EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 474 final

REPORT FROM THE COMMISSION 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 Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Table of Contents

1. Introduction

According to Europol`s 2016 Internet Organised Crime Threat Assessment (IOCTA), cybercrime is becoming more aggressive and confrontational. This can be seen in various forms of cybercrime, including attacks against information systems[1]. Some serious forms of attacks that Europol mentions are the use of malicious software and social engineering to infiltrate and gain control over an information system or to intercept communications and the launch of wide-scale network attacks, including on critical infrastructure. These attacks are identified as key threats to our society.

With more and more information stored in clouds and information and criminals now highly mobile, cross-border cooperation between law enforcement authorities has become crucial for most cybercrime investigations.

To fight these crimes effectively, Member States need to commonly define what acts should be considered attacks against information systems. They also need to have approximated levels of sanctions and the operational means to report offences and exchange information between authorities. Accordingly, on 12 August 2013, the European Parliament and the Council adopted Directive 2013/40/EU (the 'Directive') on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.[2]

1.1. Objectives and scope of the Directive

The objectives of the Directive are to approximate the criminal law of the Member States[3] 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.

On the **definition** of relevant terms, the Directive refers to:

- An 'information system' in Article 2(a)[4]. The definition is close to the definition of a computer system as provided by Article 1(a) of the Council of Europe Convention on Cybercrime of 23 November 2001 (the 'Budapest Convention'), with the exception that the Directive also explicitly covers computer data itself.
- 'Computer data' in Article 2(b). The definition follows the one of Article 1(b) of the Budapest Convention, referring to an information system instead of a computer system.
- A 'legal person' in Article 2(c). The definition aims to ensure liability of both natural and legal persons while excluding States, public bodies or public international organisations.

[1] Europol, 2016 Internet Organised Crime Threat Assessment (IOCTA), available at https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf.

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:pdf.

[3] From this point onwards and unless explicitly indicated differently, 'Member States' or 'all Member States' refer to the Member States bound by the Directive, i.e. all EU Member States except Denmark, which did not take part in the Directive's adoption, in accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on the European Union and to the Treaty on the Functioning of the European Union (TFEU). In accordance with Article 3 of Protocol 21 on the position of the United Kingdom and Ireland, both took part in the Directive's adoption and are bound by it.

[4] All Articles mentioned refer to those of the Directive unless indicated otherwise.

- 'Without right' in Article 2(d). The definition concerns a general principle of criminal law and aims to avoid criminal liability for a person acting either as permitted under national law or with the authorisation of the owner or of another right holder of the information system or part of it.

Specific criminal offences are defined, namely:

- Illegal access to information systems as such (Article 3);
- Illegal system interference (Article 4) which includes any illegal access to an information system causing its functioning to be seriously hindered or interrupted;
- Illegal data interference (Article 5) which refers to any unlawful interference with computer data as such impairing its integrity or availability;
- Illegal interception (Article 6) of non-public transmissions of computer data and electromagnetic emissions from an information system carrying such data;
- Illegal provision of tools used for committing the mentioned offences (Article 7). In this context, such tools could be a computer programme as well as a computer password or any other data allowing access to an information system.

In addition, the Directive **extends criminal liability** to incitement, aiding and abetting by natural and/or legal persons to commit and their attempt to commit the offences mentioned above (Article 8). While inciting, aiding and abetting cover all the offences referred to in Articles 3 – 7, the attempt refers only to Articles 4 and 5.

Minimum levels of maximum **penalties** for offences referred to in the Directive are provided for in Article 9:

- As a baseline, a maximum penalty of imprisonment of at least 2 years is set for all the offences except for the ones under Article 8 (Article 9(2)).
- At least 3 years of imprisonment as a maximum penalty apply to offences under Articles 4 and 5 where a significant number of information systems has been affected (generally referred to as botnet offences; Article 9(3).
- At least 5 years of imprisonment as a maximum penalty are required for offences under Articles 4 and 5 committed by a criminal organisation (Article 9(4)(a)), causing serious damage (Article 9(4)(b)) or committed against a critical infrastructure information system (Article 9(4)(c)).
- Whenever an offence under Articles 4 and 5 is committed in the context of misuse of personal data of another person, Member States should ensure that it may be considered as aggravating circumstances unless those circumstances are already covered by another offence (Article 9(5)).

The subsequent Articles set up minimum conditions for the **liability of legal persons** (Article 10) and provide an exemplary list of possible sanctions against them (Article 11).

Recognising that the offences mentioned above can be committed (in the sense of 'executed') in a place where the offender actually acts while their effects on the targeted information system might take place somewhere else, Article 12 provides for obligations to establish **jurisdiction** differentiating between:

- the place where the offender is physically present when committing the offence,
- the location of the targeted information system,

- the nationality of the offender,
- his / her habitual residence, and
- the place of establishment of a legal person for whose benefit the offence is committed.

Regarding exchange of information, Article 13(1) requires Member States to ensure that they have operational national **points of contact** available 24 hours a day and 7 days a week, so that they can reply to any urgent foreign request within 8 hours.

Furthermore, Member States must take the necessary measures to **facilitate the reporting** of the offences mentioned above to the competent national authorities (Article 13(3)) and to collect and share a minimum amount of **statistical data** on these offences (Article 14).

1.2 Purpose and methodology of the report

Article 16 of the Directive requires Member States to bring into force the laws, regulations and administrative provisions necessary to comply with the Directive by 4 September 2015 and communicate them to the Commission.

This report responds to the requirement under Article 17 of the Directive for the Commission to 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 the Directive. The aim of the report is therefore to provide a concise yet informative overview of the main transposition measures taken by Member States.

Member State transposition involved collecting information on the relevant legislation and administrative measures, analysing it, drafting new legislation or — in most cases — amending existing acts, seeing it through to adoption and finally reporting it to the Commission.

By the transposition date, 22 Member States had notified the Commission that they had fully completed the Directive's transposition. In November 2015, the Commission opened infringement procedures for non-communication of national transposition measures against the remaining 5 Member States: BE, BG, EL, IE and SI[5]. As of 31 May 2017, infringement procedures for non-communication of national transposition measures against BE, BG and IE were still pending.[6]

The description and analysis in this report are based on the information that Member States provided by 31 May 2017.[7] Notifications received after that date have not been taken into account. All notified measures referring to national legislations were taken into account as well as court decisions and – where appropriate – common legal theory. Furthermore, during the course of the analysis, the Commission contacted Member States directly where it was

[5] Member States in this document are abbreviated according to: http://publications.europa.eu/code/en/en-5000600.htm.

[6] Information on the Commission's decisions on infringement procedures can be found at: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=en.

[7] IE reported full transposition of the Directive on 31 May 2017.

necessary and appropriate to receive additional information or clarifications. All the information gathered was taken into consideration for the analysis.

Beyond the issues identified in this report, there may be further challenges in transposition and other provisions not reported to the Commission or future legislative and non-legislative developments. Therefore, this report does not prevent the Commission from further evaluating some provisions and from continuing to support Member States in the transposition and implementation of the Directive.

2. Transposition measures

2.1 Legal definitions (Article 2 of the Directive)

Article 2 of the Directive provides legal definitions for 'information system' (a)), 'computer data' (b)), 'legal person' (c)) and 'without right' (d)). Only CY and UK (Gibraltar) have introduced legislation covering all aspects of the definitions listed above. In detail, this means:

a) Information system

The Directive`s definition builds on the definition of the term 'computer system' as provided by Article (1)(a) of the Budapest Convention, adding computer data itself as part of the information system. CY, EL, IE, FI, HR, MT, PT and UK (Gibraltar) have introduced legislative provisions with the definition of an information system, while the information provided by DE, ES, FR, LU, LV, PL, SE and SK was not conclusive. For the remaining Member States, i.e. AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI and UK (except for Gibraltar), the respective legal definitions do not specifically mention 'computer data'. This implies a reference to Article 1(a) of the Budapest Convention with an identical scope for the definition of a computer system.

