, 24 October 2008, p. 2.

<sup>89</sup> OJ C 62 of 17.3.2009, p. 18.

2006/960/JHA<sup>90</sup> ("shall ensure that they have procedures in place so that they can respond within at most eight hours to urgent request [...]"), which limits the time period of response between law enforcement authorities when exchanging information and intelligence (see also section 4.3 above).

Each sub-option under (a) is also mutually compatible with any sub-option under (b).

### 5.3.10 *Political feasibility*

This policy option is politically feasible, as it builds upon the consensus between all stakeholders, and is compatible with both EU priorities and the priorities set out at the international level.<sup>91</sup> Indeed, as already mentioned in section 2.9, the Council of Europe's Global Project on Cybercrime has as one of its priorities the effective criminalisation of cyber-offences. The project clearly states that "[t]he legislation of different countries should be as harmonized as possible to facilitate cooperation."<sup>92</sup> The suggested policy sub-options allow sufficient manoeuvre for discussion in the final elaboration of the update.

In terms of the level of intervention needed by the Member States, almost all Member States will have to take action for each of the issues, but the proposed measures have been welcomed by all Member States in the consultation process, as they were not considered too costly and difficult to implement. Most Member States have at present low level penalties (1 to 3 years), which is in line with the current FD on attacks. Only Estonia has introduced aggravating circumstances for large-scale attacks, and France and Germany recently increased penalties to up to five years for cyber attacks. The UK Computer Misuse Act of 1990 (updated in 2004 to comply with the Council of Europe Cybercrime Convention) allows penalties of up to 10 years for cyber attacks.

The Contact points of FR, UK, IT, EE, NL and LT already usually respond within less than 12 hours to assistance requests, although they do not specify any time limit for that. Other Member States will have to modify more substantially their existing arrangements for contact points. While Member States collect statistical data relating to cybercrime, the statistics are often not comparable due to varying statistical methodologies applied by the Member States.

## 5.4 **Option (4) Introduction of comprehensive EU legislation against cybercrime**

This policy option introduces new comprehensive EU legislation, dealing with all aspects related to cybercrime. It involves the update set out in policy option 3, and adds the soft-law measures of policy option 2. It goes beyond these by tackling other legal problems related to internet usage.

### 5.4.1 *Economic impact*

- *financial cost*: ---

---

<sup>90</sup> Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

<sup>91</sup> Council Conclusions of 27/11/2008, and the European Security Strategy.

<sup>92</sup> See: [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime%5Ccy%20Project%20global%20phase%202/2079adm\\_prosummary1d%20\\_9%20mar%202009.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime%5Ccy%20Project%20global%20phase%202/2079adm_prosummary1d%20_9%20mar%202009.pdf)

- *economic benefit*: +++

The budgetary consequences of the criminal law provisions cannot be quantified since they are included in the general costs of the criminal justice system. Nevertheless, it is possible to estimate that there will be additional costs related to the obligation to set up permanent contact points and their monitoring obligation, which have been estimated at around EUR 219,000 per Member State (see Annex 1 and 2).

In addition, blocking access to websites offering tools to carry out attacks against information systems would involve financial costs. The economic impact of a similar measure to restrict access to material inciting terrorism was assessed in revising the Framework Decision on Combating Terrorism and Framework Decision on combating the sexual abuse and sexual exploitation of children.<sup>93</sup> Although the impact assessments accompanying the respective Commission proposals stated, the cost of imposing any of the different filtering methods to all internet service providers based in the EU is impossible to calculate, an upper limit of EUR 10 per computer is given on the basis of a specific example of implementing filtering in a network of 100,000 computers at 4,000 schools in Ireland. The cost of running a list of websites to be blocked may be borne by those in charge of it, whether law enforcement authorities or specific NGOs. This can be estimated at about EUR 110,000 and EUR 90,000 per year for maintenance. However, EU funding may be available for managing blacklists and exchanging information on illegal content, such as under the financial programme 'Prevention of and fight against Crime'.

The economic impact related to the decrease of severe forms of crime is likely to be positive, since this option is most likely to produce deterrent effects and a substantial reduction of the scale of the crime in the medium-to-long term.

The Directive on attacks will criminalise the use, sale and putting at the disposal of tools such as botnets; thereby undermining the ability of organised crime to launch large-scale attacks. This criminalisation will also affect the ability to use these tools for committing other types of cybercrimes, and gives law enforcement agencies a tool in fighting certain crimes related to terrorism, such as cyber attacks against critical infrastructure.

However, the considerable economic losses resulting from cybercrime are unlikely to be reduced in the short term by an attempt to introduce a comprehensive EU legislation on cybercrime. Such impact has to be viewed as medium-to-long term, as negotiating a comprehensive EU legislation would likely cause delays due to the existing disparities among Member States' practices and positions on issues, such as collection/storage/transfer of electronic evidence, the blocking of websites that can be used to sell tools facilitating attacks, and a clearer definition of jurisdiction rules. Indeed, only six EU member states currently allow blocking access to web sites with illicit web content: DK, FI, IT, NL, SE and UK. Only BE, DE and FR consider this option to be introduced this year, mostly on voluntary-based agreements with the private sector. No other countries are currently favourable to this measure.

Moreover, the current practice of blocking access is targeted principally at child-abuse web content.<sup>94</sup> However, thousands of web sites exist where tools for creating and selling custom

---

<sup>93</sup> SEC(2009) 355, p. 29.

<sup>94</sup> A number of current non-legislative activities concerning filtering/blocking of illicit web content are currently undergone in for a, such as COSPOL Internet Related Child Abusive Material Project or the

designed malware (e.g. botnets) are openly commercialised. Any of these tools poses a threat and could be used for cyber attacks, corporate espionage and theft of confidential and sensitive data. These sites may also offer stolen personal data, credit card details and other illegally obtained material. However, it is very unlikely that political agreement on blocking or 'take down' measures that go beyond child pornography can be reached at this stage.<sup>95</sup> This has to do with different interpretations in national legal systems about what content is considered harmful.

The argument is raised that blocking websites can easily be circumvented. With regard to the blocking of child pornography websites, this argument is however not convincing, as the average paedophile is not a versed IT expert. Admittedly, the situation is different in the case of websites offering tools to carry out cyber attacks. Here, the likely user will probably possess a higher level of IT skills and blocking might not be an effective measure in this context.

Similarly to the previous section, the administrative cost related to the obligation on the Member States to ensure that an adequate system is in place for the recording, production and provision of statistical data on attacks against information systems is expected to be low.

***Magnitude of the economic impact:*** ---/+++

#### 5.4.2 *Social impact*

A positive impact on public security and citizens' trust can be expected, but only in the medium-to-long term given the necessity to implement all measures of a comprehensive EU legislation. This would be made more difficult by introducing all other complementary measures on which there is currently little consensus among stakeholders (as became obvious during the consultation process). Nevertheless, one can assume that by the approximation of national law in the area of cybercrime, law enforcement and judicial cooperation improves, which in turn translates over time into a greater number and quality of investigations and prosecutions.

***Magnitude of the social impact:*** +++

#### 5.4.3 *Fundamental rights impact*

In addition to the elements outlined in option 3, this option would introduce legislation covering illicit web content, including blocking of access to websites that facilitate attacks as well as legislation covering the collection, storage and transfer of electronic evidence. Blocking of websites by public authorities may carry the risk that also legal Internet content is deemed illicit and could lead to infringements of the right to engage in legal business activities and freedom of expression. As far as the introduction of criminal procedural rules is concerned, negative impacts on the principle of presumption of innocence, the right to a fair

---

Virtual Global Taskforce, which Member States may join in the short-term. See:  
<http://www.europol.europa.eu/index.asp?page=InternetRelatedChildAbusiveMaterialProject>;  
<http://www.virtualglobaltaskforce.com/>

In this framework too, is the proposal for a new FD on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM(2009)135 final

<sup>95</sup> This is the conclusion of consultations undertaken by the Commission in preparation for this impact assessment.

trial, and the right of defence would need to be avoided (Articles 47 and 48 EU Charter). The blocking of access should be subject to adequate safeguards, in particular to ensure that the blocking is limited to what is necessary, that users are informed of the reason for the blocking and that content providers, as far as possible, are informed of the possibility of challenging it.

As for the obligation to collect statistics, statistical data is anonymous, and therefore does not have data protection implications.

***Magnitude of the fundamental rights impact: -/+***

#### *5.4.4 Effects on third countries*

The legislative update will have in the medium-to-long term a positive effect on the situation in third countries. EU measures taken will have the effect of raising the standard for other countries. Based on the conducted consultations, the EU is looked upon as a standard setter. Therefore, an EU action will have a beneficial impact in the long run due to other countries following its lead.

***Magnitude of the effects on third countries: +++***

#### *5.4.5 Relevance of the measure*

As explained above on the assessment of impacts, the policy option contributes potentially significantly to the achievement of all objectives, but unlike in previous policy option, they cannot be met in the short-to-medium term, which would not meet current expectations of stakeholders.

***Magnitude of relevance: ++ (objectives A, B and C)***

#### *5.4.6 Consistency with international law*

As already discussed above, this policy option is consistent with the Council of Europe Cybercrime Convention, but goes beyond in a number of measures as discussed in previous policy option. Moreover, a number of negative impacts on fundamental rights would have to be minimized to ensure consistency with EU Charter of Fundamental Rights.

***Magnitude of consistency: -/+***

#### *5.4.7 Proportionality*

Similarly to policy option 3, this option contributes substantially to the achievement of the objectives and, at the same time, results in positive economic, social and fundamental rights impacts. However, as the proposed solution would not be limited only to large-scale attacks against information systems (targeted update), but would also tackle other forms of cybercrime, it would be disproportionate to the objectives sought. Indeed, applying simpler Community actions, such as policy option 3, would be possible to deal with the identified problems.

#### 5.4.8 Stakeholders' views

Although most stakeholders agreed on the long-term need to deal with large-scale cyber attacks, and cybercrime in general, by introducing comprehensive measures, including legislation, no consensus emerged in the consultation process on the measures to be included in the comprehensive legislation.

#### 5.4.9 Political feasibility

This policy option is currently not politically feasible, as there is little consensus on the scale and scope of such legislation (as already discussed in 5.4.1). Moreover, Member States policies on the admissibility of electronic evidence in courts are too differently developed. An approximation in this area would be difficult to attain in the short-to-medium term.<sup>96</sup>

### 5.5 Comparison of options

#### *Option (1) Status Quo*

As cybercrime will become more advanced over time, this would also lead to an increased vulnerability for all actors (public and private). The overall security structure (law enforcement and the legal framework) will not catch up with the crime. Even at a sustained level of currently existing actions, European coordination would be required.

#### *Option (2) Development of a programme to strengthen the efforts to counter attacks against information systems with non legislative measures*

This option has all the advantages and disadvantages related to a soft law instrument. The positive side is that it is possible to describe each measure as the current best national practices, and thereby facilitate the identification of which measures are best in terms of effectiveness.

However, this option is less effective in terms of the achievement of the objectives. In addition, this option implies that a ban of botnets and similar tools will not be addressed. Furthermore, issues related to substantive criminal law and prosecution are crucial to curb and eradicate the crime; these are not properly addressed in this option.

#### *Option (3) Targeted update of FD on attacks to address the threat from large-scale attacks against information systems*

This option offers a timely and targeted response to the identified problems. It addresses the criminal law issues necessary to effectively prosecute the perpetrators of this crime. It also improves international cooperation by introducing a mechanism for immediate international assistance in cases of urgent requests for cooperation, and promotes cooperation with the private sector through accompanying measures, such as expert meetings. Finally, to enable measuring of the extent of the problem, monitoring obligations are introduced.

---

<sup>96</sup> “The Admissibility of Electronic Evidence in Court: Fighting against High-tech Crime,” Cybex report (2006); available at: [http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd\\_meeting\\_docs/contributions/libro\\_aeec\\_en.pdf](http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf)

#### *Option (4) Introduction of comprehensive EU legislation against cybercrime*

This option, like option 3, has the added value of establishing binding provisions, and therefore a higher level of effectiveness is expected if fully implemented. It is also expected to maximise the positive impact of both the legislative and non-legislative instruments in a wider range of cybercrime issues than only large-scale attacks. In addition, it would address the criminal law legal framework and at the same time improve law enforcement cooperation over the borders. However, this holistic approach at this stage is not reflecting a consensus of the stakeholders.

