The Directive on attacks against information systems

A Good Practice Collection for CERTs on the Directive on attacks against information systems

ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Jo De Muynck (ENISA)

Hans Graux (Time.lex) and Neil Robinson (RAND Europe)

Contact

For contacting the authors please use cert-relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The drafting of this Good Practice Collection would not have been possible without the feedback and cooperation kindly provided by a large number of organisations and individuals. Without endeavouring to be exhaustive, the authors would like to thank the Belgian Federal Computer Crime Unit, the Bulgarian International Cyber Investigation Training Academy, the Cyprus Research and Academic Network Security CSIRT, the National Police Academy of the Czech Republic, the French Investigations Plateau of Cybercrime and Digital Analysis and Department for the Fight against Cybercrime, the Hellenic Data Protection Authority, the Irish UCD Centre for Cybersecurity and Cybercrime Investigation, the Italian Ministry of the Interior, CIRCL in Luxembourg, the Dutch National High Tech Crime Unit and National Crime Squad, the Portuguese FCCN.PT, CERT-RO in Romania, the Slovakian National Security Authority, SI-CERT in Slovenia, CNPIC in Spain, the Swedish Defence Research Institute, and Janet in the UK. At the EU level, the authors would also like to thank the European Commission – DG Home, Europol and EC3 for their kind assistance.

At the individual level, the authors are in particular grateful for the valued contributions made by Eric Freyssinet, Andrew Cormack, Serge Droz, Gorazd Božič, Marinos Stylianou, Alexandre Dulaunoy, Matej Breznik, Dan Tofan, Bruno Halopeau, Benoit Godart and Michael Palmer.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

Executive summary

This Good Practice Collection was produced at the initiative of ENISA in the context of its support activities to ensure the efficient functioning of CERTs/CSIRTs and their cooperation with law enforcement agencies (LEAs) in the face of a new development in European cybercrime policy.

In 2010, the European Commission published a Proposal for a Directive of the European Parliament and the Council on attacks against information systems[1]. This proposal was intended to further streamline the legal framework in the Member States in relation to the definition and punishment of certain cybercrime incidents, and tackled several challenges which were not adequately dealt with under prior rules, such as notably the creation, use and dissemination of cybercrime tools, the penalisation of illegal interception, the use of botnets, and identity theft.

The proposal was adopted by the European Parliament on 22 July 2013 and published in the Official Journal on 14 August 2013 as Directive 2013/40/EU. The Directive, which Member States will need to transpose by 4 September 2015, imposes new obligations, tasks and expectations on certain key stakeholders, including CERTs/CSIRTs, LEAs, security specialists, telecommunications service providers, etc.

This report serves two major goals, which both aim at supporting CERTs/CSIRTs:

- Firstly to provide an analysis of the legal framework created by the Directive, coupled with a stock taking on relevant existing national activities and good practices;
- Secondly, the identification of key areas and, where appropriate, guidelines and recommendations derived from these good practices

In this manner, the Collection endeavours to be a useful support tool for all stakeholders.

Disclaimer
This document provides background information mainly for the attention and digestion of members of CERTs in the EU Member States. It aims at explaining the potential outcomes and implications raised by the new Directive, in order to raise awareness. It by no means aims at giving guidance for the implementation process directly, but it will hopefully enable key players to make sound decision based on the information in this Collection.

[1] European Commission. 2010. Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. COM(2010) 517: http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf [Last accessed 0ctober 14, 2013]

Table of Contents

Executive summary iv

1 Goal of the Study and introduction to the Collection 1

1.1 Context 1
1.1.1 The Directive and potential challenges 2
1.1.2 Key Stakeholders for the Directive 4

1.2 Good Practice Collection 5
1.2.1 Objectives of the Collection 5
1.2.2 Methodology behind the Collection 6

2 Substantive criminal provisions in the Directive 9

2.1 Scope and contents of the Directive 9

2.2 Illegal access 9
2.2.1 Summary of interview outcomes 9
2.2.2 Identified good practices 9
2.2.3 Reflections on the findings 10

2.3 Illegal interception 10
2.3.1 Summary of interview outcomes 10
2.3.2 Identified good practices 11
2.3.3 Reflections on the findings 11

2.4 Tools for committing offenses 11
2.4.1 Summary of interview outcomes 12
2.4.2 Identified good practices 13
2.4.3 Reflections on the findings 13

3 Aggravating circumstances in the Directive 15

3.1 Scope and contents of the Directive 15

3.2 Botnets 15
3.2.1 Summary of interview outcomes 15
3.2.2 Identified good practices 18
3.2.3 Reflections on the findings 19

3.3 Identity Theft 21
3.3.1 Summary of interview outcomes 21
3.3.2 Identified good practices 23
3.3.3 Reflections on the findings 23

4 Cooperation and information exchange procedures in the Directive 25

4.1 Scope and contents of the Directive 25
4.1.1 Summary of interview outcomes 25

4.1.2 Identified good practices 26
4.1.3 Reflections on the findings 27

5 Data collection and reporting in the Directive 29

5.1 Scope and contents of the Directive 29

5.2 Data collection 29
5.2.1 Summary of interview outcomes 29
5.2.2 Identified good practices 30
5.2.3 Reflections on the findings 31

5.3 Reporting 31
5.3.1 Summary of interview outcomes 31
5.3.2 Identified good practices 31
5.3.3 Recommendations for the implementation 32

6 Conclusions – good practices and open issues 33

6.1 Good practices for the implementation of the Directive 33

6.2 Open issues and possible future actions 36

1 Goal of the Study and introduction to the Collection of Good Practice

1.1 Context

This Study is commissioned against the broader policy background of ENISA's activities that aim to support the efficient functioning of Computer Emergency Response Teams and Computer Security Incident Response Team (CSIRT) (CERTs/CSIRTs), and their cooperation with law enforcement agencies (LEAs), etc. Earlier efforts in this area have resulted i.a. in good practice guidelines and recommendations produced by ENISA, including[2] on:

- The setting up of CERTs[3];
- Running a CERT[4], including notably the studies "A flair for sharing - encouraging information exchange between CERTs"[5], "Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime"[6], and "Give and take - Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime"[7];
- Baseline capabilities of CERTs[8];
- Incident management[9].

Furthermore, a series of workshops have been organised[10], including in cooperation with Europol, and will continue to be organised in the future in order to strengthen the effectiveness of CERTs.

The present Study aims to build upon these outputs by examining a new challenge. In 2010 already, the Commission published a proposal for a Directive of the European Parliament and the Council on attacks against information systems[11]. This proposal was intended to further streamline the legal framework in the Member States in relation to the definition and punishment of certain cybercrime incidents, and tackled several challenges which were not adequately dealt with under prior rules,

[2] ENISA overview of support for CERTs: http://www.enisa.europa.eu/activities/cert/support [Last accessed 0ctober 14, 2013]

[3] ENISA. 2006. 'A step-by-step approach on how to set up a CSIRT'. http://www.enisa.europa.eu/activities/cert/support/guide [Last accessed 0ctober 14, 2013]

[4] Basic set of good practice on how to successfully run a Computer Security and Incident Response team (CSIRT): http://www.enisa.europa.eu/activities/cert/support/guide2

[5] ENISA. 2011. 'A flair for sharing – encouraging information exchange between CERTs' http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing [Last accessed 0ctober 14, 2013]

[6] ENISA. 2012. 'The Fight against Cybercrime Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime' http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/supporting-fight-against-cybercrime [Last accessed 0ctober 14, 2013]

[7] ENISA. 2012. 'Give and Take Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime' http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime [Last accessed 0ctober 14, 2013]

[8] ENISA National/governmental CERTs - Baseline Capabilities: http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities [Last accessed 0ctober 14, 2013]

[9] ENISA. 2010. Good Practice Guide for Incident Management http://www.enisa.europa.eu/activities/cert/support/incident-management [Last accessed 0ctober 14, 2013]

[10] ENISA workshops: http://www.enisa.europa.eu/activities/cert/events/past-events [Last accessed 0ctober 14, 2013]

[11] European Commission. 2010. Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. COM(2010) 517: http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf [Last accessed 0ctober 14, 2013]

such as notably the creation, use and dissemination of cybercrime tools, the penalisation of illegal interception, the use of botnets, and identity theft. As such, the proposed Directive would also repeal the existing legal framework at the EU level, specifically the Framework Decision on attacks against information systems.

The proposal was adopted by the European Parliament on 22 July 2013, and the final text was signed on 12 August 2013[12]. It was published in the Official Journal on 14 August 2013 as Directive 2013/40/EU[13], entering into force on 4 September 2013. The Directive, which Member States will need to transpose by 4 September 2015, imposes new obligations, tasks and expectations on certain key stakeholders, including CERTs/CSIRTs, LEAs, security specialists, telecommunications service providers, etc. These relate mainly to the operation of the existing 24/7 contact points (introducing a response deadline obligation), improving criminal justice/police cooperation, and the obligation to strengthen statistical data collection in order to support accountability and rational policy making. Some of these stakeholders will already have significant experiences on these points and will thus be likely to satisfy these requirements with relative ease. Others however will not have appropriate legislation, budget, experience, know-how, operational expertise or technological tools in place, and could therefore benefit in particular from good practices, including from other Member States.

This Study therefore comprised two main activities to support the implementation process, with particular view on supporting CERTs:

- Firstly the analysis of the legal framework and collection of data on relevant national activities and good practices;
- Secondly the identification of guidelines and recommendations derived from these good practices in order to support the Member States and their CERTs.

In the following subsections our approach towards these two activities will be presented.

1.1.1 The Directive and potential challenges

As noted in the introductory section above, Directive 2013/40/EU was already proposed as early as 30 September 2010, and replaces Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[14]. The new Directive retains most of the key features of the Framework Decision, but also introduces some new elements.

