Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 30/09/2010 - Legislative proposal

PURPOSE: to propose a new legislative framework aimed at combating (large scale) attacks against information systems and to repeal Council Framework Decision 2005/222/JHA.

PROPOSED ACT: Directive of the European Parliament and of the Council.

BACKGROUND: in recent years, the number of attacks against IT 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. 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.

With regard to cybercrime, the main cause of this phenomenon is vulnerability resulting from a variety of factors. Insufficient response by law enforcement mechanisms contributes to the prevalence of these phenomena, and exacerbates the difficulties, as certain types of offences go beyond national borders. Variations in national criminal law and procedure may give rise to differences in investigation and prosecution, leading to differences in how these crimes are dealt with.

Developments in information technology have exacerbated these problems by making it easier to produce and distribute tools ('malware' and 'botnets'), while offering offenders anonymity and dispersing responsibility across jurisdictions. Given the difficulties of bringing a prosecution, organised crime is able to make considerable profits with little risk.

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. Member States were required to take the necessary measures to comply with the provisions of the Framework Decision by 16 March 2007.

On 14 July 2008, the Commission published a report on the implementation of the Framework Decision. It was noted that several emerging threats had been highlighted by recent attacks across Europe since adoption of the Framework Decision, in particular the emergence of large-scale simultaneous attacks against information systems and increased criminal use of so-called 'botnets'." These attacks were not the centre of attention when the Framework Decision was adopted.

In response to these developments, the Commission presents this proposal which aims to consider recent technical advances and the new modi operandi found in today's cyber attacks as devise better responses to the threat.

IMPACT ASSESSMENT: various policy options have been examined as a means of achieving the objective.

Option 1: Status Quo / No new EU action.

Option 2: Development of a programme to strengthen the efforts to counter attacks against information systems by means of non-legislative measures: these measures would, in addition to the programme for critical information infrastructure protection, focus on cross-border law enforcement and public-private cooperation. These soft-law instruments should aim to promote further coordinated action at EU level, including strengthening of the existing 24/7 network of contact points for law enforcement agencies; establishment of an EU network of public-private contact points involving cybercrime experts and law enforcement agencies; elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators; and support for the organisation of training programmes for law enforcement agencies on the investigation of cybercrime.

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

Option 4: Introduction of comprehensive EU legislation against cybercrime: this option would entail new comprehensive EU legislation. In addition to introducing the soft-law measures in policy option 2 and the update in policy option 3, it would also tackle other legal problems related to Internet use (such as financial cybercrime, illegal Internet content, the collection/storage/transfer of electronic evidence…)

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 doesn't seem realistic as there seems to be no international willingness to renegotiate the Convention.

The preferred policy option is a combination of non-legislative measures (option 2) with a targeted update of the Framework Decision (option 3).

LEGAL BASE: Article 83(1) of the Treaty on the Functioning of the European Union (TFEU).

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

On substantive criminal law in general, the proposed Directive:

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

2) Includes **aggravating circumstances**:

- the **large-scale aspect of the attacks** - botnets or similar tools would be addressed by introducing a new aggravating circumstance, in the sense that the act of putting in place a botnet or a similar tool would be an aggravating factor when crimes listed in the existing Framework Decision are committed;
- **when such attacks are committed by concealing the real identity of the perpetrator** and causing prejudice to the rightful identity owner. Any such rules would need to comply with the principles of legality and proportionality of criminal offences and penalties and be consistent with existing legislation on the protection of personal data .

3) Introduces **‘illegal interception’** as a criminal offence.

4) Introduces measures to **improve European criminal justice cooperation** by strengthening the existing structure of 24/7 contact points:

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

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

Taking account of gravity of the crimes: the Directive contains in the definitions of criminal offences listed in articles 3, 4, 5 (illegal access to information systems, illegal systems interference and illegal interference) a provision allowing to **criminalise only 'cases which are not minor'** in the process of transposition of the directive into national law. This element of flexibility is intended to allow Member States not to cover cases that would in abstracto be covered by the basic definition but are considered not to harm the protected legal interest, e.g. in particular acts by young people who attempt to prove their expertise in information technology. This possibility to limit the scope of criminalisation should not however lead to the introduction of additional constitutive elements of offences beyond those that are already included in the Directive, because this would lead to the situation that only offences committed with the presence of aggravating circumstances are covered. In the process of transposition, Member States should refrain in particular from adding additional constitutive elements to the basic offences such as e.g. a special intention to derive illicit proceeds from crime or the presence of a specific effect such as causing a considerable damage.

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