### **5.6 THE PREFERRED OPTION: A COMBINATION OF OPTIONS (2) "DEVELOPMENT OF A PROGRAMME TO STRENGTHEN THE EFFORTS, WITH NON-LEGISLATIVE MEASURES", AND (3) "A TARGETED UPDATE OF FD ON ATTACKS"**

The preferred policy option is neither of the four policy options alone, but a combination of policy options 2 and 3. These policy options complement each other and therefore best meet the defined objectives, and give the most value added in resolving the issues associated with the existing situation.

The preferred option combines all elements of options (2) and (3), which are:

From Option 2, the non-legislative elements:

- Strengthening of the existing 24/7 network of contact points for law enforcement authorities by establishing best practice recommendations;
- Establishment of an EU network of public-private contact points of cybercrime experts and law enforcement, and consequent opening of these contact points for requests from the private sector. This network would bring about a list containing contact details on both public and private contact points the elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators;

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

From Option 3, the legislative elements:

- Introduction of legislation against the tools used for attacks against information systems;
- Introduction of new aggravating circumstances regarding large-scale attacks, such as the act of putting in place a botnet or a similar tool enabling committing offences mentioned in Article 2 of the current FD, and when committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner (so-called identity theft);
- Introduction of an obligation for Member States to respond to an urgent request from both the public and the private sector via the 24/7 network of contact points within a certain time limit;
- Introduction of a monitoring obligation for Member States to facilitate the collection and provision of data about cyber attacks and cybercrime, including the number of prosecutions and criminal reports.

## Rationale for levels of penalisation and international cooperation

A higher level of penalisation is required to effectively pursue international cooperation in the fight against cybercrime for the following reasons:

- Firstly, higher level of penalties applied consistently across the EU, and the introduction of aggravating circumstances would mean that a criminal offence linked to a large-scale attack will be treated everywhere as a serious crime. Differences between Member States' levels of penalisation hinder cooperation, as level of penalties in some countries may not be regarded as severe enough to justify rapid cross-border law enforcement and judicial cooperation. Qualification as serious crime would allow for rapid, and fully fledged cross border law enforcement and judicial cooperation.

The currently low level of penalties across the EU (mostly up to 3 years) does not reflect the seriousness of large-scale attacks and the damage they inflict. Estonia called for higher penalties nationally and internationally following cyber attacks in 2008. Lithuania increased penalties for cyber attacks in 2007, and at the same time called for higher penalties across the EU and internationally. The minimum of the maximum penalty should therefore be set at five years, which corresponds to the level in those Member States which recently increased their penalties for cyber attacks, as well as to the generally perceived notion of what constitutes serious crime. Such an increase in the minimum level of penalties will not only send a clear message that the European Union is regarding this type of criminality with increased seriousness, but is also likely to have a deterrent effect.<sup>97</sup>

- The legislative changes that were introduced by Estonia are too recent to establish a link between the higher penalties and the number of large-scale attacks. Large-scale attacks will inevitably continue to grow in absolute terms in years to come due to the fast development in computer technologies and the growth of the Internet. The Internet will grow in terms of potential uses, applications, and number of users. Especially the new possibilities the Internet offers also come with vulnerabilities that can be exploited. However, higher penalisation may slow down the growth dynamic of the crimes, and limit the impact the attacks have on societies. Secondly, only qualification as serious crime would allow for provision of adequate resources by law enforcement. To investigate cybercrime, computer data need to be tracked by specialized officers, and specific high-tech tools need to be applied. This makes this type of investigations rather costly. As a consequence, cross-border cybercrime investigations are still rare, which compares unfavourably with the large number of cyber attacks.
- Secondly, the use of special investigative techniques (without which effective cybercrime investigation is not possible) is only allowed in a number of countries in relation to serious crimes as they potentially infringe on individual liberties. These may be electronic surveillance, phone tapping and remote investigation techniques.
- Thirdly, the deterrent function of criminal law is related to the level of penalties. The higher the penalties, the higher their deterrent function is and this is one of the fundamental principles of modern criminal policy from its beginning. This goes hand-in-hand with a stronger and more publicly visible prosecution of the crimes.

---

<sup>97</sup> For general surveys of the deterrent effect of higher penalties, see:  
<http://pricetheory.uchicago.edu/levitt/Papers/LevittWhyDoIncreasedArrest1998.pdf>

The lack of efficient international cooperation also results from problems with functioning of the contact points. Contact points are the first interlocutors among Member States and when international cooperation is sought in cybercrime investigation. Their efficiency (speed of reaction) determines the efficiency of the whole investigation. Strengthening the contact points by making them truly permanent is going to make not only the EU, but the whole network of G8 and Council of Europe contact points stronger.<sup>98</sup> Indeed, the G8 JHA Ministerial Declaration (29-30 May 2009), raised the issue of further cooperation between the Member States concerning cybercrime by stating that: "It is also essential for States to give a technologically advanced response, and to strengthen the existing forms of international cooperation such as the G8 24/7 High Tech Crime Points of Contact."<sup>99</sup> Similarly, the Council of Europe has called for greater efficiency in cooperation among the contact points, and is currently evaluating the efficiency of the contact points in a report entitled "The functions of 24/7 points of contact for cybercrime".<sup>100</sup> Therefore, by promoting the efficiency of EU contact points we promote the efficiency of the whole world network of contact points.

Due to the prioritisation of cybercrime brought by higher level of penalties, and the obligations included in the update of the FD to have the contact points operate efficiently and on a 24/7 basis, a new "institutional culture" will gradually come into existence. It will also build trust and know-how between the contact points and law enforcement authorities, which, in turn, will make the fight against large scale attacks more efficient. This culture will be reinforced by the flanking actions such as the training and the establishment of the public-private network of contact points.

Finally, training of law enforcement will also enhance the capabilities of law enforcement agencies to respond effectively to cyber attacks. Promoting cybercrime training of both law enforcement agencies and the private sector is essential if the efficiency of all the measures in the preferred policy option is to be maximized. In line with its Communication of 2007, the Commission is currently establishing with the Member States and the private sector an EU cybercrime training platform.<sup>101</sup> This support enables to bring together the best cybercrime trainers and training material in Europe, and to share this expertise with countries, which would not otherwise be able to have access to such expertise. EU funding also serves to update the training material to keep abreast of the fast-evolving techniques used by cyber criminals.

The setting up of EU cybercrime training platform also goes beyond EU borders, as the training material is currently being shared with Europol, Interpol and the Council of Europe. The EU-funded material has become a global reference for cybercrime training.

---

<sup>98</sup> There are cases of cyber criminals in the UK, Sweden and Norway being tracked within 4 hours from notification by the UK law enforcement due to swift public-private cooperation and a rapid reaction by 24/7 contact points.

<sup>99</sup> Final Declaration, G8 ministerial meeting of Justice and Home Affairs, Rome, 29- 30 May 2009, [http://www.g8italia2009.it/static/G8\\_Allegato/declaration1giu2009.pdf](http://www.g8italia2009.it/static/G8_Allegato/declaration1giu2009.pdf)

<sup>100</sup> Council of Europe paper "The functions of 24/7 points of contact for cybercrime", 2009. Still to be released.

<sup>101</sup> Communication from the Commission to the European Parliament, the Council and the Committee of the regions "Towards a general policy on the fight against cyber crime", COM(2007) 267 final

### 5.6.1 *Economic impact*

The economic impact of combining the non-legislative measures with the update of the FD on attacks will be bigger than choosing and implementing either one of the options. This is due to the synergies that are created in the combination.

The costs linked to this option are defined in the detailed assessments of options (2) & (3) above, and can be estimated at EUR 219,000 per Member State for making the contact points available 24/7. Including also the total monitoring and reporting costs (Annex 2), the overall cost linked to the obligation of Member States to keep contact points and provide statistics would amount EUR 5,960,655 for the entire EU. No other entities will be subject to new reporting obligations. The cost of the elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators has been estimated at EUR 30,000 for the Commission.

The synergies are especially in the combination of programmes, such as the establishment of networks of cybercrime experts, the use of a service level agreement and the training programmes for law enforcement agencies, with the strengthening of the legal framework (the Directive). The policy sub-options allow for the establishment of a dissuasive level of penalties, and optimize the way in which the 24/7 contact points operate.

This combination of options also allows linking the binding nature of the update with the positive results to be expected from the flanking non-legislative measures, such as training.