With respect to **substantive criminal law,** the Directive retained prior crimes from the Framework Decision – namely the penalisation of illegal access, illegal system interference and illegal data interference – but added criminalisation of certain tools for committing offenses, as well as the notion of 'illegal interception'. This will help keep EU level legislation in line with other international cybercrime initiatives, such as the Council of Europe's Cybercrime Convention, also known as the

[12] European Parliament. 2013. Judicial cooperation in criminal matters: combating attacks against information systems: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2010/0273%28COD%29&l=en [Last accessed 0october 14, 2013]

[13] Official Journalof the European Union. 2013. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA; OJ L 218/8, 14/08/2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF [Last accessed 0october 14, 2013]

[14] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 069, 16/03/2005: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML [Last accessed 0october 14, 2013]

Budapest Convention[15], and more importantly will allow the EU to act more effectively against more recent developments of cybercrime which were not yet adequately accounted for in the Framework Decision, such as the increased use of botnets, which could be qualified as a criminal tool under the Directive's provisions.

The 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. Finally, the Directive also introduces new and harmonised rules in relation to certain aggravating circumstances which result in an increased maximum term of imprisonment of at least five years (rather than two years, as foreseen by Framework Decision 2005/222/JHA). These aggravating circumstances again target primarily trends which are increasingly observed in the cybercrime field over recent years, and specifically include crimes:

> (a) committed within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA;
> (b) that cause serious damage; or
> (c) committed against a critical infrastructure information system.

Similarly, a new aggravating circumstance is introduced for crimes 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, a new provision which aims to tackle identity theft incidents by treating identity theft as an ancillary aggravating circumstance committed in conjunction with other crimes, such as fraud, hacking, etc.

Finally, a new substantive criminalisation was introduced in relation to botnets, described as committing the crimes of illegal system access or illegal system interference "where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose" (Article 9.3). This new provision aims to more effectively target botnet operators and/or (Distributed) Denial of Service ((D)DoS) attacks[16].

These substantive criminal law provisions, being included in a Directive, require transposition at the national level. This raises challenges of harmonisation, as divergences in phrasing or interpretation could lead to gaps in national cybercrime laws. For this reason, it is useful to consult stakeholders on what they perceive to be the main challenges in the implementation and application of these laws. This is highly relevant for the Directive, as some of the new provisions are somewhat contentious, such as e.g. the criminalisation of certain tools, which can be hard to apply considering the importance of such tools for penetration testing or white hat hacking[17], or the provisions on identity theft, which need to take into account nationally diverging stances on e.g. the permissibility of parody user accounts and satire (i.e. user accounts created under existing celebrity names that are used to clearly exaggerated positions that parody or satirize real opinions of the celebrity). Similarly,

[15] Convention 185 on Cybercrime, Budapest, 23 November 2001: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [Last accessed 0ctober 14, 2013]

[16] Defined as " an attack in which one or more machines target a victim and attempt to prevent the victim from doing useful work" in IETF RFC 4732; see http://tools.ietf.org/html/rfc4732 [Last accessed 0ctober 22, 2013]

[17] Also referred to as ethical hacking, the term generally refers to hacking undertaken without malicious intent and the particular objective of testing and improving the security of an information system; see e.g. http://en.wikipedia.org/wiki/White_hat_(computer_security) and http://www.eccouncil.org/Certification/certified-ethical-hacker [Last accessed 0ctober 22, 2013]

the Directive frequently relies on the notion of 'without right'[18], which is a concept that risks being applied in diverging ways. While some national differences are acceptable and expected (given the choice of a Directive as a regulatory instrument), alignment through the sharing of good practices is clearly advisable.

The same observations can be applied to the Directive's **procedural criminal law** provisions. Specifically, the Directive aims to improve 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 requests (at least in terms of whether the request will be answered, and the form and estimated time of the answer);
- introducing an obligation to collect basic statistical data on cybercrimes.

While these provisions were already introduced in the 2010 draft, their application in practice will be strongly affected through more recent policy developments, including the Commission's recent Communication on a European Cybercrime Centre (EC3) on 28 March 2012[19]. The Centre, which has started operations in January 2013[20] following a feasibility study conducted by RAND Europe[21], is to act as the focal point in the fight against cybercrime in the Union, serving four core functions:

- it should serve as the European cybercrime information focal point;
- it should pool European cybercrime expertise to support Member States;
- it should provide support to Member States' cybercrime investigations;
- it should become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

These functions imply that the EC3 could play a supporting role for the Member States, especially in facilitating their compliance with the procedural obligations imposed on the key stakeholders by the Directive. It is therefore useful to determine in the context of this study which of the stakeholders already have the necessary capabilities in places, and which good practices, recommendations or tips they can provide to their colleagues in other Member States.

1.1.2 Key Stakeholders for the Directive

As noted in the tender specifications, the Directive can have a significant impact on a number of stakeholders. Obviously, the direct addressees of the Directive are the legislators who will have to transpose the Directive into national law.

At the more operational level, the transposition will affect the decision and policy making bodies in EU Member States who are responsible for the establishment and operation of the national/governmental CERTs, and the national/governmental CERTs themselves. These are most

[18] Defined in the Directive as "conduct referred to in this Directive, including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law", Article 2 (d).

[19] European Commission. 2012. Communication from the Commission to the Council and the European Parliament: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf#zoom=100 [Last accessed 0ctober 14, 2013]

[20] European Cybercrime Centre (EC3): https://www.europol.europa.eu/ec3 [Last accessed 0ctober 14, 2013]

[21] The Feasibility study can be found here: http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf [Last accessed 0ctober 22, 2013]

directly impacted by the operational changes envisaged by the Directive, and were therefore the largest group of stakeholders contacted during the data collection of this Study.

Apart from the national/governmental CERTs, private CERTs who lack a formal governmental mandate could also play a significant role in ensuring the correct functioning of key national communication networks. In the course of their operations, they commonly need to work with national/governmental CERTs, law enforcement agencies, or other enforcement bodies such as data protection authorities (DPAs) and telecommunications supervisory bodies. Therefore, they constitute a group of stakeholders that should be considered as well.

Given the pivotal role that law enforcement will play in the application of national transpositions, it is important, in order to get the most complete possible picture, to chart in an appropriate manner the opinions and best practices within national law enforcement bodies, and their current and future collaboration mechanisms at the cross border level, including via the recently formed EC3, operating within Europol.

The composition of the stakeholders consulted throughout the data collection reflected this heterogeneity, covering not only national/governmental CERTs, but also other CERTs, law enforcement bodies, policy makers and other sectoral supervisory/policing bodies such as DPAs and telecommunications supervisors. In the methodological sections below, we will explain how this goal was achieved, and a list of interlocutors will be provided.

1.2 Good Practice Collection

1.2.1 Objectives of the Collection

This Good Practice Collection identifies the potential implications of the Directive on stakeholders as identified above. Proposals and recommendations to the stakeholders are included in this Collection when appropriate, based on observed and identified best practices in the Member States, as well as requests and observations on gaps made by interviewees. Opinions on the above therefore come directly from the potentially affected stakeholders.

As a practical point to assist in the interpretation of the report, it should be noted that data was collected and analysed prior to the adoption of the Directive. The questions and analysis below were therefore conducted on the basis of the draft text of the Directive[22], which underwent minor phrasing/structuring changes during its finalisation. The analysis below has been updated to reflect the final version of the Directive, and the findings have been validated through a workshop held on the 4th October in The Hague, The Netherlands, to ensure that they remain relevant. However, some of the questions below refer to proposed changes that were not ultimately retained in the finalised Directive; in such cases, this is clearly identified in the analysis itself.

The Collection specifically focuses on potential implications of the Directive in the Member States based on their existing legislation and practices[23] and addresses how it is relevant for CERTs and other stakeholders, and what potential future actions could be taken by all of them.

[22] European Commission. 2010. 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: http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf [Last accessed 0ctober 14, 2013]

[23] For an overview of cybercrime related legislation (not necessarily current or exhaustive), we can refer to the overview created by the Council of Europe; see http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/ [Last accessed 0ctober 22, 2013]

1.2.2 Methodology behind the Collection

In the first stage of the project, at least one representative from all Member States was invited to participate in a phone interview on the potential impact and challenges presented by the Directive, and on any best practices/lessons learned from their Member State. The representatives were taken from a wide range of stakeholder groups to ensure that all relevant perspectives were taken into consideration.

Ultimately, feedback was obtained from 18 Member States. While some participants indicated that they would prefer not to be identified and the list below is therefore not exhaustive, the following stakeholders among others contributed to the data used in this study:

Member State	Affiliation
Belgium	FCCU
Bulgaria	International Cyber Investigation Training Academy
Cyprus	Cyprus Research and Academic Network Security CSIRT
Czech Republic	National Police Academy of the Czech Republic
France	Coordinator of the Investigations Plateau of Cybercrime and Digital Analysis (*Plateau d'Investigation Cybercriminalité & Analyses Numériques – PI CyAN*), and Head of the Department for the Fight against Cybercrime
Greece	Hellenic Data Protection Authority
Ireland	UCD Centre for Cybersecurity and Cybercrime Investigation
Italy	Ministry of the Interior
Luxembourg	CIRCL
Netherlands	National High Tech Crime Unit (Team High Tech Crime) National Crime Squad (*Dienst Landelijke Recherche*) Netherlands' Police (*Nationale Politie, landelijke eenheid*)
Portugal	FCCN.PT
Romania	CERT-RO
Slovakia	National Security Authority
Slovenia	SI-CERT
Spain	CNPIC

Sweden	Swedish Defence Research Institute
United Kingdom	Janet

Each interview was summarised in a brief (3-5 page) report, which was subsequently sent back to each interviewee for validation.

The present report contains a comparative analysis of the responses, structured along the same topics as the interviews themselves, i.e. the substantive criminal provisions of the Directive (section 2 below), the aggravating circumstances surrounding botnets and identity theft (ID theft) (section 3), international cooperation and information exchange (section 4), and finally data collection and reporting (section 5). In each of these sections, we have set out:

- A **summary** of the **interview outcomes**, i.e. frequently recurring responses and general trends in the feedback; this may contain both positive and negative feedback on the Directive from the interviewees, as well as their lessons and experiences on each topic;
- **Identified good practice**s, i.e. positive lessons from specifically identified countries that may be transposable to other countries; these are typically grouped per stakeholder;
- **Recommendations** for the implementation, i.e. guidance towards Member States on implementation choices, generally containing both the good practices identified earlier and any additional recommendations that have been suggested by interviewees, even if there was no existing good practice in any Member State yet. Thus, the recommendations not only identify what exists in at least some Member States, but also indicate any gaps that need to be filled in the future. As with the good practices, recommendations are typically grouped per stakeholder.