b) Computer data

The term 'computer data' is provided by the legislation of AT, BG, CY, CZ, DE, EE, EL IE, FI, HR, LT, MT, NL, PT, RO and UK (Gibraltar), while the information provided by ES, FR, IT, LU, LV, PL, SE, SK and UK (except for Gibraltar) was not conclusive. However, in the case of SE, the specific set-up of the referring articles make this definition redundant. As for the remaining Member States, HU refers the definition of computer data only to offences described in Articles 4 and 5 of the Directive, while both BE and SI lack the inclusion of 'a programme suitable for causing an information system to perform a function' in the definition of computer data.

c) Legal person

Except for LU, which provided no conclusive information on the transposition of Article 2(c), the transposition of the definition of 'legal person' did not cause any problems. This is because, in general, it is already found in mostly civil law or commercial law provisions of the Member States. Only CY has a specific provision in the measures adopted to transpose the Directive.

d) Without right

As to the definition of the term 'without right' in Article 2(d), only CY, IE, RO and UK (Gibraltar) notified transposition, leaving 23 Member States without any transposition measures for this definition. However, it must be observed that in all Member States, there is the general principle of no criminal liability for whatever action if this action is carried out with according rights.

2.2 Specific criminal offences (Articles 3 – 7 of the Directive)

a) Illegal access to information systems
Referring to illegal access to an information system, Article 3 of the Directive is covered by the national legislation of AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE and SK.

For all remaining Member States, i.e. BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI and the UK, the respective national description of the criminal offence does not differ between gaining access to the whole or to only a part of the information system, even though this is explicitly provided for in the Directive. Also, DE`s transposition does not cover mere access to computer hardware, and additional requirements are provided for by AT and LU regarding a special intention (intent to gain knowledge, inflict disadvantage or fraudulent intent) and by LV regarding the cause of substantial harm. In the case of BE, BG, FR, HR, LU, MT, PT, RO, SI and the UK, the scope of the national provisions is broader than the Directive, as these provisions do not require circumventing any security measure to establish criminal liability. The remaining Member States either refer literally to the offence being committed by infringing a security measure (CY, EL and SK), or they use similar terminology to describe the aspect (AT, CZ, DE, EE, ES, FI, HU, IT; LT, LV, NL, PL and SE).

b) Illegal system interference
Article 4 of the Directive refers to illegal system interference. The Directive lists 8 possible acts (inputting computer data, transmitting, damaging, deleting, deteriorating, altering or suppressing such data, rendering it inaccessible) and 2 possible results of the respective act (seriously hindering or interrupting the functioning of an information system). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE and the UK (except for Gibraltar) have introduced corresponding legislative measures. BG refers only to inputting a virus, while for the rest of the Member States (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK and the UK), 1 or up to 4 of the possible acts are not specifically mentioned. In this context, it can be observed that most issues arose with the terms ‘deteriorating’ (lacking in 8 cases) and ‘rendering inaccessible’ (lacking in 9 cases).

c) Illegal data interference
Article 5 of the Directive covers illegal data interference and lists the following 6 possible acts: deleting, damaging, deteriorating, altering, suppressing data or rendering it inaccessible. CY, EL, IE and MT have literally transposed the provision; BE, CZ, LT, PT and SE used more generic terms to cover all the possible acts. All other Member States` transposition measures do not cover each of the possibilities but rather refer to only 5 alternatives (FI and SK) or less (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL, RO, SI and the UK). Most issues arose with ‘damaging’ (missing 8 times), ‘deteriorating’ (13 times), ‘suppressing data’ (11 times) and ‘rendering data inaccessible’ (13 times). In addition to the Directive`s wording, FI requires the 'intention to cause harm or financial loss' for criminal liability while LT and LV require the 'act to incur major damage or substantial harm'.

d) Illegal interception
Article 6 refers to illegal interception and targets the non-public transmission of computer data and electromagnetic emissions from an information system carrying such data. CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK and the UK (Gibraltar) have introduced legislation which fully covers Article 6. The general scope of the Directive referring to the interception of computer data is limited to messages (AT and BG), the observation of a person (EE) or correspondence (FR and HU). Furthermore, the following Member States` transposition measures do not cover the interception of electromagnetic emissions: BE, BG, EE, FR, HU,

IT, LT, LU, NL, PL, PT, SI and the UK (except for Gibraltar). In addition, some Member States require special intention (such as to gain knowledge or economic gain, or cause disadvantage — see AT, EL, HU) or specific additional acts (such as recording or becoming aware of the intercepted content — see BG and HU).

e) Tools used for committing offences

Article 7 criminalises a number of acts concerning tools such as computer programmes or access codes for committing the offences mentioned in Articles 3 - 6: the production of such tools, their sale, procurement for use, import, distribution or otherwise making available. AT, BE, CY, DE, EL, IE and SK have introduced corresponding national legislation. Some Member States do not cover all the referred offences (EE, IT, MT, PL and SI). Some do not refer to the Article 7 perpetrator as a person different from the offender of the mentioned offences of Articles 3 – 6 (CZ and SI). Some require a specific intention (to inflict damage or to act fraudulently - — see FI, IT and LU), a specific result such as breach of secrecy (BG) or at least a preparation level of the referred offences (SE). Finally, discrepancies between Article 7 and the national measures are found in the lack of transposition of all the possible acts listed. This is the case for BG, CZ, EE, ES, FR, HR, HU, IT, LT, LU, LV, PL, PT, RO, SI and the UK. Among these, LU`s legislation specifically mentions five of the six possible acts listed in the Directive, while the other Member States refer explicitly to only four or less.

Only ES has transposed the alternative of procurement for use.

2.3 General rules for the offences concerned (Articles 8 — 12 of the Directive)

a) Incitement, aiding and abetting

Article 8(1) requires the Member States to ensure that the incitement, or aiding and abetting to commit an offence referred to in Articles 3 - 7 is punishable as a criminal offence. All Member States have transposed this provision.

b) Attempt

According to Article 8(2), the attempt of the offences referred to in Articles 4 – 5 has to be punishable as a criminal offence. While PT does not cover all kinds of attempts to commit Article 4 offences and SE lacks criminal liability for the attempted offence of "breach of communications secrecy", all other Member States have in place legislation which transposes this provision.

c) Penalties

aa) General provision

Article 9(1) requires Member States, in general, to provide effective, proportionate and dissuasive criminal penalties for the offences covered by the Directive. While this is assumed for almost all Member States, AT, BE, BG, IT, PT, SE and SI do not meet the minimum levels of the maximum penalties set up in Article 9(2) (see section 1.1 above) for all cases. This affects the transposition of Article 9(1), as it can be concluded that the minimum requirements of Article 9(2) are a minimum for assuming an effective, proportionate and dissuasive criminal penalty.

bb) General minimum level of the maximum penalty

According to Article 9(2), the minimum level of the maximum penalty for the standard offences referred to in Articles 3 – 7 is a term of imprisonment of at least 2 years. Most Member States comply with this provision. Only 6 Member States show some discrepancies: AT (maximum 6-month term of imprisonment), BG (maximum 1 year of imprisonment for all offences except illegal interception,), IT (maximum 1 year of imprisonment for the offence of

Article 7 b)), PT (maximum 1 year of imprisonment for the offence of Article 3), SE (maximum 1 year of imprisonment for the offence of "infliction of damage") and SI (maximum 1 year of imprisonment for the offences of Articles 3, 6 and 7). In the case of BE, the minimum level of the maximum penalty for Articles 3, 6 and 7 is only reached when the offences are committed with fraudulent intent.