- *financial cost:* --
- *economic benefit:* +++

***Magnitude of the economic impact:*** --/+++

### 5.6.2 *Social impact*

The social impact in terms of improving the security and trust of citizens by the actions of existing law enforcement contact points will be enhanced: if citizens and economic operators affected by cybercrimes are given the possibilities to report these crimes in a trusted manner, and if law enforcement has the possibilities to act, the overall perceived and real security will rise. For companies and internet service providers, initiatives such as the service level agreement, will provide the tool for transmitting confidential data on attacks in a trusted way to law enforcement.

***Magnitude of the social impact:*** +++

### 5.6.3 *Fundamental rights impact*

Any measure taken by the Commission will be in line with articles 7 & 8 European Convention on Human Rights. This concerns especially measures taken concerning the storage of data and the exchange of data between law enforcement agencies. However, the existing EU and national legislation, in particular on data protection, will guarantee a minimal impact on fundamental rights.

The strengthening of EU legislation (Directive) through the penalisation of the production, sale, procurement for use, import, distribution or otherwise making available of tools for cyberattacks needs to be worded carefully in order not to criminalise lawful behaviour. This lawful behaviour includes the economic activities by internet security companies, such as the use of botnets to test the effectiveness of their products. From fundamental rights point of view, this measure needs to guarantee the freedom of expression and the free exercise of political rights and activities (Article 11 EU Charter of Fundamental Rights).

This exception can be guaranteed in the following way:

- By making explicit references to the EU Charter, and referring to it as basic law for the interpretation of the actions investigated under the terms of the FD on attacks;
- By detailing the exact conditions under which the use of ICT tools that are mainly used to launch large scale attacks, can be used for beneficial purposes. To establish these conditions, further consultations will be conducted with the relevant stakeholders, and a 'white listing' of these conditions will be done. This process implies that when these conditions are not met, the use of the tools is considered to be malicious and can therefore be prosecuted.

It will be modelled on the relevant provision in the Council of Europe's Convention on Cybercrime, article 6, paragraph 2.

***Magnitude of the fundamental rights impact: -/++***

#### 5.6.4 *Effects on third countries*

The positive effect of the combination of non-legislative actions and a proposed targeted update of the FD on attacks would be very positive, due to both the making available of knowledge and expertise on the one hand, and acting as a standard setter on the other hand.

The positive effects would be most visible in the long term, but would already become clear through international cooperation in the short-term.

***Magnitude of the effects on third countries: +++***

#### 5.6.5 *Relevance of the measure*

The preferred policy option contributes in an optimum way to the achievement of all objectives, which are expected to be met in the short-to-medium term. Furthermore, the achievement is supposed to be sustainable, through the application of the flanking non-legislative measures.

***Magnitude of relevance: +++ (objectives A, B and C)***

#### 5.6.6 *Consistency with international law*

The consistency of this option is identical to the consistency with international law of Option 3 (see point 5.3.5), as Option 2 does not have implications on international law (the Cybercrime Convention).

**Magnitude of consistency:** -/++

#### 5.6.7 *Proportionality*

The combination of the two options answers the need to not only strengthen the legal framework, but to supplement it with flanking measures. The synergies lead to the achievement of all objectives, and establish a good and positive balance in the economic, social and fundamental rights impacts.

The proposed legislative measures will, on the one hand, aim to prevent and combat large-scale attacks, whilst the flanking non-legislative measures ensure a close and efficient cooperation between the law enforcement agencies across borders.

#### 5.6.8 *Political feasibility*

The political feasibility of this option is the highest of all discussed options. It builds on the consensus amongst (public and private sector) stakeholders, on the policy documents that have been issued by the EU, and the actions that are currently developed at the international level (especially the G8).

#### 5.6.9 *Implementation of the measures*

As the real value added of the preferred option lies in the synergies created by the combination of both options, it is important to ensure the correct implementation of all its components, legislative and non-legislative.

In order to guarantee the implementation of non-legislative measures, the following examples of actions can be mentioned:

Concerning the establishment of a service level agreement, the Commission will follow the JHA Council Conclusions of 27-28 November 2008 on closer public-private cooperation. Best-practices will be learned from the Member States where such agreements are already in place, such as the German example of voluntary agreement dealing with Child Abuse Materials on the internet.

The non-legislative measure of promoting training is in line with the Communication of 2007, and the financial support is and will be provided by EU financial programmes, such as ISEC ('Prevention of and Fight against Crime'). An example is the ongoing initiative to create EU training platform.

The nature of non-legislative measures will require that their implementation is done voluntarily by the Member States. However, as mentioned above, previous experience gained in public-private cooperation agreements and training programmes suggests that the level of commitment by the Member States to other non-legislative measures is expected to be good. Moreover, by agreeing to the Stockholm programme, the Member States have committed to promote cross-border investigations of cybercrime, and called on the Commission to take measures for enhancing/improving public-private partnerships.<sup>102</sup>

---

<sup>102</sup> OJ C 115 of 4.5.2010, pp. 1-38.

## 6. COMPARING THE OPTIONS

### 6.1. Summary table: costs and benefits

Options	Economic impact	Social impact	Fundamental rights impact	Impact on third countries	Relevance for objectives A,B,C	Consistency with int'l law
Option 1: Status quo / no new EU action	0	0	0	-	0	0
Option 2: Development of a programme to strengthen the efforts to counter attacks against information systems with non-legislative measures.	-/+	++	-/+	++	A + B ++ C +	-/+
Option 3: Targeted update of FD on attacks to address the threat from large-scale attacks against information systems.	--/+++	-/+++	-/+++	+++	A +++ B +++ C +++	++
Option 4: Introduction of comprehensive EU legislation against cybercrime.	---/+++	+++	--/+++	++	A ++ B ++ C ++	-/+++
Preferred option (Options 2 and 3): combination of non-legislative measures with a targeted update of the FD on Attacks	--/+++	+++	-/+++	+++	A +++ B +++ C +++	++

## 7. MONITORING AND EVALUATION

With respect to the specific and operational objectives identified in this impact assessment, rough indicators could be the following:

Objective	Indicator
<p><b>Specific Objective:</b></p> <p><b>A. Prosecute and convict criminals responsible for large-scale attacks, through the approximation of criminal law in the area of attacks against information systems</b></p>	
<p><b>A.1</b> To address the problem of large scale attacks from a criminal law perspective; i.e. through the criminalisation of the sale, use and putting at the disposal of tools.</p>	<p>Number of investigated and prosecuted cases.</p> <p>Number of large-scale attacks detected</p>
<p><b>A.2</b> To facilitate prosecution of cross-border cybercrime cases.</p>	<p>Number of cybercrime cases in which European cooperation tools have been used.</p>
<p><b>A.3</b> To impose effective, proportionate and dissuasive penalties.</p>	<p>Level of penalties imposed.</p> <p>Number of penalties.</p>
<p><b>Specific Objective:</b></p> <p><b>B. Improve of cross-border cooperation between Law Enforcement Agencies</b></p>	
<p><b>B.1</b> To introduce mechanisms for immediate international assistance in cases of urgency in a Member State.</p>	<p>Number of occasions that the 24/7 network has been used.</p> <p>Time needed to get replies on urgent requests.</p>
<p><b>B.2</b> To improve exchange of information and best practices among Member States.</p>	<p>Number of organised best practice events in the EU.</p> <p>Number of participants.</p>
<p><b>B.3</b> To improve public-private cooperation through the establishment of contact points and cooperation agreements.</p>	<p>Creation of a service level agreement.</p> <p>Number of information exchanges between public and private sector contact points.</p>

<p><b>Specific Objective:</b></p> <p><b>C. To establish effective monitoring systems</b></p>	
<p><b>C1:</b> To record, produce and provide statistical data on the offences referred to in the Directive.</p>	<p>Monitoring mechanism established at national level.</p> <p>Tasks, human resources and budget set up.</p> <p>Number of information exchanged through the established channels.</p>

The Commission should ensure the regular monitoring and evaluation of the Directive on the basis of the proposed indicators.

An implementation report should be published within 2 years after the date of entry into force of the Directive. This report should pay attention to the exact implementation of the Directive by the Member States.

Furthermore, regular evaluations should be carried out in order to assess how and to what extent the Directive has contributed to the achievement of its objectives. The first evaluation should be carried out within five years after the entry into force of the Directive; the Commission will then publish evaluation reports every five years thereafter and these will include information on implementation. On the basis of the conclusions and recommendations of the evaluations, the Commission should take into account any further amendment to or other possible developments of the Directive.

## Annex 1

### Costs of keeping permanence of the contact points per Member State

						Tariff (€ per hour)	Time (hour)	Price (per action or equip)	Freq (per year)	Cost per Member State (€)
No.	Ass. Art.	Orig. Art.	Type of obligation	Description of required action(s)	Target group					
1			permanence <sup>103</sup>	Keeping permanence in the 24/7 contact points.	Member States	25	24	600	365	219,000

## Annex 2

### Administrative costs related to the contact points (labour costs and overhead costs)

Policy Option 3:						Tariff (€ per hour)	Time (hour)	Price (per action or equip)	Freq (per year)	N° of entities	Total cost (€)	Cost per Member State (€)	Regulatory origin (%)			
No.	Ass. Art.	Orig. Art.	Type of obligation	Description of required action(s)	Target group								Int	EU <sup>104</sup>	Nat	Reg
1			collection	Collection of cybercrime data based on reports.	Member States	25	24	600	365	27	5,913,000	219,000		0-95%	5-100%	
2			Annual reporting	Annual reporting to the national statistical office.	Member States	25	30	750	1	27	20,250	750		0-95%	5-100%	

<sup>103</sup> This obligation already exists in the existing FD 2005/222, and can therefore not be considered to be a "new" administrative cost.

<sup>104</sup> EU member states have the possibility to apply for Commission co-funding up to 95% of the overall costs associated with the relevant measures.

Total costs EUR 5,933,250

The assumption is that there are 1760 working hours per year per person (8 hours \* 20 days \* 11 months).

Average employment costs in the EU-27 public administration: Eurostat: Average hourly labour costs, defined as total labour costs divided by the corresponding number of hours worked (€20,35 in 2005). The 2005 figure has been rounded upwards, based on the assumption of economic growth and pattern over the preceding years and overheads of 10% have been added.

Source: [http://epp.eurostat.ec.europa.eu/portal/page?\\_pageid=1996,39140985&\\_dad=portal&\\_schema=PORTAL&screen=detailref&language=en&product=Yearlies\\_new\\_population&root=Y](http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996,39140985&_dad=portal&_schema=PORTAL&screen=detailref&language=en&product=Yearlies_new_population&root=Y)

### Administrative costs related to monitoring costs (labour costs and overhead costs)

Policy Option 3:						Tariff (€ per hour)	Time (hour)	Price (per action or equip)	Freq (per year)	N° of entities	Total cost (€)	Cost per Member State (€)	Regulatory origin (%)			
No.	Ass. Art.	Orig. Art.	Type of obligation	Description of required action(s)	Target group								Int	EU <sup>105</sup>	Nat	Reg
1			monitoring	retrieving relevant information from existing data	Member States	25	40,00	1,000	1	27	27,000	1,000		0-95%	5-100%	
2			monitoring	Submitting the information (sending it to the designated recipient)	Member States	25	0,1	2.5	1	27	67.5	2.5		0-95%	5-100%	
3			monitoring	filing the information	Member States	25	0,5	12.5	1	27	337.5	12.5		0-95%	5-100%	
Total costs EUR 27 405																

The assumption is that there are 1760 working hours per year per person (8 hours \* 20 days \* 11 months).

Average employment costs in the EU-27 public administration: Eurostat: Average hourly labour costs, defined as total labour costs divided by the corresponding number of hours worked (€20,35 in 2005). The 2005 figure has been rounded upwards, based on the assumption of economic growth and pattern over the preceding years and overheads of 10% have been added.

Source: [http://epp.eurostat.ec.europa.eu/portal/page?\\_pageid=1996,39140985&\\_dad=portal&\\_schema=PORTAL&screen=detailref&language=en&product=Yearlies\\_new\\_population&root=Y](http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996,39140985&_dad=portal&_schema=PORTAL&screen=detailref&language=en&product=Yearlies_new_population&root=Y)

**TOTAL ADMINISTRATIVE COSTS: EUR 27 405 + EUR 5,933,250 = EUR 5,960,655**

<sup>105</sup> EU member states have the possibility to apply for Commission co-funding up to 95% of the overall costs associated with the relevant measures.