320DT07
TABLE OF CONTENTS

With the support of the Internal Security Fund – Police Programme 2014-2020 of the European Union

This programme has been produced with the financial support of the Internal Security Fund – Police Programme 2014-2020 of the European Union.
The content of this programme reflects only ERA's view and the Commission is not responsible for any use that may be made of the information it contains

BACKGROUND DOCUMENTATION

1	DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA *(OJ L335/1 - 17.12.2011)*
2	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography *(COM(2016) 871 final)*
3	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography *(COM(2016) 872 final)*
4	Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25.10.2007 (*Council of Europe Treaty Series-No. 201)*
5	Internet Organised Crime Threat Assessment (IOCTA) 2019

A) European Criminal Law: the institutional framework

A1) Main treaties and conventions

A1-01	Protocol (No 36) on Transitional Provisions
A2-02	Statewatch Analysis, "The Third Pillar acquis" after the Treaty of Lisbon enters into force, Professor Steve Peers, University of Essex, Second Version, 1 December 2009
A1-03	Consolidated version of the Treaty on the functioning of the European Union *(OJ C115/47; 9.5.2008) – Title V (pages. 27-38)*
A1-04	Consolidated Version of the Treaty on the European Union *(OJ C321 E/1;, 29.12.2006, P. 5) – Title VI (pages 23-31)*
A1-05	Charter of fundamental rights of the European Union *(OJ. C 364/1; 18.12.2000)*
A1-06	Explanations relating to the Charter of Fundamental Rights *(2007/C 303/02)*
A1-07	Convention implementing the Schengen Agreement of 14 June 1985 *(OJ L 239; 22.9.2000, P. 19)*

A2) Court of Justice of the European Union

A2-01	Consolidated Version of the Statute of the Court of Justice of the European Union (01.07.2013)
A2-02	Consolidated version of the Rules of Procedure of the Court of Justice of 25 September 2012

A3) The EU's competence in criminal matters

A3-01	Case C-440/05, ship-source pollution, *Commission v. Council* [2007] ECR I-0000, *Judgement of 23 October 2007*
A3-02	Case C-176/03 *Commission v. Council* [2005] ECR I-07879, *Judgement of 13 September 2005*

A4) European Convention on Human Rights (ECHR)

A4-01	Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 together with additional protocol and protocols no. 4, 6, 7, 12 and 13, Council of Europe
A4-02	Case of Salduz v. Turkey (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

B) From mutual legal assistance to mutual recognition

B1) Main instruments

B1-01	Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings *(OJ L 328/42; 15.12.2009, P.42*)
B1-02	Council Act of 16 October 2001 establishing in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union *(2001/C 326/01), (OJ C 326/01; 21.11.2001,P. 1)*
B1-03	Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union *(OJ C 197/1; 12.7.2000, P. 1)*
B1-04	Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 8.XI.2001*)
B1-05	Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 17.III.1978*)
B1-06	European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 20.IV.195*9)
B1-07	Third Additional Protocol to the European Convention on Extradition (*Strasbourg, 10.XI.2010*)
B1-08	Second Additional Protocol to the European Convention on Extradition (*Strasbourg, 17.III.1978*)

B1-09	Additional Protocol to the European Convention on Extradition (*Strasbourg, 15.X.1975*)
B1-10	European Convention on Extradition (*Strasbourg, 13.XII.1957*)

B2) Mutual recognition in practice: the European Arrest Warrant

B2-01	Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial *(OJ L 81/24; 27.3.2009)*
B2-02	Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States *(OJ L 190/1; 18.7.2002, P. 1)*
B2-03	Case C-399/11 Stefano Melloni v Ministerio Fiscal, Judgment of of 26 February 2013
B2-04	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-05	C-261/09 Mantello, Judgement of 16 November 2010
B2-06	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-07	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-08	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-09	C-66/08 Szymon Kozlowski, Judgement of 17 July 2008
B2-10	C-303/05 Wereld/Ministerraad, Judgment of the Court of 3 May 2007

B3) Mutual recognition in practice: sanctions

B3-01	Proposal for a Directive on the freezing and confiscation of proceeds of crime in the European Union (COM(2012) 85 final; 12.3.2012)
B3-02	Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention *(OJ L 294/20; 11.11.2009)*
B3-03	Council Framework Decision 2008/947/JHA on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions *(OJ L 337/102; 16.12.2008)*
B3-04	Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union *(OJ L 327/27; 5.12.2008)*
B3-05	Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings *(OJ L 220/32; 15.08.2008*)
B3-06	Council Framework Decision of 6 October 2006 on the application of the principle of mutual recognition to confiscation

	orders *(OJ L 328/59, 24.11.2006, P.59)*
B3-07	Council Framework Decision of 24 February 2005 on the application of the principle of mutual recognition to financial penalties *(OJ L 76/16, 22.3.2005, P.16)*
B3-08	Council Framework Decision of 24 February 2005 on Confiscation of Crime-Related Proceeds, Instrumentalities and Property *(OJ L 68/49, 1.3.2005, P. 49)*

B4) Mutual recognition in practice: evidence

B4-01	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130/1; 1.5.2014)
B4-02	Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters *(OJ L, 350/72, 30.12.2008*)
B4-03	Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence *(OJ L 196/45; 2.8.2003*)

B5) Criminal records

B5-01	Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA *(OJ L 93/33; 7.4.2009, P. 33)*
B5-02	Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States *(OJ L 93/23; 07.4.2009)*
B5-03	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure *(6397/5/06 REV 5; 15.1.2007)*
B5-04	Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record *(OJ L 322/33; 9.12.2005)*

C) Procedural guarantees in the EU

C-01	Proposal for a Directive on provisional legal aid for suspects or accused persons deprived of liberty and legal aid in European arrest warrant proceedings (COM(2013) 824 final; 27.11.2013)
C-02	Proposal for a Directive on procedural safeguards for children suspected or accused in criminal proceedings (COM(2013) 822 final;27.11.2013)
C-03	Proposal for a Directive on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceedings (COM(2013) 821 final; 27.11.2013)
C-04	Directive 2013/48/EU of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294/1; 6.11.2013)

C-05	Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (1.6.2012; OJ L 142/1)
C-06	Strengthening mutual trust in the European judicial area – A Green Paper on the application of EU criminal justice legislation in the field of detention (COM(2011) 327 final; 14.6.2011)
C-07	Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings *(OJ L 280/1; 26.10.2010*)
C-08	Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings *(OJ C 295/1; 4.12.2009*)

D) Victims' rights

D-01	Regulation (EU) No 606/2013 of 12 June 2013 on mutual recognition of protection measures in civil matters (OJ L 181/4; 29.6.2013)
D-02	Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (14.11.2012; OJ L 315/57)
D-03	Directive 2011/99/EU of 13 December 2011 on the European protection order (OJ L 338/2; 21.12.2011)
D-04	Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims (*OJ L 261/15; 6.8.2004*)
D-05	Council Framework Decision of 15 March 2001 on the standing of victims in criminal procedures (*OJ L 82/1; 22.03.2001*)

E) Cybercrime - Council of Europe

E-01	Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (*Strasbourg, 28.I.2003*)
E-02	Convention on Cybercrime *(Budapest, 23.XI.2001*)

F) Cybercrime – European Union

F-01	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 (Official Journal L 218/8 of 14.08.2013
F-02	Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA *(Official Journal L 335/1 of 17.12.2011)*

- For a comprehensive overview of the legal instruments in the field of cybercrime please consult the ERA e-library at the following address: http://www.era-comm.eu/Cybercrime/library.html

G) Electronic Evidence

G-01	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
G-02	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014
G-03	ACPO Good Practice Guide for Digital Evidence *(March 2012)*
G-04	Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (Official Journal L 130/1 01.05.2014)
G-05	Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters *(Official Journal L 350/72, 30.12.2008)*
G-06	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce*) (Official Journal L 178/1, 17.7.2000)*
G-07	Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring security and trust in electronic communication - Towards a European Framework for Digital Signatures and Encryption *(COM (97) 503)*, October 1997

I

(Legislative acts)

DIRECTIVES

DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 December 2011

on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 82(2) and Article 83(1) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure ([2]),

Whereas:

(1) Sexual abuse and sexual exploitation of children, including child pornography, constitute serious violations of fundamental rights, in particular of the rights of children to the protection and care necessary for their well-being, as provided for by the 1989 United Nations Convention on the Rights of the Child and by the Charter of Fundamental Rights of the European Union ([3]).

(2) In accordance with Article 6(1) of the Treaty on European Union, the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union, in which Article 24(2) provides that in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. Moreover, the Stockholm Programme — An Open and Secure Europe Serving and Protecting Citizens ([4]) gives a clear priority to combating the sexual abuse and sexual exploitation of children and child pornography.

(3) Child pornography, which consists of images of child sexual abuse, and other particularly serious forms of sexual abuse and sexual exploitation of children are increasing and spreading through the use of new technologies and the Internet.

(4) Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography ([5]) approximates Member States' legislation to criminalise the most serious forms of child sexual abuse and sexual exploitation, to extend domestic jurisdiction, and to provide for a minimum level of assistance for victims. Council Framework Decision 2001/220/JHA of 15 March 2001 on the standing of victims in criminal proceedings ([6]) establishes a set of victims' rights in criminal proceedings, including the right to protection and compensation. Moreover, the coordination of prosecution of cases of sexual abuse, sexual exploitation of children and child pornography will be facilitated by the implementation of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings ([7]).

(5) In accordance with Article 34 of the United Nations Convention on the Rights of the Child, States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. The 2000 United Nations Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography and, in particular, the 2007 Council

([1]) OJ C 48, 15.2.2011, p. 138.
([2]) Position of the European Parliament of 27 October 2011 (not yet published in the Official Journal) and decision of the Council of 15 November 2011.
([3]) OJ C 364, 18.12.2000, p. 1.
([4]) OJ C 115, 4.5.2010, p. 1.
([5]) OJ L 13, 20.1.2004, p. 44.
([6]) OJ L 82, 22.3.2001, p. 1.
([7]) OJ L 328, 15.12.2009, p. 42.

of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse are crucial steps in the process of enhancing international cooperation in this field.

(6) Serious criminal offences such as the sexual exploitation of children and child pornography require a comprehensive approach covering the prosecution of offenders, the protection of child victims, and prevention of the phenomenon. The child's best interests must be a primary consideration when carrying out any measures to combat these offences in accordance with the Charter of Fundamental Rights of the European Union and the United Nations Convention on the Rights of the Child. Framework Decision 2004/68/JHA should be replaced by a new instrument providing such comprehensive legal framework to achieve that purpose.

(7) This Directive should be fully complementary with Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA ([1]), as some victims of human trafficking have also been child victims of sexual abuse or sexual exploitation.

(8) In the context of criminalising acts related to pornographic performance, this Directive refers to such acts which consist of an organised live exhibition, aimed at an audience, thereby excluding personal face-to-face communication between consenting peers, as well as children over the age of sexual consent and their partners from the definition.

(9) Child pornography frequently includes images recording the sexual abuse of children by adults. It may also include images of children involved in sexually explicit conduct, or of their sexual organs, where such images are produced or used for primarily sexual purposes and exploited with or without the child's knowledge. Furthermore, the concept of child pornography also covers realistic images of a child, where a child is engaged or depicted as being engaged in sexually explicit conduct for primarily sexual purposes.

(10) Disability, by itself, does not automatically constitute an impossibility to consent to sexual relations. However, the abuse of the existence of such a disability in order to engage in sexual activities with a child should be criminalised.

(11) In adopting legislation on substantive criminal law, the Union should ensure consistency of such legislation in particular with regard to the level of penalties. The Council conclusions of 24 and 25 April 2002 on the approach to apply regarding approximation of penalties, which indicate four levels of penalties, should be kept in mind in the light of the Lisbon Treaty. This Directive, because it contains an exceptionally high number of different offences, requires, in order to reflect the various degrees of seriousness, a differentiation in the level of penalties which goes further than what should usually be provided in Union legal instruments.

(12) Serious forms of sexual abuse and sexual exploitation of children should be subject to effective, proportionate and dissuasive penalties. This includes, in particular, various forms of sexual abuse and sexual exploitation of children which are facilitated by the use of information and communication technology, such as the online solicitation of children for sexual purposes via social networking websites and chat rooms. The definition of child pornography should also be clarified and brought closer to that contained in international instruments.

(13) The maximum term of imprisonment provided for in this Directive for the offences referred to therein should apply at least to the most serious forms of such offences.

(14) In order to reach the maximum term of imprisonment provided for in this Directive for offences concerning sexual abuse and sexual exploitation of children and child pornography, Member States may combine, taking into account their national law, the imprisonment terms provided for in national legislation in respect of those offences.

(15) This Directive obliges Member States to provide for criminal penalties in their national legislation in respect of the provisions of Union law on combating sexual abuse, sexual exploitation of children and child pornography. This Directive creates no obligations regarding the application of such penalties, or any other available system of law enforcement, in individual cases.

(16) Especially for those cases where the offences referred to in this Directive are committed with the purpose of financial gain, Member States are invited to consider providing for the possibility to impose financial penalties in addition to imprisonment.

(17) In the context of child pornography, the term 'without right' allows Member States to provide a defence in respect of conduct relating to pornographic material having for example, a medical, scientific or similar purpose. It also allows activities carried out under domestic legal powers, such as the legitimate possession of child pornography by the authorities in order to conduct criminal proceedings or to prevent, detect or investigate crime. Furthermore, it does not exclude legal defences or similar relevant principles that relieve a person of responsibility under specific circumstances, for example where telephone or Internet hotlines carry out activities to report those cases.

([1]) OJ L 101, 15.4.2011, p. 1.

(18) Knowingly obtaining access, by means of information and communication technology, to child pornography should be criminalised. To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. The intentional nature of the offence may notably be deduced from the fact that it is recurrent or that the offence was committed via a service in return for payment.

(19) Solicitation of children for sexual purposes is a threat with specific characteristics in the context of the Internet, as the latter provides unprecedented anonymity to users because they are able to conceal their real identity and personal characteristics, such as their age. At the same time, Member States acknowledge the importance of also combating the solicitation of a child outside the context of the Internet, in particular where such solicitation is not carried out by using information and communication technology. Member States are encouraged to criminalise the conduct where the solicitation of a child to meet the offender for sexual purposes takes place in the presence or proximity of the child, for instance in the form of a particular preparatory offence, attempt to commit the offences referred to in this Directive or as a particular form of sexual abuse. Whichever legal solution is chosen to criminalise 'off-line grooming', Member States should ensure that they prosecute the perpetrators of such offences one way or another.

(20) This Directive does not govern Member States' policies with regard to consensual sexual activities in which children may be involved and which can be regarded as the normal discovery of sexuality in the course of human development, taking account of the different cultural and legal traditions and of new forms of establishing and maintaining relations among children and adolescents, including through information and communication technologies. These issues fall outside of the scope of this Directive. Member States which avail themselves of the possibilities referred to in this Directive do so in the exercise of their competences.

(21) Member States should provide for aggravating circumstances in their national law in accordance with the applicable rules established by their legal systems on aggravating circumstances. They should ensure that those aggravating circumstances are available for judges to consider when sentencing offenders, although there is no obligation on judges to apply those aggravating circumstances. The aggravating circumstances should not be provided for in Member States' law when irrelevant taking into account the nature of the specific offence. The relevance of the various aggravating circumstances provided for in this Directive should be evaluated at national level for each of the offences referred to in this Directive.

(22) Physical or mental incapacity under this Directive should be understood as also including the state of physical or mental incapacity caused by the influence of drugs and alcohol.

(23) In combating sexual exploitation of children, full use should be made of existing instruments on the seizure and confiscation of the proceeds of crime, such as the United Nations Convention against Transnational Organized Crime and the Protocols thereto, the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime [1], and Council Framework Decision 2005/212/JHA of 24 February 2005 on Confiscation of Crime Related Proceeds, Instrumentalities and Property [2]. The use of seized and confiscated instrumentalities and the proceeds from the offences referred to in this Directive to support victims' assistance and protection should be encouraged.

(24) Secondary victimisation should be avoided for victims of offences referred to in this Directive. In Member States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of sexual exploitation or where the child was compelled to participate in child pornography.

(25) As an instrument of approximation of criminal law, this Directive provides for levels of penalties which should apply without prejudice to the specific criminal policies of the Member States concerning child offenders.

(26) Investigating offences and bringing charges in criminal proceedings should be facilitated, to take into account the difficulty for child victims of denouncing sexual abuse and the anonymity of offenders in cyberspace. To ensure successful investigations and prosecutions of the offences referred to in this Directive, their initiation should not depend, in principle, on a report or accusation made by the victim or by his or her representative. The length of the sufficient period of time for prosecution should be determined in accordance with national law.

(27) Effective investigatory tools should be made available to those responsible for the investigation and prosecutions

[1] OJ L 182, 5.7.2001, p. 1.
[2] OJ L 68, 15.3.2005, p. 49.

of the offences referred to in this Directive. Those tools could include interception of communications, covert surveillance including electronic surveillance, monitoring of bank accounts or other financial investigations, taking into account, inter alia, the principle of proportionality and the nature and seriousness of the offences under investigation. Where appropriate, and in accordance with national law, such tools should also include the possibility for law enforcement authorities to use a concealed identity on the Internet.

(28) Member States should encourage any person who has knowledge or suspicion of the sexual abuse or sexual exploitation of a child to report to the competent services. It is the responsibility of each Member State to determine the competent authorities to which such suspicions may be reported. Those competent authorities should not be limited to child protection services or relevant social services. The requirement of suspicion 'in good faith' should be aimed at preventing the provision being invoked to authorise the denunciation of purely imaginary or untrue facts carried out with malicious intent.

(29) Rules on jurisdiction should be amended to ensure that sexual abusers or sexual exploiters of children from the Union face prosecution even if they commit their crimes outside the Union, in particular via so-called sex tourism. Child sex tourism should be understood as the sexual exploitation of children by a person or persons who travel from their usual environment to a destination abroad where they have sexual contact with children. Where child sex tourism takes place outside the Union, Member States are encouraged to seek to increase, through the available national and international instruments including bilateral or multilateral treaties on extradition, mutual assistance or a transfer of the proceedings, cooperation with third countries and international organisations with a view to combating sex tourism. Member States should foster open dialogue and communication with countries outside the Union in order to be able to prosecute perpetrators, under the relevant national legislation, who travel outside the Union borders for the purposes of child sex tourism.

(30) Measures to protect child victims should be adopted in their best interest, taking into account an assessment of their needs. Child victims should have easy access to legal remedies and measures to address conflicts of interest where sexual abuse or sexual exploitation of a child occurs within the family. When a special representative should be appointed for a child during a criminal investigation or proceeding, this role may be also carried out by a legal person, an institution or an authority. Moreover, child victims should be protected from penalties, for example under national legislation on prostitution, if they bring their case to the attention of competent authorities. Furthermore, participation in criminal proceedings by child victims should not cause additional trauma to the extent possible, as a result of interviews or visual contact with offenders. A good understanding of children and how they behave when faced with traumatic experiences will help to ensure a high quality of evidence-taking and also reduce the stress placed on children when carrying out the necessary measures.

(31) Member States should consider giving short and long term assistance to child victims. Any harm caused by the sexual abuse and sexual exploitation of a child is significant and should be addressed. Because of the nature of the harm caused by sexual abuse and sexual exploitation, such assistance should continue for as long as necessary for the child's physical and psychological recovery and may last into adulthood if necessary. Assistance and advice should be considered to be extended to parents or guardians of the child victims where they are not involved as suspects in relation to the offence concerned, in order to help them to assist child victims throughout the proceedings.

(32) Framework Decision 2001/220/JHA establishes a set of victims' rights in criminal proceedings, including the right to protection and compensation. In addition child victims of sexual abuse, sexual exploitation and child pornography should be given access to legal counselling and, in accordance with the role of victims in the relevant justice systems, to legal representation, including for the purpose of claiming compensation. Such legal counselling and legal representation could also be provided by the competent authorities for the purpose of claiming compensation from the State. The purpose of legal counselling is to enable victims to be informed and receive advice about the various possibilities open to them. Legal counselling should be provided by a person having received appropriate legal training without necessarily being a lawyer. Legal counselling and, in accordance with the role of victims in the relevant justice systems, legal representation should be provided free of charge, at least when the victim does not have sufficient financial resources, in a manner consistent with the internal procedures of Member States.

(33) Member States should undertake action to prevent or prohibit acts related to the promotion of sexual abuse of children and child sex tourism. Different preventative measures could be considered, such as the drawing up and reinforcement of a code of conduct and self-regulatory mechanisms in the tourism industry, the setting-up of a code of ethics or 'quality labels' for tourist organisations combating child sex tourism, or establishing an explicit policy to tackle child sex tourism.

(34) Member States should establish and/or strengthen policies to prevent sexual abuse and sexual exploitation of children, including measures to discourage and reduce the demand that fosters all forms of sexual exploitation of children, and measures to reduce the risk of children becoming victims, by means of, information and awareness-raising campaigns, and research and education programmes. In such initiatives, Member States should adopt a child-rights based approach. Particular care should be taken to ensure that awareness-raising campaigns aimed at children are appropriate and sufficiently easy to understand. The establishment of help-lines or hotlines should be considered.

(35) Regarding the system of reporting sexual abuse and sexual exploitation of children and helping children in need, hotlines under the number 116 000 for missing children, 116 006 for victims of crime and 116 111 for children, as introduced by Commission Decision 2007/116/EC of 15 February 2007 on reserving the national numbering beginning with 116 for harmonised numbers for harmonised services of social value [1], should be promoted and experience regarding their functioning should be taken into account.

(36) Professionals likely to come into contact with child victims of sexual abuse and sexual exploitation should be adequately trained to identify and deal with such victims. That training should be promoted for members of the following categories when they are likely to come into contact with child victims: police officers, public prosecutors, lawyers, members of the judiciary and court officials, child and health care personnel, but could also involve other groups of persons who are likely to encounter child victims of sexual abuse and sexual exploitation in their work.

(37) In order to prevent the sexual abuse and sexual exploitation of children, intervention programmes or measures targeting sex offenders should be proposed to them. Those intervention programmes or measures should meet a broad, flexible approach focusing on the medical and psycho-social aspects and have a non-obligatory character. Those intervention programmes or measures are without prejudice to intervention programmes or measures imposed by the competent judicial authorities.

(38) Intervention programmes or measures are not provided as an automatic right. It is for the Member State to decide which intervention programmes or measures are appropriate.

(39) To prevent and minimise recidivism, offenders should be subject to an assessment of the danger posed by the offenders and the possible risks of repetition of sexual offences against children. Arrangements for such assessment, such as the type of authority competent to order and carry out the assessment or the moment in or after the criminal proceedings when that assessment should take place as well as arrangements for effective intervention programmes or measures offered following that assessment should be consistent with the internal procedures of Member States. For the same objective of preventing and minimising recidivism, offenders should also have access to effective intervention programmes or measures on a voluntary basis. Those intervention programmes or measures should not interfere with national schemes set up to deal with the treatment of persons suffering from mental disorders.

(40) Where the danger posed by the offenders and the possible risks of repetition of the offences make it appropriate, convicted offenders should be temporarily or permanently prevented from exercising at least professional activities involving direct and regular contacts with children. Employers when recruiting for a post involving direct and regular contact with children are entitled to be informed of existing convictions for sexual offences against children entered in the criminal record, or of existing disqualifications. For the purposes of this Directive, the term 'employers' should also cover persons running an organisation that is active in volunteer work related to the supervision and/or care of children involving direct and regular contact with children. The manner in which such information is delivered, such as for example access via the person concerned, and the precise content of the information, the meaning of organised voluntary activities and direct and regular contact with children should be laid down in accordance with national law.

(41) With due regard to the different legal traditions of the Member States, this Directive takes into account the fact that access to criminal records is allowed only either by the competent authorities or by the person concerned. This Directive does not establish an obligation to modify the national systems governing criminal records or the means of access to those records.

(42) The aim of this Directive is not to harmonise rules concerning consent of the person concerned when exchanging information from the criminal registers, i.e. whether or not to require such consent. Whether the consent is required or not under national law, this Directive does not establish any new obligation to change the national law and national procedures in this respect.

[1] OJ L 49, 17.2.2007, p. 30.

(43) Member States may consider adopting additional administrative measures in relation to perpetrators, such as the registration in sex offender registers of persons convicted of offences referred to in this Directive. Access to those registers should be subject to limitation in accordance with national constitutional principles and applicable data protection standards, for instance by limiting access to the judiciary and/or law enforcement authorities.

(44) Member States are encouraged to create mechanisms for data collection or focal points, at the national or local levels and in collaboration with civil society, for the purpose of observing and evaluating the phenomenon of sexual abuse and sexual exploitation of children. In order to be able to properly evaluate the results of actions to combat sexual abuse and sexual exploitation of children and child pornography, the Union should continue to develop its work on methodologies and data collection methods to produce comparable statistics.

(45) Member States should take appropriate action for setting up information services to provide information on how to recognise the signs of sexual abuse and sexual exploitation.

(46) Child pornography, which constitutes child sexual abuse images, is a specific type of content which cannot be construed as the expression of an opinion. To combat it, it is necessary to reduce the circulation of child sexual abuse material by making it more difficult for offenders to upload such content onto the publicly accessible web. Action is therefore necessary to remove the content and apprehend those guilty of making, distributing or downloading child sexual abuse images. With a view to supporting the Union's efforts to combat child pornography, Member States should use their best endeavours to cooperate with third countries in seeking to secure the removal of such content from servers within their territory.

(47) However, despite such efforts, the removal of child pornography content at its source is often not possible when the original materials are not located within the Union, either because the State where the servers are hosted is not willing to cooperate or because obtaining removal of the material from the State concerned proves to be particularly long. Mechanisms may also be put in place to block access from the Union's territory to Internet pages identified as containing or disseminating child pornography. The measures undertaken by Member States in accordance with this Directive in order to remove or, where appropriate, block websites containing child pornography could be based on various types of public action, such as legislative, non-legislative, judicial or other. In that context, this Directive is without prejudice to voluntary action taken by the Internet industry to prevent the misuse of its services or to any support for such action by Member States. Whichever basis for action or method is chosen, Member States should ensure that it provides an adequate level of legal certainty and predictability to users and service providers. Both with a view to the removal and the blocking of child abuse content, cooperation between public authorities should be established and strengthened, particularly in the interests of ensuring that national lists of websites containing child pornography material are as complete as possible and of avoiding duplication of work. Any such developments must take account of the rights of the end users and comply with existing legal and judicial procedures and the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union. The Safer Internet Programme has set up a network of hotlines the goal of which is to collect information and to ensure coverage and exchange of reports on the major types of illegal content online.

(48) This Directive aims to amend and expand the provisions of Framework Decision 2004/68/JHA. Since the amendments to be made are of substantial number and nature, the Framework Decision should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive.

(49) Since the objective of this Directive, namely to combat sexual abuse, sexual exploitation of children and child pornography, cannot be sufficiently achieved by the Member States alone and can therefore, by reasons of the scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary to achieve that objective.

(50) This Directive respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and in particular the right to the protection of human dignity, the prohibition of torture and inhuman or degrading treatment or punishment, the rights of the child, the right to liberty and security, the right to freedom of expression and information, the right to the protection of personal data, the right to an effective remedy and to a fair trial and the principles of legality and proportionality of criminal offences and penalties. This Directive seeks to ensure full respect for those rights and principles and must be implemented accordingly.

(51) In accordance with Article 3 of the Protocol (No 21) on the position of United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, the United Kingdom and Ireland have notified their wish to take part in the adoption and application of this Directive.

(52) In accordance with Articles 1 and 2 of the Protocol (No 22) on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter

This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, child pornography and solicitation of children for sexual purposes. It also introduces provisions to strengthen the prevention of those crimes and the protection of the victims thereof.

Article 2

Definitions

For the purposes of this Directive, the following definitions apply:

(a) 'child' means any person below the age of 18 years;

(b) 'age of sexual consent' means the age below which, in accordance with national law, it is prohibited to engage in sexual activities with a child;

(c) 'child pornography' means:

(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;

(ii) any depiction of the sexual organs of a child for primarily sexual purposes;

(iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or

(iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes;

(d) 'child prostitution' means the use of a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment in exchange for the child engaging in sexual activities, regardless of whether that payment, promise or consideration is made to the child or to a third party;

(e) 'pornographic performance' means a live exhibition aimed at an audience, including by means of information and communication technology, of:

(i) a child engaged in real or simulated sexually explicit conduct; or

(ii) the sexual organs of a child for primarily sexual purposes;

(f) 'legal person' means an entity having legal personality under the applicable law, except for States or public bodies in the exercise of State authority and for public international organisations.

Article 3

Offences concerning sexual abuse

1. Member States shall take the necessary measures to ensure that the intentional conduct referred to in paragraphs 2 to 6 is punishable.

2. Causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual activities, even without having to participate, shall be punishable by a maximum term of imprisonment of at least 1 year.

3. Causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual abuse, even without having to participate, shall be punishable by a maximum term of imprisonment of at least 2 years.

4. Engaging in sexual activities with a child who has not reached the age of sexual consent shall be punishable by a maximum term of imprisonment of at least 5 years.

5. Engaging in sexual activities with a child, where:

(i) abuse is made of a recognised position of trust, authority or influence over the child, shall be punishable by a maximum term of imprisonment of at least 8 years if the child has not reached the age of sexual consent, and of at least 3 years of imprisonment, if the child is over that age; or

(ii) abuse is made of a particularly vulnerable situation of the child, in particular because of a mental or physical disability or a situation of dependence, shall be punishable by a maximum term of imprisonment of at least 8 years if the child has not reached the age of sexual consent, and of at least 3 years of imprisonment if the child is over that age; or

(iii) use is made of coercion, force or threats shall be punishable by a maximum term of imprisonment of at least 10 years if the child has not reached the age of sexual consent, and of at least 5 years of imprisonment if the child is over that age.

6. Coercing, forcing or threatening a child into sexual activities with a third party shall be punishable by a maximum term of imprisonment of at least 10 years if the child has not reached the age of sexual consent, and of at least 5 years of imprisonment if the child is over that age.

Article 4

Offences concerning sexual exploitation

1. Member States shall take the necessary measures to ensure that the intentional conduct referred to in paragraphs 2 to 7 is punishable.

2. Causing or recruiting a child to participate in pornographic performances, or profiting from or otherwise exploiting a child for such purposes shall be punishable by a maximum term of imprisonment of at least 5 years if the child has not reached the age of sexual consent and of at least 2 years of imprisonment if the child is over that age.

3. Coercing or forcing a child to participate in pornographic performances, or threatening a child for such purposes shall be punishable by a maximum term of imprisonment of at least 8 years if the child has not reached the age of sexual consent, and of at least 5 years of imprisonment if the child is over that age.

4. Knowingly attending pornographic performances involving the participation of a child shall be punishable by a maximum term of imprisonment of at least 2 years if the child has not reached the age of sexual consent, and of at least 1 year of imprisonment if the child is over that age.

5. Causing or recruiting a child to participate in child prostitution, or profiting from or otherwise exploiting a child for such purposes shall be punishable by a maximum term of imprisonment of at least 8 years if the child has not reached the age of sexual consent, and of at least 5 years of imprisonment if the child is over that age.

6. Coercing or forcing a child into child prostitution, or threatening a child for such purposes shall be punishable by a maximum term of imprisonment of at least 10 years if the child has not reached the age of sexual consent, and of at least 5 years of imprisonment if the child is over that age.

7. Engaging in sexual activities with a child, where recourse is made to child prostitution shall be punishable by a maximum term of imprisonment of at least 5 years if the child has not reached the age of sexual consent, and of at least 2 years of imprisonment if the child is over that age.

Article 5

Offences concerning child pornography

1. Member States shall take the necessary measures to ensure that the intentional conduct, when committed without right, referred to in paragraphs 2 to 6 is punishable.

2. Acquisition or possession of child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.

3. Knowingly obtaining access, by means of information and communication technology, to child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.

4. Distribution, dissemination or transmission of child pornography shall be punishable by a maximum term of imprisonment of at least 2 years.

5. Offering, supplying or making available child pornography shall be punishable by a maximum term of imprisonment of at least 2 years.

6. Production of child pornography shall be punishable by a maximum term of imprisonment of at least 3 years.

7. It shall be within the discretion of Member States to decide whether this Article applies to cases involving child pornography as referred to in Article 2(c)(iii), where the person appearing to be a child was in fact 18 years of age or older at the time of depiction.

8. It shall be within the discretion of Member States to decide whether paragraphs 2 and 6 of this Article apply to cases where it is established that pornographic material as referred to in Article 2(c)(iv) is produced and possessed by the producer solely for his or her private use in so far as no pornographic material as referred to in Article 2(c)(i), (ii) or (iii) has been used for the purpose of its production and provided that the act involves no risk of dissemination of the material.

Article 6

Solicitation of children for sexual purposes

1. Member States shall take the necessary measures to ensure that the following intentional conduct is punishable:

the proposal, by means of information and communication technology, by an adult to meet a child who has not reached the age of sexual consent, for the purpose of committing any of the offences referred to in Article 3(4) and Article 5(6), where that proposal was followed by material acts leading to such a meeting, shall be punishable by a maximum term of imprisonment of at least 1 year.

2. Member States shall take the necessary measures to ensure that an attempt, by means of information and communication technology, to commit the offences provided for in Article 5(2) and (3) by an adult soliciting a child who has not reached the age of sexual consent to provide child pornography depicting that child is punishable.

Article 7

Incitement, aiding and abetting, and attempt

1. Member States shall take the necessary measures to ensure that inciting or aiding and abetting to commit any of the offences referred to in Articles 3 to 6 is punishable.

2. Member States shall take the necessary measures to ensure that an attempt to commit any of the offences referred to in Article 3(4), (5) and (6), Article 4(2), (3), (5), (6) and (7), and Article 5(4), (5) and (6) is punishable.

Article 8

Consensual sexual activities

1. It shall be within the discretion of Member States to decide whether Article 3(2) and (4) apply to consensual sexual activities between peers, who are close in age and degree of psychological and physical development or maturity, in so far as the acts did not involve any abuse.

2. It shall be within the discretion of Member States to decide whether Article 4(4) applies to a pornographic performance that takes place in the context of a consensual relationship where the child has reached the age of sexual consent or between peers who are close in age and degree of psychological and physical development or maturity, in so far as the acts did not involve any abuse or exploitation and no money or other form of remuneration or consideration is given as payment in exchange for the pornographic performance.

3. It shall be within the discretion of Member States to decide whether Article 5(2) and (6) apply to the production, acquisition or possession of material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse.

Article 9

Aggravating circumstances

In so far as the following circumstances do not already form part of the constituent elements of the offences referred to in Articles 3 to 7, Member States shall take the necessary measures to ensure that the following circumstances may, in accordance with the relevant provisions of national law, be regarded as aggravating circumstances, in relation to the relevant offences referred to in Articles 3 to 7:

(a) the offence was committed against a child in a particularly vulnerable situation, such as a child with a mental or physical disability, in a situation of dependence or in a state of physical or mental incapacity;

(b) the offence was committed by a member of the child's family, a person cohabiting with the child or a person who has abused a recognised position of trust or authority;

(c) the offence was committed by several persons acting together;

(d) the offence was committed within the framework of a criminal organisation within the meaning of Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime [1];

(e) the offender has previously been convicted of offences of the same nature;

(f) the offender has deliberately or recklessly endangered the life of the child; or

(g) the offence involved serious violence or caused serious harm to the child.

Article 10

Disqualification arising from convictions

1. In order to avoid the risk of repetition of offences, Member States shall take the necessary measures to ensure that a natural person who has been convicted of any of the offences referred to in Articles 3 to 7 may be temporarily or permanently prevented from exercising at least professional activities involving direct and regular contacts with children.

2. Member States shall take the necessary measures to ensure that employers, when recruiting a person for professional or organised voluntary activities involving direct and regular contacts with children, are entitled to request information in accordance with national law by way of any appropriate means, such as access upon request or via the person concerned, of the existence of criminal convictions for any of the offences referred to in Articles 3 to 7 entered in the criminal record or of the existence of any disqualification from exercising activities involving direct and regular contacts with children arising from those criminal convictions.

3. Member States shall take the necessary measures to ensure that, for the application of paragraphs 1 and 2 of this Article, information concerning the existence of criminal convictions for any of the offences referred to in Articles 3 to 7, or of any disqualification from exercising activities involving direct and regular contacts with children arising from those criminal convictions, is transmitted in accordance with the procedures set out in Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States [2] when requested under Article 6 of that Framework Decision with the consent of the person concerned.

[1] OJ L 300, 11.11.2008, p. 42.
[2] OJ L 93, 7.4.2009, p. 23.

Article 11

Seizure and confiscation

Member States shall take the necessary measures to ensure that their competent authorities are entitled to seize and confiscate instrumentalities and proceeds from the offences referred to in Articles 3, 4 and 5.

Article 12

Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons may be held liable for any of the offences referred to in Articles 3 to 7 committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person, based on:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person; or

(c) an authority to exercise control within the legal person.

2. Member States shall also take the necessary measures to ensure that legal persons may be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 7 for the benefit of that legal person.

3. Liability of legal persons under paragraphs 1 and 2 shall be without prejudice to criminal proceedings against natural persons who are perpetrators, inciters or accessories to the offences referred to in Articles 3 to 7.

Article 13

Sanctions on legal persons

1. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 12(1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and may include other sanctions, such as:

(a) exclusion from entitlement to public benefits or aid;

(b) temporary or permanent disqualification from the practice of commercial activities;

(c) placing under judicial supervision;

(d) judicial winding-up; or

(e) temporary or permanent closure of establishments which have been used for committing the offence.

2. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 12(2) is punishable by sanctions or measures which are effective, proportionate and dissuasive.

Article 14

Non-prosecution or non-application of penalties to the victim

Member States shall, in accordance with the basic principles of their legal systems take the necessary measures to ensure that competent national authorities are entitled not to prosecute or impose penalties on child victims of sexual abuse and sexual exploitation for their involvement in criminal activities, which they have been compelled to commit as a direct consequence of being subjected to any of the acts referred to in Article 4(2), (3), (5) and (6), and in Article 5(6).

Article 15

Investigation and prosecution

1. Member States shall take the necessary measures to ensure that investigations into or the prosecution of the offences referred to in Articles 3 to 7 are not dependent on a report or accusation being made by the victim or by his or her representative, and that criminal proceedings may continue even if that person has withdrawn his or her statements.

2. Member States shall take the necessary measures to enable the prosecution of any of the offences referred to in Article 3, Article 4(2), (3), (5), (6) and (7) and of any serious offences referred to in Article 5(6) when child pornography as referred to in Article 2(c)(i) and (ii) has been used, for a sufficient period of time after the victim has reached the age of majority and which is commensurate with the gravity of the offence concerned.

3. Member States shall take the necessary measures to ensure that effective investigative tools, such as those which are used in organised crime or other serious crime cases are available to persons, units or services responsible for investigating or prosecuting offences referred to in Articles 3 to 7.

4. Member States shall take the necessary measures to enable investigative units or services to attempt to identify the victims of the offences referred to in Articles 3 to 7, in particular by analysing child pornography material, such as photographs and audiovisual recordings transmitted or made available by means of information and communication technology.

Article 16

Reporting suspicion of sexual abuse or sexual exploitation

1. Member States shall take the necessary measures to ensure that the confidentiality rules imposed by national law on certain professionals whose main duty is to work with children do not constitute an obstacle to the possibility, for those professionals, of their reporting to the services responsible for child protection any situation where they have reasonable grounds for believing that a child is the victim of offences referred to in Articles 3 to 7.

2. Member States shall take the necessary measures to encourage any person who knows about or suspects, in good faith that any of the offences referred to in Articles 3 to 7 have been committed, to report this to the competent services.

Article 17

Jurisdiction and coordination of prosecution

1. Member States shall take the necessary measures to establish their jurisdiction over the offences referred to in Articles 3 to 7 where:

(a) the offence is committed in whole or in part within their territory; or

(b) the offender is one of their nationals.

2. A Member State shall inform the Commission where it decides to establish further jurisdiction over an offence referred to in Articles 3 to 7 committed outside its territory, inter alia, where:

(a) the offence is committed against one of its nationals or a person who is an habitual resident in its territory;

(b) the offence is committed for the benefit of a legal person established in its territory; or

(c) the offender is an habitual resident in its territory.

3. Member States shall ensure that their jurisdiction includes situations where an offence referred to in Articles 5 and 6, and in so far as is relevant, in Articles 3 and 7, is committed by means of information and communication technology accessed from their territory, whether or not it is based on their territory.

4. For the prosecution of any of the offences referred to in Article 3(4), (5) and (6), Article 4(2), (3), (5), (6) and (7) and Article 5(6) committed outside the territory of the Member State concerned, as regards paragraph 1(b) of this Article, each Member State shall take the necessary measures to ensure that its jurisdiction is not subordinated to the condition that the acts are a criminal offence at the place where they were performed.

5. For the prosecution of any of the offences referred to in Articles 3 to 7 committed outside the territory of the Member State concerned, as regards paragraph 1(b) of this Article, each Member State shall take the necessary measures to ensure that its jurisdiction is not subordinated to the condition that the prosecution can only be initiated following a report made by the victim in the place where the offence was committed, or a denunciation from the State of the place where the offence was committed.

Article 18

General provisions on assistance, support and protection measures for child victims

1. Child victims of the offences referred to in Articles 3 to 7 shall be provided assistance, support and protection in accordance with Articles 19 and 20, taking into account the best interests of the child.

2. Member States shall take the necessary measures to ensure that a child is provided with assistance and support as soon as the competent authorities have a reasonable-grounds indication for believing that a child might have been subject to any of the offences referred to in Articles 3 to 7.

3. Member States shall ensure that, where the age of a person subject to any of the offences referred to in Articles 3 to 7 is uncertain and there are reasons to believe that the person is a child, that person is presumed to be a child in order to receive immediate access to assistance, support and protection in accordance with Articles 19 and 20.

Article 19

Assistance and support to victims

1. Member States shall take the necessary measures to ensure that assistance and support are provided to victims before, during and for an appropriate period of time after the conclusion of criminal proceedings in order to enable them to exercise the rights set out in Framework Decision 2001/220/JHA, and in this Directive. Member States shall, in particular, take the necessary steps to ensure protection for children who report cases of abuse within their family.

2. Member States shall take the necessary measures to ensure that assistance and support for a child victim are not made conditional on the child victim's willingness to cooperate in the criminal investigation, prosecution or trial.

3. Member States shall take the necessary measures to ensure that the specific actions to assist and support child victims in enjoying their rights under this Directive, are undertaken following an individual assessment of the special circumstances of each particular child victim, taking due account of the child's views, needs and concerns.

4. Child victims of any of the offences referred to in Articles 3 to 7 shall be considered as particularly vulnerable victims pursuant to Article 2(2), Article 8(4) and Article 14(1) of Framework Decision 2001/220/JHA.

5. Member States shall take measures, where appropriate and possible, to provide assistance and support to the family of the child victim in enjoying the rights under this Directive when the family is in the territory of the Member States. In particular, Member States shall, where appropriate and possible, apply Article 4 of Framework Decision 2001/220/JHA to the family of the child victim.

Article 20

Protection of child victims in criminal investigations and proceedings

1. Member States shall take the necessary measures to ensure that in criminal investigations and proceedings, in accordance with the role of victims in the relevant justice system, competent authorities appoint a special representative for the child victim where, under national law, the holders of parental responsibility are precluded from representing the child as a result of a conflict of interest between them and the child victim, or where the child is unaccompanied or separated from the family.

2. Member States shall ensure that child victims have, without delay, access to legal counselling and, in accordance with the role of victims in the relevant justice system, to legal representation, including for the purpose of claiming compensation. Legal counselling and legal representation shall be free of charge where the victim does not have sufficient financial resources.

3. Without prejudice to the rights of the defence, Member States shall take the necessary measures to ensure that in criminal investigations relating to any of the offences referred to in Articles 3 to 7:

(a) interviews with the child victim take place without unjustified delay after the facts have been reported to the competent authorities;

(b) interviews with the child victim take place, where necessary, in premises designed or adapted for this purpose;

(c) interviews with the child victim are carried out by or through professionals trained for this purpose;

(d) the same persons, if possible and where appropriate, conduct all interviews with the child victim;

(e) the number of interviews is as limited as possible and interviews are carried out only where strictly necessary for the purpose of criminal investigations and proceedings;

(f) the child victim may be accompanied by his or her legal representative or, where appropriate, by an adult of his or her choice, unless a reasoned decision has been made to the contrary in respect of that person.

4. Member States shall take the necessary measures to ensure that in criminal investigations of any of the offences referred to in Articles 3 to 7 all interviews with the child victim or, where appropriate, with a child witness, may be audio-visually recorded and that such audio-visually recorded interviews may be used as evidence in criminal court proceedings, in accordance with the rules under their national law.

5. Member States shall take the necessary measures to ensure that in criminal court proceedings relating to any of the offences referred to in Articles 3 to 7, that it may be ordered that:

(a) the hearing take place without the presence of the public;

(b) the child victim be heard in the courtroom without being present, in particular through the use of appropriate communication technologies.

6. Member States shall take the necessary measures, where in the interest of child victims and taking into account other overriding interests, to protect the privacy, identity and image of child victims, and to prevent the public dissemination of any information that could lead to their identification.

Article 21

Measures against advertising abuse opportunities and child sex tourism

Member States shall take appropriate measures to prevent or prohibit:

(a) the dissemination of material advertising the opportunity to commit any of the offences referred to in Articles 3 to 6; and

(b) the organisation for others, whether or not for commercial purposes, of travel arrangements with the purpose of committing any of the offences referred to in Articles 3 to 5.

Article 22

Preventive intervention programmes or measures

Member States shall take the necessary measures to ensure that persons who fear that they might commit any of the offences referred to in Articles 3 to 7 may have access, where appropriate, to effective intervention programmes or measures designed to evaluate and prevent the risk of such offences being committed.

Article 23

Prevention

1. Member States shall take appropriate measures, such as education and training, to discourage and reduce the demand that fosters all forms of sexual exploitation of children.

2. Member States shall take appropriate action, including through the Internet, such as information and awareness-raising campaigns, research and education programmes, where appropriate in cooperation with relevant civil society organisations and other stakeholders, aimed at raising awareness and reducing the risk of children, becoming victims of sexual abuse or exploitation.

3. Member States shall promote regular training for officials likely to come into contact with child victims of sexual abuse or exploitation, including front-line police officers, aimed at enabling them to identify and deal with child victims and potential child victims of sexual abuse or exploitation.

Article 24

Intervention programmes or measures on a voluntary basis in the course of or after criminal proceedings

1. Without prejudice to intervention programmes or measures imposed by the competent judicial authorities under national law, Member States shall take the necessary measures to ensure that effective intervention programmes or measures are made available to prevent and minimise the risks of repeated offences of a sexual nature against children. Such programmes or measures shall be accessible at any time during the criminal proceedings, inside and outside prison, in accordance with national law.

2. The intervention programmes or measures, referred to in paragraph 1 shall meet the specific developmental needs of children who sexually offend.

3. Member States shall take the necessary measures to ensure that the following persons may have access to the intervention programmes or measures referred to in paragraph 1:

(a) persons subject to criminal proceedings for any of the offences referred to in Articles 3 to 7, under conditions which are neither detrimental nor contrary to the rights of the defence or to the requirements of a fair and impartial trial, and, in particular, in compliance with the principle of the presumption of innocence; and

(b) persons convicted of any of the offences referred to in Articles 3 to 7.

4. Member States shall take the necessary measures to ensure that the persons referred to in paragraph 3 are subject to an assessment of the danger that they present and the possible risks of repetition of any of the offences referred to in Articles 3 to 7, with the aim of identifying appropriate intervention programmes or measures.

5. Member States shall take the necessary measures to ensure that the persons referred to in paragraph 3 to whom intervention programmes or measures in accordance with paragraph 4 have been proposed:

(a) are fully informed of the reasons for the proposal;

(b) consent to their participation in the programmes or measures with full knowledge of the facts;

(c) may refuse and, in the case of convicted persons, are made aware of the possible consequences of such a refusal.

Article 25

Measures against websites containing or disseminating child pornography

1. Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.

2. Member States may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.

Article 26

Replacement of Framework Decision 2004/68/JHA

Framework Decision 2004/68/JHA is hereby replaced in relation to Member States participating in the adoption of this Directive without prejudice to the obligations of those Member States relating to the time limits for transposition of the Framework Decision into national law.

In relation to Member States participating in the adoption of this Directive, references to Framework Decision 2004/68/JHA shall be construed as references to this Directive.

Article 27

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 18 December 2013.

2. Member States shall transmit to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Directive.

3. When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

Article 28

Reporting

1. The Commission shall, by 18 December 2015, submit a report to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by a legislative proposal.

2. The Commission shall, by 18 December 2015, submit a report to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25.

Article 29

Entry into force

This Directive shall enter into force on the day of its publication in the *Official Journal of the European Union*.

Article 30

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Strasbourg, 13 December 2011.

For the European Parliament	*For the Council*
The President	*The President*
J. BUZEK	M. SZPUNAR

EUROPEAN
COMMISSION

Brussels, 16.12.2016
COM(2016) 871 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography

Contents

1. INTRODUCTION 3

1.1. Objectives and scope of the Directive 3

1.2. Purpose and methodology of the report 5

2. TRANSPOSITION MEASURES 7

2.1. Investigation and prosecution of offences (Articles 2 to 9 and 11 to 17) 7

2.1.1. Definitions (Article 2) 7

2.1.2. Offences concerning sexual abuse (Article 3) 7

2.1.3. Offences concerning sexual exploitation (Article 4) 8

2.1.4. Offences concerning child pornography (Article 5) 9

2.1.5. Solicitation of children for sexual purposes (Article 6) 9

2.1.6. Incitement, aiding and abetting, and attempt (Article 7) 9

2.1.7. Consensual sexual activities (Article 8) 10

2.1.8. Aggravating circumstances (Article 9) 10

2.1.9. Seizure and confiscation (Article 11) 11

2.1.10. Liability of legal persons (Article 12) 11

2.1.11. Sanctions on legal persons (Article 13) 12

2.1.12. Non-prosecution or non-application of penalties to the victim (Article 14) 12

2.1.13. Investigation and prosecution (Article 15) 12

2.1.14. Reporting suspicion of sexual abuse or sexual exploitation (Article 16) 13

2.1.15. Jurisdiction and coordination of prosecution (Article 17) 13

2.2. Assistance to and protection of victims (Articles 18 to 20) 14

2.2.1. General provisions on assistance, support and protection measures for child victims (Article 18) 14

2.2.2. Assistance and support to victims (Article 19) 15

2.2.3. Protection of child victims in criminal investigations and proceedings (Article 20) 16

2.3. Prevention (Articles 10 and 21 to 25) 16

2.3.1. Disqualification arising from convictions (Article 10) 16

2.3.2. Measures against advertising abuse opportunities and child sex tourism (Article 21) 17

2.3.3. Preventive intervention programmes or measures (Article 22) 18

2.3.4. Prevention (Article 23) 18

2.3.5. Intervention programmes or measures on a voluntary basis in the course of or after criminal proceedings (Article 24) 18

2.3.6. Measures against websites containing or disseminating child pornography (Article 25) 19

3. CONCLUSION AND NEXT STEPS 20

1. INTRODUCTION

Sexual abuse and sexual exploitation of children are particularly serious crimes. They cause long-term physical, psychological and social harm to vulnerable victims who have rights to as well as needs for special protection and care. In addition, child sexual abuse material, referred to in legislation as 'child pornography', represents multiple crimes against each victim. First, the sexual abuse which was photographed or recorded. Thereafter, every time the images and videos are posted, circulated or viewed, a gross violation of the child's privacy is committed. Trauma is added when the child knows that the images and videos are being circulated and friends or relatives may see them.

To fight these crimes effectively an integrated and holistic approach is needed, encompassing **investigation and prosecution of crimes, assistance to and protection of victims, and prevention**.

1.1. Objectives and scope of the Directive

The Directive follows the holistic approach required to fight these crimes effectively, incorporating in a comprehensive legal instrument provisions covering investigation and prosecution of offences (Articles 2 to 9 and 11 to 17), assistance to and protection of victims (Articles 18 to 20), and prevention (Articles 10 and 21 to 25).

To effectively **investigate and prosecute offences**, the Directive notably includes:

- Criminalisation of a wide range of situations of child sexual abuse and exploitation, online and offline (20 different offences, Articles 2 to 7). These include new phenomena such as online grooming (Article 6) and webcam sexual abuse and online viewing of child abuse images without downloading them (Article 5, in particular paragraph 3).
- Increased levels of penalties. The maximum penalties set by national legislation must not be lower than certain levels (ranging from 1 to 10 years in prison), depending on the seriousness of the offence (Articles 3 to 6). A number of aggravating circumstances must also be taken into account (Article 9).
- Extension of the statute of limitations after the victim has reached age of majority (Article 15(2)).
- Obligation to provide law enforcement and prosecution services with effective tools to investigate child sexual abuse, child sexual exploitation and child pornography offences, such as those used to investigate organised and serious crime (Article 15(3)). Law enforcement must also be put in a position to identify the victims of these offences (Article 15(4)).
- Removal of obstacles (created by confidentiality rules) to reporting by professionals whose main duty involves working with children (Article 16).
- Jurisdiction for cases perpetrated by offenders who are nationals of the investigating country, so that they can also be prosecuted in their country for crimes they commit in other Member States or third countries (Articles 17(1) to (3)).
- Removal of conditions of dual criminality and reporting in the place where the offence was committed when prosecuting crimes committed in other Member States or third countries (Articles 17(4) and 17(5)).

With regard to **assistance to and protection of child victims**, the Directive notably includes provisions requiring:

- Extensive assistance, support and protection measures, in particular to prevent child victims from suffering additional trauma through their involvement in criminal investigations and proceedings, inter alia by setting specific standards for interviews with child victims (Articles 18 to 20).
- Assistance and support as soon as there are reasonable grounds to suspect an offence (Article 18(2)).
- Special protection for children reporting abuse within the family (Article 19(1)).
- Assistance and support not conditional on cooperation with criminal proceedings (Article 19(2)).
- Protection of the victim's privacy, identity and image (Article 20(6)).

Finally, **to prevent these crimes**, the Directive notably includes:

- Mechanisms to enable excluding convicted offenders from professional activities involving direct and regular contact with children (Article 10(1)).
- The right of employers to request information about convictions and disqualifications for professional or organised voluntary activities involving direct and regular contact with children (Article 10(2)).
- Facilitation of the exchange of information between national criminal registers (through the ECRIS[1] system), to ensure that background checks by employers are complete and include information on offences committed by offenders anywhere in the EU (Article 10(3)).
- A requirement that Member States make intervention programmes or measures such as treatment available to convicted offenders and others who fear they could offend (Articles 22 and 24).
- An obligation on Member States to carry out prevention activities such as education, awareness raising and training of officials (Article 23).
- Mandatory assessment for all convicted offenders of the danger they represent and risk of recidivism (Article 24(4)).
- An obligation on Member States to ensure prompt removal of webpages containing or disseminating child pornography in their territory and to work to obtain removal if hosted outside their territory (Article 25(1)).
- An option for Member States to block access by users in their territory to webpages containing or disseminating child pornography through different means, including public action and self-regulation by the industry (Article 25(2)).

[1] European Criminal Records Information System, regulated by Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, and Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA. More information on ECRIS is available at http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm.

1.2. Purpose and methodology of the report

Article 27 of the Directive requires Member States[2] to bring into force the laws, regulations and administrative provisions necessary to comply with the Directive and communicate them to the Commission by 18 December 2013.

This report responds to the requirement under Article 28(1) of the Directive for the Commission to report to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with the Directive.[3] The report aims to provide a concise yet informative overview of the main transposition measures taken by Member States.

Member States have faced significant challenges inherent in transposing and implementing such a comprehensive and ambitious Directive, which:

- requires the adoption of legislation in many different areas, including substantive criminal law (e.g. definitions of offences and the level of penalties, the statute of limitations and the liability of legal persons) and procedural criminal law (e.g. extraterritorial jurisdiction, the participation of children in criminal proceedings, and legal representation);
- entails extensive administrative measures to complement the legislation (e.g. on access to information and the exchange of criminal records between Member States, training of the police and judiciary, and rules on child protection, law enforcement and prisons); and
- involves multiple actors, not only within the authorities of a Member State (i.e. at different levels of government, such as national and regional), but also in cooperation with non-governmental organisations (e.g. to disrupt the distribution of child sexual abuse material through hotlines and awareness raising campaigns), internet service providers (e.g. to disrupt the distribution of child sexual abuse material), clinical psychologists (e.g. in intervention programmes for offenders), and others.

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

On the basis of national transposition measures officially communicated to the Commission, the Directive has been transposed by means of more than 330 acts in force prior to the Directive and by around 300 new acts introduced since 2012 across all Member States.

Member States sent around 700 notifications to the Commission. 70% of these were received after the transposition deadline of 18 December 2013. The content covered legislation (new and amending acts), administrative provisions and working arrangements. Often, they included entire criminal codes and amending acts.

[2] From this point onwards, 'Member States' or 'all Member States' refer to the Member States bound by the Directive (i.e. all EU Member States except Denmark). In accordance with Articles 1 and 2 of Protocol 22 on the Position of Denmark, Denmark did not take part in the adoption of the Directive, nor does the Directive apply to it. However Council Framework Decision 2004/68/JHA continues to be applicable to and binding upon Denmark. In accordance with Article 3 of Protocol 21 on the position of the United Kingdom and Ireland, both took part in the adoption of the Directive and are bound by it.

[3] In accordance with Article 28(2) of the Directive, the implementation of Article 25 on measures against websites containing or disseminating child pornography is assessed in a separate report (COM(2016) 872) published jointly with this one.

By the transposition deadline, only 12 Member States had notified the Commission that they had completed transposition of the Directive. The Commission therefore opened infringement proceedings for non-communication of national transposition measures against the others: **BE, BG, IE, EL, ES, IT, CY, LT, HU, MT, NL, PT, RO, SI** and the **UK**.[4] All these infringement proceedings had been closed by 8 December 2016. The late adoption and notification of national transposition measures delayed the Commission's analysis and publication of the transposition reports.

The description and analysis in this report are based on the information that Member States provided by 1 November 2016. Notifications received after that date have not been taken into account. Beyond the issues identified in this report, there may be both further challenges in transposition and other provisions not reported to the Commission or further legislative and non-legislative developments. Therefore, this report does not prevent the Commission from further evaluating some provisions, to continue supporting Member States in the transposition and implementation of the Directive.

[4] Member States in this document are abbreviated according to these rules: http://publications.europa.eu/code/en/en-370100.htm

2. TRANSPOSITION MEASURES

2.1. Investigation and prosecution of offences (Articles 2 to 9 and 11 to 17)

2.1.1. Definitions (Article 2)

Article 2 lays down definitions for terms used throughout the Directive: child, age of sexual consent, child pornography, child prostitution, pornographic performance and legal person.

- All Member States except **HU** define a child as any person below age 18.
- The age of sexual consent varies across Member States: 14 years (**AT, BG, DE, EE, HU** and **PT**), 15 years (**CZ, FR, HR, PL, SE, SI** and **SK**), 16 years (**BE, ES, LT, LU, LV, NL** and **UK**), 17 years (**CY** and **IE**) and 18 years (**MT**). **FI, IT** and **RO** have different ages of sexual consent depending on the nature of the offence. In **EL,** the age of consent is different for consensual male homosexual activities (17 years), and consensual heterosexual activities and female homosexual activities (15 years).
- **BE, CY, EE, EL, ES, HR, IE, IT, LV, PT, RO, SE, SK** and **UK (Gibraltar)** use the term 'child pornography' in their legislation. All other Member States use different terms, such as pornographic depictions (**AT**), pornographic material (**BG**), pornographic work (**CZ**), pornographic picture or depiction (**FR**), and others.
- With regard to child prostitution, **CY** and **SK** have included an explicit definition in their transposing legislation which includes all elements of Article 2(d). On the other hand, in **AT, BG, CZ, DE, EL, LT, LU, SE, SI** and **UK** the transposition follows from case law and other sources in conjunction with the child prostitution offences (Articles 4(5) to 4(7)), whereas in the case of **BE, EE, ES, FI, FR, HR, IT, MT, NL, PL, PT** and **RO** it follows solely from the child prostitution offences.
- An explicit definition of pornographic performance is included in the legislation of **AT, BG, CY, EL, HU, IE, RO, SK** and **UK (Gibraltar).** Other Member States transpose Article 2 in conjunction with the offences in Articles 4(2) to 4(4) and a direct reference to information and communication technology, or case law.
- None of the Member States include states or public bodies in the exercise of state authority and public international organisations within the concept of a 'legal person'.

2.1.2. Offences concerning sexual abuse (Article 3)

Article 3 defines the intentional conduct which constitutes an offence concerning sexual abuse.

- Most Member States have adopted provisions that punish causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual activities (Article 3(2)) or sexual abuse (Article 3(3)), with the penalty levels required in the Directive.
- **CY, CZ, DE, EE, FR, IE, IT, LT, LV, MT, PL, SI** and **SK** include offences which penalise engaging in any sexual act with a child under the age of sexual consent in a similar manner as Article 3(4). **AT, BE, BG, ES, HR, LU RO, PT** and **SE** differentiate between sexual acts involving penetration and those involving no penetration.

- With regard to engaging in sexual activities with a child in which abuse is made of a recognised position of trust, authority or influence (Article 3(5)(i)) or of a particularly vulnerable situation of the child (Article 3(5)(ii)), a majority of Member States have adopted legislation that does not seem to cover all these situations, or have adopted penalty levels that are too low.

  On the other hand, most Member States have adopted legislation that penalises engaging in sexual activities with a child where use is made of coercion, force or threats, with the level of penalties required by the Directive (Article 3(5)(iii)). Whereas **CY, DE, LU** and **MT** mention 'coercion, force and threat', other Member States refer to 'violence and threat' (**CZ, EL, FI, FR, LT, LU, LV, NL, PT, SE** and **SK**), 'force and threat' (**BE, BG, DE, HR, HU, IT, PL** and **SI**), 'violence and intimidation' (**ES**), 'against a child's will' (**EE**), 'coercion by use of force' (**AT**) and other terminology.

- In relation to coercing, forcing or threatening a child into sexual activities with a third party (Article 3(6)), **CY, DE, FR, LU, MT, NL** and **PT** explicitly refer in their legislation to the commission of the offence with a third person, while **AT, BG, CZ, ES, HU, IE, IT, LT, RO, SE** and **SI** cover this implicitly or through the provision on rape, sexual assault or sexual abuse through coercion, force or threat.

2.1.3. Offences concerning sexual exploitation (Article 4)

Article 4 defines the intentional conduct which constitutes an offence concerning sexual exploitation.

- With regard to causing or recruiting a child to participate in pornographic performances (Article 4(2)), **AT, BG, CY, DE, EL, ES, IT, LT, MT, NL, RO, SK** and **UK** (**Gibraltar**) have enacted legislation that transposes this provision of the Directive. The information from the other Member States was not conclusive.

- Under Article 4(3), Member States must sanction the coercing or forcing a child to participate in pornographic performances, or threatening a child for such purposes. **AT, BG, CY, DE, EL, ES, IE, IT, LT, MT, NL, SI, SK** and **UK** (**Gibraltar**) have in place legislation that transposes this provision of the Directive. Member States use different wording in order to illustrate 'coercion, force and threat'. For example, **BG, DE, HR, HU, IT, PL** and **SI** refer to 'force and threat', **BG** to 'force, threat of serious harm', **EL** to 'coercion or violence or threat' and **ES** to 'use of violence or intimidation'.

- Article 4(4) punishes knowingly attending pornographic performances involving the participation of a child. **AT, BG, CY, DE, ES, FI, IE, IT, LT, MT, RO, SI, SK** and **UK (Gibraltar)** have in place legislation that transposes this provision of the Directive. The information from the other Member States was not conclusive.

- Under Article 4(5), Member States shall punish causing or recruiting a child to participate in child prostitution, or profiting from or otherwise exploiting a child for such purposes. **BE, BG, CY, CZ, DE, EL, ES, FR, HR, IT, LT, LU, MT, NL, PT, RO, SE, SI, SK** and **UK** have in place legislation that transposes this provision of the Directive. The information from the other Member States was not conclusive.

- Article 4(6) punishes coercing or forcing a child into child prostitution, or threatening a child for such purposes. **AT, BG, CY, CZ, DE, EE, EL, ES, FR, HR, IT, LT, LU, MT, NL, PT, RO, SI, SK** and **UK (Scotland)** have in place legislation that

transposes this provision of the Directive. The information from the other Member States was not conclusive.

- Article 4(7) penalises engaging in sexual activities with a child where recourse is made to child prostitution. Most Member States have in place legislation that transposes this provision. For **HU, IE, LV, PL, PT, RO** and **SE** the information was not conclusive.

2.1.4. Offences concerning child pornography (Article 5)

Article 5 defines the intentional conduct which constitutes an offence concerning child pornography.

- Article 5(2) punishes the acquisition or possession of child pornography. The information provided by most Member States was not conclusive, except in **AT, BG, CY, ES, FI, FR, LT, MT, RO** and **SI.**
- Article 5(3) punishes knowingly obtaining access to child pornography by means of information and communication technology. Most Member States transposed the requirement of 'knowingly obtaining access', despite some using different terminology. For example, **DE** uses the term 'undertaking to retrieve' and **HU** refers to 'obtaining and keeping'.
- Article 5(4) punishes the distribution, dissemination or transmission of child pornography. Most Member States employ different terminology when referring to 'distribution', 'dissemination' or 'transmission' of child pornography. For example, the term 'transmission' has been interpreted as the equivalent of 'mediation' (**CZ**), 'broadcasting' (**BG** and **DE**), 'spreading' (**IT**) or 'granting access' (**LT**).
- Article 5(5) penalises offering, supplying or making available child pornography. The majority of Member States use different terms to 'offering', 'supplying' and 'making available'. For example, **CZ** uses the terms 'import', 'selling' or 'provision in another manner', instead of the term 'supplying', whereas **SE** uses a general term of 'making [child pornography] available'.
- Article 5(6) penalises the production of child pornography. All Member States use the same term of 'production' in their transposition, except **FR** ('setting and recording') and **UK** ('taking', 'making' and 'permitting to take').
- Articles 5(7) and 5(8) are optional provisions concerning the applicability of Article 5 to specific situations. All Member States except **AT, DE, ES, SE** and **UK** (Article 5(7)) and **AT** and **DE** (Article 5(8)) decided not to apply them.

2.1.5. Solicitation of children for sexual purposes (Article 6)

Article 6 defines the intentional conduct which constitutes an offence concerning solicitation of children for sexual purposes.

Most Member States have in place legislation that transposes this Article. The information was not conclusive in **CY, HR, HU, IE, LU, LV, PL, RO** and **UK** (Article 6(1)) nor in **BE, CY, LV** and **PL** (Article 6(2)).

2.1.6. Incitement, aiding and abetting, and attempt (Article 7)

Article 7 requires Member States to punish the incitement, aiding and abetting and attempt to commit the offences contained in Articles 3 to 6.

- All Member States have taken measures transposing Article 7(1).
- Article 7(2) has mostly been transposed through general provisions on attempt, except in **CY, DE, FI, FR, HR, IE, LU, PT, RO** and **SE**, which have introduced specific provisions punishing the attempt of the sexual offences listed in Article 7(2).

2.1.7. Consensual sexual activities (Article 8)

Article 8 sets out three optional provisions concerning consensual sexual activities. **CY** and **UK (England/Wales)** chose to apply all three, whereas **BE, BG, CZ, EE, IE, LU, LV, MT, NL, PL, SK** chose to not apply any of them.

- **AT, CY, FI, EL, ES, HR, HU, IT, LT, LV, PT, RO, SE, SI** and **UK (England/Wales** and **Northern Ireland)** chose to apply Article 8(1).
- **CY, HR, SE** and **UK (England/Wales** and **Scotland)** chose to apply Article 8(2).
- **AT, CY, DE, FI, HR** and **UK** chose to apply Article 8(3). **DE, FI** and **UK** apply the option to both the possession and the production of child pornography, while **FR** only applies it to the production of child pornography.

2.1.8. Aggravating circumstances (Article 9)

Article 9 defines the situations that may be regarded as aggravating circumstances in relation to the offences referred to in Articles 3 to 7.

In most Member States, the situations of application of aggravating circumstances are described in the law. That was not the case for some provisions of this Article in **IE** and the **UK** (**England/Wales, Northern Ireland,** and **Scotland**) where the courts have more discretion in taking into account aggravating circumstances when sentencing.

- Article 9(a) refers to offences committed against a child in a particularly vulnerable situation, a situation of dependence or in a state of mental or physical incapacity. Most Member States have in place legislation that transposes this provision. For **BE, DE, ES, IE, LU, PL, SI** and **UK (England/Wales, Scotland** and **Gibraltar)** the information was not conclusive.
- Article 9(b) refers to offences committed by a member of the child's family, a person cohabiting with the child or a person who has abused a recognised position of trust or authority. Most Member States have in place legislation that transposes this provision. For **AT, BE, BG, DE, ES, IE, LT, LU, PL, RO, SI** and **UK** (**England**/**Wales**, **Scotland** and **Gibraltar**) the information was not conclusive.
- Under Article 9(c), if the offence was committed by several persons acting together, this should be seen as an aggravating circumstance. Whereas **CY**, **HR** and **IT** explicitly refer to 'several persons' acting together, other Member States use different terminology. For example, **BE** mentions 'one or more persons', **BG, EL, MT, NL** and **PT**, 'two or more persons', **DE** and **SE** 'more than one person'.
- Pursuant to Article 9(d), an offence should be penalised more severely if it was committed within the framework of a criminal organisation. Most Member States have in place legislation that transposes this provision, including the transposition of the definition 'criminal organisation', with **MT** making a direct reference to Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime.

- Under Article 9(e), if the offender has previously been convicted of offences of the same nature, this should constitute an aggravating circumstance. **AT, BE, CZ, HR, IT, LV, PT** and **SK** foresee a general aggravating circumstance, irrespective of whether the subsequent offence is of a similar nature or not. On the other hand, the commission of an offence of the same nature is required in **BG, CY, EE, ES, FI, HU, MT,** and **PL**. Separate consideration for both options (similar offences and unrelated offences) is foreseen in **FR** and **LT**.
- Article 9(f) foresees an aggravating circumstance when the offender has deliberately or recklessly endangered the life of the child. Most Member States have in place legislation that transposes this provision. For **BE, CZ, ES, FI, FR, IE, IT, LV, SK** and **UK** the information was not conclusive.
- Under Article 9(g), a more severe penalty should be considered if the offence involved serious violence or caused serious harm to the child. Most Member States have in place legislation that transposes this provision. For **BG, ES, FI, IE, LT** and **UK** (**Scotland**) the information was not conclusive.

2.1.9. Seizure and confiscation (Article 11)

Under Article 11, Member States must ensure that their competent authorities are entitled to seize and confiscate instrumentalities and proceeds from the offences referred to in Articles 3, 4 and 5.

Whereas some Member States (**BG, CY, DE, HR, FR, IT, LU** and **SI**) have introduced specific provisions dealing with seizure and confiscation in case of the offences referred to in Articles 3, 4 and 5, the rest of Member States rely on general rules on seizure and confiscation under criminal law, which apply to all criminal offences.

The national laws of all Member States address both the instrumentalities used and the proceeds made from the crime.

2.1.10. Liability of legal persons (Article 12)

Article 12 requires Member States to ensure that legal persons may be held liable for any of the offences referred to in Articles 3 to 7.

- With regard to Articles 12(1)(a) to (c), **CY, LT** and **PL** use the same or almost the same wording as the Directive, whereas the other Member States use different terms. For example, when transposing Article 12(1)(b), Member States refer to 'managers', 'directors' or 'board of directors', instead of 'an authority to take decisions on behalf of the legal person'.
- The liability required in Article 12(2) has been introduced by almost all Member States. For **BG, CZ, IE, LU, NL** and **PT** the information was not conclusive.
- With regard to Article 12(3), all Member States provide for the possibility of pursuing criminal proceedings against natural persons, who are perpetrators, inciters or accessories, simultaneously to the enforcement of the liability of legal persons. However, the information provided by **IE** and **PT** was not conclusive on the offences covered.

2.1.11. Sanctions on legal persons (Article 13)

Under Article 13, Member States shall introduce sanctions for the legal persons held liable pursuant to Article 12(1) or (2) and can choose to impose the sanctions foreseen in Articles 13(1)(a) to (e).

- With regard to Article 13(1), all Member States have introduced administrative or criminal penalties that are applicable to legal persons. Some Member States (**BE, CZ, FR, PL, RO** and **SK**) have also chosen to introduce the additional sanction of publishing or displaying the decision/judgement in which the legal person was found guilty of the crime. Most Member States, with the exception of **BG, DE, EE, FI, IE** and **UK (England/Wales, Northern Ireland** and **Gibraltar)** have chosen to transpose at least one of the options set out in Articles 13(1)(a) to (e).
- Most Member States' legislation does not contain provisions to specifically transpose Article 13(2), but imposes the same sanctions on legal persons held liable under Article 12(2) as on those held liable under Article 12(1). Only **EL** introduced a specific transposing measure and thus did not apply the same sanctions in both cases.

2.1.12. Non-prosecution or non-application of penalties to the victim (Article 14)

Article 14 requires Member States to take the measures needed to ensure that competent national authorities are entitled not to prosecute or impose penalties on child victims of sexual abuse and sexual exploitation for their involvement in criminal activities, which they have been compelled to commit as a direct consequence of being subjected to such crimes.

Most Member States have in place legislation that transposes this provision. For **ES, LU, MT, PL** and **SK** the information was not conclusive.

2.1.13. Investigation and prosecution (Article 15)

Article 15 lays down measures for the investigation and prosecution of the offences referred to in Articles 3 to 7.

- Under Article 15(1), Member States shall take the necessary measures to ensure that investigations into or the prosecution of the offences referred to in Articles 3 to 7 are not dependent on a report or accusation being made by the victim or by his or her representative, and that criminal proceedings may continue even if that person has withdrawn his or her statements. Whereas the national laws of **CY**, **NL, PL** and **PT** explicitly follow the principle of Article 15(1), **AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, MT, RO, SE, SI** and **SK** transposed this provision by means of general rules of criminal law regulating the opening of investigations or prosecutions. In the **UK (England/Wales, Northern Ireland** and **Scotland)**, prosecutors may initiate or continue criminal proceedings if they find that there is sufficient evidence to provide a realistic prospect of conviction and that prosecution is in the public interest. **IE** applies the same principle of public interest.
- Article 15(2) requires that Member States make it possible to prosecute offences for a sufficient period of time after the victim has reached the age of majority. **AT, BE, CY, EE, EL, ES, HR, HU, IE, LV, MT, PL, RO, SE, SI** and **UK** have in place legislation that transposes this provision. In **BG, CZ, DE, FI, IT**, **LT, NL** and **SK,** the statute of limitations for some offences runs from the date the offence was committed. This means that child victims, in particular those abused at a very young

age, may not have enough time after they have reached the age of majority to obtain prosecution.

- Under Article 15(3), Member States shall ensure that effective investigative tools are available for investigating and prosecuting offences. Whereas **CY** and **EL** explicitly reflect Article 15(3) in their legislation, most of the other Member States transpose it through a multiplicity of provisions from criminal procedural codes.
- Article 15(4) requires Member States to take the necessary measures to enable investigative units or services to attempt to identify victims, in particular by analysing child pornography material. Most Member States have in place measures that transpose this provision. For **BG, CZ, EE, FR, HU, IE, LT, PT, SK** and **UK (Gibraltar)** the information provided was not conclusive.

2.1.14. Reporting suspicion of sexual abuse or sexual exploitation (Article 16)

Article 16 aims at guaranteeing that professionals whose main duty is to work with children can report offences (Article 16(1)) and that any person who knows about or suspects these offences are being committed is encouraged to report them (Article 16(2)).

- With regard to Article 16(1), legislation in **HR**, **MT, PT, SI** and **UK** (**England**/**Wales**, **Northern Ireland** and **Gibraltar**) lays down a general obligation to report offences. However, the legislation of most Member States contains a specific provision on reporting offences in order to protect children (**AT, BG, CY, CZ, DE, EE, EL, ES, FI, HU, IT, LT, LV**, **NL, RO** and **SE**). Additionally, **BG, CY, CZ, DE, EL, FI, HU, IT, LV, RO, SE,** and **SK** provide for a specific obligation on certain professions (such as teachers, doctors, psychologists, nurses) to notify competent authorities.
- Some Member States (**AT, BE, BG, EL, FI, HR, HU, IT, LU, PL** and **SI**) have transposed Article 16(2) through a general provision obliging or encouraging the reporting of offences and/or helping people in need. Other Member States (**BG, CY, CZ, EE, ES, FR, HR, LT, LV, NL, PT, RO, SE** and **SK**) have transposed it through a more specific legal provision, making it obligatory to report offences against children. **UK (England/Wales, Northern Ireland** and **Scotland)** uses non-legislative measures.

  People are encouraged to report abuse mainly through helplines/hotlines, such as Child Focus (telephone number 116000) in **BE** or Child Line (116111) in **LT**.

2.1.15. Jurisdiction and coordination of prosecution (Article 17)

Article 17 lays down rules on the establishment of jurisdiction by Member States over the offences listed in the Directive.

- Article 17(1) covers jurisdiction where the offence is committed in whole or in part within a Member State's territory or the offender is one of its nationals. Most Member States have put in place legislation that transposes this provision. For **CY, IE, LV, NL, SI, PT** and **UK (Gibraltar)** the information was not conclusive.
- Under Article 17(2), a Member State has the option to establish further jurisdiction over an offence committed outside its territory. For example, if the offence is committed against one of its nationals or a person who is an habitual resident in its territory (17(2)(a)), the offence is committed for the benefit of a legal person established in its territory (17(2)(b)), or the offender is an habitual resident in its territory (17(2)(c)). Most Member States decided to apply the options provided for

under Article 17(2)(a) (**AT, BE, BG, CZ, EE, EL, ES, FI, FR, HR, HU, IT, MT, NL, PL, PT, RO, SI** and **SK)** and 17(2)(c) (**AT, BE, ES, FI, FR, HR, IE, LT, LU, LV, MT, NL, PT, RO, SE** and **SK**), whereas fewer of them decided to apply the options under Article 17(2)(b) (**CY, CZ, ES, HR, IT, LV, MT, PL, PT, RO** and **SI**).

- Article 17(3) requires Member States to ensure that their jurisdiction includes situations where an offence is committed by means of information and communication technology accessed from their territory, whether or not it is based on their territory. Whereas **CY, EL, MT** and **PT** have a specific provision which follows the wording of the Directive and refers directly to offences committed by means of information and communication technology, **AT, BE, BG, DE, EE, ES, FI, FR, HR, HU, IE, IT, LT, RO, SI, SK** and **UK** use a general provision establishing jurisdiction over crimes committed on their territories.
- Article 17(4) prohibits the establishment of the double criminality requirement for the prosecution of offences committed outside the territory of the Member State concerned, when the offender is one of its nationals. **BG, CZ, HU, IT, LV, MT, SK** and **UK** (**England**/**Wales** and **Northern Ireland**) do not provide for the requirement of double criminality when establishing their jurisdiction over an offence. Despite having a double criminality clause, **AT, BE, DE, EE, EL, ES, FI, FR, HR, LT, LU, NL** and **SE** provide for specific exceptions for all offences referred to in Article 17(4).
- Under Article 17(5), Member States shall ensure that their jurisdiction is not subordinated to the condition that the prosecution can only be initiated following a report made by the victim in the place where the offence was committed, or a denunciation from the State of the place where the offence was committed. Most Member States have in place legislation that transposes this provision. For **LU** and **SI** the information provided was not conclusive.

2.2. Assistance to and protection of victims (Articles 18 to 20)

2.2.1. General provisions on assistance, support and protection measures for child victims (Article 18)

Article 18 lays down general provisions on assistance, support and protection measures for child victims:

- Under Article 18(1), child victims shall be provided with assistance, support and protection taking into account the best interests of the child. Most Member States have in place legislation that transposes this provision. The information provided by **BE, DE, LV** and **SI** was not conclusive.
- Article 18(2) obliges Member States to take the necessary measures to ensure that a child is provided with assistance and support as soon as the competent authorities have a reasonable-grounds indication that the child might be a victim. About half of the Member States have in place measures that transpose this provision. For **AT, BE, BG, DE, EL, ES, FR, IT, LU, NL, PL, SI** and **UK** (**England**/**Wales**, **Northern Ireland** and **Scotland**) the information was not conclusive.
- Article 18(3) requires Member States to ensure, when the age of the person is uncertain and there are reasons to believe that he/she is a child, that the person is presumed to be a child in order to receive immediate access to assistance, support and protection. Whereas the wording of the legislation in **BG, CY, EL** and **LT** transposing this provision is very similar to the Directive, the legislation in **EE, ES, HR, LV, MT, PT, RO** and **UK** (**England**/**Wales** and **Gibraltar**) contains a general

presumption of minority in favour of the victim until the contrary is proved. For **AT, BE, CZ, DE, FI, FR, HU, IE, IT, LU, PL, SE, SI, SK** and **UK** (**Scotland**) the information was not conclusive.

2.2.2. Assistance and support to victims (Article 19)

Article 19 lays down general provisions on assistance, support and protection measures for child victims and their families.

- Under Article 19(1), Member States shall ensure that assistance and support are provided to victims before, during and for an appropriate period of time after the conclusion of criminal proceedings, in particular ensuring the protection of children who report cases of abuse within their family. Most Member States have in place legislation that transposes this provision. The information provided by **DE, HU, IE, IT, LV, PL, RO, SI** and **SK** was not conclusive.
- Article 19(2) requires Member States to ensure that assistance and support for a child victim are not made conditional on the child's willingness to cooperate in the criminal investigation, prosecution or trial. Whereas the legislation in **CY, EL, MT** and **UK** (**England**/**Wales** and **Gibraltar**) uses very similar wording to the Directive, most Member States (**AT, BE, BG, CZ, EE, ES**, **FI, FR, HR, HU, IE, IT, LT, LU, LV, NL, PL, PT, RO, SE, SK** and **UK** (**Northern Ireland** and **Scotland**)) used a variety of provisions on assistance and support. The information provided by **DE** and **SI** was not conclusive.
- Under Article 19(3), Member States shall ensure that assistance and support to child victims are provided following an individual assessment of the special circumstances of each victim, and taking due account of the child's views, needs and concerns. Most Member States have introduced measures that transpose this provision.[5] The information provided by **DE, EL, IT, LT, LU, LV, NL, PL, SI** and **UK** (**Scotland**) was not conclusive.
- Under Article 19(4), child victims of sexual offences are considered as particularly vulnerable victims pursuant Framework Decision 2001/220/JHA, replaced since 2012 by the Victims' Rights Directive.[6] Most Member States have taken measures that transpose this provision. The information provided by **DE, EL, IE, IT, SI** and **UK (Scotland)** was not conclusive.

  The recognition of children as particularly vulnerable victims is foreseen through special assistance and protection measures (except for **UK** (**Gibraltar**) that transposed literally). These measures ensure that child victims are entitled to testify in a manner that shields them from giving evidence in open court and that they are handled only by people that have been specially trained for this purpose.
- Article 19(5) requires Member States, where appropriate and possible, to provide assistance and support to the family of the child victim when the family is in their territory. **AT, BE, BG, CY, EE, FI, HR, IE, LT, MT, NL, PT, SK** and **UK** have

[5] For example, the assessment may encompass the evaluation of the child victim's situation based on information collected by the family, the child, the school, nursery, relatives or other authorities, the child's development and satisfaction of needs, parental capacity, the social environment of the child and the family, the child's views and wishes, and the child's age, health condition, intellectual maturity and cultural identity.

[6] Council Framework Decision 2011/220/JHA of 15 March 2001 on the standing of victims in criminal proceedings, replaced by Directive 2012/29/EU of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime.

taken measures to transpose this provision, whereas in the other Member States the information provided was not conclusive.

2.2.3. Protection of child victims in criminal investigations and proceedings (Article 20)

Article 20 lays down requirements for Member States concerning the protection of victims in criminal investigations and proceedings.

- The majority of Member States (**BG, CY, CZ, DE, EE, EL, ES, FR, FI, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK** and **UK** (**Gibraltar**)) have taken measures to ensure that in criminal investigations and proceedings the competent authorities appoint a special representative for the child victim, in accordance with Article 20(1). The information provided by **AT, BE** and **UK** (**Northern Ireland, Scotland** and **England/Wales**) was not conclusive.
- Under Article 20(2), Member States shall ensure that child victims have access to legal counselling and legal representation, which must be free of charge if the victim does not have sufficient financial resources. Most Member States have in place legislation that transposes this provision. For **AT, CZ, DE, EE, IE, LT, PL, RO and UK** (**England/Wales, Scotland** and **Northern Ireland**) the information provided was not conclusive.
- Article 20(3) describes a series of requirements to take into account when conducting criminal investigations involving child victims, and in particular during interviews. Whereas **EL, HR, LT, MT, PT, RO, SE** and **UK** (**England/Wales, Northern Ireland** and **Gibraltar**) have put in place the necessary measures to transpose Article 20(3), the information provided by the other Member States was not conclusive.
- Most of the Member States have taken measures to ensure that interviews with the child victim or child witness are audio-visually recorded and can be used as evidence in criminal court proceedings, in accordance with Article 20(4). The information provided by **AT, FI, IE, MT** and **PL** was not conclusive.
- Article 20(5) requires Member States to put in place measures to ensure that it may be ordered that the hearing take place without the presence of the public or without the presence of the child. Most Member States transposed this Article although the information provided by **BE, FI, PL** and **UK (Scotland)** was not conclusive.
- In accordance with Article 20(6), most Member States have taken measures to protect the privacy, identity and image of child victims, and to prevent the public dissemination of any information that could lead to their identification. The information provided by **BE, DE, PL, PT** and **SI** was not conclusive.

2.3. Prevention (Articles 10 and 21 to 25)

2.3.1. Disqualification arising from convictions (Article 10)

Article 10 addresses the prevention of offences against children through disqualification arising from convictions.

- Article 10(1) requires Member States to put in place measures to ensure that a natural person who has been convicted of child sex offences may be temporarily or permanently prevented from exercising at least professional activities involving direct and regular contact with children. Some Member States (**BE, BG, EL, ES, LT, PT** and **RO**) opted for temporary disqualification, whereas **LU** and **SK** opted for

permanent disqualification. In **DE, FR, HR, HU, IE, MT** and **UK (England/Wales, Northern Ireland** and **Scotland)**, both the temporary and the permanent disqualifications are possible. On the other hand, it is not evident from the legislation of **CY, EE, FI, LV** and **NL** whether such disqualification is permanent or temporary. **SE** transposes this Article through systematic background checks for work involving contact with children rather than through a specific provision for disqualification.

The information provided by **AT, CZ, IT, PL, SI** and **UK (Gibraltar)** was not conclusive.

- Under Article 10(2), Member States shall put in place measures to ensure that employers are entitled to request information on criminal convictions or disqualifications when recruiting for professional or voluntary activities. Most Member States have transposed this provision. The information can be obtained, for example, by requiring the submission of the person's criminal record (**BE, ES, FI, HR, HU, IE, IT, LU, MT, NL, PT, RO, SE, SK** and **UK**), the convict register (**LT**), the punishment register (**LV**), the record of good conduct (**DE**), the police record (**CY**), the record containing criminal punishment data (**EE**) or the automated national file of sexual or violent offences authors (**FR**).
- With regard to Article 10(3), most Member States have transposed the requirement to transmit the information on criminal convictions and disqualifications in accordance with the procedures set out in Framework Decision 2009/315/JHA on the exchange of criminal records information.[7] However, a few Member States still do not seem to ensure that information is transmitted if other Member States request information on previous criminal convictions. In some cases, they do not make it a legal obligation to send that information (**BE, CZ, IE, LV, MT** and **SE**). In other cases, they go beyond the requirement of the Directive that the person concerned (a national from Member State A) must consent to the issuing of the criminal certificate by the country where he intends to work or volunteer (Member State B), by specifically requiring an additional consent from the person concerned for the information on the conviction to be sent from Member State A to Member State B (**FI, LU** and **UK** (**England/Wales, Northern Ireland** and **Scotland**)).

2.3.2. Measures against advertising abuse opportunities and child sex tourism (Article 21)

Article 21 provides for the adoption of preventive/prohibitive measures against advertising abuse opportunities and child sex tourism.

- Article 21(a) concerns the prohibition/prevention of the dissemination of material advertising the opportunity to commit child sexual offences. Whereas **AT, BE, CY, EE, EL, IT, LV, MT** and **SK** have in place a criminal offence penalising the advertising specified in Article 21(a), **DE, FI, FR, LV, PL, PT** and **RO** have transposed this provision of the Directive through the criminal offence of public incitement.
- Article 21(b) concerns the prohibition/prevention of the organisation for others of travel arrangements with the purpose of offending. Most Member States have taken a variety of measures to transpose this provision. For example, **AT, BG** and **FI** criminalize this conduct through provisions applicable to aiders/abettors and practical measures, while in **CZ, LT** and **SK** such conduct is solely penalised via the provision

[7] See footnote 1.

applicable to participants, even if the main crime was not committed. **CY, EL, IT** and **MT** have adopted a specific offence which sanctions the organisation of travels for third parties with the aim to commit child offences.

2.3.3. Preventive intervention programmes or measures (Article 22)

Article 22 requires Member States to ensure that persons who fear that they might offend may have access to effective intervention programmes or measures designed to evaluate and prevent the risk of such offences being committed. **AT, BG, DE, FI, NL, SK** and **UK (England/Wales, Northern Ireland** and **Scotland)** have put in place measures to transpose this provision, whereas the information provided by the other Member States was not conclusive.

2.3.4. Prevention (Article 23)

Article 23 requires Member States to take appropriate measures to prevent the sexual abuse and sexual exploitation of children.

- Article 23(1) concerns education and training measures. While **CY, EL, ES,** and **LT** transposed this Article through specific legislative provisions, **BG**, **CZ** and **PT** used other measures such as national action plans/strategies. **NL, PL**, **RO**, **SE** and **UK (England/Wales, Northern Ireland** and **Scotland**), used general legislative measures in combination with campaigns and projects.
- Article 23(2) concerns information and awareness campaigns, possibly in cooperation with civil society organisations. All Member States transposed this provision, for example through education programmes (**AT, BE, CY, FR, LU, LV, MT, PT, SK** and **UK (England/Wales** and **Northern Ireland)**).
- Article 23(3) concerns regular training of officials likely to come in contact with child victims. Most Member States have taken measures to transpose this provision. The information from **EL, HU**, **IE, IT** and **UK (Scotland)** was not conclusive.

2.3.5. Intervention programmes or measures on a voluntary basis in the course of or after criminal proceedings (Article 24)

Article 24 regulates the provision of intervention programmes or measures in the course of or after the criminal proceedings.

- Article 24(1) requires Member States to ensure that effective intervention programmes or measures are made available at any time during the criminal proceedings, inside and outside prison, to prevent and minimise the risks of repeated offences. Whereas a number of Member States have taken measures to transpose this provision, the information provided by **AT, CY, CZ, DE, ES, FI, FR, HU, IE, IT, LU, LV, PL, PT, RO, SE, SI, SK** and **UK (Northern Ireland, Scotland** and **Gibraltar)** was not conclusive.
- Article 24(2) requires that the intervention programmes or measures meet the specific developmental needs of children who sexually offend. Member States have transposed this provision through various means such as legislation (**BG, HR** and **RO**), a combination of legislation and other measures (**HU, LT** and **MT**), or other measures (**FI, NL** and **UK (England/Wales, Northern Ireland** and **Scotland)**).
- Article 24(3) requires that access to the intervention programmes or measures be ensured for persons subject to criminal proceedings (Article 24(3)(a)) and convicted persons (Article 24(3)(b)). **CY, EL, MT, NL, RO** and **UK** have taken measures to

transpose Article 24(3)(a) and **BG, CY, DE, EL, ES, FI, HR, IT, LT, MT, NL, RO** and **UK** have taken measures to transpose Article 24(3)(b). The information provided by the rest of Member States was not conclusive.

- Under Article 24(4), Member States shall ensure that the persons who may access intervention programmes or measures are subject to an assessment of the danger they represent and the risk of recidivism, with the aim to identify the appropriate programme or measure. **AT, EL, HR, LT, MT, RO** and **SE** have taken measures to transpose this provision whereas the information provided by the rest of Member States was not conclusive.
- Article 24(5) requires Member States to ensure that the persons who may access intervention programmes or measures are fully informed of the reasons for the proposal (Article 24(5)(a)), consent to their participation with full knowledge of the facts (Article 24(5)(b)) and may refuse and be made aware of the possible consequences in the case of convicted persons (Article 24(5)(c)). **AT, BG, CY, EE, FI, LT, MT** and **UK (Gibraltar)** have taken measures to transpose Articles 24(5)(a) and (b) and **CY, EE, FI, FR, LT, MT** and **UK (Gibraltar)** to transpose Article 24(5)(c). The information provided by the other Member States was not conclusive.

2.3.6. Measures against websites containing or disseminating child pornography (Article 25)

Please refer to the specific, separate report on the transposition of this Article.[8]

[8] See footnote 3.

3. CONCLUSION AND NEXT STEPS

The Directive is a comprehensive legislative framework which has led to substantive progress in the Member States by amending criminal codes, criminal procedures and sectorial legislation, streamlining procedures, setting up or improving cooperation schemes and improving the coordination of national actors. The Commission acknowledges the major efforts made by the Member States to transpose the Directive.

However, there is still considerable scope for the Directive to reach its full potential through complete implementation of all of its provisions by Member States.
The analysis so far suggests that some of the main challenges for Member States could be related to prevention and intervention programmes for offenders (Articles 22, 23 and 24), substantial criminal law (Articles 3, 4 and 5) and the assistance, support and protection measures for child victims (Articles 18, 19 and 20).
Less challenging provisions seem to include those related to incitement, aiding and abetting, and attempt (Article 7), consensual sexual activities (Article 8), seizure and confiscation (Article 11) and liability and sanctions on legal persons (Articles 12 and 13).

Given the comprehensive nature of the Directive, the Commission will focus on ensuring that the transposition is finalised across the EU and that the provisions are correctly implemented. Therefore, for the time being, the Commission has no plans to propose amendments to the Directive or any complementary legislation. The Commission will instead focus its efforts on ensuring that children benefit from the full added value of the Directive, through its complete transposition and implementation by Member States.
The Commission will continue to provide support to Member States to ensure a satisfactory level of transposition and implementation. This includes monitoring that national measures comply with the corresponding provisions in the Directive. Where necessary, the Commission will make use of its enforcement powers under the Treaties through infringement procedures. It will also support the implementation of the Directive by facilitating the development and exchange of best practices in specific areas such as prevention and intervention programmes for offenders.

EUROPEAN
COMMISSION

Brussels, 16.12.2016
COM(2016) 872 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography

Contents

1. INTRODUCTION 3
1.1. Objectives and scope of Article 25 3
1.2. Purpose of this report and methodology 5
2. TRANSPOSITION MEASURES 7
2.1. Removal (Article 25(1)) 7
2.1.1. Content hosted in a Member State's territory 7
2.1.2. Content hosted outside a Member State's territory 9
2.2. Blocking (Article 25(2)) 10
3. CONCLUSION AND NEXT STEPS 12

1. INTRODUCTION

The Internet has brought about a dramatic increase in child sexual abuse in that:

- it facilitates the sharing of child sexual abuse material, by offering a variety of distribution channels such as the web, peer-to-peer networks, social media, bulletin boards, newsgroups, Internet relay chats and photo-sharing platforms, among many others. Sharing is also facilitated by access to a worldwide community of like-minded individuals, which is a source of strong demand and mutual support;
- it provides technical means and security measures that can facilitate anonymity;[1]
- as a consequence of the strong demand for child sexual abuse material, children continue to be at risk of becoming victims, while anonymity can obstruct the investigation and prosecution of these crimes; and
- new child sexual abuse materials have become a currency. To obtain and maintain access to forums, participants frequently have to submit new materials on a regular basis, which encourages the commission of child sexual abuse.

Online child sexual abuse is a nefarious crime with long-term consequences for its victims. Harm is caused not only when the abuse is actually recorded or photographed, but also every time the images and videos are posted, circulated and viewed. For the victims, the realisation that the images and videos in which they are abused are 'out there' and that they could even encounter someone who has seen the material is a major source of trauma and additional suffering.

There are indications that the average age of victims of child sexual abuse material is steadily decreasing: according to the International Association of Internet Hotlines (INHOPE),[2] around 70% of the victims in the reports that INHOPE hotlines processed in 2014 appeared to be prepubescent.[3] The Internet Watch Foundation (IWF) issued similar figures in 2015, adding that 3% of the victims appeared to be two years old or younger and a third of images showed children being raped or sexually tortured.[4]

1.1. Objectives and scope of Article 25

The main objective of Article 25 of the Directive[5] is to disrupt the availability of child pornography.[6] Such provisions were first introduced with the Directive, as they were not included in the main legislative instruments in the area, i.e.:

- the Framework Decision[7] that the Directive replaces;
- the 2007 Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, from which the Directive draws inspiration in other areas; or

[1] e.g. the Onion Router (www.torproject.org).
[2] http://www.inhope.org/
[3] http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx
[4] https://www.iwf.org.uk/accountability/annual-reports/2015-annual-report
[5] Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. Article 25 of the Directive covers 'measures against websites containing or disseminating child pornography'.
[6] As defined in Article 2(c) of the Directive.
[7] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

- the Council Decision to combat child pornography on the Internet,[8] which was one of the first legal instruments at EU level that addressed child pornography.

Article 25 is one of a number of provisions in the Directive to facilitate prevention and mitigate secondary victimisation. Together with provisions on the prosecution of crimes and protection of victims, they are part of the holistic approach required to tackle child sexual abuse, child sexual exploitation and child pornography effectively.

Article 25 reads as follows:[9]

> *1. Member States shall take the necessary measures to **ensure the prompt removal** of web pages containing or disseminating child pornography hosted in their territory and to **endeavour** to obtain the removal of such pages hosted outside of their territory.*
>
> *2. Member States may take measures to **block access** to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate **safeguards**, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.*

It therefore:

- obliges Member States to **remove** promptly material on websites hosted within their territory;
- obliges them to **endeavour to secure the removal** of material on websites hosted elsewhere; and
- offers the **possibility** to **block access** to child pornography by users within their territory, subject to a number of **safeguards**.

It is important to note that Article 25 refers to 'measures', which may not necessarily involve legislation. As recital 47 of the Directive states:

> *"… The measures undertaken by Member States in accordance with this Directive in order to remove or, where appropriate, block websites containing child pornography could be based on various types of public action, such as legislative, non-legislative, judicial or other. In that context, this Directive is without prejudice to voluntary action taken by the Internet industry to prevent the misuse of its services or to any support for such action by Member States…"*

Non-legislative measures are therefore considered to transpose the Directive satisfactorily if they allow the outcomes specified in Article 25 to be achieved in practice.

Cooperation between the private sector, including industry and civil society, and public authorities, including law enforcement agencies (LEAs) and the judiciary, is crucial to implementing the measures under Article 25 and effectively fighting the dissemination of child sexual abuse material online.

[8] Council Decision 2000/375/JHA of 29 May 2000 to combat child pornography on the Internet.
[9] See also recitals 46 and 47 of the Directive concerning the measures referred to in Article 25.

The parties involved in disrupting the availability of child sexual abuse material online are:

- **information society service providers (ISSPs)**, including providers of access, hosting and online platforms. As criminals abuse the services and the infrastructure they provide, ISSPs are well placed to cooperate in the implementation of Article 25. For example, hosting providers are ultimately able to remove material hosted on their servers and access providers such as internet service providers (ISPs) can block access;
- **Internet users,** who may come across child sexual abuse material online (intentionally or unintentionally) and decide to report it to the ISSP directly if the technology to do so is in place, e.g. through a 'report abuse' button on the web page or browser. Users may also report to a dedicated hotline run by a civil society organisation, or to the LEA responsible;
- **dedicated hotlines,** usually run by an NGO or an association of ISSPs or media companies, which allow anonymous reporting by users who may not feel comfortable reporting to the police and cannot or do not wish to report to the ISSP directly. In many cases, reports received in one country refer to material hosted by providers in another. Its removal requires international cooperation, which INHOPE facilitates;
- **LEAs**, whose work is supported by reports passed on by hotlines and directly from Internet users. They also share reports with each other in Europe (directly and through Europol and its European Cybercrime Centre)[10] and beyond (through Interpol);[11] and
- the **judiciary**, which ensures application of the law in each Member State. In some countries, court orders are needed to remove or block material. Eurojust[12] helps coordinate judicial cooperation in criminal matters across Member States.

1.2. Purpose of this report and methodology

Article 27 of the Directive requires Member States[13] to bring into force the laws, regulations and administrative provisions necessary to comply with the Directive and communicate them to the Commission by 18 December 2013.

This report responds to the requirement under Article 28(2) of the Directive for the Commission to submit a report to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of the Directive.[14] The report aims to provide a concise yet informative overview of the main transposition measures taken by Member States.

[10] https://www.europol.europa.eu/ec3
[11] http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children
[12] http://www.eurojust.europa.eu/
[13] From this point onwards, 'Member States' or 'all Member States' refer to the Member States bound by the Directive (i.e. all EU Member States except Denmark). In accordance with Articles 1 and 2 of Protocol 22 on the Position of Denmark, Denmark did not take part in the adoption of the Directive, nor does the Directive apply to it. However Council Framework Decision 2004/68/JHA continues to be applicable to and binding upon Denmark. In accordance with Article 3 of Protocol 21 on the position of the United Kingdom and Ireland, both took part in the adoption of the Directive and are bound by it.
[14] In accordance with Article 28(1) of the Directive, the extent to which the Member States have taken the necessary measures to comply with the Directive is assessed in a separate report (COM(2016) 871) published jointly with this one.

By the transposition deadline, only 12 Member States had notified the Commission that they had completed transposition of the Directive. The Commission therefore opened infringement proceedings for non-communication of national transposition measures against the others: **BE, BG, IE, EL, ES, IT, CY, LT, HU, MT, NL, PT, RO, SI** and the **UK**.[15] All these infringement proceedings had been closed by 8 December 2016. The late adoption and notification of national transposition measures delayed the Commission's analysis and publication of the transposition reports.

The description and analysis in this report are based on the information that Member States provided by 1 November 2016. Notifications received after that date have not been taken into account. Beyond the issues identified in this report, there may be both further challenges in transposition and other provisions not reported to the Commission or further legislative and non-legislative developments. Therefore, this report does not prevent the Commission from further evaluating some provisions, to continue supporting Member States in the transposition and implementation of Article 25.

[15] Member States in this document are abbreviated according to these rules: http://publications.europa.eu/code/en/en-370100.htm

2. TRANSPOSITION MEASURES

2.1. Removal (Article 25(1))

2.1.1. Content hosted in a Member State's territory

Member States have adopted two types of measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in a Member State's territory: measures based on Directive 2000/31/EC[16] (E-commerce Directive), and measures based on national criminal law.

1. Measures based on the E-commerce Directive

   The E-commerce Directive defines the liability limitations of an Internet intermediary providing services consisting of mere conduit, caching and hosting. In particular, a hosting provider cannot be held liable if:[17]

   a. it has neither knowledge of nor control over the information that is transmitted or stored, and

   b. upon obtaining actual knowledge or awareness of illegal activities, it acts expeditiously to remove or to disable access to the information concerned.

   These provisions constitute the basis for the development of **notice and take down procedures** for illegal content. In the area of child sexual abuse material, these procedures take the form of mechanisms run by interested parties aimed at identifying illegal information hosted on the network and at facilitating its rapid removal.

   Member States have implemented notice and take down procedures through national hotlines, to which Internet users can report child sexual abuse material that they find online. INHOPE is the umbrella organisation for the hotlines. Supported by the European Commission's Safer Internet Programme[18], and since 2014 by the Connecting Europe Facility framework,[19] it currently represents a network of 51 hotlines in 45 countries, including all EU Member States.

   The hotlines have memoranda of understanding with the corresponding national LEAs, which set out procedures for handling the reports received from Internet users. The different operating procedures include in general the following common actions for content hosted in the Member States:

   1) Determine the hosting location.

      A hotline receives an Internet user's report of a web address (URL) with possible child sexual abuse material and determines in which country the material is hosted. In some cases, the hotline receives the report from another INHOPE network member, which has already determined that the hosting location is in the country of the hotline in question.

[16] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). The last implementation report was published in 2012: http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf
[17] Article 14 of E-commerce Directive.
[18] https://ec.europa.eu/digital-single-market/en/safer-internet-better-internet-kids
[19] https://ec.europa.eu/digital-single-market/en/connecting-europe-facility

2) Analyse content.

If the material is hosted in the country, the hotline determines whether the URL has been reported previously. If so, the report is discarded. Otherwise, the hotline analyses the images and videos on the URL and determines whether they are known and whether they may be illegal in that country.

3) Inform hosting provider.

The hotline forwards the report and the analyses to the national LEA. Depending on the memorandum of understanding, the hosting provider is then informed by:

- the hotline, after the LEA has agreed that the material can be taken down, ensuring that this would not interfere with an ongoing investigation (**AT, CZ, DE** (eco and FSM hotlines), **FR, HU, LU, LV, NL, PL, PT, RO, SE** and the **UK).** The time between the hotline first informing the LEA and the hotline communicating with the hosting provider varies depending on the procedures agreed between the hotline and the LEA in each Member State. In any case, the LEA (instead of or in addition to the hotline) may choose to inform the hosting provider as circumstances require.
- the LEA only. In **BG, DE** (Jugendschutz hotline), **EE, EL, FI, MT, SI** and **SK**, the LEA communicates with the hosting provider, while the hotline monitors that the content is actually removed.

  In **CY** and **HR,** a court order is required to request the removal of the material. In both countries, access to the website is temporarily blocked until the court order is obtained.

After being made aware of the existence of illegal material on its servers, the hosting provider can be held liable if it fails to remove it in accordance with the national implementing laws. The only limit to the attribution of liability is the liability exemption under the E-commerce Directive as implemented by Member States (see above).

At the time of writing, most Member States have hotlines that are capable of assessing reported content to implement notice and take down procedures, except **BE, ES** and **IT:**

- **BE** notified recently adopted legislation that allows an INHOPE hotline to operate in the country and handle reports according to the general procedure described above. At the time of writing, the Belgian police and judiciary were negotiating with the hotline a memorandum of understanding and the operating protocols.
- The situation in **ES** requires closer examination with regard to the hotline situation.
- **IT** has two INHOPE hotlines, but the current legislation does not allow them to check the content of reports received from Internet users or other hotlines. Therefore, they simply forward the reports to the LEA (the National Centre for Combatting Online Child Pornography, CNCPO), without checking the content.

2. Measures based on national criminal law

Member States have notified two types of criminal law provisions which also allow the removal of illegal content hosted in their territory:

a. general provisions that allow the seizure of material relevant to criminal proceedings, e.g. material used in the commission of an offence: **AT, CZ, HU, IT, LU, NL, SE** and **SK**; and

b. specific provisions on the removal of child pornography: **CY, EE, EL, ES, SE,** and **UK (Gibraltar)**.

The legislation in **CZ**, **EL**, **HU** and **UK (Gibraltar)** makes explicit reference to the requirement of prompt removal: 'without undue delay' (**CZ**), 'executed immediately' (**EL**), 'within 12 hours' (**HU**) or 'prompt removal' (**UK (Gibraltar)**).

Other Member States transpose this requirement through the notice and takedown procedures described above, which may lead to the criminal law channels being used only in an ancillary way to deal with cases where notice and takedown mechanisms encounter difficulties (e.g. for lack of cooperation of the hosting provider) or where material is linked to an ongoing criminal investigation. In Member States without functional notice and take down mechanisms or where criminal law does not specify prompt removal, more information is needed on the measures taken to transpose this requirement.

2.1.2. Content hosted outside a Member State's territory

All Member States except **BE, ES** and **IT** have transposed this provision through a fully operational hotline (i.e. a hotline authorised to assess the material) and the following operating procedure to endeavour to remove content hosted outside their territory:

1) once the operators of the hotline that has received the report determine that the hosting location is outside of the Member State, they verify whether there is an operational INHOPE hotline in the hosting country;

2) if the hosting country has an INHOPE hotline, the report is sent to it through the internal INHOPE information exchange system, so that it can process the report according to the national procedure for content hosted in the country;

3) if the hosting country does not have an INHOPE hotline, the report is sent to the LEA of the country in which it was received, which forwards it, usually via Europol or Interpol, to the LEA of the hosting country.

Although the procedures across hotlines follow in general a similar pattern, there are some specificities depending on what has been agreed between the hotline and the LEA. For example, some hotlines (e.g. in **DE, LT** and **LV**) notify the hosting provider abroad if no action has been taken after a certain time. Some hotlines (e.g. in **AT, CZ, DE, FR, LU, MT**) inform the LEA of their country when they forward a report to a hotline abroad, while others (e.g. in **HU**, **NL, PL, SE** and the **UK**) generally do not. Finally, if there is no INHOPE hotline in the hosting country, some hotlines (e.g. in **EE, LU,** and the **UK**) contact non-INHOPE hotlines there, if they exist.

Member States without a fully operational hotline (**BE, ES** and **IT**) transpose this provision by arranging for the exchange of information, usually via Europol or Interpol, between the LEA in the country in which the report originated and that of the country in which the material is hosted. In this case, more information is needed on the transposition of the provision through this mechanism, in particular in relation to cases where the web pages hosted abroad are not linked to any criminal proceedings in that Member State and are not the object of any request for mutual legal assistance (MLA).

With regard to the promptness and effectiveness of removal through the hotlines, according to their data, 93% of the child sexual abuse material processed by the hotlines

in Europe and 91% of the material processed by the hotlines worldwide was removed from Internet public access in less than 72 hours.[20]

2.2. Blocking (Article 25(2))

About half of the Member States (**BG, CY, CZ, EL, ES, FI, FR, HU, IE, IT, MT, PT, SE** and the **UK**) have chosen to apply optional blocking measures under Article 25(2). The variety of the measures reflects the wording of recital 47 of the Directive (legislative, non-legislative, judicial or other, including voluntary action by the Internet industry).

One way to classify the measures is according to whether a court order is required to block a website. A court order is:

- required in **EL, ES** and **HU**;
- not mandatory in
    - **CY, FR, IT** and **PT**, where ISPs are required by law to comply with the request of the authorities (i.e. the LEA or the national regulator) to block the site; and
    - **BG, CZ, IE, FI, MT, SE,** and the **UK**, where ISPs are not explicitly required by law to comply with the authorities' request but do so voluntarily.

Blacklists of websites containing or disseminating child pornography are commonly used in the implementation of blocking measures. Blacklists are typically prepared by national authorities (i.e. the LEA or the regulator) and transmitted to the ISPs. Some Member States (**EL, HU, IT, FI** and **FR**) notified legislation that governs this process.

BG uses Interpol's 'Worst of List',[21] while the **UK** uses IWF's URL list.[22] ISPs in **CZ** also use the IWF list on a self-regulatory basis.

Information received from Member States was, in general, not conclusive as to the number of webpages included in blocking lists, or the number of attempts blocked.

The Directive requires that measures taken to block access to websites containing or disseminating child pornography provide for transparent procedures and adequate safeguards. Recital 47 states that:

> *Whichever basis for action or method is chosen, Member States should ensure that it provides an adequate level of legal certainty and predictability to users and service providers. Both with a view to the removal and the blocking of child abuse content, cooperation between public authorities should be established and strengthened, particularly in the interests of ensuring that national lists of websites containing child pornography material are as complete as possible and of avoiding duplication of work. Any such developments must take account of the rights of the end users and comply with existing legal and judicial procedures and the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union.*

Specifically, Article 25(2) refers to the following requirements:

[20] http://www.inhope.org/Libraries/Statistics_Infographics_2014/INHOPE_stats_infographics_for_2014.sflb.ashx

[21] https://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/The-INTERPOL-%22Worst-of%22-list

[22] https://www.iwf.org.uk/members/member-policies/url-list/blocking-faqs#WhatistheIWFURLlist

1. transparent procedures;
2. limitation to what is necessary and proportionate;
3. information to users on the reasons for restriction; and
4. possibility of judicial redress.

Member States which opted to transpose this provision have done so incorporating a variety of transparent procedures and safeguards:

- in **EL,** the Hellenic Telecommunication and Post Commission notifies orders of the competent authorities to providers of Internet access services and urges immediate content blocking and the provision of relevant information to users. The owner of the webpage may appeal against the order within a period of two months;
- in **ES**, during the criminal proceedings, the judge may order the closure of a website containing child pornography as a precautionary measure, which can be contested. The service provider is obliged to provide the necessary information to customers;
- in **FI**, the police may establish, maintain and update a list of child pornography sites. Where a website is blocked, the police have to issue a statement giving the reasons for the blocking which must be displayed every time access to a site is blocked. Appeals against decisions by the police to add a site to the blocking list can be lodged with an administrative court;
- in **FR**, Internet providers must block access to the Internet addresses concerned within 24 hours. The list of websites is reviewed by a qualified person from the National Commission on Computing and Freedoms. Users trying to reach the service to which access is denied are redirected to an information address of the Ministry of Interior, stating the reasons for denial of access and the available redress procedures before the administrative court;
- in **HU**, access can be blocked temporarily or permanently. Requests are received by the Minister of Justice and, where appropriate, submitted to the Metropolitan Court of Budapest. The obligation to block access rests with the ISP providing connectivity. The transparency of the procedure is ensured as the decision of the court is served by way of publication and is thus accessible to the public. Judicial appeal is available against an order of permanent blocking;
- in **IT**, the National Centre for Combating Child Pornography on the Internet provides ISPs with a list of child pornography sites, to which they prevent access using filtering tools and related technology. The sites to which access is blocked will display a 'stop page' indicating the reasons for blocking; and
- in the **UK** (**England**/**Wales**, **Northern Ireland** and **Scotland**), measures to block access to such webpages are taken through IWF, which works as a private self-regulatory body that makes recommendations to have content blocked or filtered. There is an appeals process whereby anyone with a legitimate association with or interest in the content in question can contest the accuracy of the assessment. In the **UK** (**Gibraltar**), the Gibraltar Regulatory Authority may, in conjunction with IPSs, block access to web pages that contain or disseminate child pornography to users in Gibraltar. Such measures must be transparent, limited to what is strictly necessary, proportionate and reasoned.

In **BG, CY, CZ, IE, MT, PT** and **SE** the information provided on safeguards applicable to blocking measures was not conclusive and will require further examination.

3. CONCLUSION AND NEXT STEPS

The Commission acknowledges the significant efforts made by the Member States in the transposition of Article 25 of the Directive.

There is still room, however, to use its potential to the full by continuing to work on its complete and correct implementation across Member States. Some key challenges ahead include ensuring that child sexual abuse material in Member States' territory is removed promptly and that adequate safeguards are provided where the Member State opts to take measures to block access to Internet users within its territory to web pages containing child sexual abuse material.

Therefore, for the time being, the Commission has no plans to propose amendments to Article 25 or complementary legislation. It will instead focus its efforts on ensuring that children benefit from the full added value of the Article, through its complete transposition and implementation by Member States.
That said, in its recent Communication on Online Platforms,[23] the Commission highlighted the need to sustain and develop multi-stakeholder engagement processes aimed at finding common solutions to voluntarily detect and fight illegal material online and committed to reviewing the need for formal notice and action procedures.

The Commission will continue to provide support to Member States to ensure a satisfactory level of transposition and implementation. This includes monitoring that national measures comply with the corresponding provisions in the Article and facilitating the exchange of best practices. Where necessary, the Commission will make use of its enforcement powers under the Treaties through infringement procedures.

[23] Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM/2016/288), of 25 May 2016.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Council of Europe Treaty Series - No. 201

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse [*]

Lanzarote, 25.X.2007

Preamble

The member States of the Council of Europe and the other signatories hereto;

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Considering that every child has the right to such measures of protection as are required by his or her status as a minor, on the part of his or her family, society and the State;

Observing that the sexual exploitation of children, in particular child pornography and prostitution, and all forms of sexual abuse of children, including acts which are committed abroad, are destructive to children's health and psycho-social development;

Observing that the sexual exploitation and sexual abuse of children have grown to worrying proportions at both national and international level, in particular as regards the increased use by both children and perpetrators of information and communication technologies (ICTs), and that preventing and combating such sexual exploitation and sexual abuse of children require international co-operation;

Considering that the well-being and best interests of children are fundamental values shared by all member States and must be promoted without any discrimination;

Recalling the Action Plan adopted at the 3rd Summit of Heads of State and Governments of the Council of Europe (Warsaw, 16-17 May 2005), calling for the elaboration of measures to stop sexual exploitation of children;

Recalling in particular the Committee of Ministers Recommendation No. R (91) 11 concerning sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults, Recommendation Rec(2001)16 on the protection of children against sexual exploitation, and the Convention on Cybercrime (ETS No. 185), especially Article 9 thereof, as well as the Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197);

Bearing in mind the Convention for the Protection of Human Rights and Fundamental Freedoms (1950, ETS No. 5), the revised European Social Charter (1996, ETS No. 163), and the European Convention on the Exercise of Children's Rights (1996, ETS No. 160);

(*) The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community entered into force on 1 December 2009. As a consequence, as from that date, any reference to the European Economic Community shall be read as the European Union.

Also bearing in mind the United Nations Convention on the Rights of the Child, especially Article 34 thereof, the Optional Protocol on the sale of children, child prostitution and child pornography, the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, as well as the International Labour Organization Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour;

Bearing in mind the Council of the European Union Framework Decision on combating the sexual exploitation of children and child pornography (2004/68/JHA), the Council of the European Union Framework Decision on the standing of victims in criminal proceedings (2001/220/JHA), and the Council of the European Union Framework Decision on combating trafficking in human beings (2002/629/JHA);

Taking due account of other relevant international instruments and programmes in this field, in particular the Stockholm Declaration and Agenda for Action, adopted at the 1st World Congress against Commercial Sexual Exploitation of Children (27-31 August 1996), the Yokohama Global Commitment adopted at the 2nd World Congress against Commercial Sexual Exploitation of Children (17-20 December 2001), the Budapest Commitment and Plan of Action, adopted at the preparatory Conference for the 2nd World Congress against Commercial Sexual Exploitation of Children (20-21 November 2001), the United Nations General Assembly Resolution S-27/2 “A world fit for children” and the three-year programme “Building a Europe for and with children”, adopted following the 3rd Summit and launched by the Monaco Conference (4-5 April 2006);

Determined to contribute effectively to the common goal of protecting children against sexual exploitation and sexual abuse, whoever the perpetrator may be, and of providing assistance to victims;

Taking into account the need to prepare a comprehensive international instrument focusing on the preventive, protective and criminal law aspects of the fight against all forms of sexual exploitation and sexual abuse of children and setting up a specific monitoring mechanism,

Have agreed as follows:

Chapter I – Purposes, non-discrimination principle and definitions

Article 1 – Purposes

1 The purposes of this Convention are to:

a prevent and combat sexual exploitation and sexual abuse of children;

b protect the rights of child victims of sexual exploitation and sexual abuse;

c promote national and international co-operation against sexual exploitation and sexual abuse of children.

2 In order to ensure effective implementation of its provisions by the Parties, this Convention sets up a specific monitoring mechanism.

Article 2 – Non-discrimination principle

The implementation of the provisions of this Convention by the Parties, in particular the enjoyment of measures to protect the rights of victims, shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth, sexual orientation, state of health, disability or other status.

Article 3 – Definitions

For the purposes of this Convention:

a "child" shall mean any person under the age of 18 years;

b "sexual exploitation and sexual abuse of children" shall include the behaviour as referred to in Articles 18 to 23 of this Convention;

c "victim" shall mean any child subject to sexual exploitation or sexual abuse.

Chapter II – Preventive measures

Article 4 – Principles

Each Party shall take the necessary legislative or other measures to prevent all forms of sexual exploitation and sexual abuse of children and to protect children.

Article 5 – Recruitment, training and awareness raising of persons working in contact with children

1 Each Party shall take the necessary legislative or other measures to encourage awareness of the protection and rights of children among persons who have regular contacts with children in the education, health, social protection, judicial and law-enforcement sectors and in areas relating to sport, culture and leisure activities.

2 Each Party shall take the necessary legislative or other measures to ensure that the persons referred to in paragraph 1 have an adequate knowledge of sexual exploitation and sexual abuse of children, of the means to identify them and of the possibility mentioned in Article 12, paragraph 1.

3 Each Party shall take the necessary legislative or other measures, in conformity with its internal law, to ensure that the conditions to accede to those professions whose exercise implies regular contacts with children ensure that the candidates to these professions have not been convicted of acts of sexual exploitation or sexual abuse of children.

Article 6 – Education for children

Each Party shall take the necessary legislative or other measures to ensure that children, during primary and secondary education, receive information on the risks of sexual exploitation and sexual abuse, as well as on the means to protect themselves, adapted to their evolving capacity. This information, provided in collaboration with parents, where appropriate, shall be given within a more general context of information on sexuality and shall pay special attention to situations of risk, especially those involving the use of new information and communication technologies.

Article 7 – Preventive intervention programmes or measures

Each Party shall ensure that persons who fear that they might commit any of the offences established in accordance with this Convention may have access, where appropriate, to effective intervention programmes or measures designed to evaluate and prevent the risk of offences being committed.

Article 8 – Measures for the general public

1 Each Party shall promote or conduct awareness raising campaigns addressed to the general public providing information on the phenomenon of sexual exploitation and sexual abuse of children and on the preventive measures which can be taken.

2 Each Party shall take the necessary legislative or other measures to prevent or prohibit the dissemination of materials advertising the offences established in accordance with this Convention.

Article 9 – Participation of children, the private sector, the media and civil society

1 Each Party shall encourage the participation of children, according to their evolving capacity, in the development and the implementation of state policies, programmes or others initiatives concerning the fight against sexual exploitation and sexual abuse of children.

2 Each Party shall encourage the private sector, in particular the information and communication technology sector, the tourism and travel industry and the banking and finance sectors, as well as civil society, to participate in the elaboration and implementation of policies to prevent sexual exploitation and sexual abuse of children and to implement internal norms through self-regulation or co-regulation.

3 Each Party shall encourage the media to provide appropriate information concerning all aspects of sexual exploitation and sexual abuse of children, with due respect for the independence of the media and freedom of the press.

4 Each Party shall encourage the financing, including, where appropriate, by the creation of funds, of the projects and programmes carried out by civil society aiming at preventing and protecting children from sexual exploitation and sexual abuse.

Chapter III – Specialised authorities and co-ordinating bodies

Article 10 – National measures of co-ordination and collaboration

1 Each Party shall take the necessary measures to ensure the co-ordination on a national or local level between the different agencies in charge of the protection from, the prevention of and the fight against sexual exploitation and sexual abuse of children, notably the education sector, the health sector, the social services and the law-enforcement and judicial authorities.

2 Each Party shall take the necessary legislative or other measures to set up or designate:

a independent competent national or local institutions for the promotion and protection of the rights of the child, ensuring that they are provided with specific resources and responsibilities;

b mechanisms for data collection or focal points, at the national or local levels and in collaboration with civil society, for the purpose of observing and evaluating the phenomenon of sexual exploitation and sexual abuse of children, with due respect for the requirements of personal data protection.

3 Each Party shall encourage co-operation between the competent state authorities, civil society and the private sector, in order to better prevent and combat sexual exploitation and sexual abuse of children.

Chapter IV – Protective measures and assistance to victims

Article 11 – Principles

1 Each Party shall establish effective social programmes and set up multidisciplinary structures to provide the necessary support for victims, their close relatives and for any person who is responsible for their care.

2 Each Party shall take the necessary legislative or other measures to ensure that when the age of the victim is uncertain and there are reasons to believe that the victim is a child, the protection and assistance measures provided for children shall be accorded to him or her pending verification of his or her age.

Article 12 – Reporting suspicion of sexual exploitation or sexual abuse

1 Each Party shall take the necessary legislative or other measures to ensure that the confidentiality rules imposed by internal law on certain professionals called upon to work in contact with children do not constitute an obstacle to the possibility, for those professionals, of their reporting to the services responsible for child protection any situation where they have reasonable grounds for believing that a child is the victim of sexual exploitation or sexual abuse.

2 Each Party shall take the necessary legislative or other measures to encourage any person who knows about or suspects, in good faith, sexual exploitation or sexual abuse of children to report these facts to the competent services.

Article 13 – Helplines

Each Party shall take the necessary legislative or other measures to encourage and support the setting up of information services, such as telephone or Internet helplines, to provide advice to callers, even confidentially or with due regard for their anonymity.

Article 14 – Assistance to victims

1 Each Party shall take the necessary legislative or other measures to assist victims, in the short and long term, in their physical and psycho-social recovery. Measures taken pursuant to this paragraph shall take due account of the child's views, needs and concerns.

2 Each Party shall take measures, under the conditions provided for by its internal law, to co-operate with non-governmental organisations, other relevant organisations or other elements of civil society engaged in assistance to victims.

3 When the parents or persons who have care of the child are involved in his or her sexual exploitation or sexual abuse, the intervention procedures taken in application of Article 11, paragraph 1, shall include:

– the possibility of removing the alleged perpetrator;

– the possibility of removing the victim from his or her family environment. The conditions and duration of such removal shall be determined in accordance with the best interests of the child.

4 Each Party shall take the necessary legislative or other measures to ensure that the persons who are close to the victim may benefit, where appropriate, from therapeutic assistance, notably emergency psychological care.

Chapter V – Intervention programmes or measures

Article 15 – General principles

1 Each Party shall ensure or promote, in accordance with its internal law, effective intervention programmes or measures for the persons referred to in Article 16, paragraphs 1 and 2, with a view to preventing and minimising the risks of repeated offences of a sexual nature against children. Such programmes or measures shall be accessible at any time during the proceedings, inside and outside prison, according to the conditions laid down in internal law.

2 Each Party shall ensure or promote, in accordance with its internal law, the development of partnerships or other forms of co-operation between the competent authorities, in particular health-care services and the social services, and the judicial authorities and other bodies responsible for following the persons referred to in Article 16, paragraphs 1 and 2.

3 Each Party shall provide, in accordance with its internal law, for an assessment of the dangerousness and possible risks of repetition of the offences established in accordance with this Convention, by the persons referred to in Article 16, paragraphs 1 and 2, with the aim of identifying appropriate programmes or measures.

4 Each Party shall provide, in accordance with its internal law, for an assessment of the effectiveness of the programmes and measures implemented.

Article 16 – Recipients of intervention programmes and measures

1 Each Party shall ensure, in accordance with its internal law, that persons subject to criminal proceedings for any of the offences established in accordance with this Convention may have access to the programmes or measures mentioned in Article 15, paragraph 1, under conditions which are neither detrimental nor contrary to the rights of the defence and to the requirements of a fair and impartial trial, and particularly with due respect for the rules governing the principle of the presumption of innocence.

2 Each Party shall ensure, in accordance with its internal law, that persons convicted of any of the offences established in accordance with this Convention may have access to the programmes or measures mentioned in Article 15, paragraph 1.

3 Each Party shall ensure, in accordance with its internal law, that intervention programmes or measures are developed or adapted to meet the developmental needs of children who sexually offend, including those who are below the age of criminal responsibility, with the aim of addressing their sexual behavioural problems.

Article 17 – Information and consent

1 Each Party shall ensure, in accordance with its internal law, that the persons referred to in Article 16 to whom intervention programmes or measures have been proposed are fully informed of the reasons for the proposal and consent to the programme or measure in full knowledge of the facts.

2 Each Party shall ensure, in accordance with its internal law, that persons to whom intervention programmes or measures have been proposed may refuse them and, in the case of convicted persons, that they are made aware of the possible consequences a refusal might have.

Chapter VI – Substantive criminal law

Article 18 – Sexual abuse

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:

a engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities;

b engaging in sexual activities with a child where:

– use is made of coercion, force or threats; or

– abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or

– abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.

2 For the purpose of paragraph 1 above, each Party shall decide the age below which it is prohibited to engage in sexual activities with a child.

3 The provisions of paragraph 1.a are not intended to govern consensual sexual activities between minors.

Article 19 – Offences concerning child prostitution

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:

a recruiting a child into prostitution or causing a child to participate in prostitution;

b coercing a child into prostitution or profiting from or otherwise exploiting a child for such purposes;

c having recourse to child prostitution.

2 For the purpose of the present article, the term “child prostitution” shall mean the fact of using a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment, regardless if this payment, promise or consideration is made to the child or to a third person.

Article 20 – Offences concerning child pornography

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:

a producing child pornography;

b offering or making available child pornography;

c distributing or transmitting child pornography;

d procuring child pornography for oneself or for another person;

e possessing child pornography;

f knowingly obtaining access, through information and communication technologies, to child pornography.

2 For the purpose of the present article, the term “child pornography” shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:

– consisting exclusively of simulated representations or realistic images of a non-existent child;

– involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.

4 Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.

Article 21 – Offences concerning the participation of a child in pornographic performances

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:

a recruiting a child into participating in pornographic performances or causing a child to participate in such performances;

b coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes;

c knowingly attending pornographic performances involving the participation of children.

2 Each Party may reserve the right to limit the application of paragraph 1.c to cases where children have been recruited or coerced in conformity with paragraph 1.a or b.

Article 22 – Corruption of children

Each Party shall take the necessary legislative or other measures to criminalise the intentional causing, for sexual purposes, of a child who has not reached the age set in application of Article 18, paragraph 2, to witness sexual abuse or sexual activities, even without having to participate.

Article 23 – Solicitation of children for sexual purposes

Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.

Article 24 – Aiding or abetting and attempt

1 Each Party shall take the necessary legislative or other measures to establish as criminal offences, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with this Convention.

2 Each Party shall take the necessary legislative or other measures to establish as criminal offences, when committed intentionally, attempts to commit the offences established in accordance with this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 to offences established in accordance with Article 20, paragraph 1.b, d, e and f, Article 21, paragraph 1.c, Article 22 and Article 23.

Article 25 – Jurisdiction

1 Each Party shall take the necessary legislative or other measures to establish jurisdiction over any offence established in accordance with this Convention, when the offence is committed:

a in its territory; or
b on board a ship flying the flag of that Party; or
c on board an aircraft registered under the laws of that Party; or
d by one of its nationals; or
e by a person who has his or her habitual residence in its territory.

2 Each Party shall endeavour to take the necessary legislative or other measures to establish jurisdiction over any offence established in accordance with this Convention where the offence is committed against one of its nationals or a person who has his or her habitual residence in its territory.

3 Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraph 1.e of this article.

4 For the prosecution of the offences established in accordance with Articles 18, 19, 20, paragraph 1.a, and 21, paragraph 1.a and b, of this Convention, each Party shall take the necessary legislative or other measures to ensure that its jurisdiction as regards paragraph 1.d is not subordinated to the condition that the acts are criminalised at the place where they were performed.

5 Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right to limit the application of paragraph 4 of this article, with regard to offences established in accordance with Article 18, paragraph 1.b, second and third indents, to cases where its national has his or her habitual residence in its territory.

6 For the prosecution of the offences established in accordance with Articles 18, 19, 20, paragraph 1.a, and 21 of this Convention, each Party shall take the necessary legislative or other measures to ensure that its jurisdiction as regards paragraphs 1.d and e is not subordinated to the condition that the prosecution can only be initiated following a report from the victim or a denunciation from the State of the place where the offence was committed.

7 Each Party shall take the necessary legislative or other measures to establish jurisdiction over the offences established in accordance with this Convention, in cases where an alleged offender is present on its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality.

8 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

9 Without prejudice to the general rules of international law, this Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its internal law.

Article 26 – Corporate liability

1 Each Party shall take the necessary legislative or other measures to ensure that a legal person can be held liable for an offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

a power of representation of the legal person;
b an authority to take decisions on behalf of the legal person;
c an authority to exercise control within the legal person.

2 Apart from the cases already provided for in paragraph 1, each Party shall take the necessary legislative or other measures to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of an offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 27 – Sanctions and measures

1 Each Party shall take the necessary legislative or other measures to ensure that the offences established in accordance with this Convention are punishable by effective, proportionate and dissuasive sanctions, taking into account their seriousness. These sanctions shall include penalties involving deprivation of liberty which can give rise to extradition.

2 Each Party shall take the necessary legislative or other measures to ensure that legal persons held liable in accordance with Article 26 shall be subject to effective, proportionate and dissuasive sanctions which shall include monetary criminal or non-criminal fines and may include other measures, in particular:

a exclusion from entitlement to public benefits or aid;
b temporary or permanent disqualification from the practice of commercial activities;
c placing under judicial supervision;
d judicial winding-up order.

3 Each Party shall take the necessary legislative or other measures to:

a provide for the seizure and confiscation of:

– goods, documents and other instrumentalities used to commit the offences, established in accordance with this Convention or to facilitate their commission;

– proceeds derived from such offences or property the value of which corresponds to such proceeds;

b enable the temporary or permanent closure of any establishment used to carry out any of the offences established in accordance with this Convention, without prejudice to the rights of *bona fide* third parties, or to deny the perpetrator, temporarily or permanently, the exercise of the professional or voluntary activity involving contact with children in the course of which the offence was committed.

4 Each Party may adopt other measures in relation to perpetrators, such as withdrawal of parental rights or monitoring or supervision of convicted persons.

5 Each Party may establish that the proceeds of crime or property confiscated in accordance with this article can be allocated to a special fund in order to finance prevention and assistance programmes for victims of any of the offences established in accordance with this Convention.

Article 28 – Aggravating circumstances

Each Party shall take the necessary legislative or other measures to ensure that the following circumstances, in so far as they do not already form part of the constituent elements of the offence, may, in conformity with the relevant provisions of internal law, be taken into consideration as aggravating circumstances in the determination of the sanctions in relation to the offences established in accordance with this Convention:

a the offence seriously damaged the physical or mental health of the victim;

b the offence was preceded or accompanied by acts of torture or serious violence;

c the offence was committed against a particularly vulnerable victim;

d the offence was committed by a member of the family, a person cohabiting with the child or a person having abused his or her authority;

e the offence was committed by several people acting together;

f the offence was committed within the framework of a criminal organisation;

g the perpetrator has previously been convicted of offences of the same nature.

Article 29 – Previous convictions

Each Party shall take the necessary legislative or other measures to provide for the possibility to take into account final sentences passed by another Party in relation to the offences established in accordance with this Convention when determining the sanctions.

Chapter VII – Investigation, prosecution and procedural law

Article 30 – Principles

1 Each Party shall take the necessary legislative or other measures to ensure that investigations and criminal proceedings are carried out in the best interests and respecting the rights of the child.

2 Each Party shall adopt a protective approach towards victims, ensuring that the investigations and criminal proceedings do not aggravate the trauma experienced by the child and that the criminal justice response is followed by assistance, where appropriate.

3 Each Party shall ensure that the investigations and criminal proceedings are treated as priority and carried out without any unjustified delay.

4 Each Party shall ensure that the measures applicable under the current chapter are not prejudicial to the rights of the defence and the requirements of a fair and impartial trial, in conformity with Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

5 Each Party shall take the necessary legislative or other measures, in conformity with the fundamental principles of its internal law:

– to ensure an effective investigation and prosecution of offences established in accordance with this Convention, allowing, where appropriate, for the possibility of covert operations;

– to enable units or investigative services to identify the victims of the offences established in accordance with Article 20, in particular by analysing child pornography material, such as photographs and audiovisual recordings transmitted or made available through the use of information and communication technologies.

Article 31 – General measures of protection

1 Each Party shall take the necessary legislative or other measures to protect the rights and interests of victims, including their special needs as witnesses, at all stages of investigations and criminal proceedings, in particular by:

a informing them of their rights and the services at their disposal and, unless they do not wish to receive such information, the follow-up given to their complaint, the charges, the general progress of the investigation or proceedings, and their role therein as well as the outcome of their cases;

b ensuring, at least in cases where the victims and their families might be in danger, that they may be informed, if necessary, when the person prosecuted or convicted is released temporarily or definitively;

c enabling them, in a manner consistent with the procedural rules of internal law, to be heard, to supply evidence and to choose the means of having their views, needs and concerns presented, directly or through an intermediary, and considered;

d providing them with appropriate support services so that their rights and interests are duly presented and taken into account;

e protecting their privacy, their identity and their image and by taking measures in accordance with internal law to prevent the public dissemination of any information that could lead to their identification;

f providing for their safety, as well as that of their families and witnesses on their behalf, from intimidation, retaliation and repeat victimisation;

g ensuring that contact between victims and perpetrators within court and law enforcement agency premises is avoided, unless the competent authorities establish otherwise in the best interests of the child or when the investigations or proceedings require such contact.

2 Each Party shall ensure that victims have access, as from their first contact with the competent authorities, to information on relevant judicial and administrative proceedings.

3 Each Party shall ensure that victims have access, provided free of charge where warranted, to legal aid when it is possible for them to have the status of parties to criminal proceedings.

4 Each Party shall provide for the possibility for the judicial authorities to appoint a special representative for the victim when, by internal law, he or she may have the status of a party to the criminal proceedings and where the holders of parental responsibility are precluded from representing the child in such proceedings as a result of a conflict of interest between them and the victim.

5 Each Party shall provide, by means of legislative or other measures, in accordance with the conditions provided for by its internal law, the possibility for groups, foundations, associations or governmental or non-governmental organisations, to assist and/or support the victims with their consent during criminal proceedings concerning the offences established in accordance with this Convention.

6 Each Party shall ensure that the information given to victims in conformity with the provisions of this article is provided in a manner adapted to their age and maturity and in a language that they can understand.

Article 32 – Initiation of proceedings

Each Party shall take the necessary legislative or other measures to ensure that investigations or prosecution of offences established in accordance with this Convention shall not be dependent upon the report or accusation made by a victim, and that the proceedings may continue even if the victim has withdrawn his or her statements.

Article 33 – Statute of limitation

Each Party shall take the necessary legislative or other measures to ensure that the statute of limitation for initiating proceedings with regard to the offences established in accordance with Articles 18, 19, paragraph 1.a and b, and 21, paragraph 1.a and b, shall continue for a period of time sufficient to allow the efficient starting of proceedings after the victim has reached the age of majority and which is commensurate with the gravity of the crime in question.

Article 34 – Investigations

1 Each Party shall adopt such measures as may be necessary to ensure that persons, units or services in charge of investigations are specialised in the field of combating sexual exploitation and sexual abuse of children or that persons are trained for this purpose. Such units or services shall have adequate financial resources.

2 Each Party shall take the necessary legislative or other measures to ensure that uncertainty as to the actual age of the victim shall not prevent the initiation of criminal investigations.

Article 35 – Interviews with the child

1 Each Party shall take the necessary legislative or other measures to ensure that:

a interviews with the child take place without unjustified delay after the facts have been reported to the competent authorities;

b interviews with the child take place, where necessary, in premises designed or adapted for this purpose;

c interviews with the child are carried out by professionals trained for this purpose;

d the same persons, if possible and where appropriate, conduct all interviews with the child;

e the number of interviews is as limited as possible and in so far as strictly necessary for the purpose of criminal proceedings;

f the child may be accompanied by his or her legal representative or, where appropriate, an adult of his or her choice, unless a reasoned decision has been made to the contrary in respect of that person.

2 Each Party shall take the necessary legislative or other measures to ensure that all interviews with the victim or, where appropriate, those with a child witness, may be videotaped and that these videotaped interviews may be accepted as evidence during the court proceedings, according to the rules provided by its internal law.

3 When the age of the victim is uncertain and there are reasons to believe that the victim is a child, the measures established in paragraphs 1 and 2 shall be applied pending verification of his or her age.

Article 36 – Criminal court proceedings

1 Each Party shall take the necessary legislative or other measures, with due respect for the rules governing the autonomy of legal professions, to ensure that training on children's rights and sexual exploitation and sexual abuse of children is available for the benefit of all persons involved in the proceedings, in particular judges, prosecutors and lawyers.

2 Each Party shall take the necessary legislative or other measures to ensure, according to the rules provided by its internal law, that:

a the judge may order the hearing to take place without the presence of the public;

b the victim may be heard in the courtroom without being present, notably through the use of appropriate communication technologies.

Chapter VIII – Recording and storing of data

Article 37 – Recording and storing of national data on convicted sexual offenders

1 For the purposes of prevention and prosecution of the offences established in accordance with this Convention, each Party shall take the necessary legislative or other measures to collect and store, in accordance with the relevant provisions on the protection of personal data and other appropriate rules and guarantees as prescribed by domestic law, data relating to the identity and to the genetic profile (DNA) of persons convicted of the offences established in accordance with this Convention.

2 Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of a single national authority in charge for the purposes of paragraph 1.

3 Each Party shall take the necessary legislative or other measures to ensure that the information referred to in paragraph 1 can be transmitted to the competent authority of another Party, in conformity with the conditions established in its internal law and the relevant international instruments.

Chapter IX – International co-operation

Article 38 – General principles and measures for international co-operation

1 The Parties shall co-operate with each other, in accordance with the provisions of this Convention, and through the application of relevant applicable international and regional instruments, arrangements agreed on the basis of uniform or reciprocal legislation and internal laws, to the widest extent possible, for the purpose of:

a preventing and combating sexual exploitation and sexual abuse of children;

b protecting and providing assistance to victims;

c investigations or proceedings concerning the offences established in accordance with this Convention.

2 Each Party shall take the necessary legislative or other measures to ensure that victims of an offence established in accordance with this Convention in the territory of a Party other than the one where they reside may make a complaint before the competent authorities of their State of residence.

3 If a Party that makes mutual legal assistance in criminal matters or extradition conditional on the existence of a treaty receives a request for legal assistance or extradition from a Party with which it has not concluded such a treaty, it may consider this Convention the legal basis for mutual legal assistance in criminal matters or extradition in respect of the offences established in accordance with this Convention.

4 Each Party shall endeavour to integrate, where appropriate, prevention and the fight against sexual exploitation and sexual abuse of children in assistance programmes for development provided for the benefit of third states.

Chapter X – Monitoring mechanism

Article 39 – Committee of the Parties

1 The Committee of the Parties shall be composed of representatives of the Parties to the Convention.

2 The Committee of the Parties shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within a period of one year following the entry into force of this Convention for the tenth signatory having ratified it. It shall subsequently meet whenever at least one third of the Parties or the Secretary General so requests.

3 The Committee of the Parties shall adopt its own rules of procedure.

Article 40 – Other representatives

1 The Parliamentary Assembly of the Council of Europe, the Commissioner for Human Rights, the European Committee on Crime Problems (CDPC), as well as other relevant Council of Europe intergovernmental committees, shall each appoint a representative to the Committee of the Parties.

2 The Committee of Ministers may invite other Council of Europe bodies to appoint a representative to the Committee of the Parties after consulting the latter.

3 Representatives of civil society, and in particular non-governmental organisations, may be admitted as observers to the Committee of the Parties following the procedure established by the relevant rules of the Council of Europe.

4 Representatives appointed under paragraphs 1 to 3 above shall participate in meetings of the Committee of the Parties without the right to vote.

Article 41 – Functions of the Committee of the Parties

1 The Committee of the Parties shall monitor the implementation of this Convention. The rules of procedure of the Committee of the Parties shall determine the procedure for evaluating the implementation of this Convention.

2 The Committee of the Parties shall facilitate the collection, analysis and exchange of information, experience and good practice between States to improve their capacity to prevent and combat sexual exploitation and sexual abuse of children.

3 The Committee of the Parties shall also, where appropriate:

a facilitate the effective use and implementation of this Convention, including the identification of any problems and the effects of any declaration or reservation made under this Convention;

b express an opinion on any question concerning the application of this Convention and facilitate the exchange of information on significant legal, policy or technological developments.

4 The Committee of the Parties shall be assisted by the Secretariat of the Council of Europe in carrying out its functions pursuant to this article.

5 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the activities mentioned in paragraphs 1, 2 and 3 of this article.

Chapter XI – Relationship with other international instruments

Article 42 – Relationship with the United Nations Convention on the Rights of the Child and its Optional Protocol on the sale of children, child prostitution and child pornography

This Convention shall not affect the rights and obligations arising from the provisions of the United Nations Convention on the Rights of the Child and its Optional Protocol on the sale of children, child prostitution and child pornography, and is intended to enhance the protection afforded by them and develop and complement the standards contained therein.

Article 43 – Relationship with other international instruments

1 This Convention shall not affect the rights and obligations arising from the provisions of other international instruments to which Parties to the present Convention are Parties or shall become Parties and which contain provisions on matters governed by this Convention and which ensure greater protection and assistance for child victims of sexual exploitation or sexual abuse.

2 The Parties to the Convention may conclude bilateral or multilateral agreements with one another on the matters dealt with in this Convention, for purposes of supplementing or strengthening its provisions or facilitating the application of the principles embodied in it.

3 Parties which are members of the European Union shall, in their mutual relations, apply Community and European Union rules in so far as there are Community or European Union rules governing the particular subject concerned and applicable to the specific case, without prejudice to the object and purpose of the present Convention and without prejudice to its full application with other Parties.

Chapter XII – Amendments to the Convention

Article 44 – Amendments

1 Any proposal for an amendment to this Convention presented by a Party shall be communicated to the Secretary General of the Council of Europe and forwarded by him or her to the member States of the Council of Europe, any signatory, any State Party, the European Community, any State invited to sign this Convention in accordance with the provisions of Article 45, paragraph 1, and any State invited to accede to this Convention in accordance with the provisions of Article 46, paragraph 1.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall enter into force on the first day of the month following the expiration of a period of one month after the date on which all Parties have informed the Secretary General that they have accepted it.

Chapter XIII – Final clauses

Article 45 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe, the non-member States which have participated in its elaboration as well as the European Community.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which 5 signatories, including at least 3 member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.

4 In respect of any State referred to in paragraph 1 or the European Community, which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of its instrument of ratification, acceptance or approval.

Article 46 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may, after consultation of the Parties to this Convention and obtaining their unanimous consent, invite any non-member State of the Council of Europe, which has not participated in the elaboration of the Convention, to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe, and by unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any acceding State, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 47 – Territorial application

1 Any State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration and for whose international relations it is responsible or on whose behalf it is authorised to give undertakings. In respect of such territory, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 48 – Reservations

No reservation may be made in respect of any provision of this Convention, with the exception of the reservations expressly established. Any reservation may be withdrawn at any time.

Article 49 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 50 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, any State signatory, any State Party, the European Community, any State invited to sign this Convention in accordance with the provisions of Article 45 and any State invited to accede to this Convention in accordance with the provisions of Article 46 of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 45 and 46;

d any amendment adopted in accordance with Article 44 and the date on which such an amendment enters into force;

e any reservation made under Article 48;

f any denunciation made in pursuance of the provisions of Article 49;

g any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Lanzarote, this 25th day of October 2007, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, to the European Community and to any State invited to accede to this Convention.

IOCTA

INTERNET ORGANISED CRIME THREAT ASSESSMENT

[2019]

EUROPOL | EC3 European Cybercrime Centre

IOCTA
[2019]

EUROPOL

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019

www.europol.europa.eu

CONTENTS

foreword 04 **abbreviations** 05 **executive summary** 06

#1

key findings 08

#2

recommendations 10

#3

introduction 13

#4

crime priority: cyber-dependent crime 14

4.1. Key findings
4.2. Ransomware
4.3. Data compromise
4.4. DDoS attacks
4.5. Attacks on critical infrastructure
4.6. Website defacement
4.7. What happened to…?
4.8. Future threats and developments
4.9. Recommendations

#5

crime priority: child sexual exploitation online 29

5.1. Key findings
5.2. Online distribution of CSEM
5.3. Online sollicitation of children for sexual purposes
5.4. Production of self-generated explicit material
5.5. Sexual coercion and extortion of minors for new CSEM
5.6. Live distant child abuse
5.7. Future threats and developments
5.8. Recommendations

#6

crime priority: payment fraud 35

6.1. Key findings
6.2. Card not present fraud
6.3. Skimming
6.4. Jackpotting
6.5. Business email compromise
6.6. Future threats and developments
6.7 Recommendations

#7

the criminal abuse of the dark web 43

7.1. Key findings
7.2. Recommendations

#8

the convergence of cyber and terrorism 47

8.1. Key findings
8.2. The use of the internet by terrorist groups
8.3. Recommendations

#9

cross-cutting crime factors 50

9.1. Key findings
9.2. Social engineering
9.3. Money mules
9.4. The criminal abuse of cryptocurrencies
9.5. Common challenges for law enforcement
9.6. Future threats and developments
9.7. Recommendations

references 60

FOREWORD

I am pleased to introduce the 2019 Internet Organised Crime Threat Assessment (IOCTA), Europol's annual presentation of the cybercrime threat landscape, highlighting the key developments, threats and trends, as seen by law enforcement authorities across Europe. As always, I extend my gratitude to the invaluable contributions from our colleagues within European law enforcement and to our partners in private industry and academia for their ongoing support and input.

This year's IOCTA demonstrates that while we must look ahead to anticipate what challenges new technologies, legislation, and criminal innovation may bring, we must not forget to look behind us. 'New' threats continue to emerge from vulnerabilities in established processes and technologies. Moreover, the longevity of cyber threats is clear, as many long-standing and established *modi operandi* persist, despite our best efforts. Some threats of yesterday remain relevant today and will continue to challenge us tomorrow.

Ransomware maintains its reign as the most widespread and financially damaging form of cyber-attack, while criminals continue to defraud e-commerce and attack the financial sector. Criminals target and exploit vulnerable minors across the globe. All of these crimes seriously impact the physical, financial and psychological safety, security and stability of our society and require a coherent and coordinated response by law enforcement.

Cybercrime continues to mature and become more audacious, shifting its focus to larger and more profitable targets. To tackle it, law enforcement must be equally audacious in order to meet the challenge head-on.

To do so, however, law enforcement needs the knowledge, tools and legislation required to do so quickly and effectively. As criminals adapt, law enforcement and legislators must also innovate in order to stay ahead, and seek to capitalise on new and developing technologies. This in turn requires training to produce the specialised capabilities required to investigate technically challenging or complex cybercrimes, such as those involving the abuse of cryptocurrencies or the dark web.

Europol is addressing these challenges with its Strategy 2020+. Our agency is at the forefront of law enforcement innovation and acts as a knowledge platform for the provision of EU policing solutions in relation to encryption, cryptocurrencies and other issues. In doing so, we expand the toolbox available to law enforcement officers across Europe and beyond, increasing their technical and forensic capabilities. The European Cybercrime Centre (EC3) at Europol is the first port of call for cybercrime investigators.

This only enforces the need for greater cooperation and collaboration with the private sector and academia, with whom law enforcement shares the responsibility for fighting cybercrime, and with the policy-makers who shape our society.

The IOCTA continues to celebrate the many successes of law enforcement in the fight against cybercrime, and the feats that can be achieved from the synergistic relationships with its partners in both the public and private sector. I have no doubt that such relationships will continue to go from strength to strength, but their full potential can only be realised under the right legislative and budgetary conditions. We can look forward to reporting further successes in the years to come.

Catherine De Bolle
Executive Director of Europol

ABBREVIATIONS

AMLD 5 5th EU Anti-Money Laundering Directive

APT Advanced Persistent Threat

ATM Automated Teller Machine

BEC Business Email Compromise

C2C Criminal to Criminal

CERT Computer Emergency Response Team

CNP Card Not Present

CPU Central Processing Unit

CSE Child Sexual Exploitation

CSEM Child Sexual Exploitation Material

DDoS Distributed Denial of Service

DMARC Domain-based message authentication, reporting and conformance

EBA European Banking Authority

EBF European Banking Federation

EC3 Europol's European Cybercrime Centre

EMAS Europol Malware Analysis Solution

EMMA European Money Mule Actions

EMPACT European Multidisciplinary Platform Against Criminal Threats

EMV Europay, MasterCard and Visa

EPC European Payment Council

FIOD Dutch Fiscal Information and Investigative Service

GDPR General Data Protection Regulation

GPU Graphics Processing Unit

I2P Invisible Internet Project

ICANN Internet Corporation for Assigned Names and Numbers

IOCTA Internet Organised Crime Threat Assessment

IP Internet Protocol

IS Islamic State

JIT Joint Investigation Team

LDCA Live Distant Child Abuse

NCPF Non-Cash Payment Fraud

OCG Organised Crime Group

OSP Online Service Provider

PNR Passenger Name Record

RDP Remote Desktop Protocols

RWE Right-wing extremism

SGEM Self-Generated Explicit Material

SWIFT Society for Worldwide Interbank Financial Telecommunications

THB Trafficking in Human Beings

Tor The Onion Router

URL Uniform Resource Locator

VIDTF Victim Identification Task Force

VPN Virtual Private Network

EXECUTIVE SUMMARY

This annual assessment of the cybercrime threat landscape highlights the persistence and tenacity of a number of key threats. In all areas, we see how most of the main threats have been reported previously, albeit with variations in terms of volumes, targets and level of sophistication. This is not for lack of action on the side of the public and the private sector. Rather, this persistence demonstrates the complexity of countering cybercrime and the perspective that criminals only innovate when existing *modi operandi* have become unsuccessful. Therefore, while much focus in contemporary parlance is on the potential impact of future technological developments on cybercrime, such as Artificial Intelligence, we must approach cybercrime in a holistic sense. Countering cybercrime is as much about its present forms as it is about future projections*. New threats do not only arise from new technologies but, as is often demonstrated, come from known vulnerabilities in existing technologies.

This year's IOCTA demonstrates that for all cybercrime, data remains the key element, both from a crime perspective and from an investigative perspective. Criminals target data for their crimes, making data security with respect to organisations and awareness of consumers all the more important. Data security has taken centre stage even more after the implementation of the General Data Protection Regulation (GDPR). While it is too early for a full assessment, the response to data breaches — through media headlines and high fines — will potentially have a positive impact and lead to enhanced data security.

Ransomware remains the top threat in this year's IOCTA. Even though we have witnessed a decline in the overall volume of ransomware attacks, those that do take place are more targeted, more profitable and cause greater economic damage. As long as ransomware provides a relatively easy income for cybercriminals, and continues to cause significant damage and financial losses, it is likely to remain the top cybercrime threat. In the area of payment fraud, we continue to identify card not present (CNP) fraud as the main priority — as reported by law enforcement and confirmed by private sector reporting in the payment fraud arena. Criminals primarily manage to carry out CNP fraud through data gathered from data security breaches and social engineering.

Data returns to the discussion of other threats as well. A crucial priority reported by both Member States and the private industry is Business Email Compromise (BEC). While BEC is not new, it is evolving. This scam exploits the way corporations do business, taking advantage of segregated corporate structures, and internal gaps in payment verification processes. Such attacks vary by the degree of technical tools used. Some attacks can successfully employ only social engineering, while others deploy technical measures such as malware and network intrusion. In both cases, data is again at the centre of the crime scene.

While using ransomware to deny an organisation access to its own data may be the primary threat in this year's report, denying others access to that organisation's data or services is another significant threat. Distributed Denial of Service (DDoS) Attacks are yet another data-focused threat to cope with. Of all the motivations behind such attacks, those with an extortion element were overwhelmingly the most prevalent.

Whereas criminals require data for most of their crimes, law enforcement needs access to relevant data for their investigations. Indeed, the ability of law enforcement agencies to access the data needed to conduct criminal investigations is an increasing challenge. This is a result of technological developments, such as the enhanced use of encryption which criminals abuse to obfuscate their tracks, as well as cryptocurrencies

* These were usefully explored in Europol's recent publication "Do Criminals Dream of Electric Sheep? How Technology Shapes the Future of Crime and Law Enforcement" (https://www.europol.europa.eu/publications-documents/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement)

to hide their illicit earnings. However, inaccessibility of relevant data also comes due to legislative barriers or shortcomings, which we must overcome to enhance cross-border access to electronic evidence and the effectiveness of public-private cooperation through facilitated information exchange.

These barriers are often related to the principle of territoriality, which sets limits to the scope of jurisdiction and to the investigative powers which law enforcement and judiciary have at their disposal under their national law. As a result, the tools in the hands of investigators and prosecutors do not correspond to what would be needed to deal with data flows, for which questions of territoriality are of no relevance.

At the same time, there is also the ever-increasing challenge of data overload, as we can see in the area of online Child Sexual Exploitation (CSE). The amount of Child Sexual Exploitation Material (CSEM) detected online by law enforcement and the private sector continues to increase. This increase puts a considerable strain on law enforcement resources and requires a response to ensure that the volume of data does not impede law enforcement authorities' responsibility to conduct criminal investigations into CSEM. This is one example where innovation and law enforcement agencies must innovate to find ways to digest the increasing volumes of data coming in.

Related challenges also demonstrate how the evolution of existing threats is often a result of scale. Self-generated explicit material (SGEM) is more and more common, driven by a growing number of minors with access to high-quality smartphones. On top of this growing access, a lack of awareness about the risks on the side of minors exacerbates the problem. At Europol, through the organisation of the first European Youth Day, we have specifically aimed to enhance minors' awareness about online risks. The online solicitation of children for sexual purposes remains a serious threat, with a largely unchanged *modus operandi* in terms of grooming and sexual coercion, demonstrating again the tenacity of existing forms of cybercrime.

Access to data allows criminals to carry out various forms of fraud. Such data is also available on the dark web, which is often a key enabler of many other forms of illegal activity. Within this report, it once again becomes evident how the dark web underpins many crime areas and how investigators highlight the phenomenon as a priority.

Moreover, as the dark web evolves, it has become a threat in its own right, and not only as a medium for the sale of illicit commodities such as drugs, firearms or compromised data. The impact of law enforcement action in this arena is palpable as the environment remains in a state of flux. As a result, more coordinated investigation and prevention actions targeting the phenomenon are required, demonstrating the ability of law enforcement to have a lasting impact and deterring users from illicit activity on the dark web.

As more and more companies outsource areas of their business, such as moving more infrastructure to third-party cloud services, we expect to see a growth in supply chain attacks, and the evolution of such attacks to become increasingly complex. This develops a clear interdependency between organisations and leads to the necessity of having a higher level of cybersecurity across the spectrum to ensure the minimisation of successful cybercrime attacks. When an attack does occur, being prepared to respond rapidly is essential. Therefore, building on important steps already taken, we need to continue to enhance synergies between the network and information security sector and the cyber law enforcement authorities, in order to improve the overall cyber resilience of the entire cybersecurity ecosystem.

The IOCTA is a resource for the intelligence-led deployment of law enforcement resources. It also contains recommendations for policy-makers and for the orientation of further research and prevention measures. The diversity and complexity of online threats is such the full range of public and private actors must work together to make progress in prevention, legislation, enforcement and prosecution. All of these elements are necessary in order to disrupt organised crime activity and reduce the online threat to businesses, governments and, above all, EU citizens.

KEY FINDINGS #1

CYBER-DEPENDENT CRIME

- While ransomware remains the top threat in this report, the overall volume of ransomware attacks has declined as attackers focus on fewer but more profitable targets and greater economic damage.
- Phishing and vulnerable remote desktop protocols (RDPs) are the key primary malware infection vectors.
- Data remains a key target, commodity and enabler for cybercrime.
- Following the increase of destructive ransomware, such as the Germanwiper attacks of 2019, there is a growing concern within organisations over attacks of sabotage.
- Continuous efforts are needed to further synergise the network and information security sector and the cyber law enforcement authorities to improve the overall cyber resilience and cybersecurity.

CHILD SEXUAL EXPLOITATION ONLINE

- The amount of CSEM detected online by law enforcement and the private sector continues to increase, putting considerable strain on law enforcement resources.
- The online solicitation of children for sexual purposes remains a serious threat with a largely unchanged *modus operandi*.
- SGEM is more and more common, driven by growing access of minors to high quality smartphones and a lack of awareness of the risks.
- Although commercial CSE remains limited, live distant child abuse (LDCA) is a notable exception to this.

PAYMENT FRAUD

- CNP fraud continues to be the main priority within payment fraud and continues to be a facilitator for other forms of illegal activity.
- Skimming continues to evolve with criminals continuously adapting to new security measures.
- Jackpotting attacks are becoming more accessible and successful.

THE CRIMINAL ABUSE OF THE DARK WEB

- The dark web remains the key online enabler for trade in an extensive range of criminal products and services and a priority threat for law enforcement.
- Recent coordinated law enforcement activities, combined with extensive Distributed Denial of Service (DDoS) attacks have generated distrust in The onion router (Tor) environment. While there is evidence administrators are now exploring alternatives, it seems the user-friendliness, existing market variety and customer-base on Tor makes a full migration to new platforms unlikely just yet.
- There are increases in single-vendor shops and smaller fragmented markets on Tor, including those catering for specific languages. Some organised crime groups (OCGs) are also fragmenting their business over a range of online monikers and marketplaces, therefore presenting further challenges for law enforcement.
- Encrypted communication applications enhance single-vendor trade on the dark web, helping direct users to services and enabling closed communications. Although there is no evidence of a full business migration, there is a risk the group functions could become increasingly used to support illicit trade.

THE CONVERGENCE OF CYBER AND TERRORISM

- The wide array of online service providers (OSPs) exploited by terrorist groups presents a significant challenge for disruption efforts.
- Terrorist groups are often early adopters of new technologies, exploiting emerging platforms for their online communication and distribution strategies.
- With sufficient planning and support from sympathetic online communities, terrorist attacks can rapidly turn viral, before OSPs and law enforcement can respond.

CROSS-CUTTING CRIME FACTORS

- Phishing remains an important tool in the arsenal of cybercriminals for both cyber-dependent crime and non-cash payment fraud (NCPF).
- While cryptocurrencies continue to facilitate cybercrime, hackers and fraudsters now routinely target crypto-assets and enterprises.

RECOMMENDATIONS

#2

The following recommendations respond to the Key Findings found above in chapter 1 and the threats described throughout this report. These recommendations are intended to support law enforcement, regulators and policy-makers in their decision-making processes. Crucially they are of fundamental importance in informing the respective European Multidisciplinary Platform Against Criminal Threats (EMPACT) priorities when setting the actions for the 2020 Operational Action Plans for the three sub-areas of the EMPACT priority in cybercrime: cybercrime attacks against information systems, NCPF, and CSE online. These recommendations should also help inform research and innovation efforts and programmes at national and EU level.

CYBER-DEPENDENT CRIME

Successfully tackling major crime-as-a-service providers can have a clear and lasting impact. Law enforcement should continue focusing its concerted efforts into tackling such service providers.

Enhanced cooperation and improved data sharing between law enforcement, computer security incident response teams and private partners will be the key to tackling complex cyberattacks, and allow the private sector to take the necessary preventative security measures to protect themselves and their customers.

In response to major cross-border cyber-attacks, all cooperation channels should be explored, including Europol's and Eurojust's support capabilities as well as legal instruments designed for closer cross-border cooperation (such as Joint investigation Teams (JITs) and spontaneous exchange of information) in order to share resources and coordinate.

Further enhance the collaboration between the network and information security sector and the cyber law enforcement authorities by involving the latter in cyber resilience-related activities such as cyber simulation exercises.

Low-level cybercrimes such as website defacement should be seen as an opportunity for law enforcement to intervene in the criminal career path of young, developing cybercriminals.

CHILD SEXUAL EXPLOITATION ONLINE

Coordinated action with the private sector and the deployment of new technology, including Artificial Intelligence, could help reduce the production and distribution of online CSEM, facilitate investigations, and assist with the processing of the massive data volumes associated with CSEM cases.

A structural educational campaign across Europe to deliver a consistent high-quality message aimed at children about online risks is of the utmost importance to reduce the risks derived from SGEM such as sexual coercion and extortion.

As much CSEM, particularly that arising from LDCA, originates from developing countries, it is essential that EU law enforcement continues to cooperate with, and support the investigations of, law enforcement in these jurisdictions.

Fighting CSE is a joint effort between law enforcement and the private sector and a common platform is needed to coordinate efforts and prevent a fragmented approach and duplicated efforts.

To prevent child sex offenders from travelling to third countries to sexually abuse children, EU law enforcement should make use of passenger name record (PNR) data accessible through the Travel Intelligence team within Europol.

PAYMENT FRAUD

Cooperation between the public and the private sector as well as within the sectors is crucial to come to fruitful results. To this point, speedy and more direct access to and exchange of information from the private sector is essential for Europol and its partners.

Organisations must ensure they train their employees and make their customers aware of how they can detect social engineering and other scams.

THE CRIMINAL ABUSE OF THE DARK WEB

More coordinated investigation and prevention actions targeting the phenomenon are required, demonstrating the ability of law enforcement and deterring users from illicit activity on the dark web.

The ability to maintain an accurate real-time information position is necessary to enable law enforcement efforts to tackle the dark web. The capability needs to enable the identification, categorisation, collection and advanced analytical processing, including machine learning and AI.

An EU-wide framework is required to enable judicial authorities to take the first steps to attribute a case to a country where no initial link is apparent due to anonymity issues, thereby preventing any country from assuming jurisdiction initiating an investigation.

Improved coordination and standardisation of undercover online investigations are required to de-conflict dark web investigations and address the disparity in capabilities across the EU.

THE CONVERGENCE OF CYBER AND TERRORISM

Limiting the ability of terrorists to carry out transnational attacks by disrupting their flow of propaganda and attributing online terrorism-related offences requires continued and heightened counterterrorism cooperation and information sharing across law enforcement authorities, as well as with the private sector.

Any effective measure to counter terrorist groups' online propaganda and recruitment operations entails addressing the whole range of abused OSPs, especially start-ups and smaller platforms with limited capacity for response.

Cross-platform collaboration and a multi-stakeholder crisis response protocol on terrorist content online would be essential to crisis management the aftermath of a terrorist attack.

A better understanding of new and emerging technologies is a priority for law enforcement practitioners. Upcoming policy debates and legislative developments should take into account the features of these technologies in order to devise an effective strategy to prevent further abuse.

CROSS-CUTTING CRIME FACTORS

Law enforcement and the judiciary must continue to develop, share and propagate knowledge on how to recognise, track, trace, seize and recover cryptocurrency assets.

Law enforcement must continue to build trust-based relationships with cryptocurrency-related businesses, academia, and other relevant private sector entities, to more effectively tackle issues posed by cryptocurrencies during investigations.

Despite the gradual implementation of the Directive (EU) 2018/843 of the European Parliament and of the Council[1] (known as AMLD 5, 5th Anti-Money Laundering Directive) across the EU, investigators should be vigilant concerning emerging cryptocurrency conversion and cash-out opportunities and share any new information with Europol.

INTRODUCTION

#3

The European Union Serious and Organised Crime Threat Assessment (SOCTA) 2017 identified cybercrime as one of the 10 priorities in the fight against organised and serious international crime[2]. This overarching category includes cybercrime attacks against information systems, NCPF, CSE online and other enabling criminal activities.

Aim

The IOCTA aims to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, to direct the operational focus for EU law enforcement. The 2019 IOCTA will contribute to the setting of priorities for the 2020 EMPACT operational action plan in the three above-mentioned sub-areas of the EMPACT priority of cybercrime, as well as cross-cutting crime enablers.

Scope

The 2019 IOCTA focuses on the trends and developments pertinent to the above-mentioned priority crime areas. In addition to this, the report will discuss other cross-cutting factors that influence or impact the cybercrime ecosystem, such as criminal abuse of cryptocurrencies and social engineering.

This report provides an update on the latest trends and the current impact of cybercrime within Europe and the EU. Each chapter provides a law enforcement-centric view of the threats and developments within cybercrime, based predominantly on the experiences of cybercrime investigators and their operational counterparts from other sectors. Furthermore, it draws on contributions from strategic partners in private industry and academia to support or contrast this perspective. The report seeks to highlight future risks and emerging threats and provides recommendations to align and strengthen the joint efforts of EU law enforcement and its partners in preventing and fighting cybercrime.

Methodology

The 2019 IOCTA was drafted by a team of Europol analysts and specialists drawing predominantly on contributions from 26 Member States and European third-party members, the European Union Cybercrime Taskforce, Eurojust, Europol's Analysis Projects Cyborg, Dark Web, Terminal, Twins and the Cyber Intelligence Team of Europol's European Cybercrime Centre (EC3), via structured surveys and feedback sessions. This has been enhanced with open source research and input from the private sector, namely EC3's Advisory Groups on Financial Services, Internet Security and Communication Providers. These contributions have been essential to the production of the report.

Acknowledgements

Europol would like to extend thanks to all law enforcement and private sector partners who contributed to this report, in particular the European Banking Federation (EBF) and the EC3's Academic Advisory Network.

#4

CRIME PRIORITY

cyber-dependent crime

Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). Such crimes are typically directed at computers, networks or other ICT resources. In essence, without the internet criminals could not commit these crimes[3]. It includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data and denial of service attacks to cause financial and/or reputational damage.

4.1 » KEY FINDINGS

- While ransomware remains the top threat in this report, the overall volume of ransomware attacks has declined as attackers focus on fewer, but more profitable targets, and greater economic damage.
- Phishing and vulnerable RDPs are the key primary malware infection vectors.
- Data remains a key target, commodity and enabler for cybercrime.
- Following the increase of destructive ransomware, such as the Germanwiper attacks of 2019, there is a growing concern within organisations over attacks of sabotage.
- Continuous efforts are needed to further synergise the network and information security sector and the cyber law enforcement authorities to improve the overall cyber resilience and cybersecurity.

4.2 » RANSOMWARE

Ransomware evolves as it remains the most prominent threat

The majority of private sector reporting indicates that there was a notable decline in ransomware attacks throughout 2018[4]. This may be attributable to a number of factors: an increased awareness among potential victims — fuelled by industry and law enforcement initiatives to mitigate the threat (such as NoMoreRansom); the increasing use of mobile devices by consumers (with most ransomware targeting Windows-based devices); and a decline in the use of exploit kits (which were a key delivery method).

Despite this, the number of victims is still high, and ransomware clearly and overwhelmingly retains its position as the top cyber threat faced by European cybercrime investigators, the second most prominent threat for the private sector[5], and one of the most common samples submitted to the Europol Malware Analysis Solution (EMAS). Moreover, as long as ransomware provides a relatively easy income for cybercriminals, and continues to cause significant damage and financial losses, it is likely to remain the top cybercrime threat.

Investigators cited over 25 individual identifiable families of ransomware, targeting citizens, and private and public entities within Europe. Several of these featured more prominently in law enforcement reporting, including the various versions of *Dharma/CrySiS, ACCDFISA, GlobeImposter,* and *Rapid*. GandCrab, Locky, and Curve-Tor-Bitcoin-Locker also featured prominently in EMAS submissions. While the Rapid ransomware only surfaced in January 2018, the other families, and many of the less frequently reported families have been in circulation for several years, highlighting the persistence of these threats once released into the wild.

Attacks shift to more valuable targets

Last year law enforcement began to see the shift from untargeted, scattergun attacks affecting citizen and businesses alike, to more targeted attacks. Both European law enforcement and Europol's private sector partners confirm a diminishing number of ransomware attacks targeting individual

citizens, and more attacks specifically engineered towards individual private and public sectors entities. This is also a likely explanation for the apparent decline in the overall volume of attacks.

While targeting specific companies is potentially more labour-intensive and technically challenging, requiring the attackers to follow the cyber kill-chain[6], it also means that attackers are able to pitch the ransom for decrypting the victim's files based on the victim's perceived ability to pay. For example, there are cases where a company's encrypted files have been ransomed for over EUR 1 million.

Remote desktop protocols and emails remain the key infection methods

Such targeted cyber-attacks require specific tactics to infect the target network. The trend in the use of social engineering and targeted phishing emails as a primary infection method continues from last year. Some reports highlight that as many as 65 % of groups rely on spear-phishing as their primary infection vector[7]. The use of vulnerable RDPs also continues to grow. Attackers can either brute force access to a target's RDP or often can buy access to the target network on a criminal forum. In this area, the importance of patching once again becomes apparent. In May 2019, for example, Microsoft published the security vulnerability CVE-2019-0708, named sometime later as BlueKeep.

An attacker can exploit this vulnerability by connecting via RDP to the target machine and sending specifically crafted requests. This particular vulnerability does not require either victim interaction nor user authentication, allowing any attacker who succeeds in exploiting the vulnerability to execute arbitrary code on the compromised machine. The exploit works completely filelessly, providing full control of a remote system without having to deploy any malware. In addition, it also does not require an active session on the target.

Almost one million devices may be vulnerable to this exploit[8].

case study

Ransomware attacks against local and state government agencies in the United States:

Most visible ransomware attacks in 2019 were those against local governments, specifically in the United States. This trend commenced earlier. In 2018, a ransomware attack paralysed the city of Atlanta for several weeks and this only proved to be the tip of the iceberg. After that, already more than half a dozen cities and public services across the US had fallen victim to ransomware, on a near-monthly basis[11]. Other examples of 2019 include Baltimore and Florida. The Governor of Louisiana even declared a state of emergency after another local ransomware attack[12]. According to an extensive historical overview of ransomware attacks targeting local and state governments, based on public disclosures, every state in the US has been hit with an attack with the exception of Delaware and Kentucky[13]. Whether this trend will also become a threat to Member States is something to be seen, but the experiences in the US definitely function as a warning.

devices will likely remain unpatched, allowing cybercriminals to include the BlueKeep vulnerability exploitation attack in their arsenal to be used with other well-known malicious software, like ransomware inside private and business networks.

While their use continues and new ones continue to be developed, exploit kits did not feature in law enforcement reporting this year.

Sabotage: a growing fear for the private sector

Another key development in the wake of attacks such as *NotPetya*, is that many private sector companies now fear not only 'conventional' ransomware attacks, but also destructive cyber-attacks; acts of sabotage which would permanently erase or otherwise irreversibly damage company data. Such concerns are particularly valid given the conclusion that cyberattacks designed to cause damage doubled during the first six months of 2019, of those attacked 50 % are in the manufacturing sector[9]. Whereas historically speaking destructive malware was predominantly associated with nation-state actors, since late 2018 cybercriminals are also increasingly incorporating 'wiper elements' as part of their attacks, through new strains of malware. GermanWiper surfaced during the summer of 2019 as a new type of ransomware which rather than encrypting the victim's files, rewrites the content resulting in the permanent destruction of the victim's data[10]. Without back-ups, victims are most likely to have permanently lose their data.

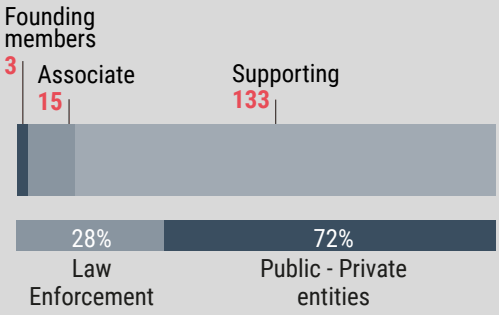
case study

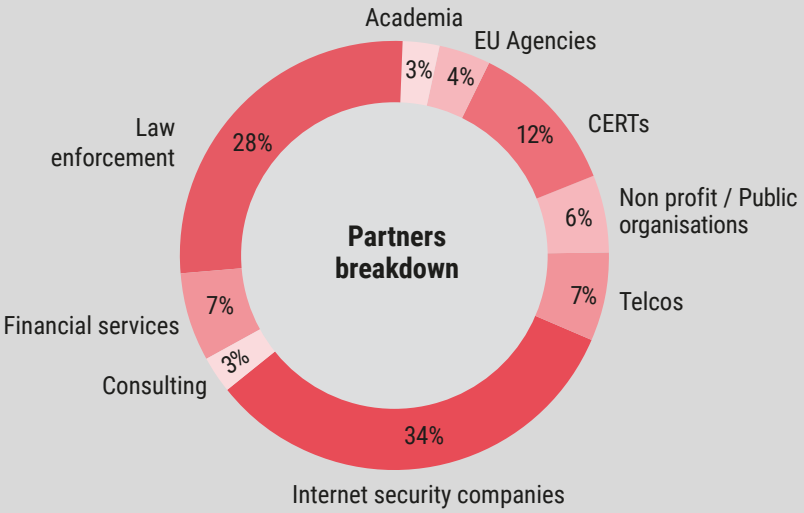
In January 2019, authorities from several US agencies, along with police and prosecutors from Belgium and Ukraine as part of a JIT assisted by Eurojust, seized the xDedic marketplace in an operation supported by the German Federal Criminal Police Office and Europol. Law enforcement seized the servers and domain names of the xDedic marketplace, and the website's criminal activities stopped.

The xDedic marketplace sold access to compromised computers worldwide as well as personal data and operated on both the clear and dark web. Users of xDedic could search for compromised computer credentials by criteria, such as price, geographic location, and operating system. The victims came from all around the globe and a variety of industries, including local, state, and federal government infrastructure, hospitals, emergency services, major metropolitan transit authorities, accounting and law firms, pension funds, and universities. Authorities believe the website facilitated more than EUR 60 million in fraud.

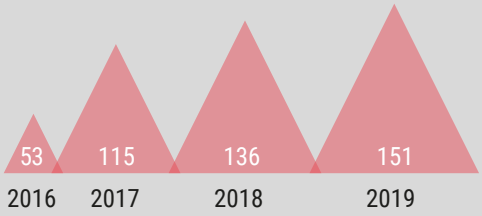
NO MORE RANSOM!

Partners 151

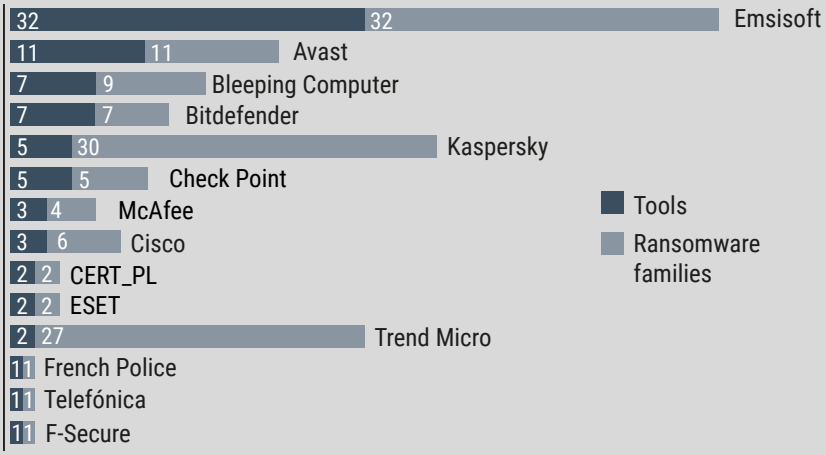




Partners annual growth



Tools 82



109
ransomware families covered

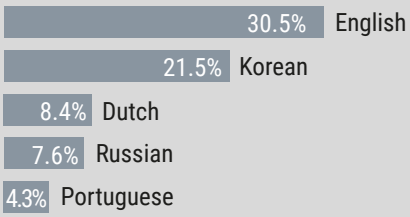
200K
victims helped

$108M
criminal profit prevented

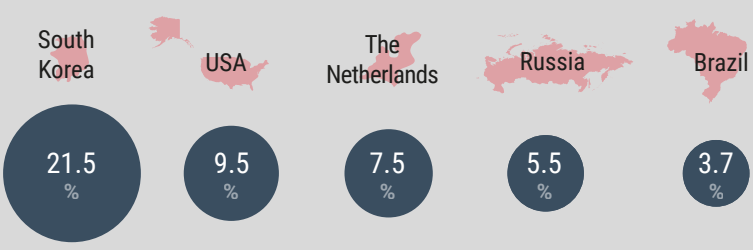
188
countries have accessed the NMR portal

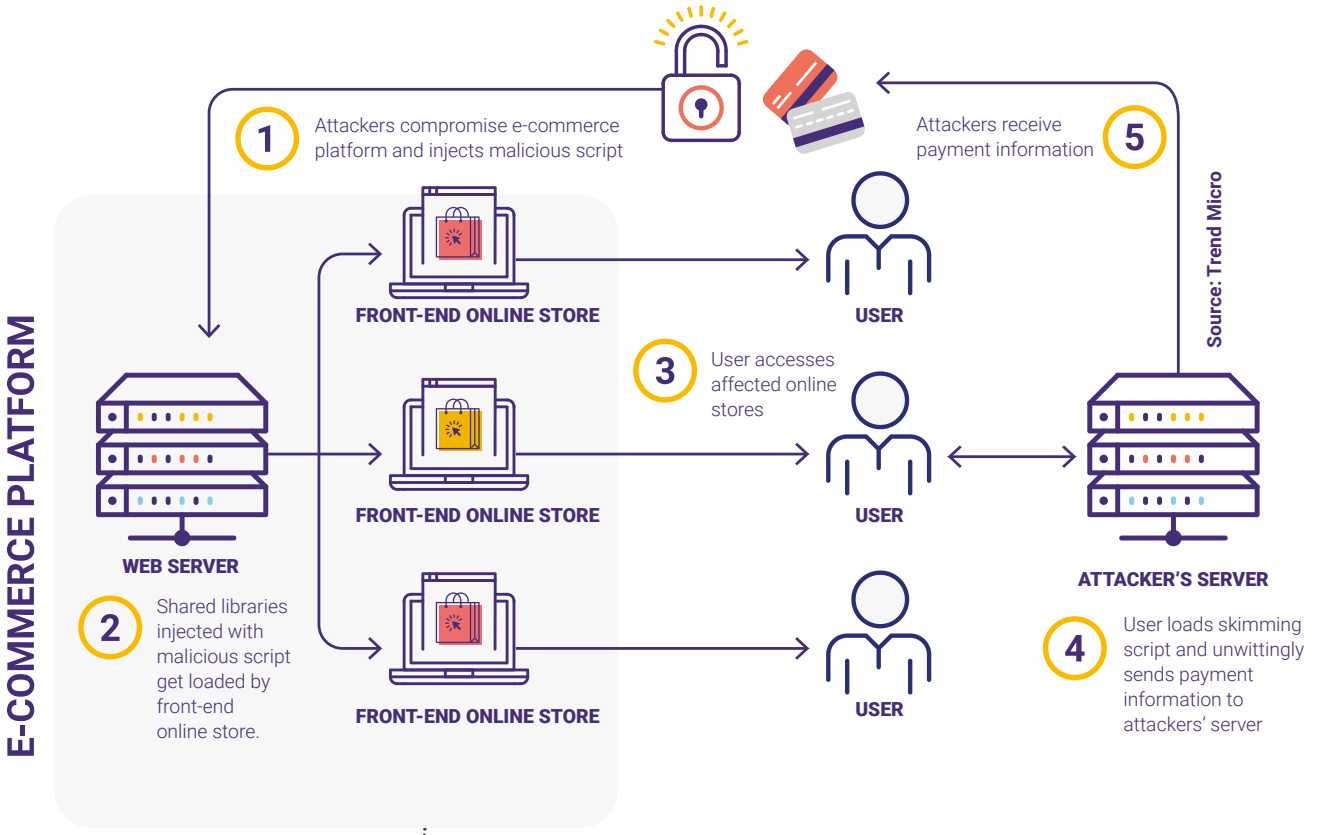
Language & countries

Top 5 languages among 36 available



Top 5 countries of traffic





criminal case study

The Magecart group

The Magecart group, which actually comprises at least six distinct groups operating independently, has been active since approximately 2015. It came to notoriety throughout 2018 when a number of prominent companies suffered massive data breaches. One breach alone resulted in the compromise of over 380 000 credit card details and a fine for the company of over GBP 183 million under GDPR[14].

The groups share a common *modus operandi* — attacking shopping cart platforms or third-party services used by e-commerce websites by injecting code that allows them to skim sensitive customer data; a technique known as formjacking.

The above illustration demonstrates the process of how the crime takes place step by step, from its inception until the attackers receive payment information.

4.3 » DATA COMPROMISE

Compromised data continues to fuel the cybercrime engine

After ransomware, the compromise of data represents the second-most prominent cyber-threat tackled by European cybercrime investigators. This most frequently relates to the illegal acquisition of financial data, such as credit card information, online banking credentials or cryptocurrency wallets, through means such as phishing, data breaches and information gathering malware. Such data is easily monetisable, either through its sale on the digital underground or direct use in fraud. This is also a major source to facilitate CNP fraud (see chapter 6).

Second to financial data, is personal data and other login credentials. While not directly monetisable (other than through its sale), such data is potentially much more valuable, particularly to the more sophisticated cybercrime gangs who may have the capability to best exploit it. Criminals can use the data to facilitate other targeted cyberattacks such as spear phishing, CEO/BEC fraud, account takeover, business process compromise and other frauds, any of which could yield much more significant criminal profits.

Most data breaches yield a variety of data types. One of the largest data breaches of 2018 was hotel giant Marriot International. Over 300 million records were disclosed. These records included data such as names, postal addresses, phone numbers, dates of birth, gender, email addresses, passport numbers and credit card data. Much of the data was encrypted however.

> As hardware and software manufacturing supply chains become ever more extended, the cybersecurity of some extremely important targets will become dependent upon the weakest link in this chain. Due diligence and sound engineering processes must be a part of any Secure Development Life Cycle.
>
> – PROFESSOR ALAN WOODWARD, UNIVERSITY OF SURREY, UK

The growing threat from within

The threat from malicious insider activity is an increasing concern for financial institutions, according to Europol's private sector partners, some of whom rank insider threats as the third-most significant threat actors. The potential impact of such attacks made apparent by a number of attacks publicised in 2019, such as the attacks on US telecoms company AT&T, where insiders allegedly took bribes to unlock more than 2 million devices and planted malware on the company network[15].

The threat from such attacks is amplified where the malicious insider works for a third-party service provider, who may have access to the data of multiple companies and their customers. Such was the case with the Capital One breach, where a former employee of Amazon Web Services is suspected of accessing data belonging to 106 million Capital One customers stored on Amazon's Simple Storage Servers (S3)[16].

GDPR implemented but more time needed to evaluate impact

Closely connected to the crucial threat of data compromise is the implementation of the GDPR. Perhaps one of the most anticipated pieces of legislation of the last few years, one year after entering into effect, many stakeholders demonstrated a welcomed eagerness to take stock of the developments and to gauge the impact of the legislation. In terms of available figures, the International Association of Privacy Professionals (IAPP) appears to have developed one of the most comprehensive overviews of the numbers pertaining to the GDPR one-year anniversary.

Others describe how, despite the passage of a year, we are too early in the process to evaluate the impact of the legislation[17]. Yet, momentum is essential and some write '[i]n the absence of large headlines about closed investigations that result in enormous fines, one of the questions

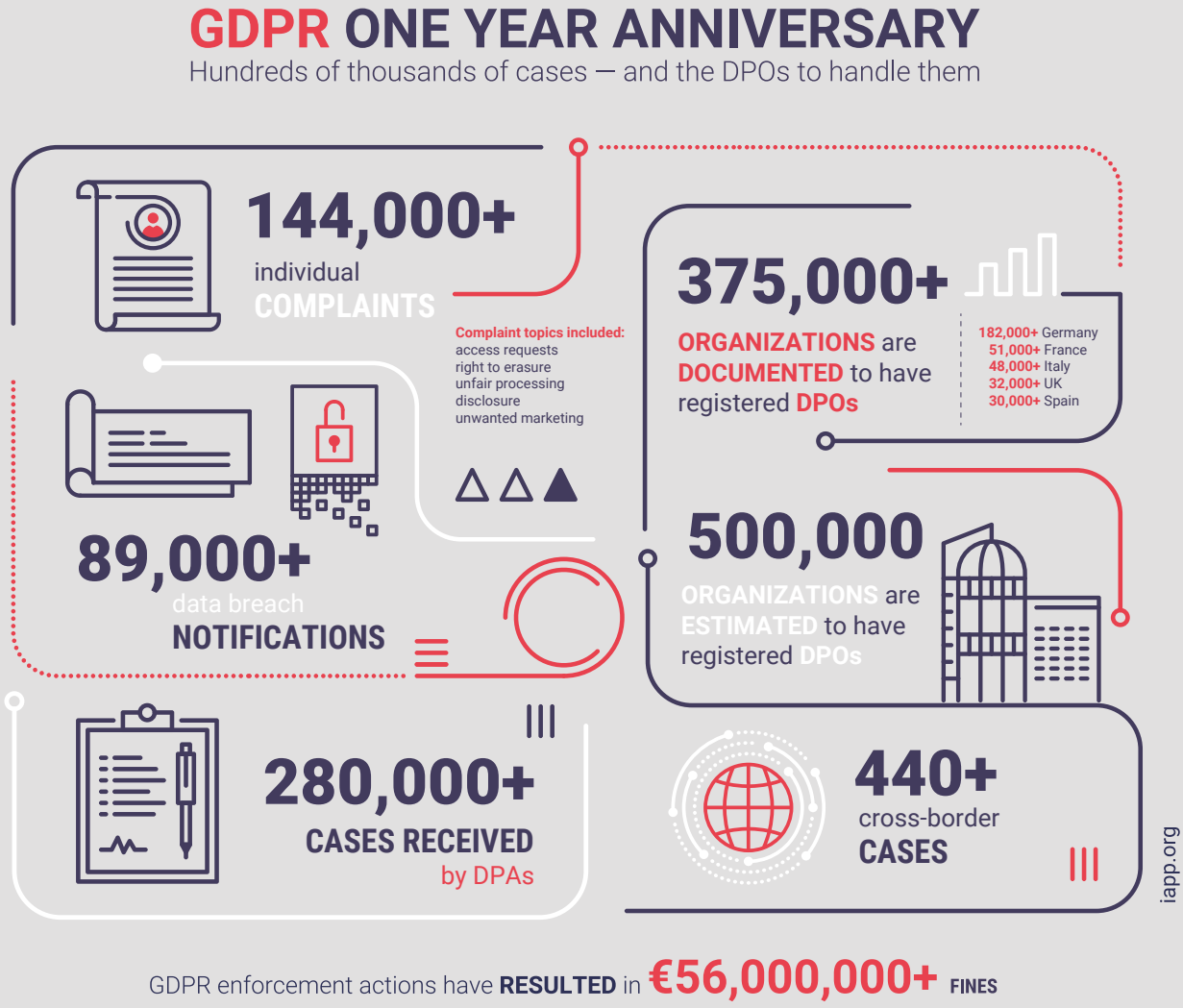
industry insight

Supply Chain Attacks

A clear and growing concern for Europol's private sector partners was attacks directed at them through the supply chain, i.e. the use of compromised third parties as a means to infiltrate their network. Often this will be suppliers of third-party software or hardware, but also other business services. Large companies may have a multitude of third-party suppliers, some with which they have a high degree of connectivity, each bringing its own risk. Such risks are similarly incurred when a larger company acquires a smaller company which may have lower cybersecurity maturity. Such was the case in the Marriot International breach.

Several partners have even indicated that supply chain attacks are considered to be the highest risk to their business. Some industry reporting indicate that supply chain attacks increased by 78 % in 2018[23].

Such attacks are becoming more complex, with compromised fourth or even fifth party suppliers exploited in multi-tier supply chain attacks[24]. Moreover, many companies are becoming increasingly reliant on third-party services such as the cloud.



criminal case study

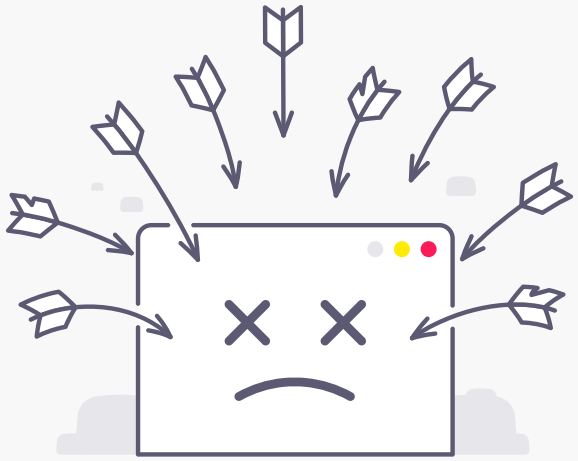
Operation ShadowHammer

In January 2019, Kaspersky Lab discovered that a server for a live software update tool for users of ASUS products had been compromised by attackers and that an estimated 500 000 Windows machines had received a compromised file that effectively acted as a backdoor to the devices for the attackers. The malicious file was signed with legitimate ASUS digital certificates to make it appear to be an authentic software update from the company.

However, the malware was designed to only activate on about 600 unique machines, based on their MAC addresses, indicating that despite the number of affected machines, the attack was extremely targeted[25].

about GDPR now is whether companies will become complacent and downscale their privacy programs[18]. At the time of its one-year anniversary, the largest fine issued — to Google — did not concern a data security breach, rather the French Data Protection Authority issued the fine because of the processing of data by the company.

After the passage of the one-year anniversary mark, however, at least two companies received a 'headline' fine. The United Kingdom's Information Commissioner's Office (ICO) issued its biggest penalties to date when it fined British Airways for GBP 183 million[19] and the Marriott for nearly GBP 100 million[20]. The fines are perceived as a wake-up call to improve means of data security on the side of companies that handle customer data. In this sense, the impact of such an action based on legislation such as GDPR could be significant; especially the public coverage of the development can lead to improved security practices. Previous research with regard to investment in cybersecurity demonstrates the value of incidents in terms of enhancing security practices of companies[21]. The magnitude of the fine combined with increasing public awareness of the impact of data compromise must act as a strong incentive for boards to closely examine their cybersecurity posture. At the same time, high fines could also backfire, as it could bring the potential for GDPR extortion back into the discussion[22].



criminal case study

Memcached amplification attacks[28]

2018 witnessed the two largest DDoS attacks seen to date, using a previously unknown amplification technique. Memcache is an open-source application that can be used to store small chunks of arbitrary data; its purpose to help websites and applications load content faster. Social networks and other content providers commonly use it.

By spoofing the targets IP address, exposed memcached-enabled servers can be used to mount a UDP-based reflection attack, with an amplification factor of over 50 000[29].

Such was the case in February of 2018, when two record breaking DDoS attacks of 1.35 terabytes per second and 1.7 terabytes per second were launched against attack against code depository GitHub, and an unnamed United States-based website respectively. Attacks in 2019, however, trumped these figures. At the start of 2019, Imperva's DDoS Protection Service mitigated a DDoS attack against one of its clients which crossed the 500 million packets per second (mpps) mark. That is more than four times the volume of packets sent at GitHub in 2018. In addition, the company believed at the time, it was the largest PPS attack publicly disclosed[30]. In April 2019, this belief became obsolete, as Imperva recorded an even larger attack against its clients of 580 mpps. These DDoS attacks have serious consequences as they paralyse organisations, including parts of critical infrastructure such as banks, as well as continuously forcing them to increase their mitigation capacity to ensure business continuity.

4.4 » DDoS ATTACKS

While denying a public or private sector entity access to its *own* data may be the primary threat in this year's report, denying others access to that entity's data or services was the third most significant threat highlighted by European cybercrime investigators. Of all the motivations behind such attacks those with an extortion element were overwhelmingly the most prevalent.

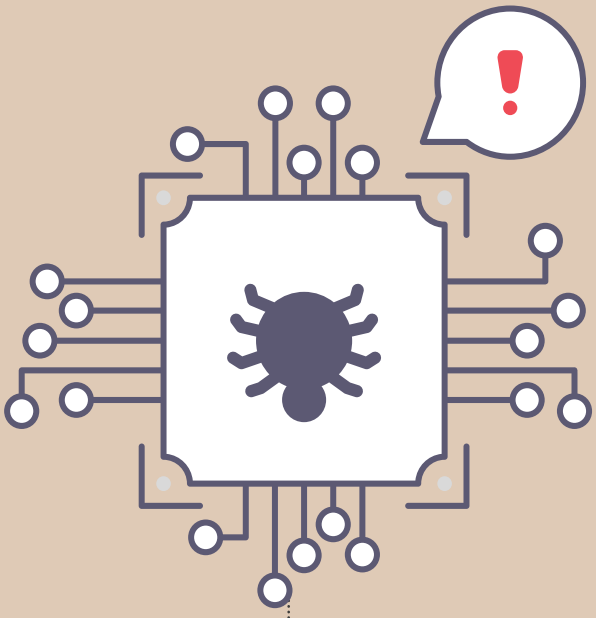
It's all about the money...

As in last year's report, while extortion was the primary motivation behind DDoS attacks reported to European law enforcement, attacks of an ideological/political nature were also common, as were attacks without an apparent motive and which appeared purely malicious.

Where stated, the most commonly identified targets were financial institutions, and public sector entities such as police or local governments. Other targets included the likes of travel agents, internet infrastructure, and services related to online gaming.

No honour among thieves

Interestingly, not only 'legitimate' enterprises are targets for DDoS attacks. Anyone familiar with any Darknet market listing service, such as the now defunct DeepDotWeb, will know that markets are typically listed with an 'uptime', with the primary reasons for downtimes being DDoS attacks. Hidden services are more vulnerable to DDoS attacks due to traits associated with the Tor browser itself. In early 2019



industry insight

DDoS attacks were one of the most prominent threats reported to Europol by its private sector partners, superseded only by phishing and other social engineering attacks, and ransomware.

Despite a noted decline in attacks by several banks following Operation Power Off, many banks report that DDoS attacks remain a significant problem, resulting in the interruption of online bank services, creating more of a public impact rather than direct financial damage.

Such attacks typically originate from low-capability actors, who can still leverage easily accessible DDoS-for-hire services that exploit booters/stressers. While most attacks can be successfully mitigated, emerging DDoS techniques which may be significantly harder to defend against, such as memcached attacks, are a concern for the financial sector.

the three largest Darknet markets were all under intense and prolonged DDoS attacks, with the moderators of Dream Market allegedly being extorted for USD 400 000 (≈ EUR 356 000), showing that anyone vulnerable to such attacks and with the means to pay is fair game to a DDoS extortionist[26].

Operation Power Off has significant and lasting impact on DDoS-as-a-service

Operation Power Off was executed in April 2018, led by the Dutch Police and the UK's National Crime Agency, and supported by Europol and a dozen law enforcement authorities from around the world. The operation resulted in the takedown of webstresser.org — considered at the time to be one of the world's largest marketplaces for hiring DDoS services — with over 150 000 registered users, and the source of 4 million attacks. A year later and the success of the operation still resonates. Moreover, the activity continues as several law enforcement authorities pursue the users of these services, and target other DDoS-for-hire services[27].

4.5 » ATTACKS ON CRITICAL INFRASTRUCTURE

The fourth cyber threat highlighted by European cybercrime investigators was attacks that disrupt or subvert the internal functions of one or more critical infrastructures. Predictably, there is some overlap between these attacks and some of the attack tools earlier in this chapter, i.e. these attacks may have involved DDoS or cryptoware, but these cases focus on attacks where the primary motive was to attack the infrastructure itself.

Law enforcement is increasingly responding to attacks on critical infrastructure

This year law enforcement appears to have become involved in a much wider variety of investigations into attacks on critical infrastructures, including attacks on the energy, transport, water supply, and health sectors. It is not possible to say whether this is due to an increasing number of attacks, or simply the growing involvement of law enforcement in such investigations. Attacks on these infrastructures by financially motivated criminals remain unlikely, as such attacks draw the attention of multiple authorities and as such pose a disproportionate risk. The most likely potential perpetrators include nation states as well as script kiddies. The accessibility of crime as a service allows such attackers to carry out potentially destructive attacks.

criminal case study

In March 2019, Norwegian company Norsk Hydro AS — renewable energy supplier and one of the world's largest aluminium producers — was compromised by the LockerGoga ransomware in a targeted cyber-attack. The attack affected large parts of the business, resulting in production stoppages in Europe and the USA. Projected costs for the company are up to NOK 350 million (≈EUR 35 million).

LockerGoga currently targets multiple industries with targeted attacks[36].

Emergency Response Protocol developed to improve cyber preparedness

The coordinated response to large-scale cyber-attacks remain a key challenge to effective international cooperation in the cybersecurity ecosystem. The development of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises (Blueprint) and especially the EU Law Enforcement Emergency Response Protocol have significantly improved the cyber preparedness by shifting away from incongruent incident-driven and reactive response measures and acting as critical enablers for rapid response capabilities that support cyber resilience. Furthermore, such standardised procedures facilitate the multi-stakeholder coordination and ensure effective de-confliction between the different national competent authorities, international bodies and relevant private partners. Since law enforcement play a crucial role in investigating such cyber-attacks (e.g. electronic evidence collection, technical attribution, prosecution of suspects, etc.), their early involvement in the emergency response to cybersecurity incidents or crises of a suspected malicious nature is essential. Their proactive participation in cyber resilience-related activities such as cyber simulation exercises is also indispensable as such collaboration raises awareness of the roles, responsibilities and capabilities of each actor and increase the level of trust. In terms of next steps, it is crucial for the Blueprint to be operationalised, while ensuring alignment and de-confliction among the different procedures within the EU's crisis response architecture, especially the EU's Hybrid Threats framework[31].

Financial sector increasingly hit by APT-style cybercrime gangs

Another area of concern, highlighted by both European law enforcement and Europol's private sector partners, is attacks directed at internal networks within the financial sector. There are a growing number of cases of complex attacks on banks by sophisticated cyber-crime gangs employing Advanced Persistent Threat (APT)-style tactics to take control over certain aspects of a bank's internal network. Such attacks can manipulate internal fund transfer systems, such as those interfacing with the SWIFT network, in order to make illicit payments, or take control of card processing systems to allow mass cash-outs at ATMs.

Financially motivated criminal APT-style groups such as Cobalt, MoneyTaker, and Silence largely carry out such attacks[32]. In some instances however, nation states are involved, such as in the case of the Lazarus group. This APT group, which has ties to North Korea, was allegedly responsible for over half a billion USD in cryptocurrency thefts since 2017[33], and ongoing attacks against banks in South East Asia[34].

Cryptocurrency exchanges continue to be a magnet for financially motivated hacking groups. In 2018, over USD 1 billion in cryptocurrencies were stolen from exchanges and other platforms worldwide[35].

Such attacks not only result in huge criminal profits, but cause severe reputational damage to the victims and undermine confidence in the financial sector as a whole.

4.6 » WEBSITE DEFACEMENT

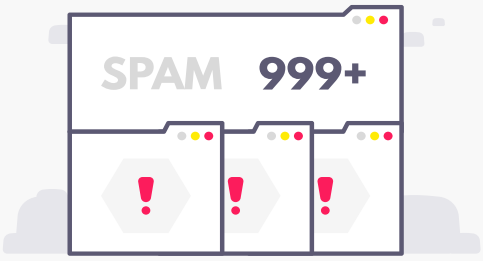
Defacing websites — a gateway to more serious cybercrime

While not a top priority for any individual country, collectively a significant number of European states have highlighted simple website defacement as one of the priorities for their jurisdiction. This implies that such activity, while low impact, is sufficiently common to result in a significant number of cases and commands a corresponding proportion of limited law enforcement resources.

The motive behind such attacks varies, but is typically for political/ideological reasons, or without purpose and purely malicious. The latter likely represents budding cybercriminals testing their capabilities.

The reason this crime area has been highlighted as a key threat is that by investigating these attacks, it provides law enforcement the opportunity to intervene with the perpetrators at an early stage in their cybercrime career. This could be a pivotal moment in preventing them from pursuing a career in cybercrime, which is the foundation of many national cybercrime prevention campaigns.

4.7 » WHAT HAPPENED TO...?



DATA STEALING/MANIPULATING MALWARE

For the second year running, data stealing malware did not feature prominently in law enforcement reporting, with only two Member States stating it as a priority. What industry reporting highlighted, is that criminals use some banking Trojans, particularly those with a modular and therefore variable functionality, such as Emotet and Trickbot, more for their network intrusion and malware delivery capabilities than simply their data-stealing capacity[37]. In some cases, criminals use such malware to install other malware, including ransomware.

Some of Europol's private sector partners report that banking Trojans remain a moderate threat and indeed they were submitted as samples to Europol's EMAS in significant numbers. While losses from banking Trojan activity against customers are at an all-time low, the ability of this malware to affect network hygiene remains a key concern. Banking Trojan veterans Dridex, Trickbot and Gozi still present the most significant banking threats, with some new Trojans such as BackSwap also now coming to the fore. Moreover, some malware families, such as Retefe, had a revival throughout 2018 and 2019, highlighting that while the popularity and prevalence of data gathering malware and banking Trojans may have declined, their development and refinement continues within certain cyber OCGs.

CRYPTOMINING

Last year we highlighted a massive surge in cryptomining; both passive cryptomining through scripts running in a victim's internet browser and more intrusive cryptojacking malware. Both techniques exploit a victim's processing power without their permission to mine cryptocurrencies — typically Monero. The size of this surge varies wildly across industry reporting but the veracity of the trend is almost unanimous. Some reports also attribute the decline in ransomware to attackers shifting to stealthier cryptojacking attacks[38].

Despite this, and despite some submissions of crypto-related malware to Europol's EMAS, we found no representation of this phenomenon in law enforcement reporting from 2018. This is likely due to its comparatively low impact (in most cases) compared to other cyber threats. Apart from the occasional exceptional case, cryptomining is likely to remain a low-priority threat for EU law enforcement.

The closure of Coinhive in March 2019 has led to a decline in the instances of browser-based cryptomining. However, attacks against public and private sectors entities not only continue, but continue to evolve (see also 9.4). There are reports of cryptojacking malware both going 'file-less[39]', and incorporating the Eternal Blue exploit in order to adopt worm-like spreading properties[40].

MOBILE MALWARE

Despite a large number of mobile malware submissions to Europol's EMAS, once again mobile malware featured only marginally in law enforcement reporting for 2018, although there was still an increase in reporting from the previous year. What law enforcement reported, related to data stealing malware, ransomware, and cryptomining malware, and, as in previous years, this largely related to Android phones. Private sector comments — from both Europol's private sector partners, and industry reporting — mirrored this. The latter highlighted parallel trends in mobile malware, such as the expansion of cryptomining malware and a general decline in ransomware[43]. Other mobile threats, such as banking Trojans continue to grow though, capitalising on the increase in m-banking.

4.8 » FUTURE THREATS AND DEVELOPMENTS

The majority of attacks rely on existing *modi operandi* and benefit from known vulnerabilities. Often, existing attacks will spread to previously untapped victims, such as ransomware targeting data centres or backup servers, and existing attack tools will continue to evolve, such as banking Trojans routinely incorporating self-propagating worm functionality.

New threats do not only arise from new technologies but, as is often demonstrated, come from pre-existing vulnerabilities in pre-existing technologies. For example, Memcached was first released in 2003[41] and yet the first DDoS attack exploiting it only occurred 15 years later.

As more and more companies outsource areas of their business, we expect to see a growth in supply chain attacks, and the evolution of such attacks to become increasingly complex. Cloud services pose a particular risk in this regard, as one company is likely to store the data for multiple clients, marking itself as a valuable target for financially motivated criminals and having a major impact if compromised.

While attacks on internal bank systems, which may interface with the SWIFT network, may have been mitigated by banks that have implemented the SWIFT recommended security program, it is not unlikely that sophisticated attackers could identify other upstream applications that generate transfers and similarly exploit those in a comparable fashion.

Various entities within the cryptocurrency ecosystem have presented themselves as profitable targets for competent cybercriminals. As the trend of crimes that traditionally target fiat currencies evolving to targeting cryptocurrencies continues, we will see more financially motivated APT-style cybercrime gangs shift their focus to any entity with large cryptocurrency assets[42] — hacking exchanges and manipulating the Blockchain with 51 % attacks*.

In early, 2019, Internet Corporation for Assigned Names and Numbers (ICANN) issued a warning over an 'ongoing and significant risk to key parts of the Domain Name System (DNS) infrastructure'. The warning relates to attacks with the potential to see data in transit, redirect traffic or allow attackers to 'spoof' specific websites. It is likely that either further existing, ongoing attacks on the DNS infrastructure will come to light, or that a new incident will occur.

* 51 % attacks can hypothetically occur when attackers control 51 % of the blockchain hashing power and can effectively double spend cryptocurrencies by reversing transactions.

> The biggest cybercrime threat of the future may be familiar to us already. The major threats we face today, such as ransomware or business email compromise, have been around for years. While we may see something quite novel, it's more likely that cybercriminals will continue refining attacks that have been shown to work, even relatively unsophisticated frauds that leverage social engineering for great monetary gain.
>
> — DR JONATHAN LUSTHAUS, UNIVERSITY OF OXFORD, UK

4.9 » RECOMMENDATIONS

Successfully tackling major crime-as-a-service providers can have clear and lasting impact. Law enforcement should continue focusing its concerted efforts into tackling such service providers.

Enhanced cooperation and improved data sharing between law enforcement, computer security incident response teams and private partners will be key to tackling complex cyberattacks and will allow the private sector to take the necessary preventative security measures to protect themselves and their customers.

In response to major cross-border cyber-attacks, all cooperation channels should be explored, including the support capabilities of Europol and Eurojust and legal instruments designed for closer cross-border cooperation (such as JITs and spontaneous exchange of information) in order to share resources and coordinate.

Further enhance the collaboration between the network and information security sector and cyber law enforcement authorities by involving the latter in cyber resilience-related activities such as cyber simulation exercises.

Low-level cybercrimes such as website defacement should be seen as an opportunity for law enforcement to intervene in the criminal career path of young, developing cybercriminals.

#5

CRIME PRIORITY

child sexual exploitation online

Online CSE refers to the sexual abuse and exploitation of children via the internet. Whereas the sexual abuse or exploitation very much takes place in the physical world, the subsequent sharing of images and videos depicting this abuse significantly aggravates the impact of this crime. The amount of online CSEM is staggering and continues to increase. As the number of young children accessing the internet grows, and offenders become more aware of anonymisation techniques, law enforcement authorities and industry partners fighting these disturbing crimes continue to face considerable challenges.

5.1 » KEY FINDINGS

- The amount of CSEM detected online by law enforcement and the private sector, continues to increase, putting a considerable strain on law enforcement authorities' resources.
- The online solicitation of children for sexual purposes remains a serious threat, with a largely unchanged *modus operandi*.
- SGEM is more and more common, driven by growing access of minors to high quality smartphones and a lack of awareness about the risks.
- Although commercial CSE remains limited, LDCA is a notable exception to this.

5.2 » ONLINE DISTRIBUTION OF CSEM

The amount of detected online CSEM continues to increase, as is reported by both law enforcement authorities and industry partners[44]. This has a serious impact on victims, who are repeatedly victimised every time such pictures or videos are shared. Out of 19 Member States who responded to this question, 10 have seen an increase in this criminal activity, with the other 9 believing the online distribution of CSEM has remained relatively stable. 5 out of 7 third partners also see an increase in this activity.

Referrals from industry and third country partners have reached record highs, putting a serious strain on the capacity of law enforcement authorities in the EU to investigate these crimes. At least 18 Member States received referrals from the USA through Europol and all Member States received referrals from Canada through Europol. Many of the referrals from the USA come via law enforcement partners from the National Center for Missing and Exploited Children, an NGO that collects reports of online CSEM. Electronic service providers in the USA are obliged to report content or links that involve CSEM.

In 2017, Europol handled 44 000 referrals from the USA for 18 Member States, increasing to 190 000 in 2018. In June 2019, the number of referrals had already reached 170 000. Referrals from Canada have seen a similar trend, increasing from 6 000 for all 28 Member States in 2018 to a current conservative prediction of 24 000 in all of 2019 for the same number of countries. Moreover, there are currently over 46 million unique images or videos relating to CSEM in Europol's repository[45].

The vast majority of online CSEM is detected on image host websites on the open web, with the Netherlands continuing to be the main hosting country[46]. Offenders keep using a number of ways to disguise online CSEM, making it more complicated for law enforcement authorities to detect such images and videos. Although online distribution of CSEM continues to take place via a variety of platforms, peer-to-peer sharing remains among the most popular way among perpetrators to share CSEM. This includes both one-on-one communication and larger groups.

case study

Over the course of two weeks in May 2019, Europol hosted the sixth Victim Identification Taskforce (VIDTF 6), an exercise where experts from Member States gather to analyse CSEM in order to identify victims and perpetrators. The taskforce continues to expand annually, with 34 experts from 24 countries, supported by INTERPOL specialists, and intelligence analysts from Europol staff.

During VIDTF 6, 466 new datasets were uploaded to the International Child Sexual Exploitation database hosted at INTERPOL, and new data was added to more than 280 existing datasets, increasing the chance victims could be identified.

The efforts led to three victims being tentatively identified: one in Europe, one in the USA and one in Russia, with another investigation ongoing to identify another European victim and offender.

However, dedicated bulletin boards on the Darknet are increasingly popular among offenders as a channel for the distribution of CSEM. This is especially the case for offenders with niche interests, including CSEM with infants and non-verbal children and demeaning material depicting torture and severe cruelty against children[47]. More generally, in many cases offenders use encryption and install software to cover their IP address and prevent identification, such as Virtual Private Networks (VPNs) and TOR.

There is an ongoing increase in the distribution of CSEM via social media applications. The self-destruct function of some of these applications make investigations particularly complicated. In some cases, this is the result of self-generated material being shared with peers, after which it is further distributed via social media and eventually ends up on CSEM platforms. There are also instances where fake social media accounts are created in order to spread private pictures and videos of underage victims together with their personal information. Although such accounts are often quickly deleted, it is easy for perpetrators to simply create a new account.

In many cases, offenders distributing CSEM online are also involved in hands-on CSE. The demand for such material perpetuates the ongoing abuse of children. However, there are also many perpetrators who possess and share such material, but are not involved in the actual sexual exploitation of children.

5.3 » ONLINE SOLICITATION OF CHILDREN FOR SEXUAL PURPOSES

The online solicitation of children for sexual purposes remains a serious threat in the EU, with many Member States reporting this crime is on the rise. As more and more minors are active on social media at a younger age, the number of potential victims continues to be high. At the same time, some countries have reported a decrease in cases related to online solicitation since the last IOCTA, possibly as a result of growing public awareness or offenders operating more carefully.

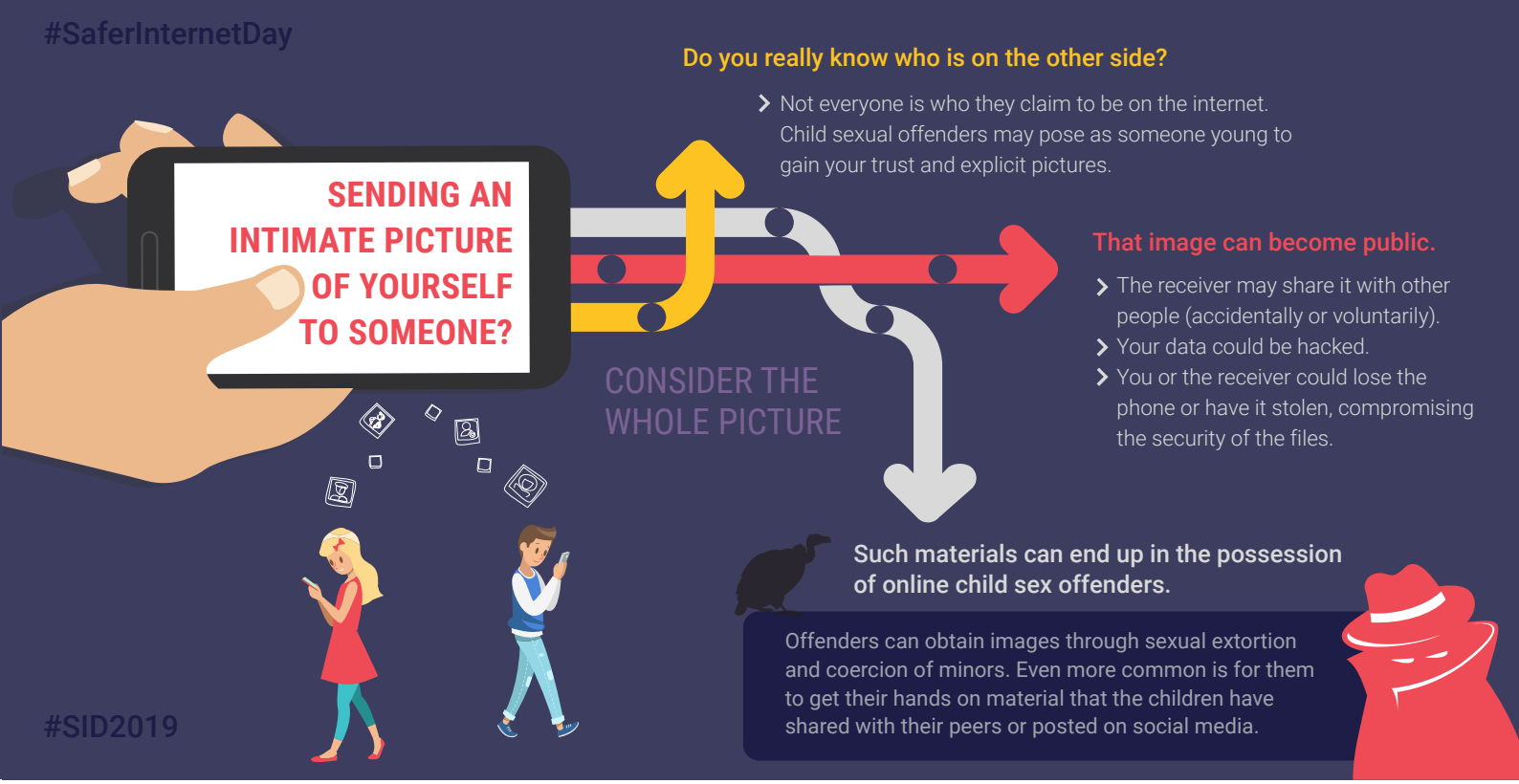
The *modus operandi* for this criminal activity remains largely unchanged. Offenders generally use the open web, as it simply much easier to get in contact with children than on the dark web. They get in touch with potential victims through a variety of social media services, creating fake profiles and frequently pretending to be of the same age. This can happen on many different platforms, ranging from Facebook and Instagram to online gaming environments. Minors are also sometimes approached on live video platforms. Once trust has been established, communication is quickly moved to encrypted online messaging applications, such as WhatsApp or Viber. Whereas explicit material is initially shared voluntarily, offenders subsequently use this material for further coercion and extortion for new CSEM. In some cases, suspects will harass their victims so that they do not file a complaint against them.

Victims are mostly young teenagers, both girls and boys. Some offenders specifically target profiles with many friends, as they believe this means a higher chance of successfully establishing contact.

case study

In March 2019, a German court convicted four men to sentences between 4 and 10 years in prison for running the online CSE platform 'Elysium' on the Darknet. They had set up, administered and moderated what was one of the largest forums of its kind, with more than 11 000 registered users from all over the world. One of the men was also convicted for the sexual abuse of two young children. None of the men involved had known each other in person. The forum had a wide range of different categories of CSEM, including serious violence and very young children.

A man in Sweden was sentenced to 10 years imprisonment for forcing children, all under the age of 15, from primarily North America and the United Kingdom to commit sexual acts in front of a camera or webcam. Despite the fact that he was not physically present at the crime scenes, the court nonetheless convicted him as a hands-on offender on the basis of the concept of 'virtual rape'. It was the first time an online CSE perpetrator had been convicted as a hands-on abuser.



5.4 » PRODUCTION OF SELF-GENERATED EXPLICIT MATERIAL

SGEM has been a growing problem for several years, as more and more young children share explicit material online. Growing access to high quality smartphones and other devices, in combination with relatively low awareness of the risks of producing and sharing SGEM, means this trend is likely to continue.

A distinction can be made between SGEM produced voluntarily and SGEM produced under coercion or extortion by a child sex offender. Regarding the first category, there is a growing number of minors sharing sexual pictures or videos with peers. Children are making themselves vulnerable on a number of levels through this behaviour, including in the context of online solicitation by child sexual offenders. Moreover, in many cases the pictures or videos may be spread further, first between other peers, but eventually ending up in the collections of online child sex offenders. Such cases can subsequently lead to the minors being subjected to sexual coercion and extortion by online child sex offenders for new SGEM or material involving their siblings or other friends.

case study

European Youth Day to raise awareness

On 20 November 2018, Europol introduced a new initiative: The European Youth Day. This was a first event of its kind, which brought together Europol experts and around 100 young students aged between 12 and 15 years old under the topic 'Digital Rights of Youth against Violence'. Following on from the #SayNo initiative, the 2018 European Youth Day at Europol took the discussion one step further, allowing young people themselves to bring their opinions to the table on current cyber threats affecting them, as well as how best to tackle these.

5.5 » SEXUAL COERCION AND EXTORTION OF MINORS FOR NEW CSEM

Although sexual coercion and extortion of minors also happens for financial gain, in the majority of cases the aim is to obtain new CSEM. Offenders mostly use existing explicit pictures or videos of a victim and threaten to share this with the victim's network or on social media, unless they receive more material. These existing pictures or videos can come from two sources: either through online solicitation of minors for CSEM, or because they have found SGEM and have been able to identify and contact the victim. Some offenders will send explicit images and messages to a minor. Even if they do not receive any explicit pictures, they use screenshots of the conversations for coercion purposes. As stated above, such coercion can involve producing material of or with other children within or outside their own family. The impact is significant as sextortion can lead to significant trauma for the victim or in some cases even to suicide. This makes educating children about the risks of sextortion as well as the need to seek help when victimised crucial.

5.6 » LIVE DISTANT CHILD ABUSE

Monetisation of online CSE is generally limited, as offenders are more often driven by a desire to obtain more CSEM than by financial gain. However, in a small number of cases offenders do seem to seek financial gain from online CSE. One method is hosting legitimate 'pay-per-click' advertisements on websites hosting CSEM. Especially when the CSEM is disguised, this increases the platform's click rate and the potential profits per click. There have also been instances of offenders sharing CSEM in exchange for money, but this is far less common than exchanging images for other images. On rare occasions, offenders also use SGEM to coerce victims for money instead of producing new CSEM. However, the most common form of commercial CSE is LDCA.

Because of growing internet speed in many third countries, offenders can watch live streams of CSE taking place on the other side of the world. In many cases, perpetrators pay for watching this kind of CSE. The Philippines remains the most prominent country in terms of location of the victims, although there are indications this is taking place in a larger number of countries. Contact is established in a variety of ways. In some cases, first contact takes place on commercial adult porn websites, after which conversations take place on encrypted messaging platforms. In most cases, the CSE is live streamed on online platforms with the possibility of video conference. Often perpetrators have the chance of orchestrating and directing the abuse in real time. Perpetrators generally pay via online payment methods, but cryptocurrencies are still rarely used. Some of the offenders also travel to third countries to engage in hands-on abuse.

case study

In May 2019, a British man was sentenced to five years in prison for attempting to incite minors under 13 to engage in sexual acts and planning to sexually abuse several minors in the Philippines. The offender was based as a teacher in Malaysia and Thailand at the time of the offences, but was convicted under a section of the British Sex Offences Act that allows British nationals to be prosecuted for offences committed abroad. He was arrested upon arrival in the United Kingdom after investigators found he had made money transfers to online payment accounts of members of a Filipino OCG involved in LDCA.

Evidence showed the offender had also sent money to a Filipino mother of two girls aged 7 and 11 and a boy aged 5, based in Cebu. The money was sent in order for her to buy food for her children, with the offender requesting pictures of her 11-year-old daughter in return. He subsequently also had direct conversations with the girl that were sexual in nature. After he sent more money, the offender expressed an interest in the 7-year-old child and indicated he would like to meet her in order to have sex with her. An arrangement was made to meet in Manilla, although there are no records of the offender actually travelling to the Philippines.

5.7 » FUTURE THREATS AND DEVELOPMENTS

The main threats related to online CSE have remained relatively stable over the last number of years and it is unlikely that there will be any major changes in this crime area in the foreseeable future. However, one development that could be of concern for online CSE is the ongoing improvements of so-called deepfakes. Deepfake technology is an AI-based technique that places images or videos over another video. It has already been used to place the faces of celebrities on existing pornographic videos. Although the technology is still relatively new, it is rapidly improving and becoming more accessible and easy to use. It may be a matter of time before the first deepfakes appear depicting online CSE, resulting in the generation of new 'personalised' CSEM. This can also have serious implications for law enforcement authorities, as it might raise questions about the authenticity of evidence and complicate investigations.

5.8 » RECOMMENDATIONS

Coordinated action with the private sector and the deployment of new technology, including Artificial Intelligence, could help reduce the production and distribution of online CSEM, facilitate investigations and assist with the processing of the massive data volumes associated with CSEM cases.

A structural educational campaign across Europe to deliver a consistent, high-quality message aimed at children about online risks is of the utmost importance to reduce the risks derived from SGEM such as sexual coercion and extortion.

As much CSEM, particularly that arising from LDCA, originates from developing countries, it is essential that EU law enforcement continues to cooperate with and support the investigations of law enforcement in these jurisdictions.

Fighting CSE is a joint effort between law enforcement and the private sector and as a common platform is needed in order to coordinate efforts and prevent a fragmented approach and the duplication of effort.

To prevent child sexual offenders from travelling to third countries to sexually abuse children, EU law enforcement should make use of PNR data accessible through the Travel Intelligence team within Europol.

CRIME PRIORITY

#6 payment fraud

6.1 » KEY FINDINGS

- CNP fraud continues to be the main priority within payment fraud and also continues to be a facilitator for other forms of illegal activity.
- Skimming continues to evolve with criminals continuously adapting to new security measures.
- Jackpotting attacks are becoming more accessible and successful.

6.2 » CARD NOT PRESENT FRAUD

CNP fraud is the main priority for investigators of payment card fraud within Member States. One law enforcement respondent specifically states 'it is the single most common form of fraud'. This follows the pattern from previous years, especially since the number of online transactions and the e-commerce industry continue to evolve. Within CNP fraud, fraud relating to the purchase of physical goods is at the top of the list. Member States mention the purchase of (high-value) electronic devices such as mobile phones, laptops and tablets several times. Another Member State specifically notes how the *modi operandi* in this area of cybercrime have not seen any major innovation during the last year. While there has been no major shift in 2018, according to private sector input, CNP is increasingly moving into other sectors such as travel (hotels, car rentals, etc.) postal services, giftcards, etc. Fewer cases have been reported to law enforcement since there is not yet the same level of awareness as in, for instance, e-commerce.

The data required to execute CNP fraud generally seems to originate from data compromise, including third-party breaches, phishing emails and scam text messages (see section 4.3). Magecart attacks, for example, briefly described in chapter 4, have hit nearly 17 000 e-commerce websites since April 2019. The criminals are able to exploit vulnerabilities that occur when website owners inadvertently misconfigure their Amazon Web Server (AWS) S3 storage servers. According to Farinelli, '[t]hese servers act as cloud-based "buckets" that store important data — including credit card numbers that are collected by e-commerce websites. AWS S3 servers are secure when their standard settings are used; however, many companies customize these settings. If the customisation is misconfigured, a security gap can occur[48].' This misconfiguration provides anyone with an AWS account with the opportunity to not only read the content of the 'bucket' but also develop new code — such as code to collect card data from an e-commerce site.

More interestingly, Magecart attacks now target smaller vendors that supply functionality services to large enterprise websites including analytics, browser display requirements, social media,

case study

In May 2018, a regional unit in a Member State uncovered the criminal activities of an organised group from Côte d'Ivoire and Morocco specialising in the theft of credit card numbers for the purpose of distance selling fraud. The *modus operandi* set up by the scammers consisted of obtaining credit card numbers (by phishing victims or following purchases on the Darknet) as well as connection identifiers to victims' internet boxes in order to schedule a call forwarding to the scammers. As a result, calls from banks to confirm purchases were forwarded directly to the criminals. Law enforcement recovered technological products purchased fraudulently. Intangible products (Western Union mandates and TransCash cards) were recovered in Morocco.

marketing and chatbots. This means that when the code from one of these vendors is compromised, the compromise affects all of the websites that contract with the vendor[49]. This also connects to the increasing threat and growing concern with respect to supply chain attacks (see Industry insight in section 4.3).

The European Central Bank (ECB) also recognises the 'ongoing shift of fraud from the card-present to the card not present environment'. Data seems readily available. 23 million stolen credit cards are for sale on the dark web in the first half of 2019[50]. With all the data available and accessible for criminals, the focus ought to be on monitoring and detection of accounts as a means to curb the number of frauds and the amount of damage. From that perspective, the ECB notes how 'the market has started to develop a plethora of fraud prevention and detection security tools with the objective of bringing online fraud rates down (e.g. implementation of 3D Secure, risk-based analysis, Tokenization)[51]'.

More detailed data to circumvent detection

Simultaneously, criminals expand on their existing repertoire of methods as the prevention and security measures of companies improve. One relatively new development, for example, is a crime-as-a-service facility where criminals provide a platform with available bots that contain a victim's real digital fingerprint, cookies, saved passwords and other personal information including bank and payment information. These fingerprints contain all the necessary information to enhance the possibility of avoiding detection mechanisms of companies, namely e-commerce. Criminals obtain the fingerprints as real-time fingerprints or generated when scratched by the bot from the user's device.

The platform provides a simple user-friendly interface which allows other criminals to set up a different digital identity. This way it is much easier for criminals to commit fraud compared to purchasing compromised credit card details or account details and risk the detection of security measures.

CNP fraud used to facilitate other forms of crime

Whereas we often discuss CNP fraud purely from a financial perspective, this type of crime also facilitates other types of illegal activity. Examples include the facilitation of illegal immigration and more specifically Trafficking in Human Beings (THB). Criminals do this through the purchase of plane tickets with compromised credit card credentials, booking hotels, rentals, etc. They do this through CNP fraud in combination with forged identification documents.

One of our cases illustrates how CNP fraud can underpin and facilitate other forms of illegal activity. In September 2018, with the support of Europol and Frontex, two suspects were arrested in a series of coordinated raids across Germany and Sweden in an investigation targeting a Syrian OCG suspected of cyber fraud. The arrestees are believed to be the key organisers of a cyber fraud gang.

6.3 » SKIMMING

The German Federal Criminal Police Office initiated operation Goldring in October 2017. The intelligence-led operation uncovered an OCG, composed of Syrian nationals, which was involved in fraudulently purchasing airline and train tickets. According to information from Germany, more than 493 fraudulent bookings were identified. The tech-savvy smugglers avoided detection by making the bookings using compromised corporate credit cards and credentials, purchased online from other criminals offering them for sale.

The private sector brought the fraudulent transactions to the attention of law enforcement, highlighting once again how instrumental public-private partnerships are in fighting this type of fraud. This effective working relationship has been established over the course of recent years as a result of Europol's Global Airport Action Day, a recurrent operation bringing together law enforcement, the airline industry and payment card companies to target airline fraud. As part of this operation, Europol and Frontex have jointly identified significant crossovers between payment card fraud and irregular migration and THB, leading to a number of arrests in recent years. The operational successes have confirmed this trend.

Skimming surfaced as the second priority as reported by investigators of payment card fraud within the Member States throughout 2018. As one Member State describes, 'the phenomena of credit card fraud continue to evolve with increasingly sophisticated skimming or shimming tools, often deployed by criminal groups from Central Europe or the Balkans, in real raids targeting the whole continent'. Industry also confirms the lingering threat of skimming. In general, the European Payment Council (EPC) echoes law enforcement reporting when it states how skimming remains one of the most common frauds[52]. The ongoing threat of skimming is the direct result of the fact that not all payment terminals and ATMs in Europe contain the necessary anti-skimming measures. This makes the copying of magnetic-stripe track data at Point of Sales terminals and ATMs possible and still a predominant type of fraud in Europe. Subsequent usage of a cloned magnetic-stripe payment card is hardly possible in the European area since the industry has secured cards with Europay, MasterCard and Visa (EMV) chip technology. On a global level, the situation is different especially with concern to countries that have yet to introduce EMV compliance. As a result, this remains a major concern for European card issuers.

Law enforcement provides the same perspective on the matter. As one respondent writes: 'The European card data collected is then resold, both on the Darknet and via traditional websites. Several cases by the judicial police have shown that this fraudulently acquired data is being reused in bank withdrawals, mainly in America and South-East Asia'. Other Member States echo this conclusion. As long as EMV compliance in those parts of the world remains absent, skimming cards and subsequently using the data remains profitable. The EPC confirms this when it writes: 'Concerning card payment fraud, as long as the mag-stripe is needed for international transactions, skimming will remain an issue[53]'.

Deep insert skimmers frequently used by criminals

With respect to the *modus operandi,* several Member States describe how suspects use deep insert skimmers in order to copy the data stored on the magnetic stripe. This type of skimmer is composed of metal or plastic. The criminal also installs a camera on the ATM in order to steal the PIN. Other Member States specifically report on investigations pertaining to criminals who actually prepare and distribute the devices for skimming. Different OCGs then use these devices to skim ATMs both in and outside the EU. Software skimming malware intercepts card and PIN data at the ATM, allowing the criminal to copy the data and later create counterfeit cards for use at non-EMV compliant ATMs. Alternatively, criminals send the skimmed data with the pin codes to other offenders to facilitate the unauthorised withdrawals from ATMs outside the EU.

6.4 » JACKPOTTING

Nowadays, jackpotting — also referred to as black-box attacks — to cash-out the ATM is the most widespread type of logical ATM attack. Criminals perform jackpotting in one of two ways. Either the criminal uses malware which sends commands to the dispenser, or uses their own 'black box' hardware device connected directly to the dispenser, to cash-out the ATM and empty it of cash. These attacks can only be performed against certain 'old' ATMs which, due to lower security standards, are vulnerable for these type of attacks.

Jackpotting attacks appear to be evolving

Compared to last year, jackpotting attacks appear to be evolving. Several Member States describe how perpetrators have committed these attacks or at least attempted to do so. This may also be due to the necessary equipment becoming more available and accessible. *WinPot* and *Cutlet Maker* are both available on the dark web[54]. This seems to be an unusual development, as ATM hackers have generally kept their work more protected[55]. According to one law enforcement respondent, 'attacks on ATMs using the "jackpotting" technique have diversified and intensified'. The same Member State describes how in 2018, its law enforcement unit recorded 39 cases, including 27 attempts, mainly in the capital region. The financial losses from such attacks can vary between EUR 2 200 and EUR 128 800 depending on the point of attack. Based on law enforcement intelligence, the authors of the malware appear to come from Romania, Moldova and Russia. The majority of reported jackpotting attacks have involved some physical access to the ATM. This is the main obstacle for criminals, since physical access increases the risk of being caught.

According to one Member State, the *modus operandi* of piercing the front of an ATM in order to connect a computer seems to have disappeared. Criminals appear to have started using different methods. The first method consists of disconnecting the front of the ATM from its base in order to allow direct access to the connections. The second method requires simply removing the screen from the ATM and a few technical operations in order to access also the connections of the server managing the cash registers. One Member State reported three cases of black box attacks in 2018, where the attacks involved melting a hole above the monitor of the ATM and plugging a USB cable into the ATMs printer cable. Other Member States confirm this *modus operandi.* Once criminals have gained physical access, they use, for example, the *Cutlet Maker* software. More recent cases involved criminals breaking the deposit slot plastic, opening the monitor and connecting the ATM USB cable. Subsequent withdrawal of cash occurred through usage of the software *ATMdesk*.

Some law enforcement respondents do indicate how in certain cases perpetrators get to the ATM without any damage, using the original key to install a laptop that connects to the USB output. The laptop is also connected to the internet via hotspot from a prepaid phone. The laptop is removed after withdrawing money. Overall, the time of the ATM attack is about 10 minutes.

6.5 » BUSINESS EMAIL COMPROMISE

One of the most economically damaging attacks is business email compromise (BEC). Several industry partners highlight that perpetrators aim more and more attacks at upper (C-level) level management, and that such attacks are becoming more professional and convincing. Such attacks were also a top priority for European law enforcement. According to the Internet Crime Complaint Centre, between December 2016 and May 2018, there was a 136 % increase in identified global exposed losses, and more than USD 12 billion in losses since October 2013[56].

While BEC is not a new phenomenon, criminals are finding new *modi operandi* to take advantage of this technique. The main or original techniques used by criminals are the use of social engineering strategies to impersonate a company staff member, usually a CEO or other staff member who can authorise transfers, and deceive employees and executives within the company. The target companies are usually firms with frequent wire transfers or with foreign suppliers. However, the attacks take place through different methods: the compromise of legitimate email accounts, social engineering or intrusion techniques.

BEC exploits the way corporations do business, taking advantage of segregated corporate structures, and internal gaps in payment verification processes. Such attacks vary by the degree of technical tools used. Some attacks can only successfully employ social engineering, while others deploy technical measures such as malware and network intrusion. This variety in *modi operandi* also requires a variety in response. At the low-tech end, where social engineering reigns, awareness and training for staff are key. BEC was part of the broader cyber scams campaign organised by EC3 as part of the cybersecurity month in 2018. Yet, even though creating awareness among employees can assist in detection of social engineering attacks as a means for criminals to engage in BEC, more high-tech methods such as malware and network intrusion require a different type of response. Those enterprises without the resources to enact such measures, such as many server message blocks, remain particularly at risk.

6.6 » FUTURE THREATS AND DEVELOPMENTS

The landscape of payment fraud demonstrates the resilience of certain criminal *modi operandi*. As a result, for payment fraud, the past and present are important indicators for what we can anticipate in the future. As long as CNP fraud as well as skimming remain profitable, criminals shall carry out such *modi operandi.* For CNP fraud the added problem is the role it plays in facilitating other forms of criminal activity.

With regard to jackpotting, some evolution is evident. The accessibility and availability of jackpotting-related malware may make jackpotting a more accessible crime. Authors of the malware also look for ways to reduce obstacles, better target their efforts in order to steal more money in a lesser amount of time[57]. Simultaneously, even if unsuccessful, jackpotting tries are still a problem as they cause considerable damage to the infrastructure. This makes it a particularly complex problem to tackle.

In the previous IOCTA, we reflected on the potential for instant payments to complicate fraud prevention and especially mitigation. Since 2017, a number of instant payment schemes have been launched; most recently, the ECB launched the TARGET instant payment settlement service in November 2018. Such schemes allow the settling of electronic payments between European banks (almost) instantly. While these provide clear benefits to the financial sector and commerce, they can also inadvertently expedite various frauds. Such transactions not only provide money launderers with better option for money mule accounts, but also make it harder for the financial sector to block suspect transactions.

CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

CEO/BEC fraud occurs when an employee authorised to make payments is tricked into paying a fake invoice or making an unauthorised transfer out of the business account.

HOW DOES IT WORK?

A fraudster calls or emails posing as a high ranking figure within the company (e.g. CEO or CFO).

They have good knowledge about the organisation.

They require an urgent payment.

They use language such as: 'Confidentiality', 'The company trusts you', 'I am currently unavailable'.

They refer to a sensitive situation (e.g tax control, merger, acquisition).

The employee is requested not to follow the regular authorisation procedures.

Instructions on how to proceed may be given later, by a third person or via email.

The employee transfers funds to an account controlled by the fraudster.

Often, the request is for international payments to banks outside Europe.

WHAT ARE THE SIGNS?

- Unsolicited email/phone call
- Direct contact from a senior official you are normally not in contact with
- Request for absolute confidentiality
- Pressure and a sense of urgency
- Unusual request in contradiction with internal procedures
- Threats or unusual flattery/promises of reward

WHAT CAN YOU DO?

AS A COMPANY

Be aware of the risks and ensure that **employees are informed and aware too**.

Encourage your staff to **approach payment requests with caution**.

Implement internal protocols concerning payments.

Implement a procedure to verify the legitimacy of payment requests received by email.

Establish **reporting routines** for managing fraud.

Review information posted on your company website, **restrict information and show caution** with regard to social media.

Upgrade and update technical security.

Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

AS AN EMPLOYEE

Strictly apply the security procedures in place for payments and procurement. **Do not skip any steps and do not give in to pressure**.

Always **carefully check email addresses** when dealing with sensitive information/money transfers.

In case of doubt on a transfer order, **consult a competent colleague**.

Never open suspicious links or attachments received by email. Be particularly careful when checking your private email on the company's computers.

Restrict information and show caution with regard to social media.

Avoid sharing information on the company's hierarchy, security or procedures.

If you receive a suspicious email or call, always inform your IT department.

Alongside instant payments, developments with respect to the Directive (EU) 2015/2366 of the European Parliament and of the Council[58] (known as the Payment Services Directive 2, PSD 2) are also ongoing. The implementation deadline of the Directive has passed however on 14 September 2019, financial service providers (from banks to Fintechs) must adhere to certain security requirements with respect to strong customer authentication. The European Banking Authority (EBA) has indicated that if needed providers can receive an extension. The EBA has a crucial role in the establishment of the security standards with respect to PSD 2. As the EBA notes in its opinion, '[o]ne of the fundamental changes introduced by PSD 2 is to formalise payment security requirements in national law. One such requirement is for PSPs to apply SCA to electronic transactions[59]'. In principle, if implemented, the SCA should enhance security; yet, the ability to file for an extension could in theory make certain providers more vulnerable to attacks in case criminals discover SCA is not yet in place by the deadline.

Other developments around the same date are relevant for the criminal landscape. As we reported last year, one of the central issues arising out of open banking revolves around the concept of screen scraping. Screen scraping allows third-party providers to access customers' interfaces and collect relevant data to gain access to a bank account. While aimed at improving consumer experience, screen scraping is susceptible to man-in-the-middle attacks and other forms of fraud. Given the number of security-related concerns, the European Commission has decided to ban screen scraping from September 2019 as part of the regulatory technical standards of PSD 2. If this goes through, it would be a positive development as it eliminates a criminal opportunity. Despite this, the overall open banking development remains one to monitor from a threat perspective and makes proper and timely implementation of SCA all the more important to manage fraud. As Fortuna notes, '[w]ith Open Banking, data will increasingly be passing through a client (a customer) to an open interface, becoming extremely vulnerable to attacks as there is no way to control the customer's device, whether that be a mobile phone or a web browser. By facilitating access to customer data, third-party providers also become targets for client-side attacks[60]'.

On a final note, the current legislative situation with respect to non-cash means of payment fraud is unsatisfactory to both private industry and law enforcement. However, Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment[61] (known as the non-cash-payment fraud (NCPF) Directive) — which Member States have two years to implement — will help in ensuring that a clear, robust, and technology-neutral legal framework is in place. It will help eliminate existing challenges to investigation and prosecution of fraud and is expected to make a very positive impact in the fight against NCPF. A particular focus of the NCPF Directive is on improving cooperation on cross-border fraud cases. Such cooperation requires a fertile environment which facilitates parties to engage in information exchange. Most often, criminals attack the financial sector as a whole rather than a specific institution. As such, information exchange of new *modi operandi* or ongoing criminal campaigns require information exchange between private parties as well as between public and private parties.

6.7 » RECOMMENDATIONS

Cooperation between the public and the private sector as well as within the sectors is crucial to come to fruitful results. To this point, speedy and more direct access to and exchange of information from the private sector is essential for Europol as well as its partners.

Organisations must ensure they train their employees as well as make their customers aware of how they can detect social engineering and other scams.

#7 the criminal abuse of the dark web

7.1 » KEY FINDINGS

- The dark web remains the key online enabler for trade in an extensive range of criminal products and services and a priority threat for law enforcement.
- Recent coordinated law enforcement activities, combined with extensive DDoS attacks, have generated distrust in the Tor environment. While there is evidence administrators are now exploring alternatives, it seems the user-friendliness, existing market variety and customer-base on Tor, makes a full migration to new platforms unlikely just yet.
- There are increases in single-vendor shops and smaller fragmented markets on Tor, including those catering for specific languages. Some OCGs are also fragmenting their business over a range of online monikers and marketplaces, therefore presenting further challenges for law enforcement.
- Encrypted communication applications enhance single-vendor trade on the dark web, helping direct users to services and enabling closed communications. Although there is no evidence of a full business migration, there is a risk the group functions could become increasingly used to support illicit trade.

Often used interchangeably are the terms Darknet and dark web. For the purpose of this report, the Darknet is the encrypted part of the internet accessed using specific software that in themselves are not criminal, such as the Tor browser. The dark web is the many criminal websites and services hosted on these networks.

Investigator feedback across all the crime areas in this report highlighted the dark web as a priority threat area. These reports related almost exclusively to the sale of criminal products and services, including drugs, weapons and explosives, compromised data and credit cards, malware, counterfeit goods and currency and fake documents. This highlights the extent to which this threat facilitates a range of criminality[62].

Highlighted each year is the volatility of the dark web ecosystem. This continues to be the case, intensified by effective coordinated law enforcement activity in early 2019. Authorities undertook global action against vendors in February, and Dream Market, arguably the largest market at that time, shut down voluntarily, after this. This was supposedly in response to a prolonged and persistent DDoS attack as discussed earlier in section 4.4. Soon after law enforcement announced the shutdown of two of the remaining top dark web markets, Wall Street Market and Valhalla, followed by Bestmixer, the mixing and tumbling service hosted in part on the dark web (see section 9.7). Lastly, law enforcement shut down the online dark web information resource DeepDotWeb after its administrators received millions of euros in kickbacks for referrals to dark web marketplaces selling fentanyl, heroin and other illegal goods.

The coordinated law enforcement efforts, together with continued DDoS attacks, have had a significant impact on the dark web in terms of generating distrust and, at the time of writing, the environment remains in a state of flux. The emergence of new multi-vendor top markets is apparent, however, as are increased exit scams, including some of those initially appearing to dominate. The apparent re-emergence of the Dream Market, which claims to have re-opened in July 2019 as Samsara Market has also taken place.

Evolution of online trade continues

Dark web reports almost exclusively refer to use of the Tor platform, although there is evidence of criminality on most similar privacy-orientated software i.e., Tor, I2P, Zeronet, Freenet, Openbazaar, etc. In previous reports, the suggestion was the succession of law enforcement takedowns and other security issues would push the dark web sites and services to these other platforms. The Libertas Market did briefly switch to solely operating on I2P following the recent law enforcement activities, only to cease operating shortly after due to a low customer base. There are no other examples of this type of move, therefore, while the risk of alternatives remains, it seems the user-friendliness, existing market variety and customer-base on Tor, makes a full migration from customers or markets to new platforms unlikely just yet.

case study

In May 2019, two prolific dark web marketplaces, the Wall Street Market and Valhalla (also known as Silkkitie), were taken down in simultaneous global operations by EU law enforcement.

After the takedown of the three largest markets in 2017, Wall Street was one of the largest remaining illegal online markets. At the time of its closure, it had over 1 150 000 users and 5 400 vendors. The German Federal Criminal Police Office, supported by the Dutch National Police, Europol, Eurojust, and a number of US government agencies, arrested three suspects in Germany. Police officers seized over EUR 550 000 in cash, as well as cryptocurrencies Bitcoin and Monero in six-digit amounts. Two of the markets highest-selling suppliers of narcotics were also arrested in the USA.

Finnish Customs seized the Valhalla marketplace server and its contents in close cooperation with the French National Police and Europol. As a result of the operation Finnish Customs also made a significant Bitcoin seizure. Valhalla was one of the oldest and internationally best-known Tor trade sites.

case study

In mid-2018, German authorities identified a Darknet market vendor selling various narcotic drugs, counterfeit currency and counterfeiting equipment. The vendor had been active for over two years on multiple marketplaces and was suspected to be living in Germany.

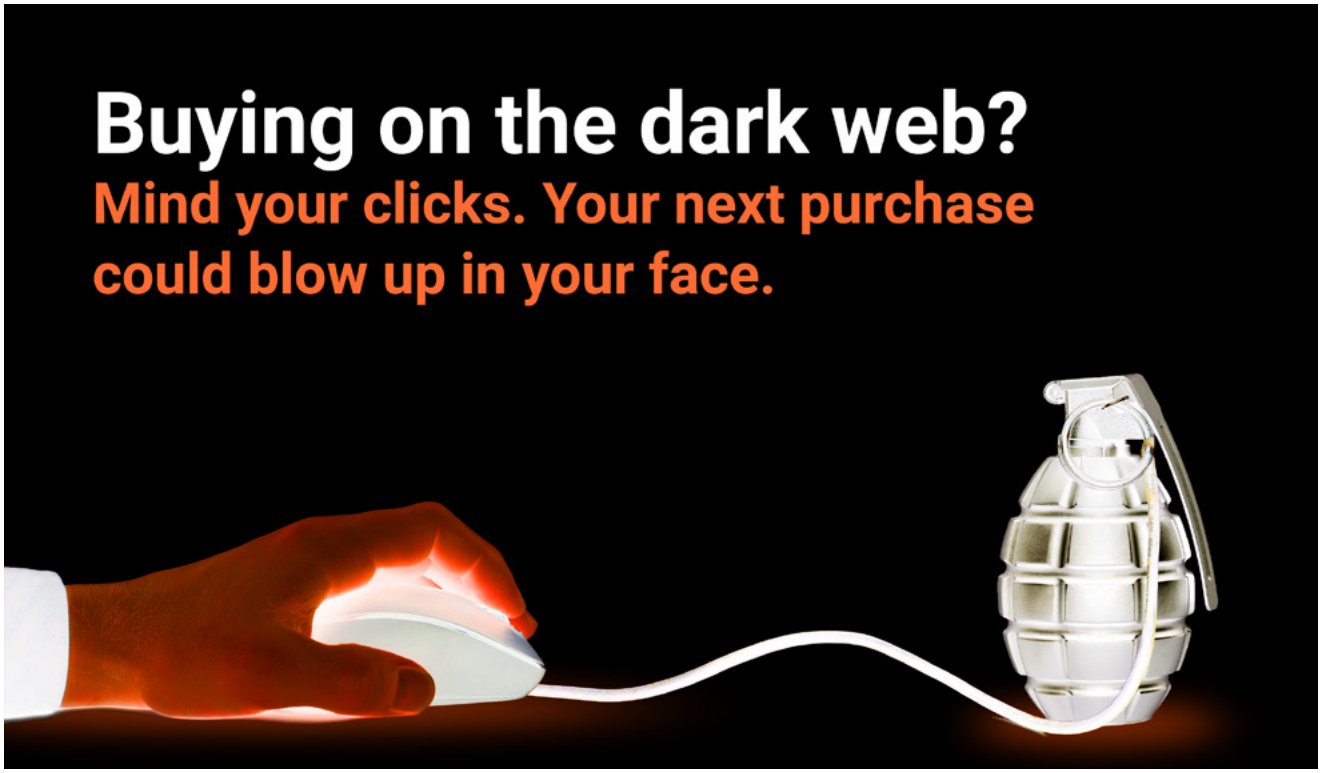
Officers trained in cryptocurrency investigation were able to identify the vendor as a 35-year-old German national and affect an arrest. The suspect had made over EUR 700 000 over the two years he was active.

However, for this market growth has been slow due to continued suspicion over law enforcement involvement. Finally, some markets have changed their policies to prohibit the sale of fentanyl and weapons and explosives in an attempt to avoid law enforcement attention, albeit the sale of these commodities continues under different guises and on other sites.

Instead, criminals are exploring alternative means of circumventing law enforcement within the Tor environment. In last year's report, the suggestion was the closure of larger marketplaces would result in a growth in the number of single-vendor shops and smaller fragmented markets. This forecast is indeed true with confirmed increases in single-vendor shops operating on independent .onion sites and smaller markets, including those catering for specific languages. However, not anticipated last year was the emergence of multi-identity business models, where OCGs maintain multiple profiles online, on multiple platforms, in order to operate as multiple distinct individuals rather than a single entity. By fragmenting their business over a range of online monikers on marketplaces and disparate vendor shops, it reduces the perception of the scale of the OCG, and keeps them under the radar of law enforcement, compared to the attention they might receive operating as a single multi-commodity vendor with a higher customer base. This creates further challenges for law enforcement, as in addition to the usual attribution issues associated with dark web investigations, investigators must also make these connections on order to determine the true scope and scale of an OCG.

In addition to circumventing law enforcement, criminal developers are also motivated by the need to increase trust with their customer-base on Tor, both in terms of anonymity but also by reducing the risk of exit scams. An example of such a market is Black Dog, scheduled for launch in August 2019. It claims to be the 'first ever truly decentralised crypto market' and depends on the Ethereum blockchain to facilitate transactions, without the need for a traditional marketplace GUI as found on Tor markets. The market also utilises the smart contracts component of the Ethereum blockchain to allow credible transactions without the need for a third party. As with alternative platforms, it is unclear how, and to what extent, cybercriminals will adopted this type of market model, again taking into account the effects of AMLD 5.

Separate to Darknet platforms, predicted last year was that some vendors might migrate their business to encrypted communications applications, running their shops within private channels/groups and even the encrypted messaging platforms evolving into functional marketplaces. Although there does appear to be an increased use of encrypted communications applications to enhance the single-vendor trade on the dark web, helping direct users to services and enabling closed communications, there does not appear to be a full business migration. There have been some instances where group functions have supported functional marketplaces with perpetrators selling different criminal commodities, much like the different sub-forums on a typical online forum. However, these markets, although simple to set up (as the platform provides the infrastructure) and easy to revive if taken down, offer little in the way of security for their customers, i.e. there is no escrow or similar services. They can also be less technically challenging than a Tor-based site to take down, as they sometimes only require an abuse notification sent to the provider, who, if they respond to such requests (not always the case), can ban or delete the group. It is therefore unclear how and to what extent cybercriminals may adopt this market approach, and much of which depends on law enforcement relationships with industry partners in this sector and the ability to locate and effectively take them offline once identified.



The currency of the dark web enterprises remains virtual and an estimated USD 1 billion has been spent on the dark web this year alone[63]. Bitcoin remains the most frequently used currency, believed to be a consequence of familiarity within the customer base (see also section 9.4). However, there has been a more pronounced shift towards more privacy-orientated currencies, a trend that it is anticipated will continue as criminal users become more security aware.

7.2 » RECOMMENDATIONS

More coordinated investigation and prevention actions targeting the dark web as a whole are required, demonstrating the ability of law enforcement and deterring those who are using it for illicit activity. An improved real-time information position must be maintained to enable law enforcement efforts to tackle the dark web. The capability will enable the identification, categorisation and analysis through advanced techniques including machine learning and artificial intelligence.

An EU-wide framework is required to enable judicial authorities to take the first steps to attribute a case to a country where no initial link is apparent due to anonymity issues, thereby preventing any country from assuming jurisdiction initiating an investigation.

Improved coordination and standardisation of undercover online investigations are required to de-conflict dark web investigations and address the disparity in capabilities across the EU.

#8 the convergence of cyber and terrorism

8.1 » KEY FINDINGS

- The wide array of OSPs exploited by terrorist groups presents a significant challenge to disruption efforts.
- Terrorist groups are often early adopters of new technologies, exploiting emerging platforms for their online communication and distribution strategies.
- With sufficient planning and support from sympathetic online communities, terrorist attacks can rapidly turn viral, before OSPs and law enforcement can respond.

8.2 » THE USE OF THE INTERNET BY TERRORIST GROUPS

The loss of the Islamic State's (IS) territorial control into core areas of Iraq and Syria denied the group one of its most potent propaganda assets. IS' online capabilities in 2018 reflect the overall collapse of the physical caliphate, previously the central pillar of its project. However, this collapse combined with the group's battlefield attrition did not stop the group's online sympathisers from exploiting the internet to advance their cause.

In parallel, the 15 March 2019 right-wing extremism (RWE) motivated terrorist attack on two mosques in Christchurch, New Zealand, has brought about unprecedented elements in the exploitation of the internet for terrorist purposes. The attack's recorded livestreaming video and the gunman's manifesto rapidly went viral and gained digital depth, highlighting new challenges in the fight against terrorist content online.

Terrorist groups boast a diversified online infrastructure

Terrorist groups continue to expand and diversify their conduits for the dissemination of their propaganda online. In doing so, they exploit a wide array of OSPs, which are spread across multiple jurisdictions and differ greatly in terms of size, services offered, business models, and abuse policies. While certain platforms are more abused than others, the sheer number of OSPs exploited for terrorist purposes presents a challenge for disruption efforts. These include forums, file-sharing sites, pastebins, video streaming/sharing sites, URL shortening services, blogs, messaging/broadcast applications, news websites, live streaming platforms, social media sites and various services supporting the creation and hosting of websites (including registries* and registrars**). The ongoing abuse of legitimate services by terrorist groups extends also to VPNs, anonymised cryptocurrencies and DDoS mitigation services.

Faced with the loss of its state-building project and increasingly hostile attitudes towards its online propaganda machine, IS continues to reconfigure its tactics to remain relevant online. In spite of intensified takedown campaigns in 2018 by law enforcement and social media platforms — including Telegram — the group still boasts a highly diversified online infrastructure for the dissemination of its propaganda and persists in publishing on a wide array of media and file-sharing sites, especially smaller platforms with reduced capacity for disruptive actions[64].

Similarly, the spread of terrorist content linked to the Christchurch attack involved the concurrent exploitation of multiple kinds of OSPs by different communities of Internet users, spurred by different motives but a common purpose: making this type of terrorist content viral and resilient.

IS propagandists strive to remain relevant online

IS' critical situation in 2018 had a significant impact on its digital capabilities: propaganda produced by official IS media outlets has visibly declined[65]. The only publication that continued to be issued on a regular basis throughout 2018 was the group's official Arabic weekly newsletter al-Naba' (The News). In their quest for virtual survival, IS and its supporters responded to frequent deletions of content in 2018 by promoting ways to enhance online resilience. Pro-IS media outlets, including the *al-Saqri Corporation for Military Sciences, Horizons Electronic Foundation* and the *United Cyber Caliphate* became more prolific in providing guidelines on cyber and operational security. The instructions ranged from suggesting

* A registry is an organisation that manages the administrative data for the TLD domains and subdomains under its authority, including the zone files that contain the addresses of the name servers for each domain. Source: Google Domains Help, "About registrars and registries", https://support.google.com/domains/answer/3251189?hl=en, 2019.

** A registrar is an organisation that manages the registration of domain names for one or more top-level domain (TLD) registries. Source: Google Domains Help, "About registrars and registries", https://support.google.com/domains/answer/3251189?hl=en, 2019.

secure browsers and privacy-oriented applications to promoting the use of the Tor browser and decentralised platforms. These unofficial but increasingly specialised media outlets also provided advice on how to circumvent account suspension, with suggestions including using channel names and profile pictures that cannot be associated with IS. Additionally, IS sympathisers created multiple versions of the same account, allowing them to swiftly rebound from account suspensions. IS-affiliated websites that act as repositories for the organisation's propaganda responded to recurrent suspensions by creating new domain names and re-emerging at new locations from backup copies, including from and to the dark web. Yet despite its advantageous features in terms of privacy and resilience, the exploitation of the dark web for propaganda dissemination purposes remained limited and propagandists continued to prefer the visibility and reach afforded by the surface web.

IS continue to seek out new vectors for their online propaganda

Terrorist groups continue to lay claim to a degree of technological adaptability and are often early adopters of new technologies. A case in point is IS' seemingly coordinated and near-synchronous shift to open source, decentralised platforms***. In the aftermath of an intense suspension campaign carried out by Telegram in late 2018, IS supporters on Telegram started advocating for the use of alternative platforms and software. Since then, the IS has established a presence on a number of open source, decentralised platforms. Accounts and pages disseminating mostly official IS propaganda have been created on Mastodon, Nextcloud, Rocket.Chat and ZeroNet. The resilient character of these platforms, coupled with multiple options for anonymity and enhanced usability, are all features that play into the online communication and distribution strategies of terrorist groups.

However, jihadist activities on these platforms failed to gain traction in 2018. This is probably due to the alternative platforms' smaller user base and weaker outreach capabilities. Thus, Telegram remains the platform of choice for terrorist sympathisers, who continue to exploit its advantageous encryption and file-sharing capabilities.

Terror goes viral with Christchurch mosques attack

The Christchurch attack marks a defining point in the fight against terrorist content online: the attack was livestreamed and its recording, alongside the gunman's manifesto, spread rapidly online. The exceptional virality, velocity and volume of the materials' online diffusion points to a savvy use of internet technologies and communication, not only by the attacker, but by multiple communities of internet users, beyond RWE sympathisers.

The interplay of online communities who share the same Internet slang and memes contributed to the widespread dissemination of the content and its digital endurance.

Internet users have adopted different techniques to circumvent disruption efforts by OSPs. In particular, edited versions of the Christchurch video appeared to fly under the radar of detection measures enforced by OSPs. Reponses by practitioners and OSPs could not measure up to the scale of online dissemination and with the existing cooperation frameworks keeping terrorist content at bay remains challenging.

8.3 » RECOMMENDATIONS

Limiting the ability of terrorists to carry out transnational attacks by disrupting their flow of propaganda and attributing online terrorism-related offences requires continued and heightened counterterrorism cooperation and information sharing across law enforcement authorities, as well as with the private sector.

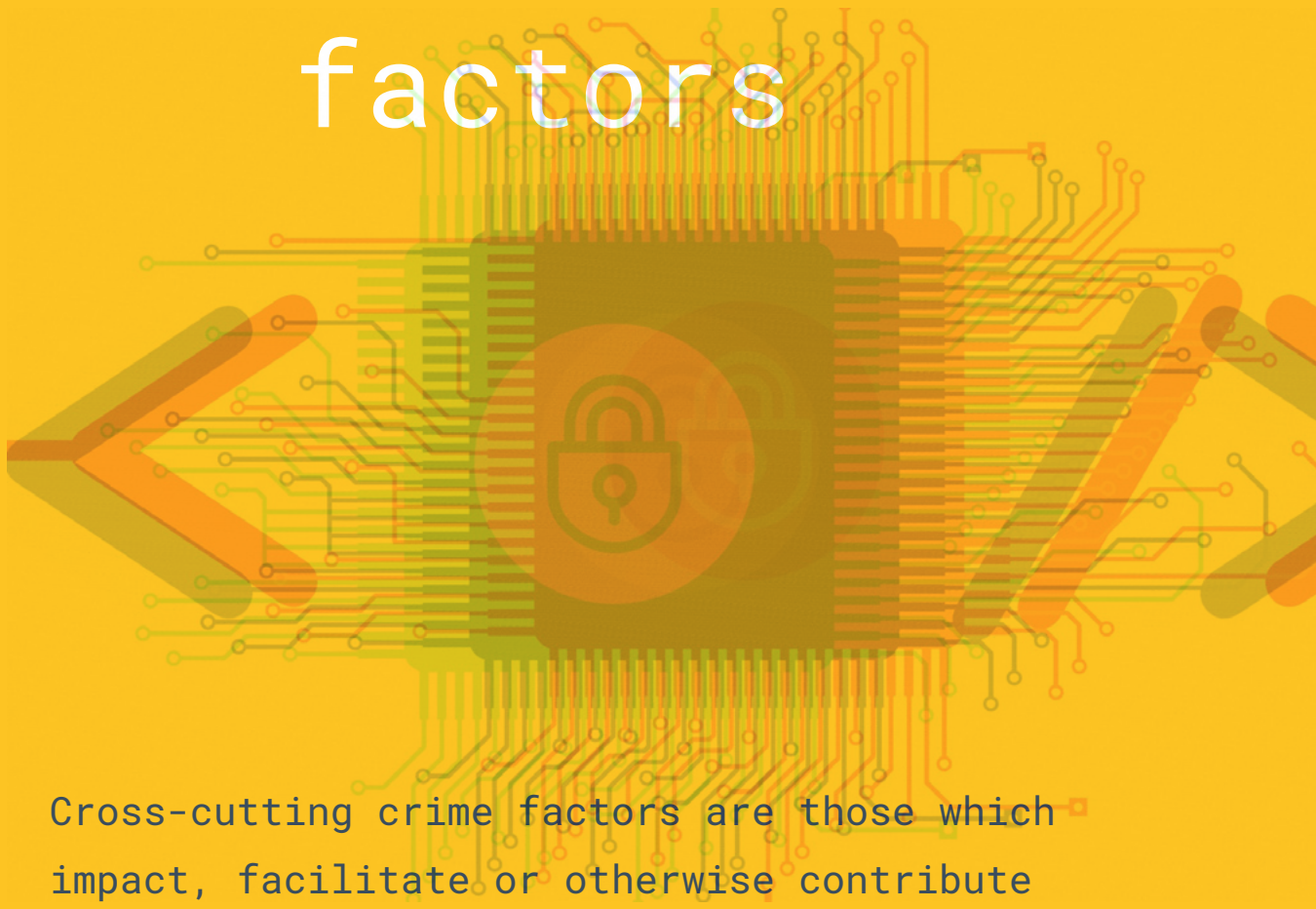
Any effective measure to counter terrorist groups' online propaganda and recruitment operations entails addressing the whole range of abused OSPs, especially start-ups and smaller platforms with limited capacity for response.

Cross-platform collaboration and a multi-stakeholder crisis response protocol on terrorist content online would be essential to crisis management the aftermath of a terrorist attack.

A better understanding of new and emerging technologies is a priority for practitioners. Upcoming policy debates and legislative developments should take into account the features of these technologies in order to devise an effective strategy to prevent further abuse.

*** Decentralised systems are a particular type of distributed system where no single entity is in control of the underlying infrastructure. Source: Blockstack PBC, *Blockstack Technical Whitepaper v2.0*, 2019.

#9 cross-cutting crime factors



Cross-cutting crime factors are those which impact, facilitate or otherwise contribute to multiple crime areas but are not necessarily inherently criminal themselves.

9.1 » KEY FINDINGS

- Phishing remains an important tool in the arsenal of cybercriminals for both cyber-dependent crime and NCPF.
- While cryptocurrencies continue to facilitate cybercrime, hackers and fraudsters now routinely target crypto-assets and enterprises.

criminal case study

GDPR entered into effect across the EU in May 2018 (see also section 4.3). Prior to this, many companies sent out emails to their customers, detailing privacy policies and the rights of their customers concerning their data. It was not long before criminals exploited these legitimate messages with a wave of copycat phishing emails. These malicious emails would typically contain links to fake sites that would then capture victims' data to be used or sold by the cybercriminals.

case study

In March 2019, the Spanish Civil Guard, as part of operation Neptuno, dismantled a criminal organisation dedicated to scamming victims through phishing. The investigation originated in September 2018, when an increase in complaints related to banking scams were detected, whose common link was the withdrawal of money from the bank accounts of the victims. The perpetrators sent out phishing emails pretending to be one of six banks.

The operation has resulted in 11 people arrested, aged between 17 and 28 years of age. In addition, police seized several laptops, more than 20 mobile phones, EUR 7 500 in cash, notes with identity documents and access codes to online banking, virtual currencies (bitcoin) and bankcards.

9.2 » SOCIAL ENGINEERING

Social engineering, and in particular phishing, overwhelmingly represented the most significant cross-cutting cyber-threat faced by both European cybercrime investigators, and the most significant cyber-threat overall by Europol's private sector partners.

Phishing — a core attack method for all cybercrime

Both investigators of cyber-dependent crime and NCPF highlighted phishing as a key threat. In cases related to NCPF, perpetrators primarily used phishing to gather personal banking credentials, payment card data, or other login credentials. Criminals either sell such data on underground markets, or use it directly to commit fraud.

In cases related to cyber-dependent crime, criminals also use phishing to gain login credentials. However, as highlighted in section 4.2, it is also currently the dominant malware delivery method, through either malicious attachments, or links to malicious URLs. Either may ultimately lead to attackers gaining unauthorised access to a private network.

Some law enforcement respondents note how criminals use some phishing attacks for extortion. Attackers can create a pretext either based on genuine data found on the internet from a previous data breach, or a purely fictitious scenario to extort money from a victim. Such extortions are often of a sexual nature.

While the financial sector is, and always will be, a significant target for such attacks, industry reporting indicates that most phishing attacks are currently targeting Software-as-as-Service such as cloud services, and webmail[66].

Even though phishing remains an ongoing challenge, certain solutions or mitigating measures do exist. Domain-based message authentication, reporting and conformance (DMARC) is one such option, which has been introduced years ago. DMARC is an email authentication, policy, and reporting protocol. DMARC makes it easier for email senders and receivers to determine whether or not a given message is legitimately from the sender and what to do if it is not. This makes it easier to identify spam and phishing messages and keep them out inboxes. Yet, according to one study, DMARC adoption is non-existent at 80 % of organisations[67]. This is a missed opportunity as the United Kingdom National Cyber Security Centre (UK NCSC) demonstrates

65 % of targeted attack groups used spear phishing as the primary infection vector [70]

32 % breaches involve phishing [73]

48 % of malicious email attachments are office files [71]

1 in 3 207 emails are phishing emails [74]

IN 2018

up to 0.55 % of all incoming emails were phishing emails [72]

phishing was present in 78 % of cyber espionage incidents [75]

how it has achieved recent success by using 'Synthetic DMARC.' This 'works by assigning a DMARC record for all domains attempting to pass-off as gov.uk domains, by analysing and vetting non-existing subdomains against DNS records and building on authentication systems of the past[68].' Because of the technology, the UK NCSC has been able to stop 140 000 separate phishing attacks in the last year and has taken down a record 18 067 phishing sites. This is a noticeable improvement when compared to the takedown rate of 14 124 in 2018[69]. The technology comes with its challenges, namely from an interoperability perspective, but still provides promising results for those able to implement it.

9.3 » MONEY MULES

Money mule activity continues to support all aspects of cybercrime

The use of money mules to launder criminal funds was the second most prominent cross-cutting threat highlighted by European law enforcement. Again, this pertained to both cyber-dependent crime and NCPF investigations, although the majority of references related to the latter.

While this was a top threat, law enforcement did not identify new *modi operandi* this year. Instead, they confirmed the use of typical recruitment methods such as job advertisements targeting disadvantaged or low-income individuals. In some instances, perpetrators recruited mules with a stronger financial standing, allowing them to open corporate accounts through which the funnelling of international funds may attract less attention.

case study

In 2018, over the course of three months, law enforcement and private sector partners from over 30 countries participated in the fourth European Money Mule Action (EMMA). Europol, Eurojust, the EBF and more than 300 banks supported the initiative.

The action resulted in the identification of over 1 500 money mules and 140 money mule organisers, and over 168 arrests. Financial sector participants reported 26 376 fraudulent money mule transactions, preventing an estimated loss of over EUR 36 million.

The campaign also raised awareness of the dangers of becoming a money mule throughout the participating nations.

“I thought it was part of the job”

MONEY MULING HELPS PERPETRATE CRIME

IGNORANCE IS NO EXCUSE

Criminals will try to dupe innocent victims into laundering money on their behalf by making the job offer seem as legitimate as possible.

Be wary of adverts that are poorly written with grammatical errors and spelling mistakes.

#dontbeaMule

Created by Europol

EUROPOL EC3 European Cybercrime Centre

EUROJUST

EBF European Banking Federation

9.4 » THE CRIMINAL ABUSE OF CRYPTOCURRENCIES

In previous years' reports, we have extensively highlighted the criminal abuse of cryptocurrencies across all areas of cyber-related criminality due to the perceived level of anonymity they provide. This trend persists as investigators of cyber-dependent crime and NCPF report that these currencies continue to pose investigative challenges for law enforcement. Crypto investigations are now a core part of daily business for law enforcement. As a result, investigators require training to ensure they have the appropriate skills to handle such investigations.

Predominantly, such currencies play an essential role in the underground economy. They are used for most criminal to criminal (C2C) payments on criminal forums and marketplaces. In addition to C2C payments, many attackers demand payment from victims for attacks such as ransomware or DDoS extortion by cryptocurrencies. Such criminally obtained funds, while already inherently challenging to trace, are often further laundered through mixing services, which serve to obfuscate the financial trail.

Crypto-assets now routinely targeted by fraudsters

The most apparent development with regards to cryptocurrencies, first highlighted in last year's report, is that attacks and frauds which historically targeted other payment systems or fiat currencies have now been adapted to incorporate cryptocurrencies. As such, we now routinely see malware and phishing targeting crypto-investors and enterprises, and new frauds, such as investments frauds related to cryptocurrency investment. Such approaches may be more successful due to the lower levels of knowledge potential victims are likely to have about these assets.

Cryptojacking remains an issue, but not a priority

Cryptojacking remains an issue. The activity appears to have peaked in 2018 and decreased throughout 2019, partially due to the shut down of Coinhive, the most popular mining script, in March. The most suitable cryptocurrencies were those that are memory intensive, meaning that they are suitable for CPU or GPU mining, and that are difficult to trace; Monero ticked both boxes, as such it was the first choice for this type of abuse. Although these incidents affect many, the damage per victim is typically low and thus such abuse is rarely reported (see also 4.7).

While we have previously reported a small shift towards more privacy-focused cryptocurrencies such as Monero, Bitcoin still remains the currency of choice for both legitimate and criminal use. The main developments regarding this trend are on the Darknet markets, several of which also accept Monero, or in some cases exclusively trade in it.

case study

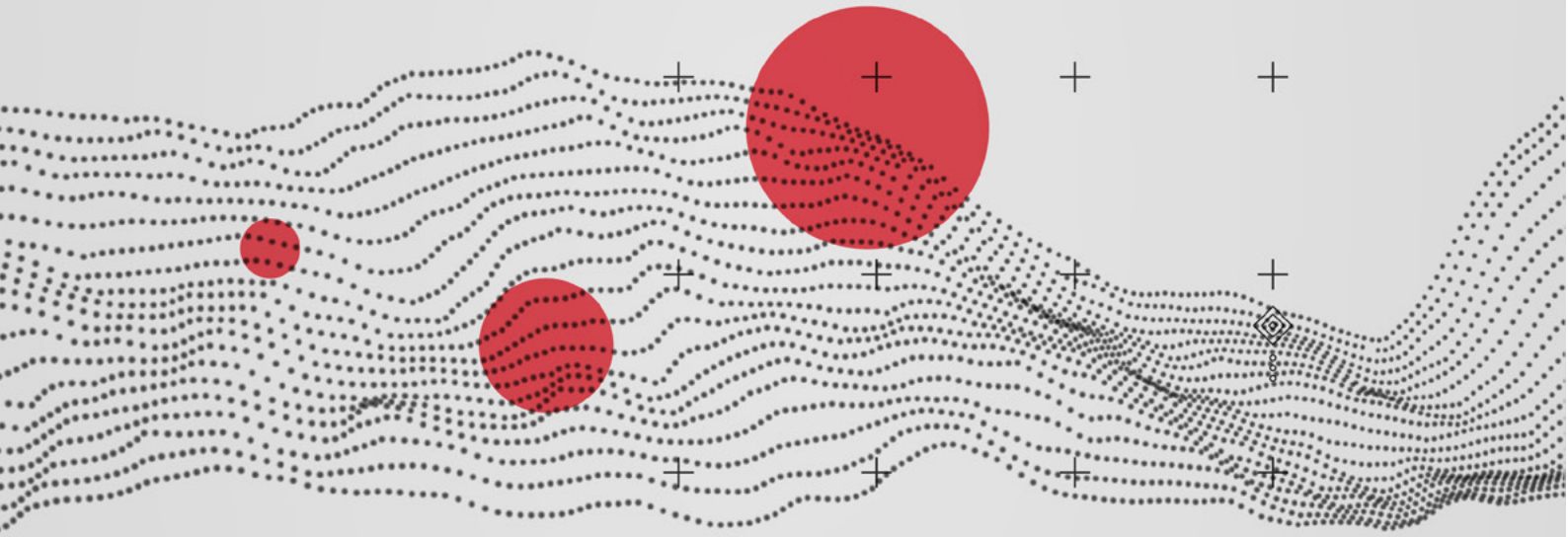
In June 2019, six offenders were arrested in the UK and the Netherlands after a 14-month investigation into phishing activities that netted the perpetrators over EUR 24 million in cryptocurrencies. The phishing relied on typosquatting, where a large number of websites belonging to well-established cryptocurrency wallets and exchanges were recreated by criminals with the sole purpose of stealing users' credentials and funds.

While phishing is commonplace across both traditional financial as well as cryptocurrency sector, what makes this operation unique was the scale — over 4 000 victims had their funds stolen with the numbers continuing to grow.

The operation was another demonstration of exemplary cooperation between law enforcement and the private sectors, particularly security researchers and cryptocurrency exchanges.

> Global uptakes of digital currencies, combined with proliferation of AI-based applications, are gradually becoming the main means of exchanging goods and services. The key challenge for law enforcement agencies and other stakeholders such as national/international authorities and financial services are to protect public and economy against full spectrum of criminal acts using artificial intelligence and digital currencies (e.g. cyber-enabled fraud, misuse of personal data, money laundering, serious and organised crime to CSE).

— PROFESSOR BABAK AKHGAR, DIRECTOR OF CENTRIC, UK



> As technology continues to become more complex and distributed systems even more intertwined fewer people understand the dependencies and interaction patterns. One particularity interesting form of distributed systems are cryptocurrencies and smart contracts. They are based on assumptions some of which are still poorly understood. There is a risk in wide-spread adoption because attacks have huge immediate financial implications; correctly working financial incentives are, however, a basic building block of public blockchains. Attacks can be executed globally at unprecedented speeds and difficult to fix.

— DR EDGAR WEIPPL, SBA RESEARCH, AUSTRIA

9.5 » COMMON CHALLENGES FOR LAW ENFORCEMENT

Much of the IOCTA is focused on the threat posed by criminal actors and their *modi operandi.* At the same time, it is crucial to reflect on how law enforcement can and does respond to these threats, and what barriers the law enforcement and judicial community encounter in responding. In June 2019, Europol and Eurojust revisited their joint 2017 paper on the *Common Challenges in Combatting Cybercrime* with a fresh look at how these challenges developed over the preceding two years. Many of these challenges are not unique to cybercrime and cut across all areas of serious organised crime and terrorism.

These challenges are extremely relevant to this assessment and therefore we will summarise some of the most pertinent issues. For full details, including ongoing activities and open issues, readers should refer to the full report[76].

The key challenges remain unchanged and fall into five main areas of discussion.

The loss of data

This refers to several legislative changes and technologies that effectively either deny law enforcement access to data or have resulted in there being limited or no data for law enforcement to access for a criminal investigation. The overturning of the Data Retention Directive in 2014 and the implementation of the GDPR in 2018 has deprived law enforcement of a number of key sources of data, namely communications data and WHOIS data. In contrast, the wide-scale implementation of carrier-grade network address translation technologies by internet service providers results in often prohibitively large volumes of data (as one IPv4 address may be shared by multiple end-users at one).

In last year's report, we highlighted the impact of WHOIS 'going dark', particularly in the scope of cyber investigations. In September 2018, ICANN published the draft results of a survey that directly measured the impact of the unavailability of WHOIS data. Almost 26 % of respondents indicated that it had resulted in investigations being discontinued, with a further 52 % indicating that it delayed investigations to some degree. Moreover, only 33 % of respondents indicated that WHOIS (at least partially) met their investigative needs, compared to 98 % prior to the changes[77].

Encryption, while recognised as an essential element of our digitised society, also facilitates significant opportunities for criminals. Investigative techniques, such as lawful interception, are becoming increasingly ineffective (or even impossible) as criminals exploit encrypted communication services, applications and devices. Similarly, criminals can deny forensic

investigators access to critical evidence by encrypting their data. The criminal abuse of encryption technologies, whether it be anonymisation via VPNs or Tor, encrypted communications or the obfuscation of digital evidence (especially in cases of CSEM), was a significant threat highlighted by respondents to this year's IOCTA survey.

Cryptocurrencies are another application of encryption technology, and, as outlined in 13.4, also present significant challenges for law enforcement[78].

The loss of location

The increasing level of criminal use of encryption and/or anonymisation tools, crypto-currencies and the Dark Web, as well as the growing use of cloud-based technologies, have also led to situations in which law enforcement may no longer (reasonably) establish the physical location of perpetrators, criminal infrastructure or electronic evidence. The territoriality-based investigative powers and jurisdiction of the competent national authorities offer no appropriate tools to tackle these situations.

Challenges associated with national legal frameworks

Differences between domestic legal frameworks in the member states and international instruments continue to be a serious impediment to the international criminal investigation and prosecution of cybercrime. The main differences relate to the criminalisation of conduct and provisions to investigate cybercrime and gather e-evidence. For example, should legislation that regulates law enforcement presence and action in an online environment be harmonised at EU level, this would allow for more effective joint operational actions such as large-scale botnet takedowns, or increased possibilities to monitor criminal activities online and to lawfully collect critical evidence on the Deep Web and Dark Web.

Obstacles to international cooperation

The lack of a common legal framework which exists for the expedited sharing of evidence continues to hamper criminal investigations and judicial proceedings, with the current process of Mutual Legal Assistance being perceived as too slow to gather and share electronic evidence effectively. The use of the European Investigation Order (EIO) may go some way towards addressing these issues for the majority of Member States, but may not provide the speed that is required to capture electronic evidence.

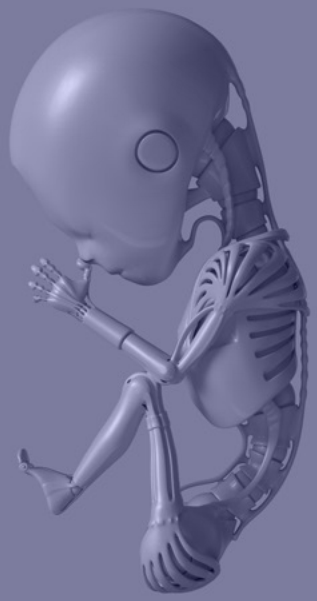
Another issue under this banner is law enforcements ability to respond to large-scale cyber-attacks, particularly where such attacks rapidly affect multiple industries across a range of sectors and geographies, such as the WannaCry and NotPetya attacks of 2017. Such attacks constitute a specific challenge to international cooperation.

Challenges of public-private partnerships

The private sector plays a key role in many cyber investigations and cybersecurity activity, being the custodians of crucial data, having essential capabilities in the takedown of criminal infrastructures and removal of illicit content. Public-private partnerships also play a key role in mitigating cybercrime and increasing cybersecurity through prevention and awareness. There is, however, little consensus on the legal framework that is required to facilitate effective and trust-based cooperation with the private sector, while at the same time regulating legal and transparency issues surrounding that cooperation.

This challenge also includes those associated with new and emerging technologies. The criminal misuse of technology has become an engine of cybercrime, although many of these technologies can be equally dual-purposed to assist law enforcement. Technologies such as quantum computing, and artificial intelligence may have applications at both ends of the lawful spectrum*.

* For a more extensive description of these please see: Europol & Eurojust, *First Report of the Observatory Function on Encryption,* 2019.



> If the speed of developments with regard to quantum computing continues (currently already exceeding 50 qubit) this has the potential to end the effectiveness of currently used encryption methods within the next five years. Within the same time period, it is likely that while artificial intelligence is not capable to fully draw level with human strengths it is surpassing what is necessary to exploit human weaknesses. As a consequence we will most likely see an increasing use of artificial intelligence in areas of crime where it is currently not utilised.

— PROFESSOR DR MARCO GERCKE, UNIVERSITY OF COLOGNE, GERMANY

9.6 » FUTURE THREATS AND DEVELOPMENTS

To combat phishing, leading platform providers are investing in engineering to deploy machine learning and other AI-based approaches, leveraging the newest technologies to protect consumers. However, enterprise adoption and deployment of these technologies is slow, therefore phishing is likely to continue to be a primary attack vector for attack for the near future. Equally, criminals will apply such methods too to bypass these systems.

The incorporation of innovation, as part of an effective crime response, however, is not exclusively a private sector affair. Europol already works together with industry partners and the European Commission to identify challenges and opportunities for law enforcement arising from new and emerging technologies, such as 5G. However, to tackle previously identified as well as future challenges, one consideration is to establish a hub for law enforcement innovation, bringing together the most relevant partners, tailored to the needs of Member States' law enforcement authorities. Such an entity could enhance the EU's ability to articulate an operational vision of innovation with-in the realm of internal Security, to decide on key partnerships, critical investments and be ready for future disruptions. The objective would be to identify and categorise common challenges in the area of innovation and emerging technologies in order to provide guidance and opportunities for EU Law Enforcement in these areas as well as to inform research priorities[79].

In July 2018, the 5th EU Anti-Money Laundering Directive (AMLD 5) entered into force. With 18 months to transpose the new Directive into national legislation, all member states should adopt the Directive by the closure of 2019. One of the key changes proposed by the Directive was the regulation of virtual currency platforms (exchanges) and custodian wallet providers (wallet services where the service holds its users' private keys). Such entities will be required to apply full customer due diligence, thereby de-anonymising their clients, and to report suspicious transactions to financial intelligence units.

While this new legislation may capture a significant proportion of cryptocurrency users, those using hardware or software wallets, or trading via other peer-to-peer exchange systems, can still operate largely anonymously[80]. Similarly, users of privacy-orientated cryptocurrencies such as Dash and Monero, until they are required to interact with a virtual currency exchange or add their holdings to a custodian wallet provider can also remain anonymous.

How the criminal community will react to these developments remains to be seen. However, it is likely we will see the rise of criminal exchange services operating on the digital underground, exchanging fiat and cryptocurrencies outside the regulated sector.

case study

In May 2019, the Dutch Fiscal Information and Investigation Service (FIOD), in close cooperation with Europol and the authorities in Luxembourg, took down on one of the world's leading cryptocurrency mixing service Bestmixer.io. The operation, which was initiated in 2018 by the FIOD with the support of the internet security company McAfee, resulted in the seizure of six servers in the Netherlands and Luxembourg. Bestmixer.io was one of the three largest mixing services for cryptocurrencies and offered services for mixing bitcoins, bitcoin cash and litecoins. The service started in May 2018 and achieved a turnover of at least USD 200 million (approx. 27 000 bitcoins) over one year.

The operation had a significant impact on the mixer community, resulting in at least one other mixing service voluntarily shutting down[81].

9.7 » RECOMMENDATIONS

Law enforcement and the judiciary must continue to develop, share and propagate knowledge on how to recognise, track, trace, seize and recover cryptocurrency assets.

Law enforcement must continue to build trust-based relationships with cryptocurrency-related businesses, academia, and other relevant private sector entities, to more effectively tackle issues posed by cryptocurrencies during investigations.

Despite the gradual implementation of AMLD 5 across the EU, investigators should be vigilant concerning emerging cryptocurrency conversion and cash-out opportunities, and share any new information with Europol.

REFERENCES

1 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

2 Europol, *European Union Serious and Organised Crime Threat Assessment: Crime in the age of technology,* 2017.

3 McGuire, M & Dowling, S., "Cyber crime: A review of the evidence", *UK Home Office Research Report 75*, 2013.

4 Symantec, *Internet Security Threat Report (ISTR) Vol. 24, 2019; IBM, X-Force Threat Intelligence Index, 2019; Microsoft, Microsoft Security Intelligence Report Vol. 23*, 2018.

5 EC3 Advisory Groups.

6 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

7 Symantec, *Internet Security Threat Report (ISTR) Vol. 24*, 2019.

8 https://blog.erratasec.com/2019/05/almost-one-million-vulnerable-to.html#.XUvgvm9LiUk

9 https://www.zdnet.com/article/cyberattacks-against-industrial-targets-double-over-the-last-6-months/#ftag=RSSbaffb68

10 https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/

11 Newman, L., "Ransomware Hits Georgia Courts as Municipal Attacks Spread", https://www.wired.com/story/ransomware-hits-georgia-courts-municipal-attacks-spread/, 2019.

12 https://www.zdnet.com/article/louisiana-governor-declares-state-emergency-after-local-ransomware-outbreak/

13 Liska, A., "Early Findings: Review of State and Local Government Ransomware Attacks", https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf, 2019.

14 Jay, J. "Formjacking attacks compromised over 50,000 retailer websites in 2018", https://www.scmagazineuk.com/formjacking-attacks-compromised-50000-retailer-websites-2018/article/1526282, 2019; Stone, J. "British Airways fined $229 million under GDPR for data breach tied to Magecart", https://www.cyberscoop.com/british-airways-gdpr-fine-magecart/, 2019.

15 https://www.zdnet.com/article/at-t-employees-took-bribes-to-plant-malware-on-the-companys-network/

16 https://www.scmagazine.com/home/security-news/capital-one-breach-exposes-not-just-data-but-dangers-of-cloud-misconfigurations/; https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/

17 Weinbaum, N, "The GDPR- One Year Later", https://securingtomorrow.mcafee.com/business/data-security/the-gdpr-one-year-later/, 2019.

18 King, A. & Weaver, R., "GDPR One Year Later: What We've Learned So Far", https://www.fireeye.com/blog/executive-perspective/2019/05/gdpr-one-year-later-what-we-ve-learned-so-far.html, 2019.

19 O'Flaherty, K., "British Airways Hit With Record Fine Following 2018 Cyberattack", https://www.forbes.com/sites/kateoflahertyuk/2019/07/08/british-airways-hit-with-record-fine-following-2018-cyberattack/#795491d21f8e, 2019.

20 Sweney, M., "Marriott to be fined nearly £100m over GDPR breach", https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico, 2019.

21 Van der Meulen, *Investing in Cybersecurity*, 2015.

22 Boiten, E., "Nearly £100m for Marriott, £138m for BA- what is the take home message from these sudden massive ICO fines?", https://www.computing.co.uk/ctg/opinion/3078677/gdpr-marriott-ba-ico-massive-fines, 2019.

23 Symantec, Internet Security Threat Report (ISTR) Vol. 24, 2019.

24 Microsoft, "Attack inception: Compromised supply chain within a supply chain poses new risks", https://www.microsoft.com/security/blog/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks/, 2018.

25 Zetter, K., "Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers", https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers, 2019.

26 Cimpanu, C. "Dark web crime markets targeted by recurring DDoS attacks", https://www.zdnet.com/article/dark-web-crime-markets-targeted-by-recurring-ddos-attacks/, 2019; Crawley, K. "What about all those Dark Web DDoS attacks?", https://www.peerlyst.com/posts/what-about-all-of-those-dark-web-ddos-attacks-kimberly-crawley, 2019.

27 Europol, "Authorities Across the World Going After Users of Biggest DDoS-for-hire Website", https://www.europol.europa.

eu/newsroom/news/authorities-across-world-going-after-users-of-biggest-ddos-for-hire-website, 2019.

28 Akamai, "Memcached DDoS explained", https://www.akamai.com/us/en/resources/our-thinking/threat-advisories/ddos-reflection-attack-memcached-udp.jsp.

29 Cloudflare, "Memcached DDoS Attack", https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/.

30 Shani, T., "Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important", https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/, 2019.

31 European Commission, *Communication from the Commission to the European Parliament, the European Council and the Council: Nineteenth Progress Report towards an effective and genuine Security Union,* 2019; Fiott, D. & Parkers, R., *Protecting Europe: the EU's response to hybrid threats,* 2019.

32 Group-IB, "Two hacker groups attacked Russian banks purporting to be Central Bank of Russia", https://www.group-ib.com/media/cbrf-double-attack/, 2019.

33 Canellis, D., "North Korean hacker crew steals $571M in cryptocurrency across 5 attacks", https://thenextweb.com/hardfork/2018/10/19/cryptocurrency-attack-report/, 2018.

34 Stolarchuk, J., "Hackers hit government agencies and banks hard in Singapore", http://theindependent.sg/hackers-hit-government-agencies-and-banks-hard-in-singapore/, 2019.

35 Chainalysis, *Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams,* 2019; CipherTrace, *Cryptocurrency Anti-Money Laundering Report,* 2018.

36 CERT-EU, *Threat Landscape Report Q1 2019,* 2019.

37 Zamora, W. "TrickBot takes over as top business threat", https://blog.malwarebytes.com/101/2018/11/trickbot-takes-top-business-threat/, 2018.

38 IBM, *X-Force Threat Intelligence Report,* 2019.

39 Palmer, D., "This new cryptomining malware targets Business PCs and servers", https://www.zdnet.com/article/this-new-cryptomining-malware-targets-business-pcs-and-servers/, 2018.

40 Symantec, *"Beapy: Cryptojacking Worm Hits Enterprises in China",* https://www.symantec.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china, 2019.

41 Wikipedia, "Memcached", https://en.wikipedia.org/wiki/Memcached, 2019.

42 Akamai, *State of the Internet Report,* 2018.

43 Trend Micro, "2018 Mobile Threat Landscape", https://www.trendmicro.com/vinfo/in/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape, 2019.

44 Inhope, *Inhope Statistics 2018,* 2019; Internet Watch Foundation, *Once upon a year,* 2018; Netclean, Netclean *Report 2018: A report about child sexual abuse crime,* 2018.

45 Analysis Project Twins.

46 Internet Watch Foundation, *Once upon a year,* 2018; Netclean, *Netclean Report 2018: A report about child sexual abuse crime,* 2018.

47 Analysis Project Twins.

48 Farinelli, B., "Could a Magecart Attack Hit Your E-Commerce Website?", https://blog.clear.sale/could-a-magecart-attack-hit-your-e-commerce-website, 2019; see also: Cimpanu, C., "New Magecart attacks leverage misconfigured S3 buckets to infect over 17K sites", https://www.zdnet.com/article/new-magecart-attacks-leverage-misconfigured-s3-buckets-to-infect-over-17k-sites/, 2019.

49 Alberts, A., "Why Online Fraud Prevention Controls are Failing", https://medium.com/@aalberts/why-online-fraud-prevention-controls-are-failing-ba90d7036c4f, 2019.

50 Preminger, B., "23 Million Stolen Credit Cards for Sale on the Dark Web in the First Half of 2019", https://www.cybersixgill.com/stolen_credit_cards/, 2019.

51 European Central Bank, "Card Fraud Report", https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html, 2019.

52 European Payments Council, *2018 Payment Threats and Fraud Trends Report,* 2018.

53 European Payments Council, *2018 Payment Threats and Fraud Trends Report,* 2018.

54 Barret, B., "ATM Hacking Has Gotten So Easy, The Malware's A Game", https://www.wired.com/story/atm-hacking-win-pot-jackpotting-game/, 2019.

55 Barrett, "ATM Hacking Has Gotten So Easy, The Malware's A Game", 2019.

56 Federal Bureau of Investigation, "Business e-mail compromise the 12 billion scam", https://www.ic3.gov/media/2018/180712.aspx, 2018.

57 Seals, T., "ATM Jackpotting Malware Hones Its Heist Tools", https://threatpost.com/atm-jackpotting-malware-win-pot/141960/, 2019.

58 Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

59 European Banking Authority, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2,* 2019.

60 Fortuna, P., "Is Security The Loser As Open Banking Takes Hold?", https://www.infosecurity-magazine.com/opinions/security-loser-open-banking/, 2019.

61 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.

62 Europol, *Do Criminals Dream of Electric Sheep?,* 2019, p. 13.

63 Kharif, O., "Bitcoin Criminals Set to Spend $1 Billion on Dark Web This Year", https://www.bloomberg.com/news/articles/2019-07-01/bitcoin-criminals-set-to-spend-1-billion-on-dark-web-this-year, 2019.

64 Europol, *European Union Terrorism Situation and Threat Report,* 2019, p. 39.

65 Europol, *European Union Terrorism Situation and Threat Report,* 2019, p. 34.

66 APWG, *Phishing Activity Trends Report*, 1st Quarter 2019; Europol Advisory Groups.

67 Seals, T., "ThreatList: DMARC Adoption Nonexistent at 80 % of Orgs", https://threatpost.com/dmarc-adoption-nonexistent/146751/, 2019.

68 Abbott, C. & Aggromito, M., "The Battle Against Phishing", https://www.natlawreview.com/article/battle-against-phishing, 2019.

69 National Cyber Security Centre, *Active Cyber Defence: The Second Year,* 2019.

70 Symantec, *Internet Security Threat Report Vol. 24,* 2019.

71 Symantec, *Internet Security Threat Report Vol. 24,* 2019.

72 Microsoft, *Microsoft Security Intelligence Report Vol. 23,* 2018.

73 Verizon, *Data Breach Incident Report,* 2019.

74 Symantec, *Internet Security Threat Report Vol. 24,* 2019.

75 Verizon, *Data Breach Incident Report,* 2019.

76 Europol & Eurojust, "Common challenges in combatting cybercrime", https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime, 2019.

77 ICANN, *Registration Directory Services (RDS)-WHOIS2 Review,* 2019, p. 24.

78 Europol, *Do Criminals Dream of Electric Sheep?,* 2019, p. 13.

79 Europol, *Do Criminals Dream of Electric Sheep?,* 2019, p. 21.

80 European Parliament, *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion,* 2018.

81 Redman, J., "Mixing Service Bitcoin Blender Quits After Bestmixer Takedown", https://news.bitcoin.com/mixing-service-bitcoin-blender-quits-after-bestmixer-takedown/, 2019.

IOCTA
[2019]

EUROPOL | EC3 European Cybercrime Centre

www.europol.europa.eu