cc) A significant number of information systems affected

Article 9(3) raises the minimum level of the maximum penalties to 3 years of imprisonment when a significant number of information systems is affected by an offence referred to in Articles 4 and 5. In general, Member States have introduced corresponding legislation, DE refers only to information systems "which are of substantial importance to another", FI requires the assessment of the offence "as a whole" to apply the higher term of penalty, and LV does not refer to a significant number of information systems (or a similar wording), but only to causing "substantial harm". The information provided by BG and SI was not conclusive.

dd) Criminal organisations

According to Article 9(4)(a), a minimum term of 5 years of a maximum penalty of imprisonment applies for the offences under Articles 4 and 5 when committed by a criminal organisation as defined in Framework Decision 2008/841/JHA.

Again, most Member States comply with the provision of Article 9(4)(a). Under the criminal law of LU and SI, the provisions for an offence committed by a criminal organisation do not cover cybercrimes. BE`s legislation provides a maximum term of only 3 years of imprisonment for offences referred to in Article 5, DE`s legislation does not cover natural persons as victims of the offences, FI`s legislation requires an additional assessment of the offence "as a whole" and SE`s legislation provides a maximum penalty of 4 years of imprisonment for "gross infliction of damage".

ee) Serious damage caused

Article 9(4)(b) determines 5 years as the minimum term for the maximum penalty of imprisonment for any offence referred to in Articles 4 and 5 if serious damage is caused. Although there is no definition of what should be considered as serious damage, all Member States except BG, DE, FI, HU, LU and SE have introduced legislation which corresponds to the Directive. The information provided by HU was not conclusive. BG does not reach the minimum 5-year level of the maximum penalty, while LU refers to a general penalty clause for causing serious damage which does not cover any cybercrimes. There are minor discrepancies in DE (natural persons as victims of the offences not covered), FI (higher penalty requires additional assessment of the offence "as a whole") and SE (maximum of 4 years of imprisonment for "gross infliction of damage").

ff) Critical infrastructure information systems

The involvement of critical infrastructure information systems in offences referred to in Articles 4 and 5 also lead to a minimum of 5 years of the maximum penalty of imprisonment, as stated in Article 9(4)(c).

While most Member States comply with this provision, BG provided no specific transposition information. BE has set a maximum 3-year term for offences of Article 5. DE does not cover natural persons as victims. FI requires an additional assessment of the offence "as a whole", IT requires actually causing "destruction", PT requires an attack in a "severe and lasting manner" and does not refer to Article 5, and SE meets the Directive`s requirements only for the offence of "gross sabotage".

gg) Identity theft and other identity-related offences

Article 9(5) requires the Member States to ensure that for any offence referred to in Articles 4 and 5 which is 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 criminal offence. The wide range of discretion has led to a wide scope of transposition measures among Member States. BE and EL have not notified any transposition, and there is no specific provision in CZ`s criminal legislation. The aggravation approach has been chosen by AT, CY, ES, IE, MT, PT and SE (the latter referring to the circumstance of "special planning"), while all other Member States refer to extra provisions for the specific criminal offence. Among those referring to specific provisions, transposition issues can be observed as follows: BG and NL require a special intent ("to procure a benefit" and "the aim to disguise or misuse the identity"), DE refers only to "personal data not generally accessible", FR refers only to the name of a person and no other personal data, LV requires "substantial harm" caused, RO covers only the use of "a document" and requires the commission of deceit.

d) Liability of legal persons

aa) In general

Article 10(1) requires the establishment of liability of legal persons for the offences covered by Articles 3 – 8 if the offender has a power of representation of the legal person (a), has an authority to take decisions on behalf of the legal person (b) or has an authority to exercise control within the legal person (c). All Member States have introduced legislation corresponding to this Article with only the following minor issues: BG does not cover the offence of Article 6 and HR does not refer to an offender having an authority to exercise control within the legal person (Article 10(1)(c)).

bb) For lack of supervision or control

Article 10(2) requires Member States to introduce liability of legal persons when any offence referred to in Articles 3 – 8 has been allowed by the lack of supervision or control by a person referred to in Article 10(1). While almost all Member States comply with this provision, the information provided by LU was not conclusive and BG lacks a reference to the commission of an offence which falls under Article 6.

e) Sanctions against legal persons

aa) Mandatory sanctions

Article 11(1) of the Directive requires Member States to provide for criminal or non-criminal fines as effective, proportionate and dissuasive sanctions for legal persons. All Member States have notified complying national measures except for IE and UK. In these two countries, the maximum amount of possible fines remains undetermined due to the lack of concrete legislative provisions. Thus, neither the effectiveness nor the proportionality nor the dissuasiveness of the respective fines can be assessed.

bb) Optional sanctions

Article 11(1) continues with a list of possible options of additional sanctions for legal persons. These are: exclusion from entitlement to public benefits or aid (opted for by CY, CZ, EL, ES, HR, HU, LU, MT, PL, PT and SK), temporary or permanent disqualification from the practice of commercial activities (AT, BE, CY, CZ, EL, ES FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI and SK), the placing under judicial supervision (CY, ES, FR, MT, PT and RO), judicial winding-up (CY, CZ, EL, ES, FR, HR, HU,LT, LU, LV, MT, PT, RO, SI and SK) and the temporary or permanent closure of establishments which have been used for

committing the offence (BE, CY, WS, FR, LT, MT, PT and RO). This leaves BG, DE, EE, IE, FI, NL and the UK without having chosen any of the options.

cc) Sanctions for omission

According to Article 11(2), Member States have to ensure that effective, proportionate and dissuasive sanctions apply for legal persons who are liable for omission offences as referred to in Article 10(2). The information provided by LU was not conclusive. All other Member States except for IE and the UK have provided for corresponding legislative provisions. In the case of IE and the UK, the same issue arises for Article 11(1): (see point aa) above).

f) Jurisdiction

aa) Required jurisdiction grounds

Article 12(2) and (3) of the Directive requires Member States to determine their own jurisdiction for offences referred to in Articles 3-8 when the offence has been committed in whole or in part within their territory – be it that the offender was physically present there at the time of commitment or be it that the affected information system was located in the Member State's territory — or when the offence has been committed abroad by one of the Member State`s nationals. Most Member States have introduced corresponding national legislation, IT`s legislation does not determine jurisdiction for nationals abroad in the case of the basic offences, LV`s and SI`s legislation refer to unclear provisions regards territorial aspects, MT`s jurisdiction for partial commission on own territory is unclear and the UK refer to a computer instead of an information system.

bb) Other jurisdiction grounds

Article 12(3) provides that where Member States establish jurisdiction for cases where the offender has his or her habitual residence in the respective territory (opted for by AT, CY, CZ, IE, FI, HR, LT, LV, NL, SE and SK) or if the offence was committed for the benefit of a legal person established in the respective territory (CY, CZ, LV, PT, RO and SK), this should be communicated to the Commission.

2.4 Operational issues (Articles 13 – 14 of the Directive)

a) Provision on operational national points of contact

Article 13(1) calls on the Member States to establish operational national points of contact for the purpose of exchanging information relating to the offences referred to in Articles 3 to 8. On the basis of the provision, Member States need to ensure that procedures are in place to allow the competent authority to reply within 8 hours of receipt to any urgent request for assistance. According to the information notified, most Member States have set up the required infrastructure. IE and RO mentioned that the respective points of contact are only available for limited hours every day, which would not allow the authority to provide a reaction within 8 hours of receipt of a request in every possible case. Several Member States indicated that they are making use of existing networks of operational points of contact established through the G7 network or under the Council of Europe Budapest Convention on Cybercrime.

b) Information about the established operational national points of contact

Under Article 13(2), Member States are required to provide contact details of their points of contact to the Commission which will forward the details to the other Member States. All Member States have provided the necessary information.

c) Reporting channels
Article 13(3) requires Member States to ensure that appropriate reporting channels are made available in order to facilitate the reporting of the offences referred to in Articles 3 to 6 to the competent national authorities. The information provided by HR, IT, IE and PT was not conclusive. Of the remaining Member States, there appear to be different approaches to implementing the reporting channels. Most Member States (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK and the UK) have notified measures providing for channels to make reporting easier for the person or organisation initially reporting an offence, e.g. the victim of a cyberattack (with the actual reporting channels left unclear by LV). However, other Member States (AT, ES and LU) have provided identical information on the implementation of Article 13(1) and (2), from which it appears that their measures will mainly facilitate the communication between authorities.

d) Collection of statistical data
According to Article 14 (1) and (2), Member States must ensure that a system is in place for the recording, production and provision of statistical data, at least on the number of offences referred to in Articles 3 to 7 registered by the Member States, and the number of persons prosecuted for and convicted of these offences. Relying on the obtained notifications, most Member States appear to have put in place both legislative and administrative measures to ensure collection of the information, usually on the basis of a general national electronic system. Information from a number of Member States was not conclusive (EL, IE, UK (Gibraltar, Northern Ireland and Scotland)). One reason was that information on the specific offences referred to in the Directive may not be collected separately (BE, DE and SE) or the information collected may not cover all of the offences referred to in the Directive (RO).

e) Transmission of statistical data to the Commission
Article 14(3) calls on the Member States to transmit the respective statistical data to the Commission. All Member States who notified measures, except for the UK (Gibraltar, Northern Ireland and Scotland) and HU, have confirmed the implementation of either legal or administrative measures or both to ensure compliance with this obligation. For EL, ES, LU and SI, the information provided was not conclusive.

3. Conclusion and next steps

The Directive has led to substantive progress in criminalising cyberattacks on a comparable level across the Member States, which facilitates the cross-border cooperation of law enforcement authorities investigating this type of offences. Member States have amended criminal codes and other relevant legislation, streamlined procedures, and set up or improved cooperation schemes. The Commission acknowledges the major efforts by the Member States to transpose the Directive.

However, there is still considerable scope for the Directive to reach its full potential if Member States were to fully implement all of its provisions. The analysis so far suggests that some of the main improvements to be achieved by the Member States include the use of definitions (Article 2), which has an effect on the scope of offences defined by national law on the basis of the Directive. In addition, Member States appear to have found it challenging to include all the possibilities defining actions in relation to offences (Articles 3 to 7) and include common standards of penalties for cyberattacks (Article 9). Other issues appear to relate to the implementation of administrative provisions on appropriate reporting channels (Article 13(3)) and the monitoring and statistics for the offences included in the Directive (Article 14).

The Commission will continue to provide support to the Member States in their implementation of the Directive. In view of the potential contribution to cross-border cooperation, this refers especially to the operational provisions of the Directive on the exchange of information (Article 13(1) and (2)), reporting channels (Article 13(3)) and monitoring and statistics (Article 14). For this the Commission 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. In this context, to also support criminal investigations on attacks against information systems, cyber-enabled crimes and other types of crimes, the Commission is considering measures to improve cross-border access to electronic evidence for criminal investigations, including proposing legislative measures by the beginning of 2018.[8] The Commission is also considering the role of encryption in criminal investigations and will report on its findings by October 2017.[9]

The Commission is committed to ensuring that the transposition is finalised across the EU and that the provisions are correctly implemented. This includes monitoring that national measures comply with the corresponding provisions in the Directive. Where necessary, the Commission will make use of its enforcement powers under the Treaties through infringement procedures.

[8] Inception Impact Assessment on Improving cross-border access to electronic evidence of 4 August 2017, available at ec.europa.eu

[9] Communication on the Eighth progress report towards an effective and genuine Security Union, COM(2017) 354 final.