Through this methodology, the Good Practice Collection presents an overview of the state of the art, including the lessons learned by the various stakeholders, and aims to provide useful suggestions and guidance for implementation activities.

This report was circulated among the ENISA Expert Group, constituted largely of persons interviewed in the course of this Study, in order to ensure the validity and representative character of the findings and recommendations. The report was thereafter discussed during an Expert Group meeting in The Hague on 4 October 2013, and subsequently updated to reflect the suggestions. It should be noted however that this report contains opinions, suggestions and recommendations originating from various parties, and that these do not necessarily reflect any ENISA position.

2 Substantive criminal provisions in the Directive

2.1 Scope and contents of the Directive

With respect to substantive criminal law, the Directive retains prior crimes from the Framework Decision – namely the penalisation of illegal access, illegal system interference and illegal data interference – but adds criminalisation of certain tools for committing offenses, as well as the notion of 'illegal interception'. This will help keep EU level legislation in line with other international cybercrime initiatives, such as notably the Council of Europe's Cybercrime Convention, and more importantly will allow to act more effectively against more recent developments of cybercrime which were not yet adequately accounted for in the Framework Decision, such as the increased use of botnets, which could be qualified as a criminal tool under the Directive's provisions.

2.2 Illegal access

With respect to the crime of illegal access (hacking), the initially proposed Directive brought an interesting change as compared to the prior Framework Decision. The Framework Decision allowed Member States to decide that the conduct was incriminated only where a security measure was breached (i.e. unlawfully accessing an unprotected information system was not required to be criminalised in the Member States). The proposal for a Directive as studied below did not retain this option, and illegal access would always be considered as a crime, irrespective of whether a security measure was breached.

However, the ultimately adopted Directive (finalised after the interviews in this study were already completed) reintroduced the terminology of the Framework Decision, noting that criminalisation of illegal access was only needed "where committed by infringing a security measure". The legal framework was thus ultimately not changed, and the comments below are therefore mainly useful as an exercise examining the potential impacts of changing this rule.

2.2.1 Summary of interview outcomes

The interviews showed that the legal framework in most countries was brought in line with the requirements of the original proposal for a new Directive: either the legislation never required a breach of security measures, or such a requirement had been removed in preceding years (e.g. in the Netherlands). Of the 18 interviewed countries, only the Czech Republic indicated that a security breach requirement was retained as a requirement in the law. Bulgaria noted that its legislation was generally very strictly interpreted by judges, and that the 'without permission' criterion would generally be interpreted as requiring that there is a lock or other security measure which needs to be broken.

Interviewees in other countries (e.g. France and Italy) noted a similar perspective: even in the absence of an explicit legal requirement, security breaches would always play a significant role in the assessments made by judges: in the absence of security measures, the unlawfulness of access attempts would be significantly harder to demonstrate.

As noted above, the Directive does not require any changes as compared to the Framework Decision, and legislation in all Member States can thus remain 'as is'.

2.2.2 Identified good practices

The primary challenge in relation to this provision in the Directive clearly relates to the interpretation of unlawfulness of access attempts: especially in the absence of security measures

that were breached, it can be hard for prosecutors to decide when to initiate legal proceedings in countries that permit prosecutors to exercise discretion on this point.

The presence of security measures can be indicative: in the absence of security measures, accidental access is more likely. E.g. a recent decision from a French court found that access to documents on an unsecured webserver did not constitute illegal access, since they were made freely accessible to the public[24].

Coherence on this issue is important to avoid arbitrary enforcement, and to avoid courts being overburdened with seemingly trivial cases.

A number of countries have therefore reported the existence of prosecution guidelines that assist in the interpretation and the application of the law. E.g. the United Kingdom reported the existence of prosecution guidelines within the Crown Prosecution Service, which help in the interpretation of laws and prioritisation of prosecutions[25]. Similar but non-public guidelines were reported in Sweden, and Portugal reported the existence of guidance documents for judges (but not for prosecutors).

2.2.3 Reflections on the findings

To reduce legal uncertainty, it could be advisable for countries to publish guidance on the interpretation and application of the unlawful access provisions, and particularly on the element of intent (i.e. the unlawfulness – without right) in cases where no security measures were breached, if this is permitted under national law. This can be done in the form of prosecution guidelines in countries that permit this, and/or in the form of jurisprudence overviews to show how courts apply the law in reality.

Collection and dissemination of such guidance at the EU level could also help to ensure homogeneous application of the law across the European territory.

2.3 Illegal interception

The offense of illegal interception was newly introduced in the Directive. It requires Member States "*to ensure that the intentional interception by technical means, of non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed without right.*"

2.3.1 Summary of interview outcomes

The provision is very similar to Article 3 of the Cybercrime Convention on which it was based. As a result, most countries could logically be expected to already have implemented suitable legislation.

[24] Tribunal de Grande instance de Créteil 11ème chambre correctionnelle Jugement du 23 avril 2013: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3739 [Last accessed 0ctober 14, 2013]

[25] The Crown Prosecution Service. *Computer Misuse Act 1990*: http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/ [Last accessed 0ctober 14, 2013]

The interview summaries showed that this was indeed the case: no interviewee indicated that legislation covering illegal interception was unavailable in their jurisdiction. However, a small number of countries (notably Luxembourg, Bulgaria and Slovakia) noted that their legislation on this offense was currently being revised or tightened, as a part of the implementation of the Budapest Convention, or in response to recent incidents where wiretaps were used inappropriately. This illustrates a broader trend: many of the respondents spontaneously linked provisions on wiretaps organised by law enforcement as an investigative measure to provisions on illegal interception as envisaged by the Directive; likely because transgressions of rules on the former would result in a violation of the latter.

The CERT from Luxembourg noted a particular concern, namely that excessively broad legislation could impact e.g. the analysis of how malware works. What is non-public communication, e.g. in a company network? Is monitoring how malware works in a system illegal interception? The law on this point should be clear, to ensure that CERTs (or other investigators outside of law enforcement) are not accused of interception simply because of an investigation of hacker activity. The provision in the Directive states that only acts committed without right are considered unlawful, and regular activities of CERTs should therefore not be interfered with. None the less, the CERT noted that there should be more explicit guidance to ensure that the normal activities of CERTs aren't considered to be criminal, not so much because of a real risk of criminal investigation to CERTs, but mainly because such discussions take up time and resources.

2.3.2 Identified good practices

No unique good practices were identified on this topic, but the concern outlined above by Luxembourg could be similarly addressed by guidance documents. Thus, the same good practices as discussed above under illegal interception could apply here as well.

2.3.3 Reflections on the findings

Similar to the above, uncertainty could be reduced through the publication of guidance on the interpretation and application of the illegal interception provisions, and particularly on the legitimacy of the activities of CERTs and network operators themselves.

Collection and dissemination of such guidance at the EU level could also help to ensure homogeneous application of the law across the European territory.

2.4 Tools for committing offenses

The Directive introduces a new offence related to tools used for committing offences, defined as follows: Member States must "*ensure that 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 in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:*"

> (a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences above;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

2.4.1 Summary of interview outcomes

As with the offence of illegal interception above, this provision is very similar to Article 6 of the Cybercrime Convention on which it was based[26]. Thus, it could again be expected that most countries had already implemented it prior to the adoption of the Directive.

Indeed, the feedback obtained during the interviews confirmed that this was the case: of all the interviewed respondents, none indicated that provisions on tools for committing offenses were missing in their jurisdictions. However:

- One respondent (Sweden) was not sufficiently aware of legislation on this point, and thus could not provide conclusive information on Swedish law.
- Three respondents (Portugal, Slovakia and Slovenia) indicated that there was no unique provision on ICT tools specifically, but rather that existing generic provision on tools for committing crimes were applied. E.g. in Slovenian law the applicable provision is the articles on the manufacture or production of weapons for a criminal act: the same rules are applied to possession, manufacturing, selling, distributing, importing/exporting of tools for illegal access to information systems.
- Some respondents however also indicated that the existing rules were somewhat too generic to be applied consistently. This was the case for the legislation in Bulgaria and Slovakia. In Bulgaria for instance, a challenge is that the concept of a 'tool' is not defined in Bulgarian law (or in EU law). As a result, judges are very careful in applying this concept. It is thus likely that Bulgarian criminal law will need to be made more explicit to address this issue before judges are systematically willing to apply/enforce it.
- Other countries signalled either no need to update their legislation at all, or only on minor points (e.g. procurement for use of tools is not yet included in Portuguese law whereas it is included in the Directive; thus, the law would need to be amended on this point).

The interviewees were also polled on the well-known debate of whether the Directive's rules were sufficiently clear to ensure that CERTs, academic researchers, security professionals etc. could operate lawfully. Whether this is the case or not depends on the interpretation of the Directive's language, and specifically on whether the tools are produced, sold, etc. 'without right for the purpose of committing any of the offences'. Here, there was a distinction between respondent profiles:

- Respondents representing law enforcement or policy makers almost unanimously noted that this debate was largely academic, and that there were no known cases of actual unwarranted prosecutions in practice. They were satisfied that the language of the Directive would be appropriate and sufficient to safeguard lawful activities.
- Respondents representing CERTs were less certain: while most were confident that the provisions would never be applied to them, some still expressed doubts. This was notably the case in Luxembourg and the Czech Republic. These respondents called for a clearer confirmation that the normal activities of CERTs, academic institutions, researchers, network operators and security service professionals would be exempted from the scope of

[26] Convention 185 on Cybercrime, Budapest, 23 November 2001: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [Last accessed 0ctober 14, 2013]

application of this provision, as should any actions at the lawful request of businesses, governments and end users.

A respondent from Ireland also noted a separate concern, namely the involuntary use of such tools, such as the JS-LOIC tool (a javascript implementation of the Low Orbit Ion Cannon software used to commit DDoS-attacks). Once integrated on a website, any visitor of that website automatically and possibly unknowingly participates in a DDoS-attack on a preconfigured target. The provisions on tools could target unwitting participants in such attacks, since law enforcement and criminal investigators have no way of distinguishing such unwitting users (who have no criminal intent and therefore would not be targeted by the criminal provisions of the Directive) from willing participants (who visit the site with the intent to participate in a DDoS attack and therefore would fall within the scope of the Directive). The provision could thus be hard to apply in such cases.

Thus, while the purpose-oriented language was seen as positive, more explicit legal carve-outs (excluding criminal liability for clearly lawful activities) were seen as desirable for some respondents.

2.4.2 Identified good practices

Most countries had directly implemented the legislation already, and notable good practices were therefore rare. However, the French experiences were instructive: the applicable provision in French criminal law states that creation, owning, distribution without legal motive is a crime. The interviewee noted that practical cases on this issue were rare, this is probably because the Parliament in France explicitly discussed the fact that security and research purposes constituted a lawful motive for keeping the tools, removing most of the doubt. The uncertainty thus seemed to be largely theoretical. Cases do still occur, however: in a practical case, a company was prosecuted for publishing exploits and actual code that allowed their exploitation; this was considered unlawful[27]. None the less, the clear Parliamentary debate seemed to have deflected some of the concerns.

2.4.3 Reflections on the findings

Based on the observed feedback, three sets of suggestions could be forwarded which are based on good practices or suggestions from interviewees:

- Firstly, **implementing legislation should be clear and explicit, and include clear carve-outs of the applicability of the provision** for the normal activities of CERTs, academic institutions, researchers, network operators and security service professionals, and any actions undertaken at the lawful request of businesses, governments and end users.

[27] Criminalités numériques weblog. 2009. 'Est-il illégal de publier des failles de sécurité?' http://blog.crimenumerique.fr/2009/12/24/est-il-illegal-de-publier-des-failles-de-securite [Last accessed 0ctober 14, 2013]

- The respondent from one of the countr suggested that a pure legislation based solution would not be ideal, as legislation would never be able to consider every abstract possibility that might occur in practice. Rather, he suggested that **it should be up to the security community itself to come up with guidelines and recommendations on how to comply with the law**, e.g. on responsible disclosure. It is not the task of lawmakers or prosecutors to define all the details through legislation or interpretative documents. **This recommendation should be applied at the international level**: it would be beneficial for the industry and academia itself to formalise its good practices to remove or at least reduce any sense of unease. That would give judges a baseline of criteria to appreciate cases.
- The Irish respondent suggested that future initiative might further consider **the responsibility and liability of service providers, e.g. operators of websites which run outdated software with known security vulnerabilities**. The interviewee noted that it could be useful to at least place some degree of responsibility/liability for damages resulting from the hacking of such systems with the operators. Irrespective of technical awareness of the website operator, they should at least have some responsibility for choosing/maintaining functioning and secure systems. A similar suggestion of economic incentivisation was provided by the national CERT from Luxembourg, noting that the original owner of a breached system should perhaps bear some liability as well, in order to incentivise proper security practices. Perhaps even financial/fiscal incentives could be considered to encourage security investments. While technically out of scope of the implementation of the Directive, the suggestion may still be useful for future cybersecurity policy actions.

3 Aggravating circumstances in the Directive

3.1 Scope and contents of the Directive

The Directive aims to increase the penalties for certain crimes, and introduced a new set of aggravating circumstances in order to more effectively address identity theft and botnets. Specifically:

- Under the Framework Decision, the maximum penalty for committing crimes in the framework of a criminal organization was at least 2-5 years. In the Directive, this is uniformly set at 5 years, i.e. the upper bound of the previous range. This should increase penalties for organized criminal activity, and would thus help the fight against criminal gangs engaged in identity theft or the use of botnets.
- The Framework Decision allowed (but did not require) the same penalty (2-5 years) when the offense caused serious damages or has affected essential interests. The Directive requires the same uniform (5 year) penalty for the same circumstance, as well as when the crimes are committed against a critical infrastructure information system.
- In addition, a 3 year penalty applies when botnets are used ("*where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose*");
- Finally, for identity theft ("*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*"), Member States must ensure that this may be qualified as an aggravating circumstance under national law.

Given that the increase in maximum penalties is not susceptible to good practices (all penalties are merely required to be increased when needed, without much margin for creativity), the interviews mainly focused on provisions and practices in relation to botnets and identity theft. The outcomes will be briefly discussed below.

3.2 Botnets

3.2.1 Summary of interview outcomes

Under the Directive, Member States are required to ensure that the crimes of illegal system interference and illegal system access "*are punishable by criminal penalties of a maximum term of imprisonment of at least three years where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose*" (Article 9.3). Thus, botnets are addressed as the outcome of a tool (namely the software used to take over the systems constituting the botnet) designed to launch attacks via the botnet ('a significant number of information systems').

To identify good practices, interviewees were mainly asked whether their countries had already implemented legislation addressing botnets (including as an aggravating circumstance), and what the operational practices in their countries were that could be used as a good practice.

With respect to **existing legislation**, none of the interviewees indicated that specific legislation had been adopted in their respective countries to address botnets, either as a separate crime or as an aggravating circumstance. In practice, botnet attacks are universally dealt with at this time through existing legislation, such as illegal access (hacking), fraud, forgery, conspiracy to commit a crime etc., depending on the impact of botnet activity.

In the UK however, existing legislation was amended to ensure that botnets could be comprehensively addressed, without mentioning or defining botnets precisely: up until 2006, builders of botnets were clearly committing an offense, but users of botnets (the botnet herders) weren't necessarily. Existing provisions focused on unlawful access, and builders (who infected third party machines) were guilty of that crime. However, botnet herders who launched e.g. DDoS attacks didn't fall under this rule. Therefore, changes in the legislation were needed, and separate rules for (D)DoS attacks were introduced. Under the amended Section 3 of the Computer Misuse Act[28], it is an offence to deliberately or recklessly impair the operation of any computer or program, or reliability of data, or to prevent or hinder access to data. That includes both the previous offence of unlawful modification of data, and any additional DoS activities.

Several interviewees expressed concerns or reservations about amending legislation: both Bulgaria and Luxembourg indicated that botnets would fall under the broader umbrella of unlawful tools, and that this is a notion that is not very clearly defined under the Directive. For instance, the question could be presented whether grids[29] are also a form of botnet, or peer-to-peer (P2P) networks[30], or partially distributed communication networks such as Skype? There is a clear concern that newer and more specific legislation could inadvertently create new legal discussions rather than solving them: the Belgian interviewee noted that the definition in the Directive could actually make it harder to pursue cases, because defendants might try to argue on technicalities: e.g. what is "a significant number of information systems"? The inclusion of these criteria in the law could actually have an adverse effect of giving defendants new elements to attack in their prosecution. Thus, any new legislation should be implemented only if strictly necessary to achieve the objectives of the Directive, and would need to be sufficiently precise to avoid creating new loopholes.

With respect to **operational practices**, the feedback provided by the interviewees was more substantive and contained useful guidance from the perspective of CERTs, law enforcement bodies, data protection supervisors and policy makers:

- **CERTs** often face the practical challenge of what they are allowed to do in case of botnet incidents. Some CERTs note that they did not report incidents to law enforcement proactively, leaving this up to the victims, whereas others would inform law enforcement themselves independent of any complaints. Taking forceful action by disconnecting infected systems was only done by CERTs that had been explicitly authorised to supervise and police well-defined networks, such as academic or military CERTs for their own academic or military networks, and only on a limited scale. Outside of that specific context, CERTs can only provide recommendations to network operators on how to address incidents, which the operators could then choose to follow on a voluntary basis. However, such CERTs cannot

[28] *Police and Justice Act, 2006*: http://www.legislation.gov.uk/ukpga/2006/48/section/36 [Last accessed 14 October, 2013]; and see *Computer Misuse Act 1990*: http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/#an09 [Last accessed 14 October, 2013] for guidance on its interpretation and application.

[29] Grid computing can be defined as a system that coordinates resources that are not subject to centralized control, using standard, open, general-purpose protocols and interfaces to deliver nontrivial qualities of service. I.Foster, "*What is the Grid? A Three Point Checklist*", Argonne National Laboratory & University of Chicago; see http://dlib.cs.odu.edu/WhatIsTheGrid.pdf [Last accessed 22 October, 2013]

[30] Peer to peer networks can be defined as a type of decentralized and distributed network architecture in which individual nodes in the network (called "peers") act as both suppliers and consumers of resources. R. Schollmeier, "*A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications*", Proceedings of the First International Conference on Peer-to-Peer Computing, IEEE (2002); see http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=990434 [Last accessed 22 October, 2013]

impose specific actions. Standard procedures for dealing with botnets are generally not available.

- **Law enforcement bodies** noted that they generally took a passive role, as active monitoring of networks was either not legally possible or created privacy concerns. However, they signalled that many operators (network operators or website operators) do monitor their own networks, but are often uncertain as to what they can legally do when they see anomalous behaviour. Passing on information to law enforcement causes them concern, because it would require an acknowledgement that they monitor and analyse their users. Even if this is only done to identify and address incidents, it could still give rise to privacy concerns. For the identification of command & control nodes in a botnet, this means that the information is often available, but operators are reluctant to hand it to law enforcement bodies without a court order, due to privacy compliance concerns. De facto, that means that botnet incidents can go unreported: operators are unwilling to risk the publicity of filing a report and are content if an incident can be resolved quietly, and law enforcement is typically unaware of incidents unless it is reported.
- In some cases, botnets have been addressed through **joint coordinated action between law enforcement, CERTs and the private sector**. Responses on such actions are positive, although law enforcement bodies stress the need for their involvement. A concern has been noted that solo-actions from the private sector (including private CERTs, security companies etc.) without the backing of law enforcement may be effective in shutting down isolated incidents, but ultimately leave criminals unharmed and free to resume their activities. Such actions can furthermore harm ongoing investigations, as crucial data might be destroyed or corrupted, making it unusable as evidence in potential criminal proceedings.
- In **international botnet cases**, it is worth noting that the feedback universally indicated that CERTs frequently interacted with other foreign CERTs and occasionally with foreign operators, but virtually[31] never directly with foreign law enforcement bodies. In such international botnet cases, CERTs would work exclusively with their own national law enforcement bodies, or would attempt to resolve the attack without involving law enforcement at all.
- As was already well established through prior studies, **data sharing between operators, CERTs and law enforcement is problematic due to data protection concerns.** The interpretation that an IP address is always personal data was mentioned as an anomaly that raised constant issues of compliance even in the absence of significant privacy risks. E.g. if a software company sent out a list of IP addresses that are seemingly infected with a virus within the Zeus botnet, then the CERT felt that it would have to file notifications with its data protection authority; the same would apply of this information was then sent on by the CERT to ISPs. This example provided by an operational CERT, whether correct or not, shows the need for guidance on this point. Some good practices have been observed however that are used to address or mitigate this problem.
- CERTs occasionally but not systematically work closely with **data protection authorities and/or telecommunications regulators** in their countries. In e.g. the Czech Republic such contacts were found to be useful to obtain guidance on data protection compliance. In other countries, contacts with supervisors were limited due to the perceived lack of competences or resources with these bodies.
- A frequently related frustration from the side of CERTs was that **information exchanges with law enforcement tend to be unidirectional**: from CERT to law enforcement, but rarely the

[31] In a rare number of instances, CERTs reported working directly with foreign law enforcement, such as the FBI.

other way around. This is known and understood to be necessary to protect the secrecy of ongoing investigations. However, it would still be useful to CERTs if investigators could inform them of steps taken and expected future actions at a high level, without going into specific details in a case, merely to know what (if anything) happened and to see how CERTs could streamline their activities and improve their usefulness.

3.2.2 Identified good practices

With respect to legislation, only one country (the UK) had modified its legislation to ensure that botnets could be addressed. As noted above, an update in 2006 was deemed to be necessary to ensure that botnet herders who used a botnet without necessarily having infected any machines themselves could also be prosecuted. This can be considered a good practice, as it covered a legislative gap through generic language: it became an offence to deliberately or recklessly impair the operation of any computer or program, or reliability of data, or to prevent or hinder access to data. The provision also avoided the pitfall of introducing new technology specific concepts.

On the operational front, several good practices have been observed that could serve as examples for other countries:

- For CERTs, the definition of a clear mandate is crucial:
  - **Private CERTs** and academic CERTs benefit from implementing clear agreements with their constituency that define precisely what their remit and competences are. This was e.g. observed in the UK through Janet, which can intervene within the networks that it supervises (principally university networks), on the basis of the policy agreements that it has concluded with the network operators. Principal responsibility still lies with the universities, since they are the only ones who know exactly what the impact of interventions will be.
  - **Public CERTs** benefit from a clear legal framework that grants them clear authorities and powers. For instance, the Swedish MilCERT has a clear legal mandate established by law, and Swedish law requires public authorities to cooperate with each other in the investigation of incidents. This can often facilitate interactions between the CERT and law enforcement.
- The Dutch national CERT noted the importance of **working in partnership with representatives of key sectors, including a number of large telcos and banks**. This partnership includes frequent meetings that allow all stakeholders – law enforcement, CERTs and private companies – to identify and address issues that the private sector faces through an ISAC (Information Sharing and Analysis Center).
- **International cooperation with other CERTs is supported by the Trusted Introducer and FIRST networks**. Among others, the Romanian CERT-RO noted that these were considered to be trust frameworks, since all member CERTs have to sign certain paperwork and accept certain obligations.
- To facilitate **data sharing between operators, CERTs and law enforcement**, it is worth noting that no country reported having received clear guidance from data protection authorities on how to comply with data protection law. It should however also be noted that the Greek DPA that was interviewed indicated that it had not received any requests on this point, and that it would be open to providing constructive advice, which it believed would not be prohibitive. Positive experiences were reported notably in Slovenia. After a recent DoS attack, the national CERT published an advisory for ISPs on how to proceed, including a recommendation to conduct some network monitoring and traffic analysis. This advisory resulted in a critical comment via Twitter, stating that this advice was illegal as a violation of Slovenian data protection law. The CERT retweeted

this message to the Information Commissioner, who replied – also via Twitter – that it considered such monitoring and analysis to be lawful and proportionate to the danger that such an attack could cause, as the law could not be reasonably expected to define every possible hypothesis in which data would need to be processed. This was useful, because it resulted in a quick, public and highly visible communication towards CERTs, ISPs and the Internet community. More generally, the CERT noted that it was very aware of the need to explain carefully what analysis they do and why, as this proportionality and transparency is important to keep trust of their stakeholders. In case of grey areas, the CERT maintains a good relationship with the Information Commissioner to obtain quick advice when needed. This was noted to be important to keep the trust of the community.

- When addressing botnets, most CERTs lacked any **standardised process or playbook for taking appropriate action to respond to botnets**, and decided on this on a case by case basis. The Romanian CERT however noted that there was a standard procedure for responding to botnets, which is followed in each case to ensure that all incidents are handled in the same manner. Similarly, the French Gendarmerie reported that they are currently devising a standard procedure for basic malware distribution (small botnets). The idea is to help others through improved international cooperation: the collected information could be proactively shared with international law enforcement partners. The strategy will also include procedures for dealing with assistance requests from ISPs or from CERTS (in France and abroad), and also push the collected information via Europol to other countries (third countries, including Russia, Ukraine, etc.).

3.2.3 Reflections on the findings

Based on the analysis and good practice discussed above, a number of suggestions can be derived.

With respect to legislation, given the concerns outlined above, it seems advisable to **assess whether new legislation is necessary to achieve the effects of the Directive under existing law, and if so, to implement the required changes through generic and technology neutral language.** This would achieve the desired outcome of fighting botnets, while avoiding the risk of putting in place language that creates new technical discussions on what constitutes a botnet, and whether the thresholds for botnet prosecution have been cleared. The example of the UK is instructive in that respect.

Operationally, one of the main challenges is that most CERTs have no **guidelines on how botnets can be dealt with. Standardised guidance on this point, preferable on at least the EU level, would be useful**, e.g. covering the questions that CERTs would need to ask, what information and recommendations they should provide, and what could proportionately and lawfully be done. This would also be useful to strengthen the image and perceived effectiveness of CERTs (and law enforcement) for criminals. This guidance would also **need to take into account the different mandates and tasks that CERTs may have**: private CERTs can benefit from contractual agreements with their constituency as seen in the good practices noted above, whereas public CERTs benefit from a clear relationship with law enforcement bodies (either by liaising systematically, or by the integration of seconded law enforcement officials).

The **mandate of CERTs needs to be clearly defined, taking into account the consequences of any choices made in this respect**. Private CERTs can benefit from legal agreements with their main constituency, which can serve as a legal basis for data sharing and which can limit the responsibilities and liabilities of the CERT. Public CERTs can benefit from a mandate established by law that defines their responsibilities and competences; however, their position is made more delicate because of the need to keep the functions of CERTs and law enforcement separate. While a close integration of CERTs and law enforcement has clear efficiency benefits, it also means that network operators and service providers may become less willing to share information with a CERT, due to the concern that the CERT will not only serve its traditional 'fire brigade' role, but also contribute to initiating legal proceedings. The latter may be beneficial from a public policy perspective, but can be (perceived as) highly negative for service providers, since they lose the option of informally consulting the CERT. Thus, if the latter approach is chosen, additional effort will be required to set up a trust relationship with the constituency of the public CERT.

To effectively address botnet crime, **joint coordinated actions between law enforcement, CERTs and the private sector (such as network operators) are recommended**. CERTs and the private sector should avoid taking actions without law enforcement support, as this might solve a single attack but ultimately leaves the criminals unharmed. The recent case of the b54 botnet operation was mentioned as a good practice example, where Microsoft was able to work with the FBI to shut down the Citadel botnet[1]. Linked to this, the organisation of **frequent meetings that allow all stakeholders – law enforcement, CERTs and private companies – to identify and address issues that the private sector faces through an ISAC** (Information Sharing and Analysis Center) has been found to be effective, as seen in the Dutch experiences.

To facilitate cooperation between CERTs at the international level (including for botnet incidents), **the Trusted Introducer and FIRST networks act as strong enablers which generally meet with highly positive feedback from CERTs**. Membership of these networks is thus strongly recommended.

It would be advisable to **examine how feedback could be provided from law enforcement to CERTs on any matters reported by the CERT or in which the CERT intervened**. To protect the secrecy of ongoing investigations, such information could only be provided at the aggregate (non-case specific) level.

Finally, with respect to **data sharing, pragmatic guidance at the EU level, e.g. from the Article 29 Working Party, on the interpretation and impact of data protection rules for CERTs and network operators in their day-to-day security related activities is still needed.** While the theoretical framework and the potential consequences are well known, CERTs and service providers are still largely experimenting on what type of monitoring, analysis and reporting activities are lawful, and which activities are excessive. This has a stifling effect on the fight against cybercrime. **In the absence of such guidelines, Member States should at a minimum ensure that data protection authorities at the national level are easily reachable to provide ad-hoc recommendations.** The best practice of Slovenia as reported above can serve as a useful example of up-to-date, efficient and pragmatic advisory services.

3.3 Identity Theft

3.3.1 Summary of interview outcomes

Under the Directive, Member States are required to "*take the necessary measures to ensure that when [the crimes of illegal system access or illegal system 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, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.*" (Article 9.5). Thus, identity theft is defined in terms of two constituent elements: misuse of personal data to gain the trust of a third party, prejudice to the rightful identity owner.

To identify good practices, interviewees were mainly asked whether their countries had already implemented legislation addressing identity theft (including as an aggravating circumstance), and what the operational practices in their countries were that could be used as a good practice. Additionally, they were also queried on how one might determine concealment of the real identity of the perpetrator against the lawful use of pseudonyms, alter egos, avatars, usernames, or anonymisation software, and on the determination of prejudice taking into account individual sensitivity, satire, parody, freedom of speech rights, etc.

With respect to **existing legislation**, most countries indicate that they have not adopted any ID theft specific legislation, and that incidents are addressed through existing generic criminal laws, such as breaches of telecommunications confidentiality laws, fraud, illegal access/hacking, interfering with computer systems, illegal interception, etc., depending on the circumstances. In rarer cases, the applicability of data protection law is signalled, as are possible civil law qualifications (such as violation of personality rights).

However, a smaller number of countries have reported specific legal initiatives. In Italy, legislation is currently under discussion in Parliament, which introduces ID theft as an independent crime, qualifying it as impersonation if there is an intent to gain a profit or to harm the identity owner. The integration of this intent was seen generally as useful to avoid abuses. The Italian proposal remains however subject to significant debate, and its chances of adoption are unclear.

In France, a specific provision was introduced in 2011 that covered cases of ID theft that were not clearly covered by adequate criminal law before. Before 2011, ID theft was an offence only when it would put a victim in a position of possibly being accused of committing an offence (also including abuse of titles or functions, e.g. pretending to be a policeman to commit an offence was already covered). The new legislation covers usurping the identity of a third person or to make use of one or more data allowing the identification of that person, with a view to damage the tranquillity of someone else, or to harm the honour or standing of that person. The law explicitly states that the law also applies when committed on a public communication network (i.e. the Internet).

The main debate on the ID theft provision in France remains whether this opposes any right to parody, or comic use of someone's identity (freedom of speech). The Parliament has stated that these rights should remain respected, so that judges need to consider this balance in actual cases. The provision specifically aims to apply when people's identity was being used on online forums, or when their identity was abused by others to make people look bad.

With respect to **operational practices**, it is worth noting that both law enforcement and CERTs stress the importance of good interactions with service providers such as social network sites or hosting companies in addressing simple identity theft cases effectively. In more complex fraud cases (including spear phishing in the financial services sector), both stakeholders noted the importance of frequent contacts with sector specific organisations in order to rapidly disseminate information on identified threats. Awareness raising is still seen as the primary tool in fighting identity theft, as the main cause of successful identity theft cases is still the uninformed and insecure behaviour of end users.

For less technically complex cases (e.g. creating Facebook under someone else's name), a number of countries noted the supporting role of data protection authorities, as such incidents could be prosecuted as a violation of data protection law. The Greek DPA affirmed that a few such cases have been brought before it, likely as a result of opinions published by the DPA on the topic. The DPA is seen by many citizens as a lower threshold contact point that can then help them to contact the service provider (e.g. Facebook) or by referring them to another competent DPA (e.g. the Irish DPA in case of Facebook). Bigger cases would be addressed by law enforcement.

With respect to **concealment of identities** (an issue that would not be covered by the Directive's provisions, as they focus on the misuse of another person's personal data), most respondents noted that they do not consider the use of pseudonyms or anonymization networks as problematic in their own rights, nor as indicative of any problem that makes a qualification as identity theft significantly greater. However, it is interesting to note that at least three respondents (in France, in Slovenia and in the Netherlands) saw a concern from the opposite angle: they noted that law enforcement officials had no competences to use anonymisation technologies themselves, and that this was a real

need to enable them to take effective action. As this issue is outside the scope of the Directive, it will not be examined further in this report.

Finally, with respect to **determining prejudice**, all interviewees were asked how grey area cases (pseudonyms, joke accounts on Facebook, parody etc.) were addressed, and notably whether the prejudice criterion was applied in practice. Interviewees almost unanimously noted that such cases occurred with relative frequency, but that they were themselves rarely involved. This is likely because the majority of interviewees were CERTs or law enforcement bodies: CERTs would not generally be implicated in such technologically simple and relatively benign cases; and law enforcement bodies would generally not be responsible for the assessment of prejudice, as this would be done at a later stage by courts in case of prosecution.

Practically speaking, if any actions would be undertaken against these types of files, the interviewees indicated that this would generally be done by the victims contacting service providers directly to voluntarily take action, or by civil claims before civil courts. Criminal case law for such cases was therefore noted to be extremely limited.

3.3.2 Identified good practices

Most of the good practices that were already described in the preceding sections on botnets also apply to identity theft. However, several additional good practices can be found in the interview outcomes.

On the legislative front, the primary good practices are the Italian example that emphasise the intent to cause harm as a precondition for criminalisation, and the French example that was more broadly phrased but benefited from discussions in Parliament that emphasized the importance of respecting freedom of expression. Both of these elements (intent and freedom of expression) are vital for the correct functioning of ID theft legislation.

Operationally, several respondents indicated that smaller ID theft cases in which no significant interests were involved could often be addressed effectively by requesting appropriate interventions (typically deletion of the offending materials) by the service providers themselves, as the use of false identities in an attempt to cause harm to a third party is usually a violation of terms of service.

3.3.3 Reflections on the findings

With respect to implementing legislation, it will be important for national laws to **stress the importance of the criminal intent** of the alleged ID thief, and to emphasse that the **provisions should be interpreted and applied taking into account the legitimate exercise of the fundamental right to freedom of expression**. It would not be feasible or desirable to enumerate cases covered by this fundamental right (such as parody, satire, societal criticism, polemic discussion, etc.), but the primacy of this fundamental right should be recognized in order to support the development of rational and consistent case law. Legal intervention on this point should thus be well considered. The interpretation of this balance between criminal conduct and controversial but legal free speech should be left to the courts; CERTs should at any rate not play a role in assessing the balance.

As noted above, ID theft cases could often be solved by **requesting service providers to take voluntary action**, such as removal of the offending materials from any public website. This approach is often more efficient than formal legal proceedings. However, **such requests must be carefully phrased in order to minimise the impact on potential future proceedings**. Deletion could result in the destruction of evidence, making future legal actions against criminals impossible or at least substantially harder. For this reason, information should be made inaccessible rather than deleting it, unless it has been determined with a sufficient degree of certainty that no future criminal or civil actions will be undertaken.

Linked to this, and similar to the recommendation with respect to botnets noted above, the organisation of **frequent meetings that allow all stakeholders – law enforcement, CERTs and private companies – to identify and address issues that the private sector faces through an ISAC** (Information Sharing and Analysis Center) can be effective. This is notably useful to proactively identify and address commonly recurring ID theft attacks, such as spear phishing in the financial services industry.

4 Cooperation and information exchange procedures in the Directive

4.1 Scope and contents of the Directive

With respect to procedural revisions, arguably the most significant improvements in the Directive relate to **information exchange and data collection.** The Framework Decision merely specified that Member States should "make use of the existing network of operational points of contact available 24 hours a day and seven days a week", in accordance with data protection rules, and that Member States should inform the General Secretariat of the Council and the Commission of its appointed point of contact.

The tasks of the Member States on this point are significantly clarified in the new Directive. On the exchange of information, the existing obligations are retained, and a response time obligation is added: Member States should implement the necessary procedures to respond within a maximum of eight hours to urgent requests. Such responses "*shall at least indicate whether and in what form the request for help will be answered and when*"; thus, substantive responses are not necessarily required in this initial response.

In the sections below, we will briefly examine the feedback from the interviewees with respect to this update.

4.1.1 Summary of interview outcomes

Given that the obligation relates to information exchanges organised between investigative authorities in the different Member States, the question was primarily relevant for representatives of law enforcement bodies.

CERT interviewees on the other hand noted that they were generally able to exchange information relatively quickly and flexibly between each other, as their interactions typically wouldn't require compliance with procedural law obligations, nor would their information exchanges necessarily result in legal action. For more formal assistance requests, the CERTs generally indicated that they only worked with law enforcement bodies in their own countries and would prefer to keep it this way, since this simplifies trust and legal compliance.

Several CERTs (including e.g. from the UK) indicated a preference for keeping technical investigation and legal investigations separate whenever possible, since the former (mainly between CERTs, but also the flow of intelligence between CERTs and law enforcement) is significantly quicker and easier than the latter (involving evidence, rather than intelligence). Intelligence and evidence should be kept separate. A similar perspective was noted by the Slovenian CERT, indicating that CERTs could occasionally act as rapid intelligence collectors at the request of law enforcement, who could then use this intelligence to determine whether formal evidence would be needed. This difference in focus is also why CERTs are not highly in favour of further regulation of CERT activities: this would make the CERTs a separate flavour of police/law enforcement with the same disadvantages and the same impact on their communicative efficiency. The non-legal route enabled by CERTs is sometimes more effective, and regulation wouldn't necessarily help them. Regulation could turn the non-legal route into an illegal route.

As the obligation of the Directive would not formally apply to CERTs, the primary feedback was obtained from law enforcement bodies, and CERT suggestions are not discussed in further detail below.

Most of the law enforcement interviewees noted some reservations with respect to the Directive:

- They acknowledged that the 8 hour time limit for responses to urgent requests was generally feasible.
- However, they stressed that – as permitted by the Directive – such quick responses were not likely to be very substantive or useful to the party making the requests, as material help (e.g. the identification of a subscriber behind an IP address) would take 24-36 hours at the most optimistic end of the spectrum, with some respondents noting that a response time of a week or more was more realistic. This was mainly due to the need to follow formal judicial aid request procedures, and the requirement to obtain national court orders before any ISP or other service provider could be required to hand over certain information.
- Contacts are generally organised bilaterally (based on existing judicial assistance agreements, and via legal aid requests through ministries of justice when necessary), or via Europol and Interpol. The main difficulty in international collaboration (including within Europe) is drafting the requests, which must be translated and put into a legally valid format; this takes time and resources, even for relatively basic types of information. Streamlining of these processes is seen as useful, although the French interviewee questioned whether this was an appropriate topic for a cybercrime oriented initiative: policy makers should be working on better processes and better mechanisms within Europol for cooperation in general, i.e. in all criminal cases. Cybercrime specific rules and response obligations therefore did not seem to be necessary, according to the interviewee.
- Finally, as was noted by the interviewee from the Netherlands, the existence of a single national high tech crime unit is highly beneficial to streamline communications: in decentralised countries or countries with multiple contact points, information exchange doesn't always work well because a foreign body cannot determine reliably who should be contacted. In principle, every country should have a single contact point; they can then delegate any requests as necessary according to internal policy rules and principles.

4.1.2 Identified good practices

Good practices were relatively rare as most respondents indicated their basic requirement of complying with formal rules without much margin for innovation or creativity. None the less, a few interesting examples could be noted.

In the French Gendarmie, a current ongoing project is aiming to devise a standard procedure to proactively address basic malware distributions (small botnets). This will fit into a more general strategy being created right now, looking at any cases where infrastructure in France is used to commit a crime, even if there are no known victims in France. The idea is to help others through improved international cooperation: the **collected information could be proactively shared with international law enforcement partners**. This strategy would need to be tested in a number of cases; presently the idea is still in its early stages. The strategy will also include procedures for dealing with assistance requests from ISPs or from CERTS (in France and abroad), and will include proactively pushing the collected information via Europol to other countries (third countries, including Russia, Ukraine, etc.). This approach which is currently being contemplated by the French authorities would represent a **paradigm shift from a responsive to a proactive model**, which would additionally **include international non-European partners**. Given that these countries are often more likely to host criminals taking advantage of bullet proof hosting services, this will be crucial to improve the effectiveness of anti-cybercrime measures.

The interviewee from Belgium noted that, for assistance requests sent via Europol/Interpol, the possibility exists to **append codes to the information requests that indicate which information may be disseminated to other contact points**. This is a minor but useful standardisation mechanism that can be very effective to identify contacts and obtain their collaboration.

Formal assistance networks are however not the only or even the most effective way to achieve international cooperation. Several respondents – including e.g. in Bulgaria – noted that the **organisation of face-to-face meetings between law enforcement representatives outside of the EU (e.g. non-EU Southeast European countries)** was an important enabler, as cooperation with non-EU countries can be more complicated and personal contacts can greatly facilitate effective interactions. A similar concern was echoed by France: generally, criminals hide in countries where it's difficult to co-operate, and this is an issue that the Directive doesn't really address. In Europe, cooperation via Europol is often easier than with non-EU countries, and the EC3 is a positive development on that front. In other countries, experiences vary: there have been good examples in France recently of co-operation with the Ivory Coast.

Finally, legal compliance in international information exchanges is a clear concern with CERTs, or at least it is within Portugal. **Within the Portuguese CERT, data protection guidelines and standard policies have been drafted that determine when/which data can be shared.** These policies are reviewed and policed by the CERT's own lawyers and are discussed with the data protection authority.

4.1.3 Reflections on the findings

With a view of streamlining international information exchanges, several recommendations could be identified from the interviewees' replies:

- A number of respondents (e.g. Belgium and Bulgaria) noted that, even within the EU, replies to information requests were often delayed or partial, which can halt investigations. The reasons included lack of trust, but also misunderstandings with respect to the scope of requests, rather than resources or language barriers. **Streamlining/standardisation of communications between the 24/7 network might be useful**, which could be done by establishing templates for the most common information requests.
- As illustrated by the French best practice discussed above, it may be worth coupling the reactive information sharing model espoused by the Directive with a more **proactive information sharing strategy** in which collected information could be proactively shared with international law enforcement partners.
- Specifically **with respect to CERTs**, it was noted that there are no standard approaches/protocols to check whether there are any on-going investigations in other countries. This is inefficient, because incidents, attacks or vulnerabilities are often known to several national CERTs who are all working on them, without knowing that colleagues in other countries are also collecting relevant information. **An EU level information site (like a storm center) for CERTs/law enforcement to share such information would be useful in order to avoid duplication of investigative efforts**.

- **International cooperation outside of the EU should also be supported through face-to-face meetings between law enforcement representatives**, as a key first step to building trust and identifying effective contacts.
- Finally, **every country should have a single contact point for information requests**, irrespective of their national competences or organisational model. The contact point can then delegate any requests as necessary according to internal policy rules and principles, but this internal back office process should be irrelevant and invisible to foreign law enforcement bodies.

5 Data collection and reporting in the Directive

5.1 Scope and contents of the Directive

As a final new point, the Directive contains obligations on monitoring and statistics. Member States would be required to implement a system for the recording, production and provision of statistical data on the offences in the Directive, including at a minimum the number of offences and their follow-up, and indicating on an annual basis the number of reported cases investigated, the number of persons prosecuted, and the number of persons convicted. This data should be reported to the Commission and published in a statistical report.

5.2 Data collection

5.2.1 Summary of interview outcomes

Responses from the interviewees indicated that data collection was subject to a number of complexities, related primarily to the **fragmentation of information sources**. Depending on the country, up to five distinct information sources could be identified: CERTs, supervisory bodies, law enforcement bodies, public prosecutors and courts. The logical structure and semantics of their databases (if present) generally could not be assumed to be built on the same assumptions: the qualification given to an incident by a CERT (if any) would not necessarily be retained by investigators, nor by prosecutors, or ultimately by courts.

It is of particular interest in this respect that several interviewees noted the **importance of breach notification obligations**, e.g. in the context of the telecommunications sector, the financial services industry or in the recently proposed Directive on Network and Information Security, as an additional tool for creating a more substantive and comprehensive knowledge base on major ICT incidents and their apparent impact. Of course, these notifications would not be inherently sufficient to provide the data required by the Directive on Attacks against Information Systems (as they are not specifically linked to the criminal qualifications presented in the Directive), but they could ultimately contribute to forming a more comprehensive ecosystem of incident related data.

Responses also indicated a **reluctance towards the comprehensiveness of this data collection effort**: while some countries indicated that they could indeed identify prosecutions and convictions for the incidents enumerated in the Directive, they none the less cautioned that some cases could be given a qualification that did not match the provisions of the Directive. E.g. a case of spear phishing might ultimately be prosecuted simply as fraud and result in a conviction on this basis, despite the fact that this might clearly qualify as identity theft as described above.

Additionally, interviewees cautioned against the known '**dark number**' problem, i.e. the known fact that cybercrime is very significantly underreported[32], especially when incidents are committed against reputation-sensitive victims such as banks, who have an incentive to see incidents solved without formal investigation or prosecution, as these could result in greater visibility and thus greater reputational damage. Thus, statistical data could be useful to show trends, but would be entirely unsuitable to assess the actual scope of cybercrime problems.

[32] Discussed e.g. in the Council of the European Union's Note of 20 September 2013 on the Implementation EU Policy cycle for organised and serious international crime: Multi-Annual Strategic Plan (MASP) related to the EU crime priority "cybercrime"; see http://www.statewatch.org/news/2013/sep/eu-council-cosi-masp-2014-2017-cybercrime-12759-rev3-13.pdf [Last accessed 22 October, 2013], p.2

Finally, the respondents noted that statistics would measure identical facts differently in different countries: the aforementioned case of spear phishing could be prosecuted as fraud in one Member State and as identity theft in another, despite having the exact same factual background. Thus, **statistics would not be comparable between countries**, in the absence of a common EU level prosecutorial approach.

Despite this apparent scepticism, some good practices and suggestions have also been identified, as will be briefly discussed below.

5.2.2 Identified good practices

Within some countries, data collection has been successful in specific context, and/or projects are ongoing to improve and streamline data collection:

- In Ireland, data collection within the financial sector works relatively effectively: there is an information sharing platform for this sector where incident reports can be exchanged. This operates as **a trusted network and a relatively closed environment**, where there is less fear of publicity leaks. Similarly, gathering data from businesses is more complex than from citizens, because they have a greater commercial risk linked to openness. Collecting data from incidents that target citizens might be easier (spam, phishing, identity theft), given that this fear is less present, and this could have the benefit of increasing awareness among citizens.
- Romania notes that it faces the same challenges as most other countries: data collection is done systematically by the police, but the data is not always published. Prosecution data is also available and held by prosecutors. However, there is currently a project on-going between the police and prosecutors to bundle this information into joint statistics. There is no public data available yet right now, but the project should be completed by the end of the year, and statistics should be available at that time. Bundling data from all sources – CERT, police, prosecutors and courts – would be a good practice.
- Data collection is done systematically in France, at least for those specific crimes enumerated in the current Directive. For cybercrime offenses outside of that (e.g. fraud committed using a computer/via the Internet), statistics are not available because there is no specifically defined infraction for fraud on the Internet in French law, so that no separate convictions on this point are available (only for fraud in general). There are however numbers for investigations and convictions in 2011 for the crimes in the Directive.

5.2.3 Reflections on the findings

In countries which have multiple information sources (and the interview outcomes suggest that all Member States are in this situation) a coordinating body would need to be designated to collect comparable information and to draft reports.

The existing and emerging legal frameworks for **breach notification obligations** offer a unique opportunity for establishing a more comprehensive and coordinated ecosystem of incident related data. While breach notifications do not contain direct information on the legal qualification of incidents, nor on their prosecution or the outcome thereof, it can be reasonably foreseen that at least a number of notifications will be a trigger for cybercrime investigations, prosecutions and possibly convictions. The processes for handling breach notifications should thus be aligned with the terminology and approach envisaged by the Directive to facilitate the collection of comparable European statistical data.

In the longer term, **better alignment is needed with respect to semantics and prosecutorial policies across the EU**, at least if the goal is to obtain comparable statistics across the EU. If the goal is merely to be able to assess cybercrime trends at the national level without EU scale comparisons, then such alignment is not strictly needed.

5.3 Reporting

5.3.1 Summary of interview outcomes

As noted in the sections above, some countries have an information source in place, and some of these publish periodic statistical reports. However, it is relatively rare that a single coordinated report is published containing information from all stakeholders (law enforcement, prosecutors, courts, etc.). Furthermore, reports are sometimes only made available for internal use, and not shared with the public.

In the sections below, we will identify some of the main reporting practices.

