**Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA**

**What is the problem to be addressed?**
In recent years, the number of attacks against information systems (IT systems) – or, in common words, the illegal entering of or tampering with information systems - has risen steadily in Europe. Moreover, previously unknown large-scale and dangerous attacks against the information systems of companies, such as banks, the public sector and even the military, have been observed in the Member States and other countries. New concerns, such as the massive spread of malicious software creating 'botnets' - networks of infected computers that can be remotely controlled to stage large-scale, coordinated attacks - have emerged.

**What is a botnet?**
The term 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 people 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.
How does it work?

1) In a preparatory step a cyber criminal acquires or produces malicious software;
2) This software is placed on one computer that becomes the 'command-and-control centre' and is set-up by the hacker to remotely control other computers through malware;
3) Once installed the bot program turns the victim computer into a "zombie" that is able to infect more computers and turn them into other "zombies"; all 'zombies' together form a botnet.
4) Once bots connect zombies to controllers,
5) The cybercriminals take control and command of the servers.
6) At this point they can send commands to the zombies
7) The zombies will execute those commands against targets.

What is the size of the problem?

The number of attacks against information systems has increased significantly in the last few years and 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. In March 2009, computer systems of government and private organisations 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.

More recently 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.
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. 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.

In the last few days experts at international level have launched an alert for a new type of malicious computer worm called Stuxnet that is infecting a high number of power plants, pipelines and factories and could be used to control plant operations remotely. If confirmed, this would be the first case of a highly sophisticated botnet aimed at industrial targets, a development experts don't hesitate to define "the first directed cyber weapon". Botnets like Stuxnet could give wrong information and orders to industrial plants and operate sabotage at several levels, causing severe damages.

What is the aim of the cyber attacks?

The underlying objectives can be varied. Attacks can have criminal objectives or can be used as one of the means in a larger campaign to exert pressure. Attacks often include one or more of the following elements:

- **Diverting money** from bank accounts and stealing sensitive financial information
- **Extortion**: criminals only unlock the computers after the victims pay a certain amount of money to the controllers of the botnet;
- **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 organisation**. 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, or attempted to take out the sites and servers of governments. 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.

A strong tendency towards a stronger implication of organised crime in the attacks has been observed; organised crime groups may, for instance hire hackers or other computer specialists to conduct a specific attack. 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. 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.
What has been done so far to prevent and respond to attacks against information systems?

The issue of cyber attacks has been intensively discussed in Europe over the last few years. Following the adoption of a Framework Decision on attacks against information systems in 2005 (which is to be "updated" by the present proposal), extensive consultations at EU-level have taken place, resulting in the 2007 Communication from the Commission "Towards a general policy on the fight against cyber crime". Most recently, a Commission Communication in 2009 on Critical Information Infrastructure Protection entitled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" highlighted the threat posed by cyber attacks, and the need to secure our information systems. The present legislative proposal considers recent technical advances and the new modi operandi found in today's cyber attacks.

What are the rules in place at EU level?

On 24 February 2005, EU Member States agreed a Council Framework Decision (2005/222/JHA) that addresses the most significant forms of criminal activity against information systems, such as hacking, viruses and denial of service attacks. The Framework Decision seeks to approximate criminal law across the EU to ensure that Europe's law enforcement and judicial authorities can take action against this form of crime.

Before the Lisbon Treaty, EU rules were adopted under the former so-called "third pillar" as "Framework Decisions". For a transitional period until 2014, the Commission cannot take legal action to make sure Member States enforce these rules, as it can in other policy areas. Until then, it will continue to monitor and actively support effective implementation and compliance by Member States. This Framework Decision is currently still in force and would be repealed by the proposed Directive.

Why is the European Commission willing to adopt a new Directive on areas already covered by the Council Framework Decision?

On 14 July 2008, the Commission published a report on the implementation of the Framework Decision on attacks against information systems¹. While the conclusive part of the report stated that significant progress was made in most Member States and that the level of implementation was relatively good, it noted that implementation was still ongoing in some Member States. More importantly, the report underlined that "several 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 cited Framework Decision currently in force was a first step towards addressing the issue of attacks against IT systems. Technological advances and new methods employed by perpetrators call for an improvement of EU rules.

In addition, the entry into force of the Lisbon Treaty on 1 December 2009 provides considerable advantages for new legislation to be adopted in the field of Justice and Home Affairs from now on. Legislation will no longer need to be approved unanimously by the EU Council of Ministers (which represents national governments). Instead, it will be adopted by a majority of Member States at the Council together with the European Parliament. A single country will not be able to block a proposal.

Implementation at national level will also be improved. The Commission will now be able to monitor how Member States apply EU legislation. If it finds that EU countries violate the rules, it will be in a position to refer the case to the European Court of Justice. These considerations add to the justification for the new proposed Directive.

What is new in the proposed Directive?
The proposed Directive, while repealing the Framework Decision in force, will retain its current provisions – namely the penalisation of illegal access, illegal system interference and illegal data interference – and include the following new elements:
- Penalisation of the use of tools (such as malicious software – e.g. 'botnets' – or unrightfully obtained computer passwords) for committing the offences;
- Introduction of 'illegal interception' of information systems as a criminal offence;
- Improvement of European criminal justice/police cooperation by
  - strengthening the existing structure of 24/7 contact points, including an obligation to answer within 8 hours to urgent request and;
- Including the obligation to collect basic statistical data on cybercrimes

Furthermore, the proposed Directive raises the level of criminal penalties to a maximum term of imprisonment of at least two years. Instigation, aiding, abetting and attempt of those offences will become penalised as well.

Once adopted, the Directive raises the level of criminal penalties of offences committed under aggravating circumstances to a maximum term of imprisonment of at least five years (instead of two years, as foreseen by Framework Decision 2005/222/JHA) (i) committed within the framework of a criminal organisation (already included under Framework Decision 2005/222/JHA);

(ii) committed through the use of a tool conceived to launch either attacks affecting a significant number of information systems, or attacks causing considerable damage, such as in terms of disrupted system services, financial cost or a loss of personal data (not previously included under Framework Decision 2005/222/JHA). This provision would be relevant to tackle the spread of malicious software that is now used widely to launch most dangerous cyber attacks.

(iii) committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner (not included under Framework Decision 2005/222/JHA).
Terms of Reference

**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.

**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.

**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. 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.

**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.

For further information
Homepage of Cecilia Malmström, EU Commissioner for Home Affairs: