Basic information

2010/0273(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Directive	Procedure completed
Judicial cooperation in criminal matters: combating attacks against information systems Repealing 2002/0086(CNS) **Subject** 3.30.06 Information and communication technologies, digital technologies 3.30.07 Cybersecurity, cyberspace policy 3.30.25 International information networks and society, internet 7.40.04 Judicial cooperation in criminal matters	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	HOHLMEIER Monika (PPE)	09/12/2010
	Shadow rapporteur PICKART ALVARO Alexander Nuno (ALDE) ALBRECHT Jan Philipp (Verts/ALE) KIRKHOPE Timothy (ECR) VERGIAT Marie-Christine (GUE/NGL)	

Committee for opinion	Rapporteur for opinion	Appointed
AFET Foreign Affairs	OJULAND Kristiina (ALDE)	29/03/2011
BUDG Budgets	The committee decided not to give an opinion.	
ITRE Industry, Research and Energy	EHLER Christian (PPE)	24/11/2010

Council of the European Union

Council configuration	Meetings	Date
Justice and Home Affairs (JHA)	3096	2011-06-09

European Commission	Commission DG	Commissioner
	Migration and Home Affairs	MALMSTRÖM Cecilia

Key events

Date	Event	Reference	Summary
30/09/2010	Legislative proposal published	COM(2010)0517	Summary
07/10/2010	Committee referral announced in Parliament, 1st reading		
09/06/2011	Debate in Council		Summary
06/06/2013	Vote in committee, 1st reading		
19/06/2013	Committee report tabled for plenary, 1st reading	A7-0224/2013	Summary
03/07/2013	Debate in Parliament		
04/07/2013	Decision by Parliament, 1st reading	T7-0321/2013	Summary
04/07/2013	Results of vote in Parliament		
22/07/2013	Act adopted by Council after Parliament's 1st reading		
12/08/2013	Final act signed		
12/08/2013	End of procedure in Parliament		
14/08/2013	Final act published in Official Journal		

Technical information

Procedure reference	2010/0273(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Directive
Amendments and repeals	Repealing 2002/0086(CNS)
Legal basis	Treaty on the Functioning of the European Union TFEU 083-p1-a1
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/7/04091

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee opinion	ITRE	PE472.192	11/11/2011	
Committee draft report		PE476.089	24/11/2011	

Committee opinion	AFET	PE469.848	28/11/2011	
Amendments tabled in committee		PE480.665	27/01/2012	
Committee report tabled for plenary, 1st reading/single reading		A7-0224/2013	19/06/2013	Summary
Text adopted by Parliament, 1st reading/single reading		T7-0321/2013	04/07/2013	Summary

Council of the EU

Document type	Reference	Date	Summary
Draft final act	00038/2012/LEX	12/08/2013	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2010)0517	30/09/2010	Summary
Document attached to the procedure	SEC(2010)1122	30/09/2010	
Document attached to the procedure	SEC(2010)1123	30/09/2010	
Commission response to text adopted in plenary	SP(2013)625	24/09/2013	
Follow-up document	COM(2017)0474	13/09/2017	Summary

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	IT_SENATE	COM(2010)0517	19/11/2010	
Contribution	PT_PARLIAMENT	COM(2010)0517	01/12/2010	
Contribution	IT_CHAMBER	COM(2010)0517	16/12/2010	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EESC	Economic and Social Committee: opinion, report	CES0816/2011	04/05/2011	

Additional information

Source	Document	Date
National parliaments	IPEX	
European Commission	EUR-Lex	

Final act

Directive 2013/0040
OJ L 218 14.08.2013, p. 0008 Summary

Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 19/06/2013 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Monika HOHLMEIER (EPP, DE) on 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.

The committee recommends that the European Parliament's position adopted at first reading under the ordinary legislative procedure should be to modify the Commission's proposal as follows:

Objective of the Directive: the objective of the Directive is to establish minimum rules concerning the **definition of criminal offences and the sanctions in the area of attacks against information systems**. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.

Definitions: a definition of **"without right"** was added: "without right" means access, interference, interception, or any other conduct referred to in this Directive, not authorised by the owner, other right holder of the system or of part of it, or not permitted under national legislation.

It should also be noted that, in the recitals, a definition of **"interception"** has been introduced: interception includes (but is not necessarily limited to) the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means.

Illegal system interference: Member States shall take the necessary measures to ensure that, when **committed intentionally** and without right, at least for cases which are not minor, the serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is **punishable as a criminal offence**. The same follows in respect to the illegal access to illegal data interference or in the case of illegal interception within the meaning of the Directive.

Incitement, aiding and abetting and attempt: provision should also be made for measures to ensure that the incitement, **aiding and abetting** to commit an offence within the meaning of the Directive is punishable as a criminal offence. Member States are called upon to ensure that the **attempt** to commit an offence is punishable as a criminal offence.

Penalties: in a recital, it is stipulated that criminal sanctions should be envisaged at least for **cases which are not minor**. Member States may determine what constitutes a minor case according to their national law and practice. The case may be considered minor, for example, when the damage caused by the offence and/or the risk it carries to public or private interests, such as to the integrity of a computer system or computer data, or to a person's integrity, rights and other interests, is insignificant or is of such nature, that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.

In any event, **offences that fall within the scope of the Directive should be subject to the following penalties**:

- a maximum penalty of **at least two years** of imprisonment, in cases which are not minor;
- a maximum penalty of **at least three years** of imprisonment when certain offences covered by the Directive are **committed intentionally**, and when a significant number of information systems have been affected through the use of a tool designed or adapted primarily for this purpose;
- a maximum penalty of **at least five years** of imprisonment when offences covered by the Directive are:

  - committed within the framework of a criminal organisation, or

  - causing serious damage, or

  - committed against a **critical infrastructure information system**.

Furthermore, if certain when certain offences are committed by misusing personal data **of another person**, with the aim of gaining trust of a third party, thereby causing prejudice to the rightful identity owner, this may be regarded as **aggravating circumstances**. A recital stipulates that identity theft and other identity-related offences of the same type could require **action at EU level** in the form of a comprehensive horizontal EU instrument.

Jurisdiction: a Member State shall inform the Commission where it decides to **establish further jurisdiction over an offence** covered by the Directive **committed outside their territory**, e.g. where:

- the offender has his or her habitual residence in the territory of that Member State ; or

- the offence is committed for the benefit of a legal person established in the territory of that Member State.

National contact point: Member States should ensure that they have an o**perational national point of contact** and make use of the existing network of operational points of contact available 24 hours a day and seven days a week. They should also ensure that they have procedures in place so that in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered, as well as the form and the estimated time of this answer.

Data collection: it is stipulated that there is a need to collect comparable data on offences referred to in this Directive. Relevant data should be made available to the competent specialised agencies, such as Europol and the European Network and Information Security Agency in line with their tasks and information needs. The objective is to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby contribute to formulating more effective responses.

Replacement of the Framework Decision 2005/222/JHA: it is clearly stipulated that the Directive aims to amend and expand the provisions of Framework Decision 2005/222/JHA concerning attacks against information systems.

Reports: lastly, the Commission should submit, **within four years of the adoption of this Directive**, a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals. In this respect, the Commission shall also take into account the technical and legal developments in the field of cyber crime, particularly with regard to the scope of this Directive.

Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 04/07/2013 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 541 votes to 91, with 9 abstentions, a legislative resolution on 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.

Parliament adopted its position at first reading under the ordinary legislative procedure. The amendments adopted in plenary are the result of a compromise reached between the European parliament and the Council. They amend the Commission's proposal as follows:

Objective of the Directive: the objective of the Directive is to establish minimum rules concerning the **definition of criminal offences and the sanctions in the area of attacks against information systems**. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.

Definitions: a definition of **"without right"** was added: "without right" means access, interference, interception, or any other conduct referred to in this Directive, not authorised by the owner, other right holder of the system or of part of it, or not permitted under national legislation.

It should also be noted that, in the recitals, a definition of **"interception"** has been introduced: interception includes (but is not necessarily limited to) the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means.

Illegal system interference: Member States shall take the necessary measures to ensure that, when **committed intentionally** and without right, at least for cases which are not minor, the serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is **punishable as a criminal offence**. The same follows in respect to the illegal access to illegal data interference or in the case of illegal interception within the meaning of the Directive.

Incitement, aiding and abetting and attempt: provision should also be made for measures to ensure that the incitement, **aiding and abetting** to commit an offence within the meaning of the Directive is punishable as a criminal offence. Member States are called upon to ensure that the **attempt** to commit an offence is punishable as a criminal offence.

Penalties: offences that fall within the scope of the Directive should be subject to the following penalties:

- a maximum penalty of **at least two years** of imprisonment, in cases which are not minor;
- a maximum penalty of **at least three years** of imprisonment when certain offences covered by the Directive are **committed intentionally**, and when a significant number of information systems have been affected through the use of a tool designed or adapted primarily for this purpose;
- a maximum penalty of **at least five years** of imprisonment when offences covered by the Directive are:

  - committed within the framework of a criminal organisation, or

  - causing serious damage, or

  - committed against a **critical infrastructure information system**.

In a recital, it is stipulated that criminal sanctions should be envisaged at least for **cases which are not minor**. Member States may determine what constitutes a minor case according to their national law and practice. The case may be considered minor, for example, when the damage caused by the offence and/or the risk it carries to public or private interests, such as to the integrity of a computer system or computer data, or to a person's integrity, rights and other interests, is insignificant or is of such nature, that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.

Furthermore, if certain when certain offences are committed by misusing personal data **of another person**, with the aim of gaining trust of a third party, thereby causing prejudice to the rightful identity owner, this may be regarded as **aggravating circumstances**. A recital stipulates that identity theft and other identity-related offences of the same type could require **action at EU level** in the form of a comprehensive horizontal EU instrument.

Jurisdiction: a Member State shall inform the Commission where it decides to **establish further jurisdiction over an offence** covered by the Directive **committed outside their territory**, e.g. where:

- the offender has his or her habitual residence in the territory of that Member State ; or
- the offence is committed for the benefit of a legal person established in the territory of that Member State.

National contact point: Member States should ensure that they have an **operational national point of contact** and make use of the existing network of operational points of contact available 24 hours a day and seven days a week. They should also ensure that they have procedures in place so that in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered, as well as the form and the estimated time of this answer.

Data collection: it is stipulated that there is a need to collect comparable data on offences referred to in this Directive. Relevant data should be made available to the competent specialised agencies, such as Europol and the European Network and Information Security Agency in line with their tasks and information needs. The objective is to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby contribute to formulating more effective responses.

Replacement of the Framework Decision 2005/222/JHA: it is clearly stipulated that the Directive aims to amend and expand the provisions of Framework Decision 2005/222/JHA concerning attacks against information systems.

Reports: lastly, the Commission should submit, **within four years of the adoption of this Directive**, a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals. In this respect, the Commission shall also take into account the technical and legal developments in the field of cyber crime, particularly with regard to the scope of this Directive.

Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 12/08/2013 - Final act

PURPOSE: to approximate Member States' criminal law in the area of attacks against information systems.

LEGISLATIVE ACT: Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

CONTENT: the Directive establishes **minimum rules concerning the definition of criminal offences and sanctions** in the area of attacks against information systems. It also aims to **facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities**.

Offences: for **cases which are not minor, and are committed intentionally and without right,** the following actions must be punishable as criminal offences:

- **illegal access to information systems**: illegal access to the whole or to any part of an information system where committed by infringing a security measure;
- **illegal system interference**: seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;
- **illegal data interference**: deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible;
- **illegal interception**: intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data;
- **tools used for committing offences**: the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to above: (i) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to above; ii) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Incitement, aiding and abetting and attempt: the Directive provides that:

- the incitement, or aiding and abetting, to commit any of the five offences referred to above must be punishable as a criminal offence;
- the **attempt to commit illegal system interference and illegal data interference** must be punishable as a criminal offence.

Penalties: offences that fall within the scope of the Directive should be subject to the following penalties:

- a maximum penalty of **at least two years of imprisonment**, in cases which are not minor;
- a maximum penalty of **at least three years of imprisonment** when offences relating to illegal system interference and illegal data interference are committed intentionally, and when a significant number of information systems have been affected through the use of a tool designed or adapted primarily for this purpose;
- a maximum penalty of **at least five years of imprisonment** when offences relating to illegal system interference and illegal data interference are: (i) committed within the framework of a criminal organisation, or (ii) causing serious damage, or (iii) committed against a critical infrastructure information system.

When offences relating to illegal system interference and illegal data interference are committed by **misusing the personal data of another person, with the aim of gaining the trust of a third party**, thereby causing prejudice to the rightful identity owner, this may be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.

A recital in the Directive states that setting up effective measures against identity theft and other identity-related offences constitutes another important element of an integrated approach against cybercrime. Any need for Union action against this type of criminal behaviour could also be considered in the context of evaluating the need for a comprehensive horizontal Union instrument.

Legal persons: the Directive makes provision for ensuring that legal persons may be held liable and sanctioned.

Jurisdiction: the Directive sets out rules on the establishment of jurisdiction with regard to the offences described above. A recital notes that the **transnational and borderless nature of modern information systems** means that attacks against such systems have a cross-border dimension, thus underlining the urgent need for further action to approximate criminal law in this area.

National contact point: Member States must ensure that they have an operational national point of contact and make use of the existing network of operational points of contact available 24 hours a day and seven days a week. They must have procedures in place so that in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered, as well as the form and the estimated time of this answer.

Data collection: a recital in the text states that there is a need to collect comparable data on the offences laid down in this Directive. Relevant data should be made available to the competent specialised Union agencies and bodies, such as Europol and ENISA, in line with their tasks and information needs, in order to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby to contribute to formulating a more effective response. Member States should submit information on the modus operandi of the offenders to Europol and its European Cybercrime Centre for the purpose of conducting threat assessments and strategic analyses of cybercrime in accordance with Council Decision 2009/371/JHA.

Replacement of Framework Decision 2005/222/JHA: in relation to Member States participating in the adoption of this Directive, references to the Framework Decision 2005/222/JHA shall be construed as references to this Directive.

Report: by 4 September 2017, the Commission must submit a report assessing the extent to which the Member States have taken the necessary measures in order to comply with the Directive. It will, also take into account the technical and legal developments in the field of cybercrime, particularly with regard to the scope of the Directive.

ENTRY INTO FORCE: 3 September 2013.

TRANSPOSITION: by 4 September 2015.

Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 09/06/2011

The Council adopted a **general approach** on a draft directive on attacks against information systems, proposed by the Commission in September 2010. The general approach will constitute the basis for the Council's negotiations with the European Parliament on this proposal under the ordinary legislative procedure.

The proposal aims to update the existing rules dating from 2005 (Framework Decision 2005/222/JHA), while building on the Council of Europe Convention on Cybercrime (Budapest Convention). It establishes minimum rules for the definition of criminal offences and the penalty levels in the area of attacks against IT systems. It also aims to facilitate the prevention of such attacks and to improve the cooperation between member states' authorities in this field. The new rules would retain most of the provisions currently in place - namely the penalisation of illegal access, illegal system interference and illegal data interference as well as instigation, aiding, abetting and attempt to commit those criminal offences - and **include the following new elements**:

- penalisation of the production and making available of tools (e.g. malicious software designed to create "botnets"**1** or unrightfully obtained computer passwords) for committing the offences;
- illegal interception of computer data will become a criminal offence;
- improvement of European cooperation in criminal matters by strengthening the existing structure of 24/7 contact points, including an obligation to provide feedback within eight hours to urgent requests; and
- the obligation to collect basic statistical data on cybercrimes.

Concerning the level **of criminal penalties**, the new rules would **raise the thresholds**:

- in the general case to a maximum term of imprisonment of at least two years;
- if committed against a significant number of IT systems, e. g. in order to create a "botnet", to a maximum term of imprisonment of at least three years;
- if the attack has been committed by an organised criminal group, or has caused serious damage, e.g. through the use of a "botnet", or has affected a critical IT system, to a maximum term of imprisonment of at least five years.

These new forms of aggravating circumstances are intended to address the emerging threats posed by large scale cyber attacks, which are increasingly reported across Europe and have the potential severely to damage public interests.

Lastly, the Council has clarified the rules concerning the establishment of jurisdiction by the member states on cybercrime.

While the UK and Ireland participate in the adoption and application of this directive, Denmark would not be bound by it.

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.

Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 13/09/2017 - Follow-up document

The Commission presented a report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems.

The objectives of the Directive are to approximate the criminal law of the Member States in the area of attacks against information systems and to improve cooperation between competent authorities. This is done by establishing minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems and by requiring operational 24/7 points of contact.

By the transposition date, **22 Member States had notified the Commission that they had fully completed the Directive's transposition**. As of 31 May 2017, infringement procedures for non-communication of national transposition measures against BE, BG and IE were still pending. However, the Commission acknowledges the efforts made by the Member States to transpose the Directive.

The analysis in this report is based on the information that Member States provided by 31 May 2017.

Progress made: the report concluded that the Directive has made **real progress in criminalising cyberattacks** on a comparable level across the Member States, facilitating cross-border cooperation between law enforcement authorities investigating cyberattacks.

Member States have amended criminal codes and other relevant legislation. They have **streamlined their procedures** and set up or improved cooperation schemes.

Scope for improvement: the Commission confirmed, however, that there is **considerable scope for improvement** if Member States were to fully implement all of its provisions. The main improvements to be implemented by the Member States relate in particular to:

- **the use of the definitions** of the terms 'information system', 'computer data', 'legal person' and 'without right' provided by the Directive: only two countries have introduced legislation covering all aspects of these definitions;
- the **inclusion of all the possibilities that define specific criminal related offences** (illegal access to information systems, illegal data interference, illegal interception of computer data: tools, such as computer programmes or passwords, used to commit offences);
- the **establishment of common standards of penalties for cyberattacks** (minimum levels of maximum penalties, penalties where a significant number of information systems have been affected, offences committed by a criminal organisations, causing serious damage, involvement critical infrastructure information systems in offences, identity theft, liability of legal persons).

Other issues appear to relate to the implementation of administrative provisions on **appropriate reporting channels** and the monitoring and statistics for the offences included in the Directive.

Outlook: the Commission states that it will continue to support Member States in their implementation of the Directive and will provide additional opportunities for Member States to identify and exchange best practices in the second half of 2017.

The Commission currently **sees no need to propose amendments to the Directive**. It is considering measures to **improve cross-border access to electronic evidence** for criminal investigations, including proposing legislative measures by the beginning of 2018. It is also considering the role of encryption in criminal investigations and will report on its findings by October 2017.

Lastly, the Commission is committed to ensuring that the transposition is finalised across the EU and that the provisions are correctly implemented.