5.3.2 Identified good practices

Several countries have indicated that reports are already made publicly available on-line:

- In Belgium, statistics are published to some extent, although separately for the police and for courts. See e.g. http://www.polfed-fedpol.be/pub/rapport_activites/crimestats2011_nl.php (p.55) for the police's cybercrime statistics and http://www.om-mp.be/sa/jstat2011/n/home.html for the Ministry of Justice's statistics.
- As also noted above, data collection is done systematically in France, at least for those specific crimes enumerated in the Directive. There are numbers for investigations and convictions in 2011 , and a new report will in principle be released in the course of 2013 by

the ONDRP (French criminal statistics agency - *Observatoire national de la délinquance et des réponses pénales*): see http://www.inhesj.fr/fr/ondrp/les-publications/rapports-annuels.

5.3.3 Recommendations for the implementation

As with the data collection recommendation above, for reporting purposes too it would be necessary to **designate a coordinating body to collect comparable information and to draft reports**, and it would be necessary to **improve alignment with respect to semantics and prosecutorial policies across the EU**, at least if the goal is to obtain comparable reports across the EU. If the goal is merely to be able to assess cybercrime trends at the national level without EU scale comparisons, then such alignment is not strictly needed.

6 Conclusions – good practices and open issues

6.1 Good practices for the implementation of the Directive

As shown in the analysis above, many of the new topics introduced by the Directive have already been addressed in some countries through good practices. These are briefly summarised in the table below, which can be used as a tool to support implementation activities in the Member States.

Topic	Observed good practice	Country or organisation where the practice was observed
All substantive criminal provisions (illegal access, illegal interception, tools for committing offenses)	The **publication of guidance** on the interpretation and application of the law, and particularly on the element of intent (i.e. the unlawfulness – without right). This can be done in the form of prosecution guidelines in countries that permit this, and/or in the form of jurisprudence overviews to show how courts apply the law in reality. Guidance should also explicitly cover conduct that is considered lawful, such as the activities of CERTs or security professionals.	UK, Sweden and Portugal
All substantive criminal provisions (illegal access, illegal interception, tools for committing offenses)	**Implementing legislation should be clear and explicit**, and include clear carve-outs of the applicability of the provision for the normal activities of CERTs, academic institutions, researchers, network operators and security service professionals, and any actions undertaken at the lawful request of businesses, governments and end users.	France (carve-outs not included in legislation, but explicitly discussed in Parliamentary discussions)
Botnets & identity theft	**Implementing legislation should avoid using technology specific terminology. It should focus on the exact harm that technologically enabled crimes cause**. E.g. rather than introduce the concept of botnets or DDoS attacks, UK legislation was amended to make it an offence to deliberately or recklessly impair the operation of any computer or program, or reliability of data, or to prevent or hinder access to data. Similarly, French and Italian identity theft initiatives focus on the intent to cause harm as a precondition for criminalisation, and emphasise the importance of respecting freedom of expression.	UK, France, Italy
Botnets & identity theft	CERTs can benefit from the **development of standardised processes or playbooks for taking appropriate action to respond to botnets or incidents of identity theft**. These should e.g. cover the questions that CERTs would need to ask, what information and recommendations they should provide, and what could proportionately and lawfully be done by service providers. This would also be useful to strengthen the	Romania, France

	image and perceived usefulness of CERTs (and law enforcement) for criminals.	
CERT mandates	The definition of a **clear mandate** is crucial: **private CERTs and academic CERTs benefit from implementing clear agreements** with their constituency that define precisely what their remit and competences are. **Public** CERTs benefit from a clear legal framework that grants them clear authorities and powers. While a close integration of public CERTs and law enforcement has efficiency benefits, it also means that network operators and service providers may become less willing to share information with a CERT, due to the concern that the CERT will not only serve its traditional 'fire brigade' role, but also contribute to initiating legal proceedings. The latter may be beneficial from a public policy perspective, but can be (perceived as) highly negative for service providers, since they lose the option of informally consulting the CERT. Thus, if public CERTs are integrated with law enforcement agencies, additional effort will be required to set up a trust relationship with the constituency of the public CERT.	UK, Sweden
Cooperation between CERTs and private industry	It is crucial for CERTs to work in partnership with representatives of key sectors, including a large telcos and banks. This can be done through ISACs (Information Sharing and Analysis Center), that allow all stakeholders – law enforcement, CERTs and private companies – to identify and address issues that they face and establish streamlined cooperation processes.	Netherlands
Data protection compliance within CERTs	CERTs should maintain a close **working relationship with their data protection authorities**, in order be able to obtain quick advice when needed. This was noted to be important to maintain trust of the CERT constituency (such as ISPs).	Slovenia
Data collection and statistical analysis	While statistical data is often available at various levels (CERTs, police/law enforcement, prosecutors, courts, etc), coordination and bundling of this data is very rare. **A coordinating body can be designated to collect comparable information and to draft reports.**	Romania (test project to be initiated at the end of 2013)

6.2 Open issues and possible future actions

Despite the good practices as noted above, there are also a number of areas where further guidance or follow up actions would be necessary. These are briefly summarised in the table below, which can be used as a resource for further support actions for each of the stakeholders identified. Topics already covered by the good practices above were not included further in the table below; however, it is of course clear that such practices could be the basis for future actions in countries that have not yet implemented them.

As can be seen, further follow-up activities at the EU level are also proposed, including potential future actions in which ENISA could play a role, in a logical continuation of its support to the CERT community in the fight against cybercrime through targeted support activities. In this manner, ENISA could play a further enabling role in the successful implementation and application of the Directive on Attacks against Information Systems.

Topic	Recommended future action	Entity responsible for the action
All substantive criminal provisions (illegal access, illegal interception, tools for committing offenses)	**Collection and dissemination of guidance on the interpretation and application of the law at the EU level** could help to ensure homogeneous application of the law across the European territory. Guidance should also explicitly cover conduct that is considered lawful, such as the activities of CERTs or security professionals.	Could be done by **ENISA** as a part of its support activities to CERTs, or by the **European Commission** as a part of implementation support activities.
Implementation strategy	Member States should **assess carefully whether new legislation is necessary to achieve the effects of the Directive** under existing law, and if so, to implement the required changes through **generic and technology neutral language**. This would achieve the desired outcome while avoiding the risk of putting in place language that creates new technical discussions or escape routes for criminal behaviour.	Member State legislators
Enforcement strategies	**Joint coordinated actions between law enforcement, CERTs and the private sector (such as network operators) are recommended**. **CERTs and the private sector should avoid taking actions without law enforcement support**, as this might solve a single attack but ultimately leaves the criminals unharmed.	Law enforcement, CERTs and private industry
Enforcement strategies	**Simple cases (e.g. of identity theft) can often be solved by requesting service providers to take voluntary action**, such as removal of the offending materials from any public website. This approach is often more efficient than formal legal proceedings. However, **such requests must be carefully considered in order to minimise the impact on potential future proceedings**. Deletion could result in the destruction of evidence, making future legal actions against criminals impossible or at least substantially harder. For this reason, **alignment is needed between CERTS and law enforcement to agree upon appropriate action for specific instances, including e.g. determining when making data inaccessible is more appropriate than requesting deletion**.	Law enforcement and CERTs (depending on the level of intervention)

Communication between CERTs and law enforcement	It would be advisable to **examine how feedback could be provided from law enforcement to CERTs on any matters reported by the CERT or in which the CERT intervened**. To protect the secrecy of ongoing investigations, such information could only be provided at the aggregate (non-case specific) level.	Could be done by **ENISA** as a part of its support activities to CERTs, or by the EC3; European alignment on this topic would be beneficial.
Data protection compliance	With respect to data sharing, **pragmatic guidance at the EU level, e.g. from the Article 29 Working Party, on the interpretation and impact of data protection rules for CERTs and network operators in their day-to-day security related activities is still needed**. While the theoretical framework and the potential consequences are well known, CERTs and service providers are still largely experimenting on what type of monitoring, analysis and reporting activities (to customers, CERTs or LEA) are lawful, and which activities are excessive. This has a stifling effect on the fight against cybercrime.	Article 29 Working Party
Identity theft	National laws should **clarify the importance of the criminal intent of the alleged ID thief**, and to stress that the **provisions should be interpreted and applied taking into account the legitimate exercise of the fundamental right to freedom of expression**. It would not be feasible or desirable to enumerate cases covered by this fundamental right (such as parody, satire, societal criticism, polemic discussion, etc.), but the primacy of this fundamental right should be recognized in order to support the development of rational and consistent case law. The interpretation of the balance between criminal conduct and controversial but legal free speech should be left to the courts; CERTs should at any rate not play a role in assessing the balance.	Member State legislators
Assistance requests	Even within the EU, replies to information requests were often delayed or partial. Misunderstandings with respect to the scope of requests were commonly a part of the cause. **Streamlining/standardisation of communications between the 24/7 network might be useful, which could be done by establishing templates for the most common information requests**. For assistance requests sent via Europol/Interpol, the possibility exists to append codes to	EC3, given its role in EU level cooperation and coordination

	the information requests that indicate which information may be disseminated to other contact points. This is a minor but useful example of a standardisation mechanism that can be very effective.	
International cooperation	**International cooperation with partners outside of the EU** (e.g. with non-EU Southeast European countries, Asian and African countries) is still at an immature level. This should also be **supported through face-to-face meetings** between law enforcement representatives, as a key first step to building trust and identifying effective contacts. This is important to address current policy gaps: **bullet proof hosting services are a challenge that is currently unaffected by EU initiatives, as these services are almost universally established outside the EU.**	Law enforcement and CERTs, to be enabled via ENISA or EC3
National organisation	**Every country should have a single contact point for information requests, irrespective of their national competences or organisational model.** The contact point can then delegate any requests as necessary according to internal policy rules and principles, but this internal back office process should be irrelevant and invisible to foreign law enforcement bodies.	Member States
Data collection and statistical analysis	In the longer term, **better alignment is needed with respect to semantics and prosecutorial policies across the EU**, if the goal is to obtain comparable statistics across the EU. Crimes have different meanings in different countries, and identical incidents can be qualified differently from country to country, making statistics incomparable.	ENISA or EC3

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu