321DT02e
BACKGROUND DOCUMENTATION

1	Communication from the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - EU strategy for a more effective fight against child sexual abuse *(Brussels, 24.07.2020, COM(2020) 607 final)*
2	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)*
3	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)*
4	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)*
5	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)*
6	Internet Organised Crime Threat Assessment (IOCTA) 2020
7	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online *(Brussels, 10.9.2020, COM(2020) 568 final 2020/0259 (COD)*

A) The institutional framework for criminal justice in the EU

A1) Main treaties and conventions

A1-01	Protocol (No 36) on Transitional Provisions
A1-02	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, art. 82-86 *(OJ C 326/47; 26.10.2012)*
A1-04	Consolidated Version of the Treaty on the European Union, art. 9-20 *(OJ C326/13;, 26.10.2012)*
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 August 2016)
A2-02	Consolidated version of the Rules of Procedure of the Court of Justice (25 September 2012)

A3) European Convention on Human Rights (ECHR)

A3-01	Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 together with additional protocols No. 4, 6, 7, 12 and 13, Council of Europe
A3-02	Case of Mihalache v. Romania [GC] (Application no. 54012/10), Strasbourg, 08 July 2019
A3-03	Case of Altay v. Turkey (no. 2) (Application no. 11236/09), Strasbourg, 09 April 2019
A3-04	Case Beuze v. Belgium (Application no. 71409/10), Strasbourg, 09 November 2018
A3-05	Case of Vizgirda v. Slovenia (Application no. 59868/08), Strasbourg, 28 August 2018
A3-06	Case of Şahin Alpay v. Turkey (Application no. 16538/17), Strasbourg, 20 March 2018
A3-07	Grand Chamber Hearing, Beuze v. Belgium [GC] (Application no. 71409/10), Strasbourg, 20 December 2017
A3-08	Case of Blokhin v. Russia (Application no. 47152/06), Judgment European Court of Human Rights, Strasbourg, 23 March 2016
A3-09	Case of A.T. v. Luxembourg (Application no. 30460/13), Judgment European Court of Human Rights, Strasbourg, 09 April 2015
A3-10	Case of Blaj v. Romania (Application no. 36259/04), Judgment European Court of Human Rights, Strasbourg, 08 April 2014
A3-11	Case of Boz v. Turkey (Application no. 7906/05), Judgment European Court of Human Rights, Strasbourg, 01 October 2013 (FR)
A3-12	Case of Pishchalnikov v. Russia (Application no. 7025/04), Judgment European Court of Human Rights, Strasbourg, 24 October 2009
A3-13	Case of Salduz v. Turkey (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

A4) Brexit

A4-01	Draft text of the Agreement on the New Partnership between the European Union and the United Kingdom (UKTF 2020-14), 18 March 2020
A4-02	Draft Working Text for an Agreement on Law enforcement and Judicial Cooperation in Criminal Matters
A4-03	The Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (2019/742), 28th March 2019
A4-04	Brexit next steps: The European Arrest Warrant, House of Commons, 20 February 2020
A4-05	Brexit next steps: The Court of Justice of the EU and the UK, House of Commons, 7 February 2020
A4-06	The Law Society, “Brexit no deal: Criminal Justice Cooperation”, London, September 2019

A4-07	European Commission, Factsheet, „A „No-deal“-Brexit: Police and judicial cooperation”, April 2019
A4-08	CEPS: Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership, 29 August 2018
A4-09	Policy paper: The future relationship between the United Kingdom and the European Union, 12 July 2018
A4-10	House of Lords, Library Briefing, Proposed UK-EU Security Treaty, London, 23 May 2018
A4-11	HM Government, Technical Note: Security, Law Enforcement and Criminal Justice, May 2018
A4-12	LSE-Blog, Why Britain´s habit of cherry-picking criminal justice policy cannot survive Brexit, Auke Williams, London School of Economics and Political Science, 29 March 2018
A4-13	House of Commons, Home Affairs Committee, UK-EU Security Cooperation after Brexit, Fourth Report of Session 2017-19, London, 21 March 2018
A4-14	HM Government, Security, Law Enforcement and Criminal Justice, A future partnership paper
A4-15	European Criminal Law after Brexit, Queen Mary University London, Valsamis Mitsilegas, 2017
A4-16	House of Lords, European Union Committee, Brexit: Judicial oversight of the European Arrest Warrant, 6th Report of Session 2017-19, London, 27 July 2017
A4-17	House of Commons, Brexit: implications for policing and criminal justice cooperation (24 February 2017)
A4-18	Scottish Parliament Information Centre, Briefing, Brexit: Impact on the Justice System in Scotland, Edinburgh, 27 October 2016

B) Mutual legal assistance

B1) Legal framework

B1-01	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)*
B1-02	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)*
B1-03	Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the surrender procedure between the Member States of the European Union and Iceland and Norway (OJ L 292, 21.10.2006, p. 2–19)
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.1959*)
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: 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 law by the Court of Justice of the European Union on the European Arrest Warrant – Overview, Eurojust, 15 March 2020
B2-04	Case C-717/18, X (European arrest warrant – Double criminality) Judgement of the Court of 3 March 2020
B2-05	Case C-314/18, SF Judgement of the Court of 1 March 2020
B2-06	Joined Cases C-566/19 PPU (JR) and C-626/19 PPU (YC), Opinion of AG Campos Sánchez-Bordona, 26 November 2019
B2-07	Case C-489/19 PPU (NJ), Judgement of the Court (Second Chamber) of 09 October 2019
B2-08	Case 509/18 (PF), Judgement of the Court (Grand Chamber), 27 May 2019
B2-09	Joined Cases C-508/18 (OG) and C-82/19 PPU (PI), Judgement of the Court (Grand Chamber), 24 May 2019
B2-10	The Guardian Press Release: Dutch court blocks extradition of man to 'inhumane' UK prisons, 10 May 2019
B2-11	Case 551/18, IK, Judgement of the Court of 06 December 2018 (First Chamber)
B2-12	CJEU Press Release No 141/18, Judgement in Case C-207/16, Ministerio Fiscal, 2 October 2018
B2-13	CJEU Press Release No 135/18, Judgement in Case C-327/18 PPU RO, 19 September 2019
B2-14	Case C-268/17, AY, Judgement of the Court of 25 July 2018 (Fifth Chamber)
B2-15	Case C-220/18 PPU, ML, Judgement of the Court of 25 July 2018 (First Chamber)
B2-16	Case C-216/18 PPU, LM, Judgement of the Court of 25 July 2018 (Grand Chamber)
B2-17	InAbsentiEAW, Background Report on the European Arrest Warrant - The Republic of Poland, Magdalena Jacyna, 01 July 2018
B2-18	Case C-571/17 PPU, Samet Ardic, Judgment of the court of 22 December 2017
B2-19	C-270/17 PPU, Tupikas, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-20	Case C-271/17 PPU, Zdziaszek, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-21	Case C-579/15, Popławski, Judgement of the Court (Fifth Chamber), 29 June 2017
B2-22	Case C-640/15, Vilkas, Judgement of the Court (Third Chamber), 25 January 2017

B2-23	Case C-477/16 PPU, Kovalkovas, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-24	Case C-452/16 PPU, Poltorak, Judgement of the Court (Fourth chamber), 10 November 2016
B2-25	Case C-453/16 PPU, Özçelik, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-26	Case C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B2-27	Case C241/15 Bob-Dogi, Judgment of the Court (Second Chamber) of 1 June 2016
B2-28	C-108/16 PPU Paweł Dworzecki, Judgment of the Court (Fourth Chamber) of 24 May 2016
B2-29	Cases C-404/15 Pál Aranyosi and C-659/15 PPU Robert Căldăraru, Judgment of 5 April 2016
B2-30	Case C-237/15 PPU Lanigan, Judgment of 16 July 2015 (Grand Chamber)
B2-31	Case C-168/13 PPU *Jeremy F / Premier ministre*, Judgement of the court (Second Chamber), 30 May 2013
B2-32	Case C-399/11 *Stefano Melloni v Ministerio Fiscal*, Judgment of of 26 February 2013
B2-33	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-34	C-261/09 Mantello, Judgement of 16 November 2010
B2-35	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-36	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-37	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-38	C-66/08 Szymon Kozlowski, Judgement of 17 July 2008

B3) Mutual recognition: freezing and confiscation and asset recovery

B3-01	FATF, COVID-19-related Money Laundering and Terrorist Financing Risk and Policy Responses, Paris, 4 May 2020
B3-02	Money-Laundering and COVID-19: Profit and Loss, Vienna, 14 April 2020
B3-03	FATF President Statement – COVID-19 and measures to combat illicit financing, Paris 1 April 2020
B3-04	Moneyval Plenary Meeting report, Strasbourg, 31 January 2020
B3-05	Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA
B3-06	Commission Delegated Regulation (EU) …/... of 13.2.2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, C(2019) 1326 final
B3-07	Regulation 2018/1805 of the European Parliament and of the Council on the mutual recognition of freezing and confiscation orders, L 303/1, Brussels, 14 November 2018
B3-08	Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, L 284/22
B3-09	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 (Text with EEA relevance), PE/72/2017/REV/1 OJ L 156, p. 43–74, 19 June 2018
B3-10	Directive (EU) 2017/541 of the European Parliament and of the Council of

	15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
B3-11	Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Text with EEA relevance)
B3-12	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance)
B3-13	Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance)
B3-14	Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community
B3-15	Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA)
B3-16	Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA)

B4) Mutual recognition: Convictions

B4-01	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)*
B4-02	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)*
B4-03	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)*
B4-04	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*)
B4-05	Case C-234/18, Judgment of 20 March 2020
B4-06	Case C-390/16, Dániel Bertold Lada, Opinion of AG Bot, delivered on 06 February 2018
B4-07	Case C-171/16, Trayan Beshkov, Judgement of the Court (Fifth Chamber), 21 September 2017
B4-08	Case C-528/15, Policie ČR,Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie v Salah Al Chodor, Ajlin Al Chodor, Ajvar Al Chodor, Judgement of the Court (Second Chamber), 15 March 2017
B4-09	Case C-554/14, Ognyanov, Judgement of the Court (Grand Chamber), 8 November 2016
B4-10	Case C-439/16 PPU, Milev, Judgement of the Court (Fourth Chamber), 27 October 2016
B4-11	C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B4-12	C-601/15 PPU, J. N. v Staatssecretaris voor Veiligheid en Justitie, Judgement of the Court (Grand Chamber), 15 February 2016
B4-13	C-474/13, Thi Ly Pham v Stadt Schweinfurt, Amt für Meldewesen und Statistik, Judgement of the Court (Grand Chamber), 17 July 2014
B4-14	Joined Cases C-473/13 and C-514/13, Bero and Bouzalmate, Judgement of the Court (Grand Chamber), 17 July 2014
B4-15	C-146/14 PPU, Bashir Mohamed Ali Mahdi, Judgement of the Court (Third Chamber), 5 June 2014
B4-16	Case C-383/13 PPU, M. G., N. R., Judgement of the Court (Second Chamber), 10 September 2013

B5) Mutual recognition in practice: evidence and e-evidence

B5-01	The European Law Blog, „E-Evidence: The way forward. Summary of a Workshop held in Brussels on 25 September 2019, Theodore Christakis, 06 November 2019
B5-02	Joint Note of Eurojust and the European Judicial Network on the Practical Application of the European Investigation Order, June 2019
B5-03	European Commission, Press Release, „Security Union: Commission recommends negotiating international rules for obtaining electronic evidence", Brussels, 05 February 2019
B5-04	EURCRIM, "The European Commission's Proposal on Cross Border Access to e-Evidence – Overview and Critical Remarks" by Stanislaw Tosza, Issue 4/2018, pp. 212-219
B5-05	Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-06	Annex to the Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-07	Fair Trials, Policy Brief, „The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters", October 2018
B5-08	ECBA Opinion on European Commission Proposals for: (1) A Regulation on European Production and Preservation Orders for electronic evidence & (2) a Directive for harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Rapporteurs: Stefanie Schott (Germany), Julian Hayes (United Kingdom)
B5-09	Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, Strasbourg, 17 April 2018
B5-10	Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17 April 2018
B5-11	Non-paper from the Commission services: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward *(8 June 2017)*
B5-12	Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace *(7 December 2016)*
B5-13	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
B5-14	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130/1; 1.5.2014)
B5-15	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014
B5-16	ACPO Good Practice Guide for Digital Evidence *(March 2012)*
B5-17	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)
B5-18	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*)
B5-19	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)*
B5-20	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

B6) Criminal records, Interoperability

B6-01	Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726) (*OJ L135/85, 22.05.2019*)
B6-02	Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (*OJ L 135/85, 22.05.2019*)
B6-03	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (*OJ L 135/27, 22.05.2019*)
B6-04	Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, PE-CONS 87/1/18, Strasbourg, 17 April 2019
B6-05	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)*
B6-06	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure *(6397/5/06 REV 5; 15.1.2007)*
B6-07	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)*

B7) Conflicts of jurisdiction – *Ne bis in idem*

B7-01	Case law by the Court of Justice of the European Union on the principle of ne bis in idem in criminal matters, Eurojust, April 2020
B7-02	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*)
B7-03	European Convention on the Transfer of Proceedings in Criminal Matters (Strasbourg, 15.V.1972)

C) Procedural guarantees in the EU

C-01	Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297/1, 4.11.2016)
C-02	Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (OJ L 132 1; 21.5.2016)
C-03	Directive 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (11.3.2016; OJ L 65/1)
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	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-07	Case C-659/18, Judgement of the Court of 2 March 2020
C-08	Case C-688/18, Judgement of the Court of 3 February 2020
C-09	Case C-467/18, Rayonna prokuratura Lom, Judgment of the Court of 19 September 2019
C-10	Case C-467/18 on directive 2013/48/EU on the right of access to a lawyer in criminal proceedings, EP, Judgement of the court (Third Chamber), 19. September 2019
C-11	Case C-377/18, AH a. o., Judgment of the Court of 05 September 2019
C-12	Case C-646/17 on directive 2012/13/EU on the right to information in criminal proceedings, Gianluca Moro, Judgement of the Court (First Chamber), 13 June 2019
C-13	Case C-8/19 PPU, criminal proceedings against RH (presumption of innocence), Decision of the Court (First Chamber), 12. February 2019
C-14	Case C-646/17, Gianluca Moro, Opinion of the AG Bobek, 05 February 2019
C-15	Case C-551/18 PPU, IK, Judgment of the Court (First Chamber), 6 December 2018
C-16	Case C-327/18 PPU, RO, Judgment of 19 September 2018 (First Chamber)
C-17	Case C-268/17, AY, Judgment of the Court (Fifth Chamber), 25 July 2018
C-18	Case C-216/18 PPU, LM, Judgment of 25 July 2018 (Grand Chamber)

C-19	Joined Cases C-124/16, C-188/16 and C-213/16 on Directive 2012/13/EU on the right to information in criminal proceedings Ianos Tranca, Tanja Reiter and Ionel Opria, Judgment of 22 March 2017 (Fifth Chamber)
C-20	Case C-439/16 PPU, Emil Milev (presumption of innocence), Judgment of the Court (Fourth Chamber), 27 October 2016
C-21	Case C-278/16 Frank Sleutjes ("essential document" under Article 3 of Directive 2010/64), Judgment of 12 October 2017 (Fifth Chamber)
C-22	C-25/15, István Balogh, Judgment of 9 June 2016 (Fifth Chamber)
C-23	Opinion of Advocate General Sharpston, delivered on 10 March 2016, Case C-543/14
C-24	C-216/14 Covaci, Judgment of 15 October 2015 (First Chamber)

D) Approximating criminal law and Victims´ Rights

D1) Terrorism

D1-01	Terrorism Situation and Trend Report (TE-SAT) 2019
D1-02	Communication from the Commission to the European Parliament, the European Council and the Council, Twentieth Progress Report towards an effective and genuine Security Union, COM(2019) 552 final, Brussels, 30 October 2019
D1-03	Communication from the Commission to the European Parliament, and the Council, Towards better Implementation of the EU's anti-money laundering and countering the financing of terrorism framework, COM(2019) 360 final, Brussels, 24 July 2019
D1-04	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, L 123/18
D1-05	Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 amending Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries, L 125/4 (Text with EEA relevance)
D1-06	Council Decision (CFSP) 2019/25 of 08 January 2019 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing Decision (CFSP) 2016/1136, Brussels, 08 January 2019
D1-07	Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12.9.2018, COM(2018) 640 final
D1-08	Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327/20; 9.12.2017)
D1-09	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework

	Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88/6)
D1-10	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119/132; 4.5.2016)

D2) Trafficking in Human Beings, Migrant Smuggling and Sexual Exploitation of Children

D2-01	Regulation of the European Parliament and of the Council amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code), PE-CONS 29/19, Brussels, 15 May 2019
D2-02	European Migrant Smuggling Centre – 4th Annual Activity Report, The Hague, 15 May 2020
D2-03	Report from the European Commission to the European Parliament and the Council, Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, COM(2018) 777 final, Brussels, 03 December 2018
D2-04	UNODC – Global Study on Smuggling of Migrants 2018, Vienna/New York, June 2018
D2-05	Council Conclusions on setting the EU‘s priorities for the fight against organised and serious international crime between 2018 and 2021, Brussels, 9450/17, 19 May 2017
D2-06	Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA

D3) Cybercrime

D3-01	Internet Organised Crime Threat Assement (IOCTA) 2019
D3-02	Special Eurobarometer 480, Report, “Europeans´ Attitudes towards Internet Security”, Brussels, March 2019
D3-03	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
D3-04	Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA *(OJ L 335/; 17.12.2011*)
D3-05	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems *(OJ L 69/67; 16.3.2005*)
D3-06	Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (*OJ L 13/44; 20.1.2004*)
D3-07	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)
D3-08	Convention on Cybercrime (Budapest, 23.XI.2001)

D4) Protecting Victims´ Rights

D4-01	European Commission, Executive Summary of the Report on strengthening Victims´ Rights: From Compensation to Reparation – For a new EU Victims´ Rights Strategy 2020-2025, Report of the Special Adviser Joëlle Milquet to the President of the European Commission, Brussels, 11 March 2019
D4-02	Regulation (EU) No 606/2013 of the European Parliament and of the Council of 12 June 2013 on mutual recognition of protection measures in civil matters
D4-03	European Commission, DG Justice Guidance Document related to the transposition and implementation of 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
D4-04	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
D4-05	Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order
D4-06	Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims
D4-07	Website of the European Union Agency for Fundamental Rights (FRA) – Victims' rights
D4-08	Victim Support Europe

E) Criminal justice bodies and networks

E1) European Judicial Network

E1-01	European Judicial Network, Report on Activities and Management 2017-2018
E1-02	Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (*OJ L 348/130, 24.12.2008, P. 130*)

E2) Eurojust

E2-01	Eurojust quarterly newsletter
E2-02	Eurojust Guidelines on Jurisdiction
E2-03	Eurojust Annual Report 2019
E2-04	Guidelines for deciding on competing requests for surrender and extradition, October 2019
E2-05	Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA

E3) Europol

E3-01	Europol Report – Beyond the Pandemic – How COVID-19 will shape the serious and organised crime landscape in the EU, 30 April 2020
E3-02	Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA

E4) European Public Prosecutor's Office

E4-01	Decision 2019/1798 of the European Parliament and of the Council of 14 October 2019 appointing the European Chief Prosecutor of the European Public Prosecutor's Office (*OJ L 274/1, 28.10.2019*)
E4-02	Opinion on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) as regards cooperation with the European Public Prosecutor's Office and the effectiveness of OLAF investigations Committee on Civil Liberties, Justice and Home Affairs, Rapporteur for opinion: Monica Macovei, 11.1.2019
E4-03	German Judges' Association: Opinion on the European Commission's initiative to extend the jurisdiction of the European Public Prosecutor's Office to include cross-border terrorist offences, December 2018 (only available in German)
E4-04	Communication from the Commission to the European Parliament and the European Council: A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, Brussels, 12.9.2018, COM(2018) 641 final
E4-05	Annex to the Communication from the Commission to the European Parliament and the European Council: A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, Brussels, 12.9.2018, COM (2018) 641 final
E4-06	Council Implementing Decision (EU) 2018/1696 of 13 July 2018 on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing Enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')
E4-07	Annex to the Proposal for a Council Implementing Decision on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ("the EPPO"), Brussels, 25.5.2018, COM(2018) 318 final)
E4-08	Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')

F) Data Protection

F-01	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (4.5.2016; OJ L 119/89)

G) Police Cooperation in the EU

G1) General

G1-01	European Commission, Press Release, „Commission marks ten years of judicial and police cooperation between between Member States of the European Union", 01 December 2019
G1-02	Regulation of the European Parliament and of the Council on establishing a framework of interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726 and (EU) 2018/1862 and (EU) 2019/816 [the ECRIS-TCN Regulation], PE-CONS 31/19, Brussels, 2 May 2019
G1-03	Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU
G1-04	Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime *(OJ L 210/12; 06.08.2008)*
G1-05	Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime *(OJ L 210/1; 06.08.2008)*
G1-06	Council Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union *(OJ L 386/89; 29.12.2006, P. 89)*
G1-07	Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration of 27. May 2005 *(10900/05; 27.5.2005)*

G2) Joint Investigation Teams (JITs)

G2-01	Eurojust Information on JITs
G2-02	Third JIT Evaluation Report, Eurojust, March 2020
G2-03	Joint Investigation Teams Practical Guide (Brussels, 14 February 2017; 6128/1/17)
G2-04	Council Resolution on a Model Agreement for Setting up a Joint Investigation Team (JIT) – 2017/C18/01, Strasbourg, 19 January 2017
G2-05	Council Framework Decision of 13 June 2002 on joint investigation teams (*OJ L 162/1; 20.6.2002*)

EUROPEAN
COMMISSION

Brussels, 24.7.2020
COM(2020) 607 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

EU strategy for a more effective fight against child sexual abuse

INTRODUCTION

The EU Charter of Fundamental Rights recognises that children have the right to such protection and care as is necessary for their well-being, among other provisions. The 1989 UN Convention on the Rights of the Child establishes the right of the child to be protected from all forms of violence[1].

Child sexual abuse is a particularly serious crime that has wide-ranging and serious **life-long consequences** for victims. In hurting children, these crimes also cause **significant and long term social harm**. In many cases, children are sexually abused by persons they know and trust, and on whom they are dependent[2]. This makes these crimes particularly difficult to prevent and detect. There are indications that the **COVID-19** crisis has exacerbated the problem[3], especially for **children who live with their abusers**[4]. In addition, children are **spending more time than before online, possibly unsupervised**. While this has allowed them to continue their educational studies and stay in touch with their peers, there are signs of increased risk of children coming into contact with **online predators**[5]. With more offenders isolated at home, the **demand for child sexual abuse material** has increased (e.g. by 25% in some Member States[6]), which in turn leads to increased demand for new material, and therefore **new abuses**[7].

The Council of Europe estimates that in Europe, **one in five children fall victim** to some form of sexual violence[8]. Sexual abuse and sexual exploitation of children can take multiple forms and they can occur **both online** (e.g. forcing a child to engage in sexual activities via live streaming or exchanging child sexual abuse material online) **and offline** (e.g. engaging in sexual activities with a child or causing a child to participate in child prostitution)[9]. When the abuse is also recorded and shared online, the harm is perpetuated. Victims have to live with the knowledge that images and videos of the crimes showing the worst moments of their lives are being circulated and anyone, including their friends or relatives, may see them.

The exponential development of the digital world has been abused making this crime a **truly global one**, and has unfortunately facilitated the creation of a global market for child sexual abuse material. The past few years have seen a **dramatic increase** in reports of child sexual abuse online concerning the EU (e.g. images exchanged in the EU, victims in the EU, etc.): from 23 000 in 2010 to more than 725 000 in 2019, which included more than 3 million images and videos[10]. A similarly dramatic increase has occurred globally: from 1 million

---

1 Also of relevance for child sexual abuse in the domestic context is the Council of Europe Convention on preventing and combatting violence against women and domestic violence (CETS. 210; COM 2016(111) final).

2 This includes in particular children with disabilities living in institutional care.

3 Europol, Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, 19 June 2020.

4 WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children and UNESCO, COVID-19 and its implications for protecting children online, April 2020.

5 *Ibid.*

6 Europol, Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, 19 June 2020.

7 The number of child sexual abuse reports globally quadrupled in April 2020 (4.1 million reports) compared to April 2019 (around 1 million), as reported to the US National Centre for Missing and Exploited Children.

8 Council of Europe, One in Five campaign.

9 This strategy refers to child sexual abuse for simplicity but it should be understood as covering also child sexual exploitation and child sexual abuse material (referred to in legislation as "child pornography").

10 As reported to the US National Centre for Missing and Exploited Children (NCMEC). US law requires internet companies based in the US to report to NCMEC any instances of child sexual abuse that they find in their networks. NCMEC then forwards those reports to the relevant public authorities around the world

reports in 2010 to almost 17 million in 2019, which included nearly 70 million images and videos[11]. Reports indicate that the EU has become the **largest host of child sexual abuse material globally** (from more than half in 2016 to more than two thirds in 2019)[12].

Recently, an investigation into child sexual abuse in Germany resulted in the discovery of potentially more than 30 000 suspects using group chats and messenger services to share materials, incite each other to create new materials, and exchange tips and tricks on how to groom victims and hide their actions[13]. The use of end-to-end encryption makes identifying perpetrators more difficult if not impossible. In this particular example, to date, only 72 suspects in Germany have been identified and 44 victims.

The introduction of **end-to-end encryption**, while beneficial in ensuring privacy and security of communications, also facilitates the access to secure channels for perpetrators where they can hide their actions from law enforcement, such as trading images and videos. The use of encryption technology for criminal purposes therefore needs to be **immediately addressed** through possible solutions which could allow companies to **detect and report** child sexual abuse in end-to-end encrypted electronic communications. Any solution would need to ensure both the privacy of electronic communications and the protection of children from sexual abuse and sexual exploitation, as well as the protection of the privacy of the children depicted in the child sexual abuse material.

The fight against child sexual abuse is **a priority for the EU**. The European Parliament[14] and the Council[15] have both called for further concrete action. Similar calls have been made globally in multiple forums[16], including by the media[17], as it has become evident that the world as a whole is **losing the battle** against these crimes, and is failing to effectively protect the right of each child to live free from violence. The EU therefore needs to **reassess** and **strengthen its efforts**.

The aim of this strategy is to provide an effective response, at EU level, to the fight against child sexual abuse. It provides a framework for **developing a strong and comprehensive response** to these crimes, both in their **online and offline** form. It sets out **eight initiatives** to implement and develop the right legal framework, strengthen the law enforcement response and catalyse a coordinated multi-stakeholder action in relation to **prevention, investigation** and **assistance to victims**. The initiatives make use of all **tools available** at EU level, both as regards **substantive EU law** (section I) and as regards **funding and cooperation** (section II)[18]. This strategy is to be implemented over the next five years (2020-2025)[19].

---

for action. As the largest internet companies are based in the US, NCMEC de facto centralises the reporting of child sexual abuse globally.

11 *Ibid*.

12 Internet Watch Foundation, Annual Reports of 2016 to 2019.

13 BBC, Germany investigates 30,000 suspects over paedophile network, 29 June 2020; Frankfurter Allgemeine, Die schockierende Zahl des Tages: 30.000 Verdächtige, 29 June 2020.

14 Resolution on the 30th anniversary of the UN Convention on the Rights of the Child, November 2019.

15 Council conclusions on combating the sexual abuse of children, October 2019.

16 For example, at the December 2019 summit of the WePROTECT Global Alliance to End Child Sexual Exploitation Online, or by the "Five Eyes" (US, UK, Canada, Australia and New Zealand) in July 2019.

17 See, for example, the series of New York Times articles published from September 2019 to February 2020, which exposed to the public the depth and complexity of the problem.

18 See the roadmap for this Communication for more details on the targeted consultations conducted.

19 The implementation of this strategy will be coordinated with the implementation of other relevant strategies that the Commission has recently adopted or will soon adopt, including on the rights of the child, on victims' rights, on trafficking in human beings, on security union and on gender equality.

I. IMPLEMENT AND DEVELOP THE RIGHT LEGAL FRAMEWORK TO PROTECT CHILDREN

In 2011, the EU took an important step with the adoption of the Child Sexual Abuse Directive (2011/93/EU[20]), whose **implementation** in Member States now has to be finalised as a matter of **urgency**. In parallel, any identified legislative gaps need to be addressed through the most appropriate means.

1. Ensure complete implementation of current legislation (Directive 2011/93/EU)

The Child Sexual Abuse Directive was the first **comprehensive EU legal instrument** establishing minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children and child sexual abuse material, covering the prevention, investigation and prosecution of offences, and assistance to and protection of victims.

The criminal offences cover **offline and online** situations such as viewing and distributing child sexual abuse material online, grooming (i.e. establish an emotional connection with the child online with the purpose of sexual abuse) and webcam sexual abuse. Beyond substantive and procedural criminal law, the Directive also requires Member States to put in place extensive administrative (i.e. non-legislative) measures, such as on the exchange of criminal records between Member States via the European Criminal Records Information System (ECRIS) as part of the pre-recruitment screening for positions involving direct and regular contacts with children, or training of professionals likely to come into contact with child victims of sexual abuse. These measures require the involvement and coordination of **multiple actors** from various areas of government (e.g. law enforcement, healthcare, education, social services, child protection authorities, judiciary and legal professionals), as well as private entities (e.g. industry and civil society).

Member States have made **substantial progress** in implementing the Directive. However, there is still considerable scope for the Directive to reach its full potential through the **complete implementation** of all of its provisions by Member States. Challenges remain in the areas of **prevention** (in particular prevention programmes for offenders and for people who fear that they might offend), **criminal law** (especially the definition of offences and level of penalties), and **assistance, support and protection** measures for **child victims**[21]. In 2019, to ensure complete implementation, the Commission opened **infringement procedures** against 23 Member States[22].

The Commission will continue to work closely with Member States to resolve all remaining issues **as a matter of priority** and ensure complete implementation of and full compliance

---

20 Directive 2011/93/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, OJ L 335, 17.12.2011. For simplicity, the document refers to this as "Child Sexual Abuse Directive".

21 For more details, see the 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/2016/0871 final, as well as the 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/2016/0872 final.

22 All Member States except DK (not bound by the Directive), and CY, IE and NL (with which dialogue on conformity is ongoing).

with the Directive across the EU. The Commission will also support Member States' work in this area by continuing to facilitate the **exchange of best practices** and lessons learned[23].

Key action:

⇨ *Member States must **finalise the implementation** of the Child Sexual Abuse Directive **as a matter of priority**. The Commission will continue to make use of its **enforcement powers** under the Treaties through infringement procedures as necessary to ensure swift implementation.*

2. Ensure that EU legislation enables an effective response

The Commission will assess whether the **Child Sexual Abuse Directive** needs to be updated, taking into account the study referred to in initiative #3 below. In addition to the Child Sexual Abuse Directive, there are multiple **legislative instruments at EU level** that support and shape the fight against child sexual abuse, notably when it comes to the role that the private sector plays in preventing and combating child sexual abuse.

The **e-evidence proposals**[24], put forward by the Commission in April 2018, play a key role in facilitating swift access to key evidence held by the private sector, such as the identity of individuals who have uploaded and shared child sexual abuse material. The Commission reiterates its call for **swift adoption**.

In addition, the relevant framework includes the **e-commerce Directive**[25], which determines the existing liability rules for online intermediaries and allows for the notice and takedown mechanisms for illegal content and the **e-privacy Directive**[26]. The Commission's proposal for a **Regulation on Privacy and Electronic Communications**[27], currently being discussed by the European Parliament and the Council, will update the legal framework and replace the ePrivacy Directive. As from December 2020, the e-privacy Directive will have an extended scope as a result of the **Electronic Communications Code**[28]. This would prevent certain companies (in the absence of national legislative measures adopted in accordance with Article 15(1) of the e-privacy Directive) from continuing their own measures on voluntary detection, removal and reporting of child sexual abuse online. The Commission considers that it is essential to take **immediate action** to address this. It will therefore propose a narrowly-

---

[23] Since 2017 the Commission has organised six expert workshops to support Member States in implementing the Directive. Another workshop on prevention will take place by Q4 2020.

[24] Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225; and
Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226.

[25] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000.

[26] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002.

[27] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (Regulation on Privacy and Electronic Communications), COM/2017/010 final.

[28] Directive (EU) 2018/1972 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018 This Directive extends the scope of the e-privacy Directive to over the top (OTT) inter-personal communication services such as messenger services and email. The ePrivacy Directive does not contain a legal basis for voluntary processing of content and traffic data for the purpose of detecting child sexual abuse. Providers can only apply such measures if based on a national legislative measure, that meets the requirements of Article 15 of the Directive (proportionality etc.), for restricting the right to confidentiality. In the absence of such legislative measures, measures to detect child sexual abuse undertaken by these providers, which process content or traffic data, would lack a legal basis.

targeted legislative solution with the sole objective of allowing current voluntary activities to continue. This solution would allow the time necessary for the adoption of a new longer-term legal framework, while ensuring the respect of fundamental rights, including the rights to privacy and the protection of personal data.

The Commission has committed to make proposals on the legislative framework for digital services, which would have implications for tackling child sexual abuse material online. The **Digital Services Act** package, to be proposed by end of 2020[29], will clarify and upgrade liability and safety rules for digital services. In this context, the Commission will consider the need to remove disincentives for voluntary actions to address illegal content, goods or services intermediated online, in particular in what concerns online platform services.

The Commission considers that the fight against child sexual abuse online requires clear **mandatory obligations** to detect and report child sexual abuse online to bring more clarity and certainty to the work of both law enforcement and relevant actors in the private sector to tackle online abuse. It will start preparing **sector-specific legislation** in order to tackle child sexual abuse online more effectively, in full respect of fundamental rights, including in particular the right to freedom of expression, protection of personal data and privacy. Mechanisms to ensure accountability and transparency will be key elements of the legislation in which the centre referred to in initiative # 6 could be involved.

The **Europol Regulation**[30], which determines the scope of Europol's activities, is also of relevance[31]. The Commission has announced in its 2020 work programme a legislative proposal to strengthen **Europol's mandate** in order to improve operational police cooperation. Europol has encountered **limits** in the support it can provide because of the rapidly growing challenge of child sexual abuse. In addition, Europol's ability to support the Member States is **hampered by its inability to receive personal data directly from the private sector**, whose infrastructure is abused by perpetrators to host and share child sexual abuse material. The European Commission will further assess these issues as part of the upcoming **review of the Europol mandate**, planned for adoption in Q4 2020.

These possible legislative changes will be **consistent** with the EU's policy on combating child sexual abuse and should ensure that there is a legislative framework to enable and support relevant stakeholders in **preventing**, **detecting, reporting and acting effectively to protect children** in any instance of child sexual abuse.

---

[29] The Commission launched an open public consultation on the Digital Services Act package on 2 June 2020.

[30] Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol), OJ L 135, 24.5.2016. The Eurojust Regulation (Regulation (EU) 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust) OJ L 295/138, 21.11.2018) is also of relevance.

[31] Also relevant in this framework are:

- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, an in particular Articles 6, 23 and Recital 50.
- Directive (EU) 2018/1808 of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), in view of changing market realities, OJ L 303, 28.11.2018, has introduced new rules requiring that platforms act responsibly with regard to the third party content they host with a view to better protecting the public from the dissemination of specific illegal or harmful content (including child sexual abuse material).

Key actions:

- ⇨ *In a first stage, **as a matter of priority**, the Commission will propose the necessary legislation to ensure that providers of electronic communications services can continue their current voluntary practices to detect in their systems child sexual abuse after December 2020.*
- ⇨ *In a second stage, by Q2 2021, the Commission will propose the necessary legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities.*

3. Identify legislative gaps, best practices and priority actions

The transposition measures that Member States have communicated to the Commission include measures that are not specifically required by the Child Sexual Abuse Directive but which were considered as needed in the fight against child sexual abuse by Member States[32]. This suggests that there might be relevant issues that the Directive **does not sufficiently address**. The Commission convened an expert workshop in September 2019 to gather more information about those possible legislative gaps and concluded that further work was required to gather additional evidence.

As the Directive was adopted in 2011, there should also be an assessment of its **implementation in practice**, in terms of effectiveness, efficiency, relevance, coherence and EU added value, among other criteria. This assessment should consider in particular the **online aspects** of these crimes, where doubts exist as to whether the present framework is **fit for purpose after 9 years** that have seen significant technological changes and the exponential growth of online sharing. Technology has made it easier than ever before for perpetrators to make contact with children, share images of abuse, hide their identity and profits, and conspire with each other to avoid accountability and commit further crimes[33].

Furthermore, offenders have become increasingly sophisticated in their use of technology and technical capabilities including **encryption** and **anonymity** (e.g. peer-to-peer file sharing and the use of darknet). This criminal activity creates problems for society in general and for law enforcement in particular in its role of protecting society[34].

In light of the above, the Commission will launch as a matter of priority a **study to identify legislative and implementation gaps, best practices and priority actions** at EU level, assessing:

- whether the current EU legislation solves the **issues for which it was put in place**; and
- whether there are **new issues** in relation to these crimes that the current legislation addresses **only partially or not at all.**

The study will take into account the ongoing work by the **Council of the EU** to ensure the effective implementation of its October 2019 conclusions on combatting child sexual abuse,

---

[32] For example, measures mandating employers in professions that involve direct and regular contact with children to request the criminal records of candidates when recruiting for a position.

[33] ECPAT.org - What we do, accessed on 5 April 2020.

[34] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2019; Independent Inquiry into Child Sexual Abuse, The Internet Investigation Report 2020; Virtual Global Taskforce Online Child Sexual Exploitation, 2019 Environmental Scan.

which could lead to the creation or update of national action plans to coordinate action at national level. It will also take into account the November 2019 **European Parliament** resolution[35], the December 2017 European Parliament's report on the transposition of the Child Sexual Abuse Directive[36], and the work of the Council of Europe's Lanzarote Committee[37].

Key action:

⇨ *The Commission will launch by the end of 2020 an extensive study **to identify legislative gaps, best practices and priority actions** at EU level in the fight against child sexual abuse **online and offline**.*

II. STRENGTHEN THE LAW ENFORCEMENT RESPONSE AND ENHANCE COOPERATION AMONG ALL STAKEHOLDERS

The fight against child sexual abuse needs to be fought on many fronts, including by society at large. Real progress can only be made when work is stepped up in relation to prevention, reporting, referral, investigation, protection and identification, treatment and follow-up of each and every case. Social services, health-care professionals, academics, researchers, educators, the judiciary, law enforcement, children, families, NGOs, media and broader society each have a role to play, in a true multi-stakeholder, multi-disciplinary approach.

4. Strengthen law enforcement efforts at national and EU level

Child sexual abuse requires a **competent and comprehensive** law enforcement response, both at national and at European level. The **COVID-19** crisis has brought to light the need to improve the **digital capabilities** of law enforcement and judicial authorities to preserve their ability to protect citizens effectively, as the May 2020 Recovery Plan highlighted[38].

Law enforcement agencies in Member States vary in structure when it comes to addressing child sexual abuse. To ensure the protection of children within and beyond their borders, it is important that Member States can rely on **specialised units that are properly equipped and staffed with well-trained officers** in national policing structures. In response to a recent wave of large-scale cases, a number of Member States have chosen to increase their staff working on preventing and combating child sexual abuse, which the Commission warmly welcomes.

As part of these units, Member States should consider setting up national **victim identification** teams. Where these teams already exist, Member States should consider extending the national level capacity to the relevant regional and local teams.

To fight these crimes effectively, Member States should also be able to participate in **collaborative EU and international efforts to identify children** with Europol's European Cybercrime Centre (EC3) or through the International Child Sexual Exploitation (ICSE) database hosted at Interpol. The resources each Member State assigns to counter the threat of child sexual abuse should also take into account the country's capacity to support international collaboration in this area.

---

35 European Parliament Resolution of 26 November 2019 on children's rights on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child, 2019/2876(RSP).

36 European Parliament Report on the implementation of Directive 2011/93/EU, December 2017.

37 https://www.coe.int/en/web/children/lanzarote-committee.

38 Europe's moment: Repair and Prepare for the Next Generation, COM(2020) 456.

Child sexual abuse cases, especially those involving digital materials, are rarely limited to one Member State. In addition to maintaining national intelligence databases, Member States should therefore invest in **systematically** channelling relevant intelligence to **Europol**, as a central **EU criminal information hub**, to support each other in tackling cross-border cases[39].

Effectively fighting child sexual abuse also requires **cutting edge technical capacities**. Some national investigation teams lack the necessary knowledge and/or tools e.g. to detect child sexual abuse material in a vast number of seized photos or videos, to locate victims or offenders, or to conduct investigations in the darknet or in peer to peer networks. To **support the development of national capacities to keep up with technological developments**, the Commission provides funding to Member States through the **Internal Security Fund** (ISF-Police)[40]. In addition, the Commission also provides funds under **ISF-Police** through Union Actions, which include, for example, calls for proposals and procurement to fight the **online and offline** aspects of child sexual abuse[41]. A **new call for proposals** in the area of combatting child sexual abuse will take place by the end of **2020.** The Commission also funds **research** projects under **Horizon 2020** to support the development of national capacities (in law enforcement and other areas) to fight against child sexual abuse[42]. Future calls for proposals to fight these crimes will open under the new **Horizon Europe** framework programme on research and innovation[43].

The use of **online undercover investigation** techniques is an important asset in infiltrating the networks that are concealed behind this kind of technology. These methods have proven very effective in understanding offender behaviour and interaction on online service providers, and have ultimately facilitated the shutting down of communication channels used by these offenders, as well as their prosecution. An increasingly important need for law enforcement activity in these spaces is the ability to effectively **infiltrate** particularly dangerous online groups of offenders. This can be enabled through a number of different methods that are currently only available to a small number of Member States and non-EU partners. Consideration should be given to making this capability available across the EU to more effectively target these offenders without being dependent on other partners. EU values and fundamental rights shall stay in the core of any future measures.

Europol will set up an **Innovation Hub and Lab**[44] to facilitate Member State access to technical tools and knowledge developed at EU level. This initiative will also allow the identification of needs in Member States to tackle the challenges of digital investigations, which will help determine the allocation of EU funding for research, innovation and development of police capacities.

The Innovation Hub and Lab will further facilitate Member States' access to the resources and experience of **Europol's European Cybercrime Centre (EC3).** EC3 has played an important role in supporting Member States in combating sexual abuse of children, ever since its creation. This support takes various forms, for example:

- EC3 has contributed to **victim identification** efforts since 2014. Collaborative actions with the Member States and partners with operational agreements through the Europol

[39] Cross-border cases may require the support of Eurojust. Also, it is important that judicial authorities are trained to handle child sexual abuse cases, including on the online aspects of the problem.
[40] More information is available here.
[41] Examples of projects funded in the 2018 call for proposals include AviaTor, 4NSEEK and VERBUM SAT.
[42] Examples of projects include ASGARD, GRACE, LOCARD and INSPECTr.
[43] See here for an example of call for proposals on research, open until 22 August 2020.
[44] As discussed in the Justice and Home Affairs Council, 7-8 October 2019.

Victim Identification Task Forces[45] and use of various investigative approaches including the ICSE database have led to the identification of **almost 360 children and 150 offenders**.

- Europol (frequently in cooperation with **Eurojust**) has helped coordinate numerous **successful investigations**[46].
- Specific Operational Action Plans (OAPs) on combating child sexual abuse and exploitation, are implemented each year under the **EU Policy Cycle** / EMPACT for the fight against serious and international organised crime, supported by Europol[47].
- Europol has been instrumental in the gathering, collation and publication of reports such as the **Serious and Organised Crime Threat Assessment (SOCTA)**[48] and **Internet Organised Crime Threat Assessment (IOCTA)**[49] reports, which include specific sections on the fight against child sexual abuse.
- Europol has also worked with its international partners to provide online safety advice for parents and carers[50] to help keep children safe online during the COVID19 crisis, in addition to three weekly intelligence reports for targeted audiences [51].

Key action:

⇨ *Europol will set up an **Innovation Hub and Lab** and the Commission will provide **funding** to facilitate the development of **national capacities** to keep up with technological developments and ensure an effective response of law enforcement against these crimes.*

5. Enable Member States to better protect children through prevention

Some of the articles of the Child Sexual Abuse Directive in which Member States are incurring in more delays to fully implement are those that require putting in place **prevention programmes**[52], where multiple types of stakeholders need to take action.

As regards prevention targeted at (potential) offenders, Member States' difficulties concern programmes at **all stages**: before a person offends for the first time, in the course of or after criminal proceedings, and inside and outside prison.

Research into what motivates individuals to become offenders **is scarce and fragmented** and the **communication between practitioners and researchers is minimal:**

- The current **lack of research** makes it difficult to **draw up and put in place** effective programmes at all stages. The few programmes that are in place[53] are **rarely evaluated** to assess their effectiveness.

---

45 More information is available in these press releases from Europol of 27/05/2019 and 25/10/2019.

46 See for example these press releases from Europol of 12/03/2020, 31/03/2020, and 21/04/2020, as well as Eurojust Annual Report 2019, e.g. p.13.

47 May 2017 Council conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021.

48 The latest SOCTA report is available here.

49 The latest IOCTA report is available here.

50 More information is available here.

51 Other important initiatives at EU level on protecting children during COVID 19 include the Betterinternetforkids.eu COVID19 campaign.

52 In particular Articles 22, 23 and 24. For more details, see the 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/2016/0871 final.

- In addition, the various types of **practitioners** in this field (e.g. responsible authorities providing prevention programmes for people who fear that they might offend, public authorities in charge of prevention programmes in prisons, NGOs offering prevention programmes to support the reintegration in the community of sex offenders) **do not communicate sufficiently** with each other on the effectiveness of the programmes, including **lessons learned and best practices**.

To address these difficulties, the Commission will work on setting up a **prevention network** of relevant and reputed **practitioners and researchers** to support Member States in putting in place **usable, rigorously evaluated and effective** prevention measures to decrease the prevalence of child sexual abuse in the EU and **facilitate the exchange of best practices**. Specifically, the network would:

1. Enable a **virtuous cycle** of **practice to research and research to practice**:

   - Researchers would provide practitioners with **scientifically tested** initiatives, and practitioners would provide researchers with **continuous feedback** on the prevention initiatives to further contribute to strengthen the evidence base. **Victims' perspectives** and views would be also brought into the network's work.

   - Although the network' work would cover all areas related to preventing child sexual abuse, it would have a strong focus on **prevention programmes for offenders and for people who fear that they might offend**, as this is the area where Member States struggle the most.

   - It is known that not all offenders have a paedophilic disorder[54] (other motivations to offend include exploitation for financial gain), and not everyone who has a paedophilic disorder ends up being an offender (some people seek support in dealing with their paedophilia). Substantial **research** is needed to understand **the process** by which a person ends up offending, including **risk factors and triggers.** Some statistics suggest that up to 85% of those who view child sexual abuse images also physically abuse children[55]. Viewing child sexual abuse material is also a criminal offence, which generates demand for new material and therefore new physical abuse[56].

   - The network would follow a **scientific approach** to prevention. Although prevalence data is scarce, studies indicate that around **3%** of the male population could have a paedophilic disorder. Practitioners recognise that **tackling the problem at its root** by acknowledging that difficult fact and putting in place preventive measures, is the most effective way to protect victims and alleviate the workload of law enforcement authorities.

2. Support Member States' work to raise awareness by creating focused **media campaigns a**nd **training** materials:

---

53 For an overview of prevention programmes in the EU and third countries, see Di Gioia R., Beslay, L. (2018) Fighting child sexual abuse: prevention policies for offenders – Inception Report, EUR 29344 EN, doi:10.2760/48791.

54 In a self-report survey with a sample of 1,978 young adult males from Sweden, 4.2 % reported they had ever viewed child sexual abuse material (Seto, et al, 2015). In another self-report survey with a sample of 8,718 adult males in Germany, 2.4% of respondents reported using that material (Dombert, et al, 2016).

55 https://childrescuecoalition.org/the-issue/.

56 The Atlantic, *I, Pedophile*, David Goldberg, 26 August 2013.

- It would facilitate the exchange of information on **training materials and capacity building** and collect **'best practice' examples** to inspire **media campaigns** and training across Member States. It would help **avoid duplication** of efforts by, e.g. facilitating the adaptation and translation to the national context of materials created in other Member States.

- The Commission, supported by the network, would also launch and support **awareness raising campaigns** to help inform children, parents, carers and educators about risks and preventive mechanisms and procedures. These would be developed with the network.

- **Prevention efforts** are necessary in relation to **organisations that work with children** – sports centres and clubs, religious institutions, healthcare services, schools, afterschool activities – to **raise awareness** and to inform them about ways to prevent abuse, e.g. by providing focused **training**[57], ensuring they have in place appropriate procedures and making use of their legal empowerment under EU law to request criminal records across borders via the European Criminal Records Information System[58]. This highly effective EU system is crucial in the prevention of sexual abuses as it allows to make background checks of an individual's possible criminal history when recruiting for professional or organised voluntary activities involving direct and regular contacts with children. Professionals from all sectors, who might come in contact with children, need to be trained and equipped with the tools to **prevent and detect** early signs of possible sexual violence and abuse, and to interact with children and their families in an appropriate manner, driven by the specific needs and the best interests of the child. This also includes **law enforcement authorities and the judiciary** where child victims are involved in criminal investigations against their abusers. Families and carers, professionals and broader society need to understand the seriousness of these crimes and the devastating effect they have on children, and be given the support needed to report these crimes and support child victims. This requires **specialised information, media campaigns** and **training**.

- Children themselves need to have the **knowledge and tools** that could help them not to be confronted with the abuse when possible (e.g. on how to use the web safely), and they need to be informed that certain behaviours are not acceptable. The Commission-funded network of Safer Internet Centres[59] raises awareness on online safety and provides information, resources and assistance via helplines and hotlines on a wide range of digital safety topics including grooming and sexting[60]. The One in Five campaign by the Council of Europe[61] and Europol's "#SayNo" initiative[62] are further examples of how this can be done. When abuse occurs, children need to **feel secure and empowered** to speak up, react and report[63], even when the abuse comes from within their circle of trust (i.e. loved ones or other people they know and trust), as it is often the case. They also need to have access to safe, accessible and age-appropriate channels to report the abuse without fear. Prevention efforts also need to take into account the **specific circumstances and needs of various groups of**

---

57 See, for example, Erasmus+, the EU's programme to support education, training, youth and sport in Europe.
58 European Criminal Records Information System (ECRIS). More information is available here.
59 More information is available here.
60 See for example the Irish Safer Internet Centre here.
61 More information is available here.
62 More information is available here.
63 The upcoming Digital Education Action Plan will also cover child sexual abuse online.

children who are particularly exposed to the risks of sexual abuse, such as children with disabilities[64], children in migration (in particular unaccompanied minors) and children victims of trafficking (the majority of whom are girls).

The aim is to organise the network in **working groups** that will facilitate the exchange of best practices and the work on concrete initiatives to generate tangible output. The working groups could be organised **by practice** (i.e. by professional background, e.g. healthcare practitioners, social workers, education practitioners, law enforcement, judicial authorities, prison authorities, policy makers and researchers) and **by programme** (i.e. by type of target group of the prevention programme, e.g. offenders and people who fear that they might offend, or training and awareness raising programmes for children, families and the community).

Maximising work to prevent child sexual abuse is essential. The exponential increase of child sexual abuse reports **has overwhelmed law enforcement** in the EU and globally, reaffirming the consensus among practitioners (including law enforcement) that **this problem is impossible to solve through law enforcement action only and requires multi-agent coordination.**

The network would aim at **strengthening the capacity in the EU** on prevention of child sexual abuse and would have a **global reach** to draw on all relevant expertise **within and outside of the EU**. It would also have an important **online presence** to facilitate sharing its work within the EU and globally so that all countries could benefit from state-of-the-art research and approaches.

In summary, the prevention network would enable: a) more effective **action** in the fight against child sexual abuse (**online and offline**) in the EU; b) more effective and efficient **use of the existing (limited) resources** in the EU allocated to preventing child sexual abuse; and c) more effective **cooperation with partners globally**, so that the EU can benefit from global expertise without duplicating efforts.

Key action:

⇨ *The Commission will start **immediately** to prepare a prevention network at EU level to facilitate the exchange of best practices and support Member States in putting in place **usable, rigorously evaluated and effective** prevention measures to decrease the prevalence of child sexual abuse in the EU.*

6. A European centre to prevent and counter child sexual abuse

The Commission will start working towards the possible creation of a European centre to prevent and counter child sexual abuse, based on a thorough study and impact assessment. The centre would **provide holistic support to Member States** in the fight against child sexual abuse, **online and offline**, ensuring **coordination** to maximise the efficient use of resources and **avoiding duplication** of efforts.

The **European Parliament** called for the creation of a centre in its November 2019 **resolution**[65], and **Member States** highlighted in their October 2019 Council conclusions the need for a **coordinated and multi-stakeholder approach**[66]. The centre could build on the best practices and lessons learned from **similar centres around the world**, such as the

[64] EU Fundamental Rights Agency Report: Violence against children with disabilities, 2015.
[65] November 2019 Resolution on the 30th anniversary of the UN Convention on the Rights of the Child.
[66] October 2019 Council conclusions on combating the sexual abuse of children.

National Centre for Missing and Exploited Children (NCMEC) in the US, the Canadian Centre for Child Protection and the Australian Centre to Counter Child Exploitation.

To ensure **holistic support** to Member States in the fight against child sexual abuse, and subject to further assessment, the centre's functions could cover **three areas**:

1. **Law enforcement**: Europol is a key actor in the fight against child sexual abuse, notably through the analysis and channelling of reports of abuse received from the U.S. Building on Europol's role and experience, the centre could work with law enforcement agencies in the EU and in third countries to ensure that victims are identified and assisted as soon as possible and that offenders are brought to justice. It could support Member States by receiving reports in relation to child sexual abuse in the EU from companies **offering their services in the EU**, ensure the relevance of such reports, and forward these to law enforcement for action. The centre could also support companies by, for example, maintaining a **single database** in the EU of known child sexual abuse material to facilitate its detection in companies' systems, in compliance with EU data protection rules. In addition, the centre could also support law enforcement by coordinating and facilitating the takedown of child sexual abuse material online identified through **hotlines**.

   The centre could operate according to strict control mechanisms to ensure **accountability and transparency**. In particular, the centre could potentially play a role in helping ensure that there is no erroneous takedown or abuse of the search tools to report legitimate content (including misuse of the tools for purposes other than the fight against child sexual abuse) and in **receiving complaints** from users who feel that their content was mistakenly removed. Accountability and transparency will be key elements of the legislation referred to in the key actions of initiative #2.

2. **Prevention**: building on the work of the prevention network, the centre could support Member States in putting in place **usable, rigorously evaluated and effective** multi-disciplinary prevention measures to decrease the prevalence of child sexual abuse in the EU, taking account of differing vulnerabilities of children according to their age, gender, development and specific circumstances. It could facilitate **coordination** to support the most efficient use of resources invested and expertise available on prevention across the EU, **avoiding duplication** of efforts. A **hub for connecting, developing and disseminating research and expertise**, it could facilitate and encourage dialogue among all relevant stakeholders and help develop **state-of-the-art research and knowledge, including better data**. It could also **provide input to policy makers** at national and EU level on prevention gaps and possible solutions to address them.

3. **Assistance to victims**: the centre could work closely with national authorities and global experts to ensure that **victims** receive **appropriate and holistic support**, as the Child Sexual Abuse Directive and the Victims' Rights Directive[67] require[68]. It could also work on supporting the **exchange of best practices** on protection measures for child victims. It could also support Member States by **carrying out research** (e.g. on short and long-term

[67] Directive 2012/29/EU of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, OJ L 315, 14.11.2012. This Directive complements with general victims' rights the specific provisions for victims of child sexual abuse contained in the Child Sexual Abuse Directive.

[68] To ensure a coherent approach to EU victims' rights policy, the centre could also cooperate with the Victims' Rights Platform set up under the EU Strategy on victims' rights (2020-2025), COM/2020/258 final.

effects of child sexual abuse on victims) to **support evidence-based policy** on assistance and support to victims and serving **as a hub of expertise** to help coordinate better and avoid duplication of efforts. The centre could also **support victims in removing their images and videos** to safeguard their privacy, including through **proactively searching** materials online and notifying companies[69].

The centre could **bring together all the initiatives** in this strategy by enabling **more effective cooperation** between public authorities (including law enforcement), industry and civil society in the EU and globally, and becoming the **reference entity in the EU for expertise** in this area:

- **Legislation-focused initiatives**: the centre could **assist with its expertise the Commission** on its role to support Member States on the implementation of the Child Sexual Abuse Directive. This expertise, which would increase with time as the centre continues to identify gaps and best practices in the EU and beyond, would facilitate **evidence-based policy** by the Commission that could also ensure that EU legislation is up to date to enable an effective response.
- **Cooperation and funding-focused initiatives**: working closely with the Commission and similar centres in other countries and with the WePROTECT Global Alliance to end child sexual exploitation, the centre could ensure that all Member States have **immediate and centralised access to global best practices**, and that children around the world can benefit from EU's best practices. The centre could also draw on the results of the **prevention network**, and the experience of the Safer Internet Centres.

The Commission will work closely with the European Parliament and Member States to **explore the various implementation options**, including **making use of existing structures** for the centre's functions where appropriate, with a view to maximising the centre's added-value, effectiveness, and sustainability. The Commission will carry out an **impact assessment**, with a study to be launched immediately, to identify the best way forward including the best funding mechanisms and legal form that this centre should take.

Key action:

⇨ *The Commission will launch **immediately** a study to work towards the creation of a European centre to prevent and counter child sexual abuse to enable a **comprehensive and effective** EU response against child sexual abuse **online and offline**.*

7. Galvanise industry efforts to ensure the protection of children in their products

Providers of certain online services are **uniquely well placed** to prevent, **detect and report** child sexual abuse that occurs using their infrastructure or services.

At present, a number of companies voluntarily detect child sexual abuse. NCMEC received almost **17 million** reports of child sexual abuse from those companies in 2019 alone[70]. These reports include not only abusive images and videos but also situations that pose an **imminent danger to children** (e.g. details of arrangements to meet to physically abuse the child or suicide threats by the child following blackmail by the offender). These reports have been

[69] The centre could also serve as an advocate for child victims to ensure that their voices are heard and taken into account in policymaking at EU and national level, raising awareness of children's rights and of child victims' needs.

[70] See here the list of companies that reported to NCMEC in 2019, and the number of reports submitted by each of them.

instrumental for years in **rescuing children in the EU from ongoing abuse**. They have led to, for example:

- the rescue of 11 children, some as young as 2 years old, who were exploited by a network of abusers in Sweden[71];
- the single largest operation ever against child sexual abuse in Denmark[72];
- the rescue of a 9 year-old girl in Romania, who had been abused by her father for more than a year[73];
- the rescue of a 4 year-old girl and her 10 year-old brother in Germany, who had been abused by their father[74];
- the arrest of an offender in France who groomed 100 children to obtain child sexual abuse material from them[75];
- the rescue of 2 girls in Czechia, abused by a 52 year-old man, who recorded the abuse and distributed it online[76].

The efforts that companies make to detect and report child sexual abuse **vary significantly**. In 2019, a single company, **Facebook**, sent almost 16 million reports (94% of the total that year), while other US-based companies sent fewer than 1 000 reports, and some fewer than 10[77].

Last year, Facebook announced plans to implement **end-to-end encryption** by default in its instant messaging service. In the absence of accompanying measures, it is estimated that this could reduce the number of total reports of child sexual abuse in the EU (and globally) by **more than half**[78] and **as much as two-thirds**[79], since the detection tools as currently used do not work on end-to-end encrypted communications.

Given the key role that certain online services play in the distribution of child sexual abuse material, and the actual and potential importance of the industry in the fight against child sexual abuse, it is essential that it **takes responsibility** for protecting children in its products, in line with EU fundamental rights, including on privacy and personal data protection.

In 2020, the Commission has begun work on supporting industry efforts in the fight against child sexual abuse online under the **EU Internet Forum.** The forum, which brings together all EU Home Affairs Ministers, high-level representatives of major internet companies, the European Parliament and Europol, has served since 2015 as a model for a successful cross-sector collaboration in the fight against terrorist content online and has now expanded to also cover child sexual abuse online.

In addition to continuing to support the fight against terrorist content online, the EU Internet Forum will provide a **common space to share best practices and the challenges** that private and public actors encounter in their fight against child sexual abuse online, to **increase**

---

71 Swedish Cybercrime Centre SC3, Swedish Police.
72 2018 Internet Organised Crime Threat Assessment, Europol, page 32.
73 As reported in the Romanian media, see here and here.
74 As reported by the German Federal Police (BKA).
75 As reported by the French police.
76 As reported by the Czech police.
77 National Centre for Missing and Exploited Children, 2019 Reports by Electronic Service Providers.
78 National Centre for Missing and Exploited Children, End-to-end encryption: ignoring abuse won't stop it.
79 The New York Times, An Explosion in Online Child Sex Abuse: What You Need to Know, 29/09/2019.
80 2019 Internet Organised Crime Threat Assessment, Europol, page 34.

mutual understanding and find solutions together. It will also enable **high-level political coordination** to maximise the efficiency and effectiveness of actions across the EU.

One of the specific initiatives under the EU Internet Forum in 2020 is the creation of a technical **expert process** to map and assess possible solutions which could allow companies to **detect and report** child sexual abuse in **end-to-end encrypted electronic communications**, in full respect of fundamental rights and without creating new vulnerabilities criminals could exploit. Technical experts from academia, industry, public authorities and civil society organisations will examine possible solutions focused on the device, the server and the encryption protocol that could ensure the privacy and security of electronic communications and the protection of children from sexual abuse and sexual exploitation.

Key action:

⇨ *Under the **EU Internet Forum**, the Commission has launched an expert process with industry to map and preliminarily assess, **by the end of 2020**, possible technical solutions to **detect and report** child sexual abuse in **end-to-end encrypted electronic communications,** and to address **regulatory and operational** challenges and opportunities in the fight against these crimes.*

8. Improve protection of children globally through multi-stakeholder cooperation

Child sexual abuse is **a global reality** across all countries and social groups and it happens both **offline and online**. It is estimated that, at any given moment, across the world there are more than **750 000 predators online** exchanging child sexual abuse material, streaming live abuse of children, extorting children to produce sexual material or grooming children for future sexual abuse[81].

The following map shows the real time downloads in a given day of **a sample** of child sexual abuse material[82]:

[81] U.N. General Assembly, Human Rights Council, Report of the Special Rapporteur on the sale of children, child prostitution and child pornography, 13 July 2009.

[82] Child Rescue Coalition, real time downloads of a sample of child sexual abuse material on 13 July 2020. The different colours of the dots indicate different networks from which the material was downloaded.

There is also evidence that offenders **travel to third countries** to take advantage of more lenient legislative frameworks or fewer enforcement capacities and to commit abuse without fearing law enforcement. The ability to require those who commit sexual offences against children to **register** and comply with certain conditions imposed by the court or probation services after their release from prison plays an important role in protecting children[83].

The Commission has **supported global efforts** through multi-stakeholder cooperation[84] for years, well aware that **it takes a network to defeat a network**. One example is the Commission-funded **ICSE database**, hosted at Interpol, which holds more than 1.5 million images and videos and has helped identify **20 000 victims worldwide**, through the collaborative efforts of the more than 60 countries (and Europol) that are connected to it[85]. The Commission also co-funds the **INHOPE** network of hotlines[86] from more than 40 countries to facilitate the removal of child sexual abuse material online anonymously reported by the public[87]. The Commission will continue supporting global action with funding to enhance international cooperation. In particular, the EU will continue to support the EU-UN

[83] See recital 43 of the Child Sexual Abuse Directive (2011/93).

[84] For example, the Alliance to better protect minors online brings together the European Commission, leading ICT and media companies, NGOs and UNICEF to improve the online environment for children and young people by focusing on user empowerment, enhanced collaboration, and awareness raising.

[85] Interpol's International Child Sexual Exploitation database, as of May 2019.

[86] For over 20 years, as part of the Safer Internet policy (see European Strategy for a Better Internet for Children, COM/2012/0196, Pillar 4), the EU has supported cooperation between law enforcement, internet industries and NGOs, in the EU and globally, to combat this crime, including with EU funding to hotlines.

[87] Commission funding to the hotlines and to the central hashes database "ICCAM" is currently provided under Connecting Europe Facility; future funding has been proposed by the Commission under Digital Europe Programme. The hotlines analyse the reports and the location of hosting service providers, and forward details of confirmed CSAM to the relevant law enforcement agency, for criminal investigation and victim identification, and to the hosting service providers for content removal. See here for more information.

Spotlight Initiative[88], to prevent and eliminate all forms of violence against women and girls across five regions around the globe[89].

In 2012, the Commission co-founded with the competent US authorities the Global Alliance Against Child Sexual Abuse Online[90], which brought together 54 countries to improve victim protection, identify and prosecute offenders, raise awareness, and reduce the availability of child sexual abuse material online. This initiative merged with a similar one from the UK, WePROTECT, created in 2014, which brought governments together with industry and NGOs. In 2016, both initiatives agreed to join forces and form the **WePROTECT Global Alliance** to End Child Sexual Exploitation Online, which currently includes 97 governments, 32 global technology companies, 33 civil society organisations and international institutions, and 5 regional organisations[91]. At the end of 2019, the organisation became an **independent legal entity** in the form of a foundation with limited liability, set up in the Netherlands.

The WePROTECT Global Alliance has advanced countries' commitment towards a more coordinated response to the global fight against child sexual abuse, based on global threat assessments, and a model national response. These have helped to clarify the challenges and assist member countries in setting achievable practical goals.

The Commission will continue to support the alliance as a member **of its policy board**, given its **co-founder** status, including with funding. This will allow the Commission to **ensure coherence** with global initiatives (in particular regulatory ones), which in turn will support and strengthen the effectiveness of actions within the EU by providing Member States access to global best practices. In particular, by participating in the policy board of the WePROTECT Global Alliance, the Commission actively contributes to increase standards for the protection of children, the identification of perpetrators, and support for child victims across the globe. This facilitates the EU's efforts to share best practices with and to support national authorities in third countries in implementing international standards in the online space (i.e. protection of children), in line with the EU Action Plan on Human Rights and Democracy 2020-2024[92]. The Commission has supported this type of global cooperation for years and considers the WePROTECT Global Alliance as the central organisation for coordinating and streamlining **global** efforts and regulatory improvements, and bringing about a more effective global response.

Key action:

⇨ *The Commission will continue contributing to **increase global standards** for the protection of children against sexual abuse by promoting multi-stakeholder cooperation through the **WePROTECT Global Alliance**, and through dedicated **funding**.*

NEXT STEPS

This strategy presents a framework to respond in a comprehensive way to the increasing threat of child sexual abuse, both in its **online and offline** form. This strategy will be the reference framework for EU action in the fight against child sexual abuse for the **2020-2025**

88 More information about the Spotlight Initiative is available here.

89 The EU will also engage with civil society organisations (Joining Forces Initiative) in Sub-Saharan Africa to reduce levels of violence, abuse, exploitation and neglect against children and adolescents, especially in countries most affected by COVID-19.

90 More information about the Global Alliance Against Child Sexual Abuse Online is available here.

91 As of 17 June 2020. More information about WePROTECT Global Alliance is available here.

92 More information about the EU Action Plan on Human Rights and Democracy 2020-2024 is available here.

period. It will also inform related Commission initiatives such as the **EU strategy on the rights of the child**, to be adopted in early 2021.

The Commission will **work closely** with companies, civil society organisations, academia, practitioners, researchers, law enforcement and other public authorities, and other relevant stakeholders, in the EU (including the European Parliament and the Council) and globally, during the coming months and years to ensure an **effective exploration and implementation** of the **eight initiatives presented in the strategy**.

The right **legal framework** should be implemented to enable an effective response, including on investigations, prevention and assistance to victims, by the relevant actors, including companies.

Child sexual abuse is a complex issue that requires the **maximum cooperation** from all stakeholders, which have to be able, willing, and ready to act. The Commission will **spare no efforts** to ensure that this is the case, given the **urgent need** to take **effective action**.

Our children are our present and our future. The Commission will continue using all available tools to ensure that **nothing steals that future** from them.

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

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

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.

EUROPOL

INTERNET ORGANISED CRIME THREAT ASSESSMENT

2020

IOCTA
[2020]

get.password+

launch.attack

EUROPOL

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020

www.europol.europa.eu

Contents

Foreword

Catherine De Bolle
Executive Director of Europol

I am pleased to introduce the Internet Organised Crime Threat Assessment (IOCTA) 2020.

The IOCTA is Europol's flagship strategic product highlighting the dynamic and evolving threats from cybercrime. It provides a unique law enforcement-focused assessment of emerging challenges and key developments in the area of cybercrime. We are grateful for the many contributions from our colleagues within European law enforcement community and to our partners in the private industry for their input to the report. Combining law enforcement and private sector insights allows us to present this comprehensive overview of the threat landscape.

The data collection for the IOCTA 2020 took place during the lockdown implemented as a result of the COVID-19 pandemic. Indeed, the pandemic prompted significant change and criminal innovation in the area of cybercrime. Criminals devised both new modi operandi and adapted existing ones to exploit the situation, new attack vectors and new groups of victims.

The analysis for the IOCTA 2020 clearly highlights cybercrime as a fundamental feature of the European crime landscape. Cybercrime remains among the most dynamic forms of crime encountered by law enforcement in the EU. While ransomware, business email compromise and social engineering are familiar cybercrime threats, their execution evolves constantly and makes these criminal activities more complex to detect and to investigate. Ransomware in particular remains a priority threat encountered by cyber investigators across the EU. The amount of online child sexual abuse material detected continues to increase, further exacerbated by the COVID-19 pandemic, which has had serious consequences for the investigative capacity of law enforcement authorities.

Europol is at the forefront of law enforcement innovation and offers various policing solutions in relation to encryption, cryptocurrencies and other challenges. The European Cybercrime Centre (EC3) at Europol is the platform of choice for cybercrime investigators across the EU and beyond to connect, collaborate and communicate.

The case studies illustrating this report demonstrate the necessity and effectiveness of international law enforcement cooperation in tackling cybercrime as well as the vital role played by private-public partnerships in this area. Europol provides an ideal framework for these different stakeholders to come together, exchange information and take concerted action.

Cybercrime affects citizens, businesses and organisations across the EU. Europol plays a key role in countering cybercrime by working with our many partners in law enforcement and the private sector and by offering innovative solutions and effective, comprehensive support to investigations. I hope this analysis can inform effective responses to these evolving threats and make Europe safer.

Abbreviations

AaaS Access-as-a-Service

AI Artificial Intelligence

ATM Automated teller machine

BEC Business email compromise

BPH Bulletproof hosting

CaaS Cybercrime-as-a-Service

C&C Command & control

CNP Card-not-present

CSAM Child sexual abuse material

CSE Child sexual exploitation

DDoS Distributed Denial of Service

DNS Domain Name System

DoH DNS over HTTPs

E-commerce Electronic commerce

EC3 Europol's European Cybercrime Centre

E-skimming Electronic skimming

GDPR General Data Protection Regulation

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

HTTPs Hypertext Transfer Protocol Secure

IOCTA Internet Organised Crime Threat Assessment

IoT Internet of Things

IP Internet protocol

ISP Internet service provider

IT Information technology

J-CAT Joint Cybercrime Action Taskforce

KYC Know your customer

LDCA Live distant child abuse

MaaS Malware-as-a-Service

NCMEC The National Center for Missing and Exploited Children

OTP One time password

PC Personal computer

PGP Pretty Good Privacy

POS Point of sale

P2P Peer-to-peer

RaaS Ransomware-as-a-Service

RATs Remote access tools

RDP Remote desktop protocol

SIM Subscriber identity module

SQL Structured query language

Tor The onion router

VIDTF Victim Identification Taskforce

VPN Virtual private network

VPS Virtual private server

2FA Two-factor authentication

Executive summary

The threat landscape over the last year described in the IOCTA 2020 contains many familiar main characters. The starring roles in terms of priority threats went to the likes of social engineering, ransomware and other forms of malware. Several interviewees captured the essence of the current state of affairs of the threat landscape by stating: cybercrime is an evolution, not a revolution. As time passes, the cyber-element of cybercrime infiltrates nearly every area of criminal activity. Key elements mentioned in previous editions of the IOCTA that return this year merit more, rather than less, attention. The repetition means the challenge still exists and has, in many cases, increased, underlining the need to further strengthen the resilience and response to well-known threats. The IOCTA 2020 makes clear that the fundamentals of cybercrime are firmly rooted, but that does not mean cybercrime stands still. Its evolution becomes apparent on closer inspection, in the ways seasoned cybercriminals refine their methods and make their artisanship accessible to others through crime as a service.

The COVID-19 crisis illustrated how criminals actively take advantage of society at its most vulnerable. Criminals tweaked existing forms of cybercrime to fit the pandemic narrative, abused the uncertainty of the situation and the public's need for reliable information. Across the board from social engineering to Distributed Denial of Service (DDoS) attacks and from ransomware to the distribution of child sexual abuse material (CSAM), criminals abused the crisis when the rest of society was trying to contain the situation. The opportunistic behaviour of criminals during the pandemic, however, should not overshadow the overall threat landscape. In many cases, COVID-19 caused an amplification of existing problems exacerbated by a significant increase in the number of people working from home. This is perhaps most noticeable in the area of child sexual abuse and exploitation. As in previous years, the amount of online CSAM detected continues to increase, further exacerbated by the COVID-19 crisis, which has had serious consequences for the investigative capacity of law enforcement authorities. In addition, livestreaming of child sexual abuse increased and became even more popular during the COVID-19 crisis; a recent case shows production also takes place in the EU.

Data compromise once more features as a central aspect throughout a number of threats. Both law enforcement and private sector representatives consistently report on social engineering among the top threats. With regard to social engineering, in particular phishing, cybercriminals are now employing a more holistic strategy by demonstrating a high level of competency when exploiting tools, systems and vulnerabilities, assuming false identities and working in close cooperation with other cybercriminals. However, despite the trend pointing towards a growing sophistication of some criminals, the majority of social engineering and phishing attacks are successful due to inadequate security measures or insufficient awareness of users. In particular, as attacks do not have to be necessarily refined to be successful.

The developments in the area of non-cash payment fraud over the past twelve months reflect the overall increase in sophistication and targeting of social engineering and phishing. Fuelled by a wealth of readily available data, as well as a Cybercrime-as-a-Service (CaaS) community, it has become easier for criminals to carry out highly targeted attacks. As a result, law enforcement and industry continue to identify well-established frauds as a major threat.

Subscriber identity module (SIM) swapping is one of the new key trends this year, having caused significant losses and attracted considerable attention from law enforcement. As a highly targeted type of social engineering attack, SIM swapping can have potentially devastating consequences for its victims, by allowing criminals to bypass text message-based (SMS) two-factor authentication (2FA) measures gaining full control over their victims' sensitive accounts.

Business Email Compromise (BEC) continues to increase. As criminals are more carefully selecting their targets, they have shown a significant understanding of internal business processes and systems' vulnerabilities. At the same time, certain other forms of fraud have entered the spotlight due to the sheer number of victims they have generated.

The spread of online investment fraud all over Europe is not necessarily new but has generated increased law enforcement attention as victims at times lose their life savings to professional organised criminal groups that have incorporated cyber elements into their scams.

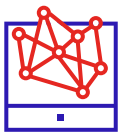
The clear majority of law enforcement respondents once again named ransomware as a top priority threat. Although this point has been made in past editions of the IOCTA, ransomware remains one of the, if not the, most dominant threats, especially for public and private organisations within as well as outside Europe. Considering the scale of damage that ransomware can inflict, victims also appear to be reluctant to come forward to law enforcement authorities or the public when they have been victimised, which makes it more difficult to identify and investigate such cases. Criminals continued making their ransomware attacks increasingly targeted. Ransomware has shown to pose a significant indirect threat to businesses and organisations, including in critical infrastructure, by targeting supply chains and third-party service providers. Perhaps one of the most crucial developments is the new way of pressuring victims to pay by stealing and subsequently threatening to auction off victims' sensitive data.

Besides ransomware, European law enforcement reported malware in the broader sense to be widely present in cybercrime cases. Criminals have converted some traditional banking Trojans into more advanced modular malware to cover a broader scope of functionality. These evolved forms of modular malware are a top threat in the EU, especially as their adaptive and expandable nature makes them increasingly more complicated to combat effectively.

With a range of threat actors, this makes drawing general conclusions about particular threats challenging. In areas ranging from social engineering and phishing, to ransomware and other forms of malware, law enforcement authorities witness a broad spectrum of threat actors. These actors vary in terms of level of skill, capability and adaptability. The top tier criminals manage to run their operations like a professional enterprise, whereas less sophisticated threat actors tend to rely on off-the-shelf materials to conduct their criminal activities. The availability of the materials through CaaS, however, continues to make such activities accessible. Moreover, across the board threat actors in different types of cybercrime demonstrate their resilience. Perhaps more importantly, in areas such as the Darkweb, criminals have enhanced their cooperation and joined forces to provide a response to shared challenges. This means they are able to make their business more robust and in particular incorporate better security solutions to ensure that law enforcement are unable to trace them. Overall, cybercriminals are showing an improved level of operational security and proving to be highly aware of how to hide their identities and criminal activities from law enforcement or private sector companies. With cryptocurrencies, criminals also manage to complicate law enforcement's ability to trace payments connected to criminal activities.

To respond to the cybercrime challenges in a more effective manner, a number of key ingredients are essential. First, information sharing is at the heart of any strategic, tactical and operational response regardless of the specific type of cybercrime. Sharing information, which needs to be purpose-driven and actionable, requires reliable coordination and cooperation from public and private partners. At the same time, information sharing requires a legal framework and attitude that is sensitive to the timely exchange of information, which is crucial as cybercriminals can move their infrastructure within the blink of an eye. This is particularly evident in the criminal abuse of the Darkweb, where short lifecycles of marketplaces influences law enforcement's ability to conduct investigations. There is also the need to foster a culture of acceptance and transparency when organisations or individuals fall victim to cybercrime. Re-victimising victims after a cyber-attack is counterproductive and a significant challenge, as law enforcement need companies and individuals who have been subject of a crime to come forward. This can help resolve the challenges in reporting we currently face. Besides information sharing through enhanced coordination and cooperation, other key elements to include in an effective response are prevention and awareness and capacity building. We can reduce the success rate of many forms of cybercrime by educating individuals and organisations in recognising criminal activity before they fall victim to it. It is worth underlining the importance of the responsibility of industry in integrating security and privacy in their design as fundamental principles, instead of shaming end users as the weakest link. Through capacity building, on the other hand, law enforcement across different crime areas will be able to understand and respond to the cyber-element of crimes. Finally, taskforce work such as coordinating and de-conflicting law enforcement operational response, for which the Europol Joint Cybercrime Action Taskforce (J-CAT) platform is vital, continues to play a key role in the current cybercrime landscape.

Key findings



CROSS-CUTTING CRIME FACILITATORS AND CHALLENGES TO CRIMINAL INVESTIGATIONS

- Social engineering remains a top threat to facilitate other types of cybercrime.
- Cryptocurrencies continue to facilitate payments for various forms of cybercrime, as developments evolve with respect to privacy-oriented crypto coins and services.
- Challenges with reporting hinder the ability to create an accurate overview of crime prevalence across the EU.

CYBER-DEPENDENT CRIME

- Ransomware remains the most dominant threat as criminals increase pressure by threatening publication of data if victims do not pay.
- Ransomware on third-party providers also creates potential significant damage for other organisations in the supply chain and critical infrastructure.
- Emotet is omnipresent given its versatile use and leads the way as the benchmark of modern malware.
- The threat potential of DDoS attacks is higher than its current impact in the EU.

CHILD SEXUAL EXPLOITATION ONLINE

- The amount of online CSAM detected continues to increase, further exacerbated by the COVID-19 crisis, which has serious consequences for the capacity of law enforcement authorities.
- The use of encrypted chat apps and industry proposals to expand this market pose a substantial risk for abuse and make it more difficult for law enforcement to detect and investigate online CSE activities.
- Online offender communities exhibit considerable resilience and are continuously evolving.
- Livestreaming of child sexual abuse continues to increase and became even more prevalent during the COVID-19 crisis.
- The commercialisation of online CSE is becoming a more widespread issue, with individuals uploading material to hosting sites and subsequently acquiring credit on the basis of the number of downloads.

PAYMENT FRAUD

- SIM swapping is a key trend that allows perpetrators to take over accounts and has demonstrated a steep rise over the last year.
- BEC remains an area of concern as it has increased, grown in sophistication, and become more targeted.
- Online investment fraud is one of the fastest growing crimes, generating millions in losses and affecting thousands of victims.
- Card-not-present (CNP) fraud continues to increase as criminals diversify in terms of target sectors and electronic skimming (e-skimming) modi operandi.

THE CRIMINAL ABUSE OF THE DARKWEB

- The Darkweb environment has remained volatile, lifecycles of Darkweb market places have shortened, and no clear dominant market has risen over the past year compared to previous years to fill the vacuum left by the takedowns in 2019.
- The nature of the Darkweb community at administrator-level shows how adaptive it is under challenging times, including more effective cooperation in the search for better security solutions and safe Darkweb interaction.
- There has been an increase in the use of privacy-enhanced cryptocurrencies and an emergence of privacy-enhanced coinjoin concepts, such as Wasabi and Samurai.
- Surface web e-commerce sites and encrypted communication platforms offer an additional dimension to Darkweb trading to enhance the overall business model.

Introduction

Aim

The IOCTA aims to inform decision-makers at strategic, tactical and operational levels about the threats of cybercrime. The 2020 IOCTA contributes to setting priorities for the 2021 EMPACT operational action plans, which follow the three current priorities defined as:

1) disrupting criminal activities related to attacks against information systems, particularly those following CaaS business models and working as enablers for online crime;

2) combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material;

3) targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present (CNP) fraud), emerging threats to other non-cash means of payment and enabling criminal activities. Furthermore, the IOCTA aims to consolidate findings on current cyber threats, which could contribute to the discussion of research and development priorities as well as planning at the EU-level.

Scope

The scope of the 2020 IOCTA lies in the threat assessment of the cybercrime landscape, consisting of trends and developments pertinent to the EMPACT priorities mentioned previously. In addition to this, the report will discuss other cross-cutting facilitators and challenges 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 the EU and beyond.

Methodological approach

For this year's IOCTA, Europol introduced a different methodological approach to gather data. For previous editions, the team shared a survey with all the Member States and several third-party countries. Each crime priority area received a survey, namely cyber-dependent crime, payment fraud, and child sexual exploitation (CSE). This year, as a means to gather more qualitative and in-depth information, the team conducted interviews with representatives from the Member States and Europol partner countries. The team also conducted interviews with Europol experts from the European Cybercrime Centre (EC3) and members of EC3's three advisory groups on internet security, financial services and telecommunication providers.

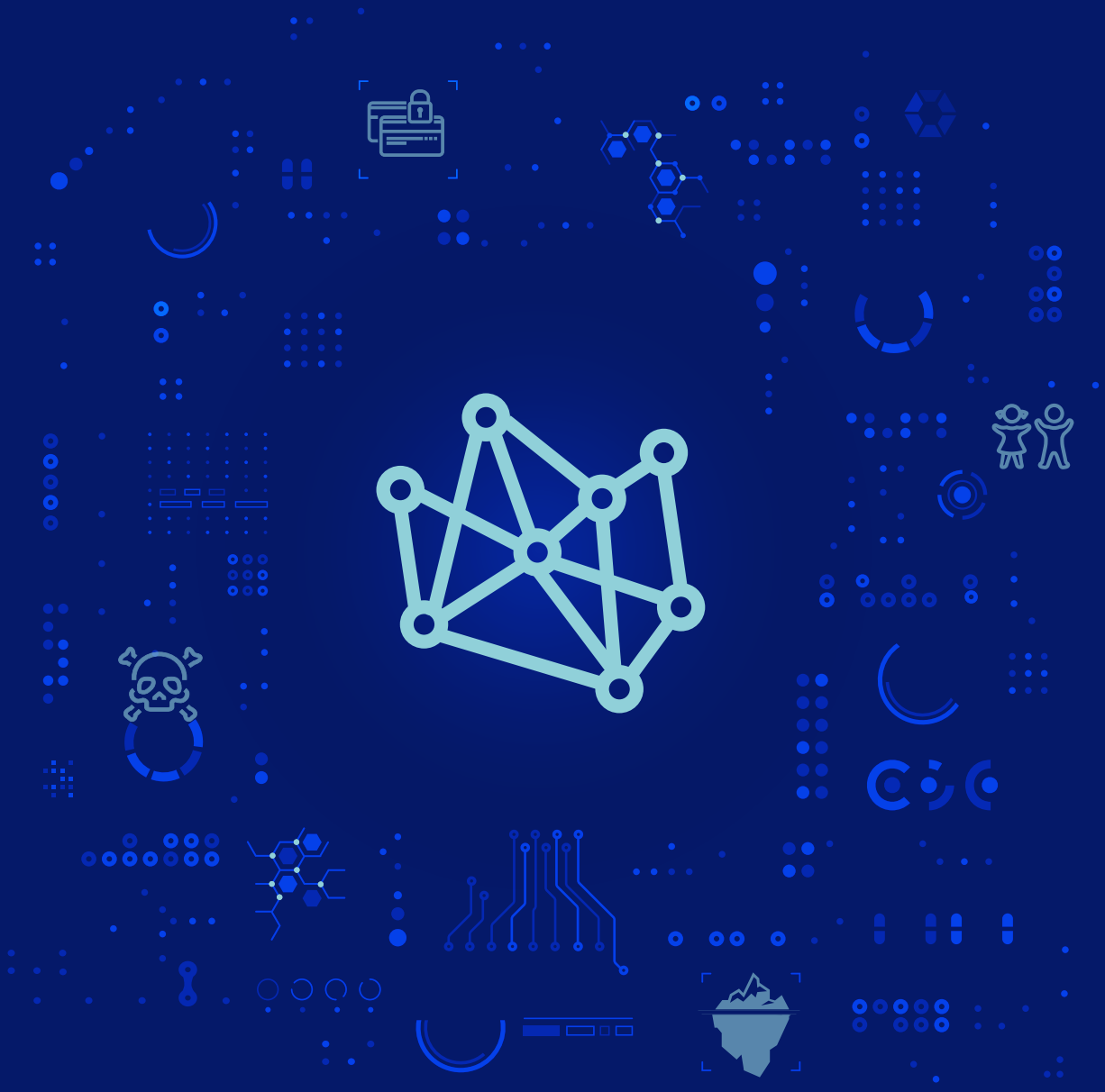
The semi-structured interviews contained open questions. As a result, the range of answers was broader than in the previous structured survey approach wherein which respondents mainly selected from a drop down menu. Through using open questions, answers became less comparable in a traditional sense, but rather than a limitation, the team perceived this is an opportunity to illustrate the complexity of cybercrime especially in connection to establishing a comprehensive threat assessment. The ultimate purpose of the IOCTA is to assist Member States in establishing priorities with respect to cybercrime. This pertains to the type of threats but also concerns other considerations such as how we approach this crime area in terms of analysis.

Cybercrime is inherently complex for a number of reasons. With different perpetrators, different motives, different targets, varying modi operandi, different jurisdictions, etc. there are many variables, which complicate both the ability to gather data as well as the ability to compare findings. Furthermore, the quality of those findings encounter challenges as a result of the ability to register them accurately. These limitations must be taken into consideration with respect to any threat landscape report.

Acknowledgements

Europol would like to extend thanks to all law enforcement and private sector partners who contributed to this report.

1 Cross-cutting crime facilitators and challenges to criminal investigations



KEY FINDINGS

- Social engineering remains an effective top threat to enable other types of cybercrime.
- Cryptocurrencies continue to facilitate payments for various forms of cybercrime, as developments evolve with respect to privacy oriented crypto coins and services.
- Challenges with reporting torment ability to create an accurate overview of crime prevalence across the European Union.

1.1 INTRODUCTION

Throughout the interviews, one message was clear: cybercrime is an evolution not a revolution[1]. The fundamentals of cybercrime stay the same, in that cybercrime is not that much different to other forms of more traditional crime.

This is a crucial observation to include in any assessment, especially as the emphasis when discussing cybercrime is often placed on how quickly cybercrime and, in particular, cybercriminals change their tactics. Perpetrators may operate at the speed of the internet, as they are able to quickly move parts of their infrastructure, alter a particular aspect of the code, adapt the functionality, gather more victim data, etc, but these changes do not inherently alter the threat, especially not at an abstract level at which we discuss the threats within the IOCTA. We can also witness the evolution of cybercrime through the integration of the cyber-component into nearly all forms of traditional crime.

Another reason to reflect on this observation is to understand that to combat cybercrime effectively we need to respond to several challenges. Some of these are included within this chapter of the report, whereas others are included within the respective chapters of the different crime areas. Several of these challenges pertain to the ability of law enforcement to execute its core mission of preventing and combatting crime, identifying suspects, protecting victims and arresting perpetrators.

This chapter contains three key components. First, a reflection on overarching threats that are cross-cutting facilitators for other forms of cybercrime. The second part includes a brief description of a general challenge with respect to gathering (accurate) data about the prevalence of specific forms of cybercrime. The third and final part focuses on challenges which pertain to law enforcement agencies' ability to conduct criminal investigations due to societal developments that criminals opportunistically manage to exploit.

1.2 COVID-19 DEMONSTRATES CRIMINAL OPPORTUNISM

While discussions and models have emerged over several decades surrounding the threats posed by a pandemic crisis, the outbreak of COVID-19 has demonstrated the unfortunate impact potential of such crises on our daily lives across the globe. As physical lockdowns became the norm, cybercrime became more popular than before. There is no denying that the arrival of COVID-19 was a crucial factor in any development discussed with respect to 2020. However, COVID-19 in connection to cybercrime needs to be placed within its context. If anything, COVID-19 demonstrated how cybercrime – at its core – remains largely the same but criminals change the narrative. They adapt the specifics of their approach to fit the societal context as a means to enhance their rate of success. This is not new, in many ways this is business as usual. The difference with COVID-19 is that due to the physical restrictions enacted to halt the spread of the virus, with a subsequent increase in working from home and remote access to business resources, many individuals and businesses that may not have been as active online before the crisis became a lucrative target.

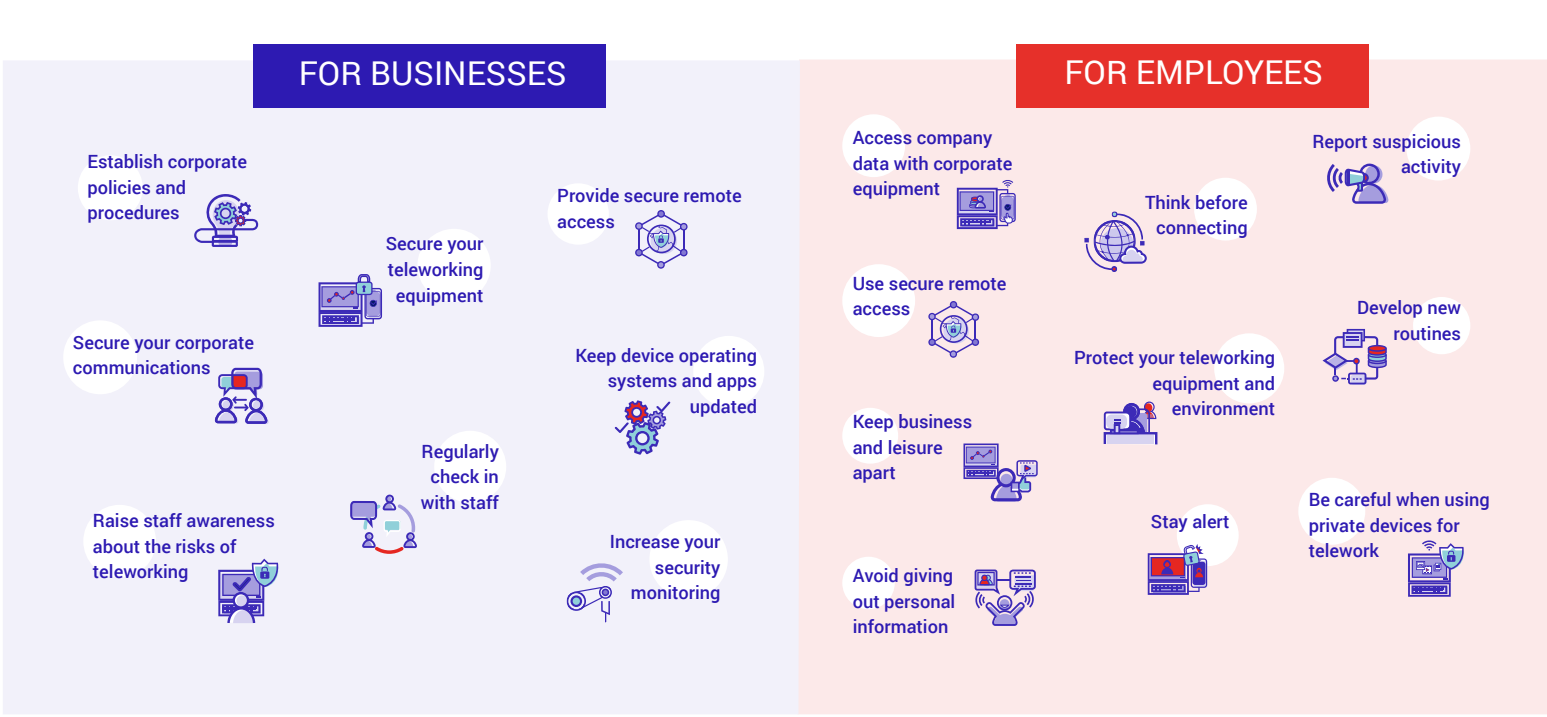
Traditional cybercrime activities such as phishing and cyber-enabled scams quickly exploited the societal vulnerability as many citizens and business were looking for information, answers and sources of help during this time. There were even more challenges for both individuals and business as teleworking during the pandemic became the norm. Europol followed all developments closely and shared its findings through frequent *corona strategic reports*[2].

Spread of disinformation enhances cybercrime opportunities

The pandemic also gave rise to disinformation campaigns and activities. Disinformation efforts are often associated with hybrid threats, which are defined as threats combining conventional and unconventional, military and non-military activities which may be used by non-state or state actors to achieve political aims[3]. A wide range of measures applied in hybrid campaigns include cyber-attacks and disinformation, disruption of critical services, undermining of public trust in governmental institutions and exploiting social vulnerabilities. The presence of disinformation became a crucial feature in the overall threat landscape during the crisis. Many Member States reported problems with respect to the spread of disinformation.

Users become vulnerable and receptive to disinformation and fake news due to the paradoxical oversaturation with available information combined with a perceived lack of trustworthy sources of news that reinforce some of the users' preconceived notions and beliefs. Disinformation can also be linked to cybercrime in efforts to make social engineering and phishing attacks more impactful.

Both seasoned cybercriminals and opportunistic individuals spread disinformation to benefit from it in different ways. Significant political motives can drive disinformation to influence elections or referendums affecting entire countries. However, for criminals the



ultimate aim is always to obtain profit. Some individuals simply seek to obtain direct financial gain through digital advertisements, as engagement with fake news messages about COVID-19 can be very high. The number of new domains and websites related to COVID-19 soared at the start of the pandemic[4].

Another strategy to profit financially from the COVID-19 crisis was to spread fake news about potential cures for the virus or effective prevention measures. Such messages also facilitated criminals seeking to sell items that they claim will help prevent or cure COVID-19, which emerged both on the Clearnet and the Darkweb.

The hybrid nature of this threat underlines the importance of a combined, hybrid response, especially considering that law enforcement agencies are not typically mandated with investigating cases involving disinformation or fake news, despite their potential to bolster criminal activities.

1.3 DATA COMPROMISE

The majority of threats discussed within the IOCTA ultimately pertain to some form of data compromise. As a result, data compromise is not dealt with as a separate category within the different chapters but rather emphasised within this cross-cutting chapter. Data compromise gathers significant attention through the obligation of organisations to report data breaches under the General Data Protection Regulation (GDPR). GDPR considers the protection of data belonging to EU citizens, thus it has an 'extra-territorial effect' applying to companies outside the EU who handle data relating to EU visitors[5]. Since the enactment of GDPR, over the past 18 months over 160 000 data breach notifications have been handed in to authorities[6], and a growth in interest over personal data handling among EU citizens[7]. In its annual data breach investigations report, Verizon reports how the company collected 157 525 incidents and 108 069 breaches[8]. The authors, however, immediately place these figures within their proper context as 100 000+ of those breaches concerned credentials of individual users. These are breaches where criminals target the users' credentials to gain access to bank accounts, cloud services, etc.

Data compromise therefore can refer to the ability of criminals to access individual user credentials or to access large databases with potentially valuable information. Examples of the latter include data breaches at companies that often become public knowledge. Both of these situations are not mutually exclusive, and often form a starting point for subsequent criminal activity. The majority of interviewees from law enforcement authorities and private sector representatives mentioned social engineering as a top threat, which cuts across different crime areas, affecting both cyber-dependent and cyber-enabled crime and illustrates the key role played by data compromise.

Social engineering

Social engineering and phishing remain a key threat. Based on interviewee responses, both demonstrate a significant increase in volume and sophistication. While some of the increase may be attributable to improved reporting mechanisms, it has also become

Law enforcement case study

European law enforcement conducted an investigation of ten cases of fraud related to technical support scams. The perpetrators initially communicated mainly via telephone with their victims, pretending to be technicians at a software company support centre. Under the pretext that their computer and/or mobile device are "infected" by malware, criminals asked the victims to install remote access software to allegedly solve the issue. In this way, the criminals gained full access to the computer or mobile device and consequently to the - stored on the devices - personal data. Through use of the personal data, the perpetrators transferred money from the electronic bank accounts (e-banking) to bank accounts controlled by themselves or their accomplices. In many cases, they even demanded the installation of remote management programmes on the victims' mobile phones, so that they could receive text messages (SMS) with the one-use codes (OTPs), which financial institutions send for security reasons. The investigation identified four individuals who were active or involved as money mules.

easier for technically inexperienced criminals to carry out phishing campaigns using existing criminal infrastructure and support services – a trend that is expected to continue in the future.

Targeting human weakness in the security chain, social engineering and phishing have a high impact on society and enable the majority of cybercrimes, ranging from scams and extortion to the acquisition of sensitive information and the execution of advanced malware attacks.

While criminals typically employ social engineering to convince targets to engage in fraudulent schemes unknowingly, criminals use phishing to either distribute malware or to obtain credentials and gain access to sensitive accounts and systems.

More sophisticated and more targeted phishing

A key trend over the past year relates to the growing sophistication[9] of phishing. Phishing has become more difficult to detect, with many phishing emails and sites being almost identical to the real ones. At the same time, phishing campaigns have become faster and more automated, forcing respondents to act quicker than before as in some cases it takes one day from a credential leak to an attack.

Overall, cybercriminals are employing a more holistic strategy to phishing by showing a high level of competency concerning the use of tools, systems and vulnerabilities they exploit, assuming false identities and working in close cooperation with other cybercriminals. Regarding the latter, criminals have shown their sense for innovation, as they use shared platforms to distribute their scams, which makes blocking or tracing difficult for incident responders. Criminals have also been observed maintaining a level of situational awareness, with a number of phishing campaigns having taken advantage of the COVID-19 pandemic[10].

Further to this, criminals have also employed a much more targeted approach when attacking their victims. Advanced actors focus more on selected victims as opposed to a random group in order to optimise financial gains, as they are becoming increasingly specialised in information gathering and victim profiling activities. As the main threat relates to spear phishing, criminals have proven apt at adapting their attacks to a specific context for fraud schemes in particular, for instance by improving their language skills or even using local 'customer agents' who communicate with their victims speaking their regional accents, or by making reference to current cultural, political, and local events.

In addition to employing a targeted approach, cybercriminals are adopting a more agile approach, constantly looking to harvest data and sensitive information from victims, which they can use to enable additional crimes. Lack of security awareness and a significant amount of open-source intelligence surrounding personal information of employees of businesses available online enable criminals to gather the information they need. Other forms of personal information harvested and abused by criminals may include financial and personal details, as well as login credentials for various sensitive accounts.

The majority of social engineering and phishing attacks are successful due to inadequate security measures potentially in combination with a lack of awareness by the users. Particularly the latter was highlighted repeatedly, as attacks do not have to be necessarily complicated or advanced to be successful – badly set up attacks still succeed by exploiting people as the weak part of the security chain. Accordingly, basic cyber hygiene and improved user awareness are some of the key success factors in curbing part of this threat.

Finally, cybercriminals are demonstrating an improved overall level of operational security and proving to be highly aware of how to hide their identities and criminal activities from law enforcement or private sector companies. In some cases, once a phishing attempt is being investigated, the whole criminal infrastructure has already vanished. Similarly, criminals may put in place technical measures to avoid suspicion. Through their deny/allow[11] lists of internet protocol (IP) addresses, for instance, criminals may forward the user to the genuine website if certain conditions are met (i.e. access through a computer, instead of a mobile phone, or from foreign IP address). As such, only the users selected as targets by criminals are re-routed to the phishing site.

CaaS as a facilitator of phishing and other forms of cybercrime

Cybercrime-as-a-Service (CaaS) facilitates phishing. Offerings on the Darkweb help criminals significantly improve overall technical complexity of their attacks without the need for advanced technical understanding. In recent years, CaaS has increasingly enabled even technically inexperienced criminals to carry out phishing campaigns by providing exploit kits, access to compromised systems and vulnerable remote desktop protocols (RDPs).

Here, criminals have also been reported to make increased use of legitimate commercial services such

Bust of hacker group selling databases with millions of user credentials

Polish and Swiss law enforcement authorities, supported by Europol and Eurojust, dismantled InfinityBlack, a hacking group involved in distributing stolen user credentials, creating and distributing malware and hacking tools, and fraud.

On 29 April 2020, the Polish National Police searched six locations in five Polish regions and arrested five individuals believed to be members of the hacking group InfinityBlack. Police seized electronic equipment, external hard drives and hardware cryptocurrency wallets, all worth around €100 000. The police closed down two platforms with databases containing over 170 million. The hacking group created online platforms to sell user login credentials known as 'combos'. The group was efficiently organised into three defined teams. Developers created tools to test the quality of the stolen databases, while testers analysed the suitability of authorisation data. Project managers then distributed subscriptions against cryptocurrency payments.

The hacking group's main source of revenue came from stealing loyalty scheme login credentials and selling them on to other, less technical criminal gangs. These gangs would then exchange the loyalty points for expensive electronic devices.

The hackers created a sophisticated script to gain access to a large number of Swiss customer accounts. Although the losses are estimated at €50 000, hackers had access to accounts with potential losses of more than €610 000. The fraudsters and hackers, among them minors and young adults, were unmasked when using the stolen data in shops in Switzerland.

as encrypted email and messaging applications as well as Virtual private network (VPN) providers to hide criminal activity, exploiting increasingly privacy-oriented policies, which make it difficult for law enforcement to gain relevant information in time.

Often, these less obvious legitimate services are safer for criminals to use and minimise risks associated with using underground services more commonly used by criminals in the past.

1.4 CRYPTOCURRENCIES FACILITATE PAYMENT FOR ALL FORMS OF CYBERCRIME

The abuse of cryptocurrencies continue to play an important role in facilitating payments for transactions across all areas of cybercrime. Reliability, irreversibility of transactions and a perceived degree of anonymity have made cryptocurrencies the default payment method for victim-to-criminal payments in ransomware and other extortion schemes, as well as criminal-to-criminal payments on the Darkweb. These activities have been long established with Silk Road emerging in 2011 and Cryptolocker hitting its first victims in 2013.

At that time, more than 20% of transactions were directly attributable to criminal activity. Although the level of criminal abuse has grown substantially, the legitimate use of cryptocurrencies grew at a much faster rate. In 2019, the overwhelming majority of bitcoin transactions were linked to investment and trading activity so, despite considerable abuse, criminal activity corresponds to only 1.1% of total transactions[12]. The figure includes transactions stemming from fraudulent activities, Darkweb trade, thefts and ransomware.

Criminals continue to use cryptocurrency as a method of payment for extortion activities

Although Initial Coin Offering scams and a wide range of Ponzi schemes abusing the increasing popularity of cryptocurrencies dominated criminal abuse by volume, most of the crimes reported to law enforcement included various forms of extortion. The last two years have seen an increase in extortion spam, where the suspect attempts to frighten the victim with a promise of a devastating event should they not receive payment in cryptocurrency, typically bitcoin corresponding to hundreds or even thousands of euros. While in its most basic form the suspect simply expects naïve victims to trust the threat, a slightly more advanced approach includes victims' passwords, typically leaked from one of the large public data breaches.

The extortion scam typically involves sextortion, theft of data or, more recently, COVID-19 related threats. While the majority of the population is immune to such attempts, criminals still seem to benefit from the activity. The scalability of cybercrime compared to traditional forms of crime presents a key challenge, as cybercriminals can target a relatively large number of potential victims with relatively low investment, being able to profit despite a small percentage of responses. According to a recent study analysing a subset of 4 million intercepted sextortion emails, over 12 500 bitcoin addresses were extracted, 245 of which received one or more payments[13]. Although such efficiency is much lower than observed across ransomware campaigns, it is still much more lucrative when compared to traditional low-tech scams.

Cryptocurrency users also target of criminals

The growing adoption of cryptocurrencies increases the number of vulnerable victims, so it is no surprise that thefts from individual and enterprise wallets have become more prominent over the last few years. In 2019, there were 10 publicly confirmed hacks of exchanges where criminals stole cryptocurrencies, resulting in a theft of €240 million worth of assets. Although the number of incidents was higher than in any of the previous years, the total amount stolen decreased compared to the previous year with €950 million stolen in 2018, including almost €500 million stolen from Japanese exchange Coincheck[14].

Cooperation with the private sector

While a massive effort has taken place in the cryptocurrency industry to deal with proceeds from criminal activities, the exchanges still differ in the degree to which they address the issue and the level of assistance they provide to investigators. In order to assess the players across the industry, Europol is

conducting the first international law enforcement survey[15] addressing the issue of cooperation with the major cryptocurrency exchanges and payment services.

The cryptocurrency industry and exchanges in particular have continued strengthening their know your customer (KYC) measures, either through their increasing effort to identify rogue clients or by a growing set of legislation affecting the industry.

In Europe, the most important legislative development in this area was a transposition of the 5th Anti-Money Laundering Directive. The Directive states that cryptocurrency exchanges and wallet providers who own private keys of their clients are obliged entities, mandating them, among other things, to a proper identification of their clients. The Directive obliges all European Union Member States to implement the legislation by January 2020. Twenty countries have implemented it on time[16] with more doing so throughout this year. While individual countries were given a large degree of flexibility when transposing the Directive, this development contributed to a much-needed harmonisation of legislation.

The number of cryptocurrency automated teller machines (ATMs) is continuously growing and surpassed 9 000 ATMs around the world in 2020[17]. Traditionally, ATMs have often been perceived as a way to privately obtain or sell cryptocurrency. Nevertheless, compliance also gradually improves, as an increasing number of operators require customer identification and flag suspicious transactions.

Challenges to feature more prominently in future investigations

A large number of factors have rendered cryptocurrency investigations more challenging and we can expect these to feature more prominently in future investigations. These include centralised and decentralised mixing services, privacy coins, exchanges with insufficient KYC requirements, clandestine over-the-counter trading, nested services, where the exchange is incorporated within a wallet or another service and decentralised exchanges.

The obfuscation methods continue to develop. Centralised mixers troubled with exit scams and high fees seem to be gradually replaced by non-custodial mixing solutions where users do not need to send bitcoins to a third party. Privacy-focused services

Looking ahead: Malicious use of artificial intelligence

Artificial intelligence (AI) is at the heart of the so-called 4th industrial revolution and promises greater efficiency, higher levels of automation and autonomy. AI is intrinsically a dual use technology: while it can bring enormous benefits to society, AI can also enable a range of digital, physical and political threats. Therefore, the risks and potential criminal abuse of AI systems need to be well understood in order to protect against malicious actors.

For instance, criminals could make use of AI to facilitate and improve their attacks by maximising opportunities for profit in a shorter time, exploiting new victims, and creating more innovative criminal business models, while reducing the chances of being caught. As 'AI-as-a-Service' becomes more widespread, it lowers the entry barrier to criminal activities by reducing the skills and technical expertise needed to employ it. This further exacerbates the potential for AI to be abused by criminals and become a driver of crime. Concrete scenarios include AI malware, AI-supported social engineering, AI-based password guessing, AI-aided reconnaissance or AI-facilitated content creation, to mention a few.

It is therefore necessary, in close cooperation with industry and academia, to develop a body of knowledge on the potential use of AI by criminals with a view to better anticipating possible malicious and criminal activities facilitated by AI, as well as to prevent, respond to, or mitigate the effects of such attacks in a pro-active manner. Understanding of capabilities, scenarios, and attack vectors is the key to enhancing preparedness and increasing resilience.

aside, the bitcoin protocol itself is expected to soon implement features that will make it less transparent to casual observers and investigators alike.

Cybercriminals will increasingly turn to marketplaces that support decentralised transactions. More marketplaces are likely to deprecate the traditional centralised model with deposit and escrow accounts in favour of direct transactions between buyers and sellers, decreasing the influence of market administrators and discouraging exit scams.

1.5 CHALLENGES WITH REPORTING PLAGUE ABILITY TO CREATE ACCURATE OVERVIEW OF CRIME

Several interviewees indicated how they are unable to provide a comprehensive overview of the number and types of crimes executed within a particular crime area. This is the result of a number of factors. First, the ability to register a specific crime is not always possible. Crime registration systems are diverse, and several interviewees indicated they were in a process of advancing their ability to gather more specific crime reporting data, i.e. specifying what type of cybercrime took place. In one Member State, ransomware, for example, was not a separate category, as the country maintains a general category for data breaches. Having a general code for data breaches led to classification problems, according to the Member State representative, as different types of crimes fall into the same category.

Second, victims often do not report the crime. Crime reporting is a general problem as such receives attention as part of a broader Victim Rights Strategy[18]. Victims may not see the value of doing so as law enforcement have limited resources to conduct investigations. Yet, reporting the crime can also help law enforcement in its quantitative justification to support the request for more resources. Moreover, the more victims report a crime, the more data law enforcement can gather and the more likely connections between different crimes can be established. One of the interviewees indicated how under-reporting prevents law enforcement from forming the bigger picture and gathering reliable data, and monitoring whether cybercrime has been increasing or decreasing in reality.

Cryptocurrency as an investigation opportunity

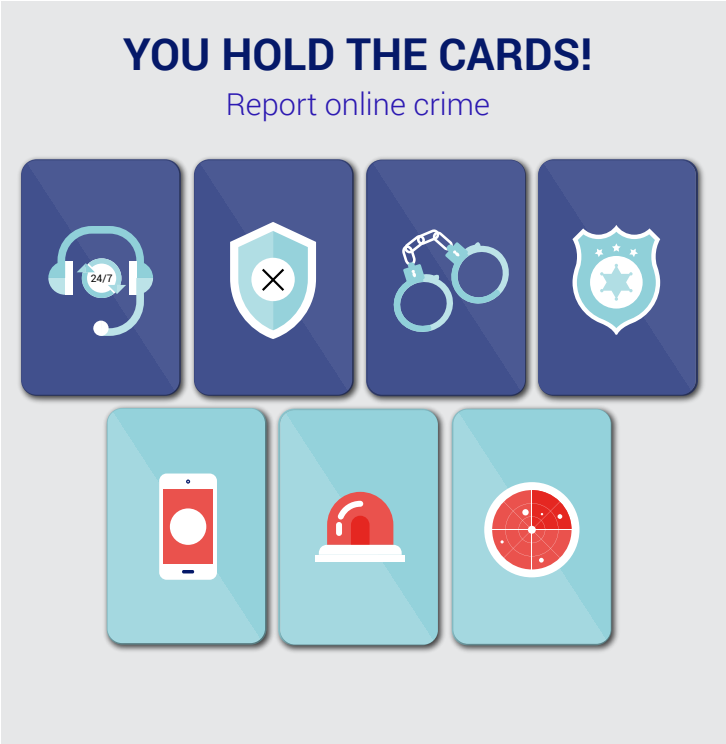
Cryptocurrency investigations have become an essential tool for many cybercrime investigators. While the role of Europol is to support investigations in the Member States, we could no longer ignore a high demand for relevant practical training. To cope with an increasing demand for a hands-on e-learning experience Europol in cooperation with CENTRIC launched CRYPTOPOL, an educational game for investigators in October 2019. CRYPTOPOL is accessible to all law enforcement cryptocurrency investigators around the world who can contact Europol to request access to the game. As the game contains information about tracing techniques used by law enforcement there is no intention of making it publicly available.

The other explanation for a lack of reporting from victims, at least with respect to the general public, is a lack of awareness. One interviewee indicated having witnessed a significant increase in cybercrime figures, but offered as an explanation that it may in fact be the result of greater awareness from the public. Others indicated there is no incentive to report as the focus is on business continuity.

Third, law enforcement at a national level often find out about a potential case through the media or through their local police. Crime registration at local police level maintains its own challenges as local police units may not have the expertise to assist a victim of cybercrime. Additionally, the information reported to local police may not find its way to national or central units, meaning law enforcement at is unable to connect the dots on a national scale and with their respective international partners.

Cybercrime in the media

Law enforcement officials also indicated using media as a source of crime reporting, which is not the preferred method as such reporting maintains its own challenges. Cybercrime is a complicated area filled with technical elements and cross-cutting issues,



which make it difficult to create a clear picture of the landscape. A lack of understanding of key terms, concepts and a limited viewpoint have shaped the way mainstream media have portrayed cybercrime to wider audiences. Sophisticated emerging technologies, human-relatable narratives, and high-profile cases (vis-à-vis victims or perpetrators) tend to dominate media headlines.

The complexity and terminological challenges of cybercrime can lead to inconsistencies between what the media reports and what the security community says about an incident. It is also not helpful that many companies name the same groups or attacks differently, enhancing the potential confusion. The complexity can lead to the perception of cybercrime as a highly sophisticated and intelligent field of crime. However, while for some cases this is an accurate assessment, this perception may lead to neglect of the human element of cybercrime, which is much less complex to comprehend. Additionally, there are many forms of cybercrime which are relatively unsophisticated, but which have substantial impact nonetheless. Cybercrime has a genuine human impact and individuals can do a lot to improve their resilience against different kinds of cyber threats if they are aware of them. Reporters may lack a coherent understanding of the cybercrime field, often mixing cyber-enabled fraud with cyber-dependent crime.

Where a high-profile incident occurs, an excessive focus on such cases may lead to indirect re-victimisation and, in some cases, directly casting blame on the victim, which harms investigations. Law enforcement view the media highlighting the more dramatic cases, while often ignoring the low-value but high volume cybercrime. When victims are essentially the only possible source of information in criminal cases, they are not likely to be willing to share information on their victimisation. This is particularly true with BEC and ransomware. Media reporting can turn the incident into a scandal story, which could lead to further victimisation and reputational damage.

Using media for awareness raising

According to law enforcement and private sector respondents, due to the receptive nature of several media outlets, there is substantial room to work collaboratively with media to raise awareness of neglected areas of cybercrime which have a substantial impact on EU citizens. There are extensive calls to have clearer, more accurate representation of cybercrime to public audiences. Law enforcement are calling for prevention to be covered more extensively. If done right, the media could become a powerful actor in cybercrime prevention, for example by exposing the adoption of new kinds of technologies and methods by cybercriminals.

Law enforcement has reported good reception among media representatives in raising awareness of concrete cybercrime issues. Active presence on social media by law enforcement, and sending out notices on cybercrime, is often well received by media and the public[19]. The media often picks up and shares the story.

This is important, as, for example, phishing and social engineering attacks rely on convincing humans to fall for fraudulent activities, which makes raising awareness on these threats potentially more impactful than focusing on disseminating high profile incidents. As national media outlets often spearhead media reporting in Member States, it would be important for the public and private sectors to engage with them regularly, raise awareness and communicate elaborately the realities of the threat landscape, which could help boost resilience against threats. People usually report crimes more after certain information is disseminated on threats.

1.6 LAW ENFORCEMENT ACCESS TO DATA CONTINUES TO CHALLENGE INVESTIGATIONS

For several years now, the advancement and increased implementation of certain technological developments have complicated the ability of law enforcement to gain access to and gather relevant data for criminal investigations. One of the most prominent examples in this regard remains the widespread use of encryption, which contains many benefits from a security perspective but is also a development that criminals have gratefully used to their advantage[20]. Europol has spoken about this in previous iterations of the IOCTA and jointly with Eurojust in its dedicated Observatory Function reports in 2019 and 2020.

Encryption continues to become a mainstream feature of an increasing number of services and tools. One example is the Domain Name System (DNS) over Hypertext Transfer Protocol Secure (HTTPs). DNS is one of the most important databases in the internet infrastructure. Increased concern over the monitoring of DNS traffic has led to the standardisation of modern DNS resolution protocols that make use of encryption. One of the protocols, which received increased popularity and adoption is DNS over HTTPS (DoH), after being introduced as a default setting on the application level. Even though the DoH protocol was created to solve historical DNS concerns regarding security and privacy, the potential centralisation of DNS traffic around a handful of commercial and private organisations has arisen as a result. Tracing historical DNS records is an effective tool when it comes to criminal investigations. Access to DNS queries is also used to great effect in dealing with botnets. Access to the network traffic between the criminal source and the remote DNS service provider, however, will now barely be possible due to traffic encryption, which will make the detection and blocking of malicious traffic, botnets and other malicious applications impossible.

As queries to the DNS will be encrypted, ability to gain access to such data will be more complicated for law enforcement, and countries hosting the majority of the DoH service providers will receive the vast majority of the internet DNS lookups, compared to the previous national decentralisation of these sensitive queries.

As a consequence of this, most of the DoH-related investigations will involve international legal requests to those jurisdictions. The DoH provider is likely to have a privacy policy in place, which will make it even more difficult for law enforcement to receive the necessary information for crime investigations. Finally, while positioned as a privacy-enhancing technology, it still allows internet service providers (ISPs) to profile users as other data points of the Hypertext Transfer Protocol (HTTP) traffic remain unencrypted.

Other related developments include the use of cryptocurrencies by criminals, as indicated earlier in this chapter. Whereas law enforcement, including Europol, continues to focus on improving capabilities in the area of cryptocurrency tracing, significant challenges remain.

Encrochat investigation provides new insights into organised crime

The value of being able to access data of criminal communication becomes most apparent when law enforcement succeeds in gaining such access. The case of Encrochat, an encrypted phone network widely used by criminals, is perhaps the most effective illustration of how encrypted data can provide law enforcement with crucial leads beyond the cybercrime area. It should be emphasised that the platform targeted by this investigation catered specifically to the needs of criminals. The phones using the platform were provided pre-configured and advertised to meet the needs of criminals and to secure the users against surveillance or investigation methods used by law enforcement parties. The phones are sold guaranteeing anonymity utilising a network of re-sellers, which are often themselves involved in other criminal activities, and are not distributed via regular retail outlets. In early 2020, EncroChat was one of the largest known providers of encrypted digital communication with a very high share of users engaged in criminal activity. User hotspots were particularly present in source and destination countries for cocaine and cannabis trade, as well as in money laundering centres. In July 2020, Europol reported on a joint investigation which made it possible for law enforcement to intercept, share and analyse millions of messages that criminals

While the activities on EncroChat have ceased, this complex operation shows the global scope of serious and organised crime and the connectivity of criminal networks who use advanced technologies to cooperate on a national and international level. The information has already been relevant in a large number of ongoing criminal investigations, resulting

in the disruption of criminal activities including violent attacks, corruption, attempted murders and large-scale drug transports. Certain messages indicated plans to commit imminent violent crimes and triggered immediate action.

This investigation confirms that advanced technologies enable criminals to secretly communicate or transfer illicit goods and resources. There is a growing risk to public safety as organised crime are drawn to using encrypted communication platforms that are almost technically impossible for law enforcement to access. Due to these emerging technologies used by criminals and the opportunities new technology may pose for law enforcement, an even more intense thinking beyond law enforcement cooperation is required, including with the private sector.

While the dismantling of EncroChat is a considerable success against serious and organised crime and the result of a multi-national investigation, the ingredients needed to come to such a success include the ideal combination of information, resources, skills, partners and opportunity. This means this type of success is an exception as the rule remains that law enforcement continues to battle the challenges of criminal use of advanced technologies.

Bulletproof hosters are the backbone of criminal infrastructure

An important building block of the criminal infrastructure is bulletproof hosting (BPH) – an essential CaaS offering, which continues to be a crucial facilitator for criminals and a hindrance for law enforcement by challenging identification and attribution efforts. BPH refers to a type of hosting or hosting provider that earns its money by consciously accepting perpetrators of crime as part of its clientele, offering them technical infrastructure resilient to law enforcement disruption or takedown. There are some hosting providers who may be negligent in acting on illegal content or criminal activity hosted by them, which is also an area of concern for law enforcement; however, the hosting providers that consciously act in or support the interest of the criminals ought to be the primary focus. These providers make their willingness to support criminal activity part of their appeal and their business model. This is a crucial advantage for criminals as hosting providers can play a central role in allowing criminal activity to continue.

As an infrastructure element, BPH facilitates a broad variety of key threats, including CSAM, terrorism-related content, command and control (C&C) servers used in cyber-attacks as well as platforms for criminal-to-criminal trade and discussion[21]. It is linked to several threats in cyber-dependent and cyber-enabled crime, making it a key concern in the threat landscape. As such, both the private and public sectors have a key role to play in hindering a BPH criminal application. This calls for cooperation internationally, as well as an appropriate legislative framework which would hinder BPH providers from acting maliciously by hosting criminal interests. For example, regional internet registries, local internet registries and ISPs have a significant responsibility in maintaining data accuracy when sub-allocating IP addresses to network operators in order to maintain traceability, with regard to combatting BPH, as IP addresses have a substantial role in BPH.

BPH providers may run their own static servers to host malicious content of their clients. BPH services have also registered as resellers with low-end service providers (for example ISPs, large hosting providers and content delivery networks) due to low-level verification and authentication requirements. With the growth of cloud services, a new modus operandi has emerged in which threat actors rent virtual private servers from legitimate hosting providers using fake or stolen identities. This highlights the need for stronger KYC policies with businesses and organisations across the sector.

Case example

In September 2019, German law enforcement managed to identify and arrest the main suspect running a BPH service from a bunker. This BPH facilitated illicit marketplaces for various kinds of drugs, CSAM and CaaS. Specifically, the WallStreet Market and Flugsvamp 2.0 were able to run on the servers of the bunker in Traben-Trarbach, Germany[22].

2

CRIME PRIORITY

Cyber-dependent crime

KEY FINDINGS

- Ransomware remains the most dominant threat as criminals increase the pressure by threatening publication of data if victims do not pay.
- Ransomware on third-party providers also creates potential significant damage for other organisations in the supply chain as well as critical infrastructure.
- Emotet is omnipresent through its versatile use as it leads the way as a benchmark of modern malware.
- The threat potential of DDoS attacks is higher than its current impact in the EU.

2.1 INTRODUCTION

The clear majority of law enforcement respondents named ransomware as a top priority threat yet again. As reported in previous years' IOCTA reports, ransomware remains one of the, if not the, most dominant threat, especially for public and private organisations within as well as outside Europe. Besides ransomware, European law enforcement reported malware in the broader sense to be widely present in cybercrime cases. Malware attacks on organisations that play a crucial role in the supply chains of major organisations have been a significant development over the past year. The third threat, the DDoS attack, celebrated its 20th anniversary in 2019 and ongoing investigations show that the DDoS threat is still prevalent in the cyber landscape.

2.2 RANSOMWARE

The clear majority of law enforcement respondents named ransomware as a top priority threat yet again. As reported in previous years' IOCTA reports, ransomware remains one of the, if not the, most dominant threat, especially for public and private organisations within as well as outside Europe. What makes it even more challenging as a threat, is the impact it has on its victims. This victimisation goes beyond the primary target, most often a public organisation or private business, as ransomware also affects those whose data is compromised. Considering the scale of damage that ransomware can inflict, victims also appear to be reluctant to come forward to law enforcement authorities or the public when they have been victimised, which makes it more difficult to identify and investigate such cases. With ransomware, criminals do not only abuse encryption to hide their identity and obfuscate their financial transactions but also actively abuse encryption as part of their modus operandi. This leads to a situation where they can almost act with impunity.

Ransomware is becoming increasingly targeted

Criminals continued the trend introduced last year by making their ransomware attacks increasingly sophisticated and more targeted. The number of targeted ransomware cases has increased over the past year, which has led to a significant increase in threat actor capability as well as a higher impact on victims.

Ransomware attackers continue to target public and private sector organisations of various size, industry and nationality rather than individual personal computers (PCs). This enables threat actors to increase both the ransom amount requested and the probability of successfully making the victim pay the ransom. Victim reconnaissance plays a significant role in the preparation of an attack. European law enforcement and Europol have observed attacks targeting local governments and ministries; other public sector organisations in healthcare and education (including hospitals, universities and high schools); as well as businesses in manufacturing, finance, energy, and transport industries. While the context of the COVID-19 pandemic crisis has affected the cybercrime field, ransomware attacks targeting the healthcare industry took place well before the crisis had a substantial effect in Europe and the US, which suggests that the COVID-19 crisis was not a trigger for these kinds of attacks[23]. What COVID-19 brought was an increase of the attack surface, with unmanaged endpoints/devices (PC systems) being remotely connected and having access to companies' information technology (IT) infrastructure. The fast shift to telework made some companies 'alleviate' some of their IT security policies and some IT security responsibility has been transferred to the individual users, where varying levels of (or lack of) associated security training has created a new gap in security. This gap has subsequently provided new ways for cyber-actors to gain access to companies' IT infrastructure.

Typically, ransomware attacks deployed against large corporations occur in different stages and are executed by different threat actors. The first initial step (performed by one group of criminals) of a ransomware infection is the computer/network intrusion which is done by the use of multiple attack vectors and malware types. The access is then sold to different cybercriminals that perform IT infrastructure mapping, privilege escalation, lateral move, data exfiltration etc. and finalised by deploying the ransomware.

Ransomware and third-party providers form a lethal combination

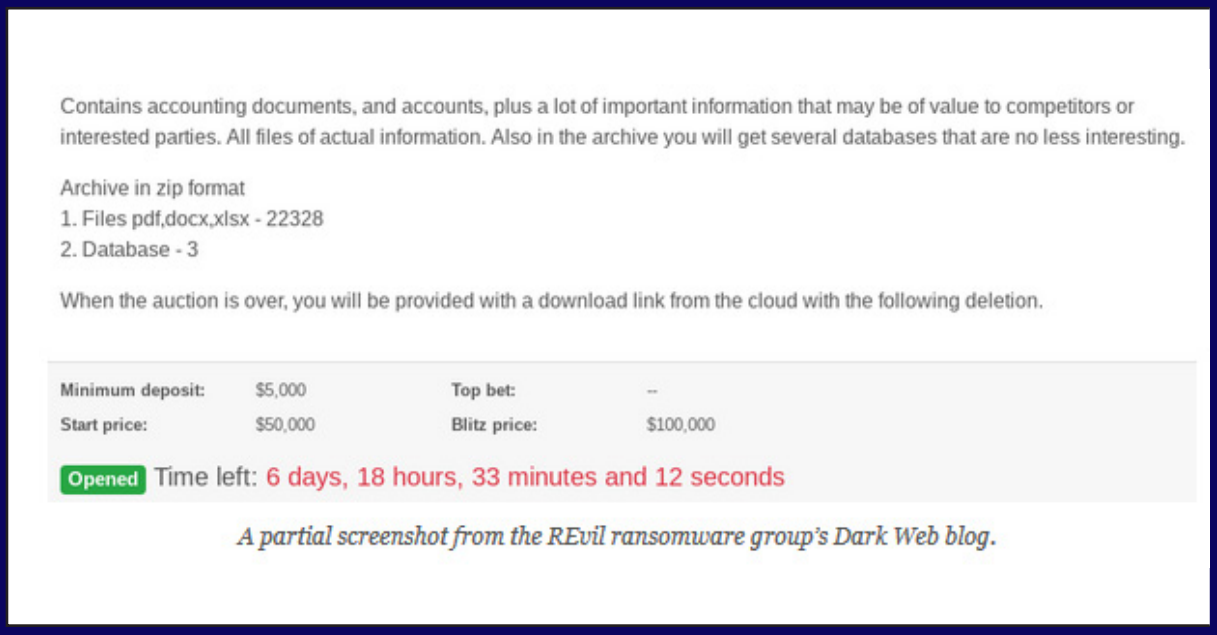
Ransomware has shown to pose a significant indirect threat to businesses and organisations by targeting supply chains and third-party service providers. Europol has followed up on attacks on organisations playing a key role in the supply chains of major financial institutions, which are believed to be an attempt by the attackers to enhance pressure on the victim to pay the ransom. Private sector respondents reported concerns over the differences in the IT security apparatus across supply chains, which leaves companies that play a key role as a service provider vulnerable to attacks. These attacks then have an impact across the whole supply chain, which may do substantial damage through long downtime or information leaks for organisations indirectly affected by the attack. One case saw an IT service provider being attacked with Maze ransomware, which can sit on the victim's servers for several months. This allows criminals to perform reconnaissance by monitoring internal communications in order to identify a key moment, such as merging, selling, big meetings with customers/sales, etc., for the deployment of the ransomware. Criminals deploy the ransomware before such events with the aim of putting pressure on the victim. At the same time, criminals can also exfiltrate

the data prior to the deployment of the ransomware to have another means of pressuring the victim. The existing presence of the criminals on the victim's servers is difficult to identify by security investigators as the security measures mainly focus on inbound detection.

A perverse twist to guarantee payment: threatening to auction or wipe data

Ransomware attackers have introduced a new way of pressuring their victims to pay by stealing the victim's sensitive data and threatening to publish it online. Once criminals gain a foothold on victims' networks, which can be done in various ways, they explore the networks and exfiltrate data, before delivering the ransomware. If the victim fails to pay the ransom demand, attackers will post the victim's sensitive data online or sell it to the highest bidder. The group behind Sodinokibi ransomware has already attempted to auction data which it gathered from a ransomware attack[24]. According to Member States and private sector respondents, several ransomware families including Sodinokibi (also known as REvil), Maze, Doppelpaymer, Nemty and Snatch published data which criminals stole from their victims over the past year. In particular, the auctioning of the data by criminal groups marks a new step and demonstrates an escalation in methods aimed at coercing victims to pay the ransom. It is anticipated that other groups will begin to adopt these coercive measures too.

Additionally, in the 2018 IOCTA Europol predicted scenarios in which fines for violating the GDPR could be used by threat actors as additional leverage with regard to the threat of leaking their victim's data online[25]. Both Member States and private sector respondents witnessed this phenomenon over the past year. Some ransom notes specifically mention GDPR fines to enhance the pressure on victims.



A partial screenshot from the REvil ransomware group's Dark Web blog.

Fig. 1 A screenshot of a data auctioning session online[26].

An alternative to the publication of data is its destruction. Some ransomware families, such as NotPetya have destructive wiper functionalities which may cause irreversible damage to the victim. Europol observed a case of destructive malware which took place in 2020, in which attackers managed to rewrite the master boot record.

Investment costs for criminals increase, but so do the potential profits

While the overall investment cost of ransomware is increasing, the amounts extorted by attackers have increased too. Attackers who launch ransomware attacks have requested ransom from anywhere between less than a thousand to millions of euros. The damages caused by e.g. downtime have increased significantly as well. When targeting their victims, European law enforcement found attackers surveying their victims and assessing both the victim's capacity

to pay (by reading e.g. financial reports) and the most effective way of infecting as many machines as possible during the attack. Attackers have also used encrypted communication means (such as Protonmail, Tutanota and cock.li) and set up customer service portals – many times a hidden service on Tor darknet – to help facilitate the extortion process.

Ransomware attackers are becoming increasingly innovative in pursuing profits from the crime area. In addition to shifting to corporate and organisational targets and finding new ways of adding leverage to their extortion, threat actors are seen collaborating with other criminals and adding new layers to their attacks, including crypto mining. Increasingly professional affiliate schemes are reflected in the increase in migration among criminal affiliates, as was seen with the migration from GandCrab to Sodinokibi.

Ransomware attacks display higher skill, sophistication and adaptivity among threat actors

Ransomware attacks continue to be a relatively diverse, low risk and easy way for cybercriminals to acquire money. The level of sophistication also varies across threat actors. European law enforcement reported at least two distinct types of ransomware actors: lone actors who utilise data and services from Darkweb market places, who demand ransom up to five thousand euros; and well-organised crime groups with better technical capabilities targeting higher-value targets for ransom of up to millions of euros. Threat actors have displayed significant adaptability in conducting lateral movement, reconnaissance and in establishing new footholds. Several stages are still executed through more manual steps (and again by using legitimate tools) where lack of strong internal controls and logging does not expose and reveal the suspicious activities. The availability of Ransomware-as-a-Service (RaaS) on Darkweb marketplaces has also decreased the barrier of entry for new, less skilful criminal actors. Lockbit, for example, which emerged in January 2020, was brokered on underground forums for other cybercriminals to use[27]. However, on the opposite side, already established and mature RaaS actors have raised the bar by including only trusted affiliates into affiliate programmes. These trusted affiliates have previously displayed the capacity to infect large companies. Affiliates that cannot infect large companies or are inactive on the platform for more than one week are expelled (e.g. Sodinokibi).

The business-type nature of ransomware attackers is also demonstrated in their engagement in online public relations activities. Some ransomware groups conduct their own information campaigns to advance their goals. The Maze ransomware group for example released a statement on their website claiming that they would 'spare' healthcare organisations during the COVID-19 pandemic crisis. This turned out to be

Ransomware | TIPS & ADVICE

THE MALWARE THAT HOLDS YOUR DATA HOSTAGE FOR A PRICE

Ransomware prevents users from accessing their system or devices, asking them to pay a ransom through certain online payment methods by an established deadline in order to regain control of their data.

HOW DOES IT SPREAD?

- Visiting compromised websites
- Clicking on malicious links and attachments
- Downloading fake application updates or compromised software
- Connecting infected external devices (such as USBs) to your computer system

disinformation, as the group allegedly attacked an urgent care centre in Texas soon after their release (refusing to pay ransom, Maze continued to publicise stolen patient data)[28]. The Maze group was also allegedly behind an attack on the Hammersmith Medicines Research facility in the UK, who have been involved in developing vaccines for the COVID-19 virus[29].

Both Member States and private sector respondents have noticed an increase in subcontracting and cooperation among threat actors, which has improved their capabilities. Similarities in how criminals behind the trio Ryuk ransomware, Trickbot and Emotet malware operate suggests that criminals across different attack approaches could either belong to the same overall structure, or that they are becoming smarter at cooperating with each other. Well-organised criminal groups who engage in ransomware, have been observed by European law enforcement cooperating over malware, infrastructure and money laundering activities. The relationship between Emotet, Ryuk and Trickbot is considered one of the most notable in the cybercrime world.

Some ransomware actors have also grown more cautious. Member States and private sector respondents reported that some of the actors behind ransomware attacks have become less vocal on underground forums, setting up alerts and alarms. They have also been observed using additional VPN layers and cryptocurrencies with mixers and swappers to hide their tracks. According to European law enforcement, attackers have also found a way of using C&C servers when deploying malware to place the payload into the memory of the company's servers. This way there is no trace on the victim's hard disk and no way of recreating it once it is gone from memory. The IOCTA 2018 and 2019 include a section on file-less malware as an emerging threat in cyber-dependent crime, and the IOCTA 2018 included a forecast that file-less malware would become an increasingly standard component of CaaS offerings by 2023.

Ransomware remains an under-reported crime

Several law enforcement authorities mentioned identifying ransomware cases through (local) media and approaching victims to assist them by potentially starting a criminal investigation. This was not generally a priority of the victim organisation, as the primary focus was on business continuity and limiting reputational damage (see Chapter 1). The shift in ransomware targeting individual PCs to more high-value targets such as businesses and public sector organisations introduces unique challenges to law enforcement investigations. Private and public sector victims of ransomware are disproportionately more affected by the threat of leaking data compared to ransomware cases in which PCs and individual persons were affected. Negative publicity leading to reputational fallout may lead to re-victimisation, which may prevent victims from coming forward to law enforcement authorities with information which could be crucial in identifying and catching the perpetrators. Victims prefer to engage with private sector security firms for investigating the attack or negotiating with the extortionists to manage the crises triggered by ransomware (some IT security firms hire specialist negotiators, some of whom get discounts from organised crime groups). Some of the companies that negotiate the ransom payment are working on the edge of legality, as they have developed a trusted business relationship with the ransomware actors.

Companies are normally referenced by cybercriminals in their negotiations as a proof or ledger that the victim's data will be decrypted after the ransom payment. Some of these companies negotiate behind the scenes with the ransomware actors to obtain a bigger discount from the ransom payment. Other companies might reflect this discount in the victim's invoice, others may not. Cyber actors provide ransom discounts to victims if they use the services of specific companies. By using such companies, victims will not file an official complaint, which increases the lack of visibility and awareness concerning real figures of ransomware attacks among law enforcement. Not reporting cases to law enforcement agencies will obviously hamper any efforts, as important evidence and intelligence from different cases can be missed.

Furthermore, a case involving personal computers being targeted by ransomware shows that victims had opted to purchase new machines rather than report the event to law enforcement. Here victims were stunned when they were contacted by law enforcement over the ransomware attacks, and were under the impression that law enforcement would not do anything about the situation.

2.3 MALWARE

Besides ransomware, European law enforcement reported malware in the broader sense to be widely present in cybercrime cases. Criminals have converted some traditional banking Trojans into modular malware to cover a broader scope of collection of PC digital fingerprints collection and are being sold to cover different needs (e.g. droppers, exfiltration, etc.). These advanced forms of modular malware are a top threat in the EU. According to European law enforcement, incidents have been steadily increasing over the past year and are likely to rise significantly later in 2020. Malware typically includes Trojans and remote access tools (RATs), which allow criminals to gain remote control over infected computers. Some threat actors use techniques similar to those in the past in some cases resurrecting old exploit codes when taking advantage of hygiene security issues, such as the targeting of unpatched structured query language (SQL) vulnerabilities, making traditional attack methods still worthwhile.

The level of complexity varies across malware attacks. Several groups have proven more adaptive and capable than others. Some groups can utilise malware to attack higher value targets with a more targeted approach, performing research and reconnaissance on their victims, whereas other less experienced actors engage in lower impact, massive attacks.

Malware attacks have been targeting third-party providers

Malware attacks on organisations that play a crucial role in the supply chains of major organisations have been a significant development over the past year. Similarly, with ransomware, other forms of malware targeting third-party or outsourced service providers put supply chains at significant risk, as the impacts of such attacks could involve data leaks or major disruptions, as well as knock-on or cascading effects. Private sector respondents reported a growing number of attacks on third-party service providers; however, it is unclear whether attackers intended to impact the supply chain in all cases.

Ransomware case example

Criminals targeted a London-based foreign currency exchange Travelex with Sodinokibi ransomware in the first weeks of 2020. The company had over 1 000 stores and 1 000 ATMs in over 26 countries. Travelex was also a third-party service provider for several well-known financial institutions internationally. As the attack left Travelex's services disrupted for several weeks, this had varying impacts across the whole supply chain. The criminals encrypted Travelex's data and allegedly managed to exfiltrate five gigabytes of sensitive data from Travelex, including personal data, social security numbers, dates of birth and payment card information, which it subsequently threatened to make public if Travelex did not pay the ransom. The company managed to restore its operations soon after, but it was reported that Travelex paid the USD 2.3 million ransom to the attackers. It is not advisable for victims to pay the ransom, as there is no guarantee the victim will gain their data back nor that similar attacks will not happen in the future.

In one case, a private sector respondent reported one of their third-party service providers had been targeted by Emotet malware which led to a high-risk situation at the respondent's organisation. Attackers were studying old email threads between the targeted company and the respondent carefully, trying to embed themselves into the conversation naturally using highly tailored messages to gather information. Staff at the respondent's organisation grew suspicious when new names and email addresses were following up on months old threads, and so they reported the messages as suspicious. This case shows that threat actors put considerable effort and preparation into an attack.

Emotet leads the way as the benchmark of modern malware as malware variants evolve

The evolution of Emotet and Trickbot malware shows how adaptive the malware threat is. The Emotet banking Trojan – which is mentioned as the top malware threat affecting the EU by both Member States and private sector respondents – has been used by cybercriminals to deliver other malicious malware payloads such as Ryuk ransomware and Trickbot. The developers behind Trickbot added a 'Trickbooster botnet' (a spam booster) to the malware. These developments signal an evolution in the malware and their capabilities.

European law enforcement case study

European law enforcement have witnessed some perpetrators using trusted third-party services in their malware attacks, including Amazon Web Cloud and Google Drive. The most downloaded PowerShell scripts are online text paste tools, such as Pastebin. These scripts are then executed in memory, making forensic analysis more difficult (what is known as file-less malware). Using phishing emails or malware payloads, threat actors are using the legitimacy of these services to trick their users. While this modus operandi has been around for a few years already, 2019 saw a significant development. Cybercriminals hack legitimate sites (for example those run on WordPress) to house various payloads and malware, using them as 'stagers' to upload malware and phishing sites within them.

Emotet is highly professional and aggressive as it seeks to maximise its profits. Private sector respondents suggest Emotet is a benchmark for modern malware with over 200 000 unique versions observed globally. The group behind Emotet seems to take long breaks over the summer and when they return in the autumn, they become highly active again. Other top malware threats affecting Europe as reported by private sector respondents include Lokibot, which stores login credential information from web browsers and data related to cryptocurrency wallets, and Qakbot, another modular banking Trojan known to facilitate ransomware infections on corporate networks.

Crime-as-a-Service (CaaS) enhances reach of attacks

Prolific malware, which criminals turn into commodity malware for others to use, is cause for concern. Threat actors collude with one another by sharing infrastructure, services and compromised credentials. Commodity malware and Malware-as-a-Service (MaaS) lower barriers for threat actors wanting to engage in cyber-attacks.

Despite a substantial decrease in exploit kits on underground markets, prolific malware such as Emotet and Trickbot have successfully filled the void. Both Emotet and Trickbot use modular structures to enable reselling and renting sections of their malware to their rivals without compromising their key differentiators. "TrickBot likely is operated by a single group as a MaaS platform that caters to a relatively small number of top-tier cybercriminals. Available information leads us to believe that individual TrickBot campaigns can be attributed to these different customers using the group tag parameter, and each customer may bring their own tactics, techniques and procedures and engage in highly targeted attacks[30]."

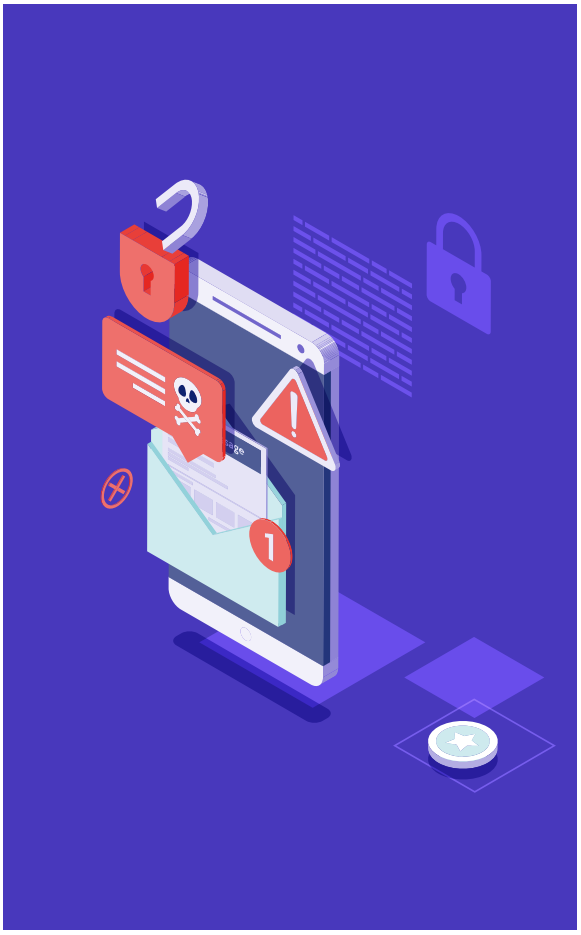
By doing the heavy lifting in acquiring access to a target's systems, Emotet can provide Access-as-a-Service (AaaS) to other cybercriminals. These other criminals can focus on monetising the opportunity with some other second stage malware. Competing solutions for electronic skimming (e-skimming) and JavaScript skimmers, with varying capabilities, each with the goal of compromising online merchant websites by harvesting payment card data, have also been offered as a service on the Darkweb by cybercriminals. These will be elaborated further in Chapter 4.

Simultaneously, European law enforcement has reported a rise in less tech-savvy cybercriminals in the context of widely available CaaS solutions. There has been an observable shift from what used to be a business for threat actors, now being more of an enterprise. Where specialist skills are needed (e.g. malware-coding, malware-distribution), criminals are able to hire developers or consultants to fill this need. This highlights increased professionalisation in the cybercrime threat landscape.

Through using combination attacks, criminals effectively challenge law enforcement's capacity to investigate incidents and attribute attacks to specific perpetrators and crime groups. Malware combinations add layers of complexity to law enforcement investigations. Encryption also presents a challenge, as malware developers often use encryption to frustrate law enforcement and industry efforts in analysing the functionality of malware and assign attribution to specific crime groups.

Mobile malware remain relatively stable

As more and more cashless payment transactions have emerged in the mobile scene, mobile threats such as mobile malware targeting cashless payment methods continue to grow. Mobile malware has yet to reach scalability as a sustainable business for cybercriminals, at least when contrasted with traditional banking Trojans. This is likely due to the limited transactions (with a cap typically set at around €50) which are enabled with mobile payments. Launching mobile malware attacks requires significant effort compared to other attack varieties which further offer larger payouts, which means they are likely conducted by less funded, amateur actors. European law enforcement also detected first signs of mobile payment fraud with attempted fraudulent transactions using app-based systems. Investigations are underway and it is unclear currently whether this involved mobile malware.



2.4 DDoS

In 2019, the DDoS attack celebrated its 20th anniversary. Ongoing investigations show that the DDoS threat is still prevalent in the cyber landscape. However, this topic has also had several success stories in prevention, mitigation and investigation. Attackers have adapted to these security measures by using attacks more efficiently, using both new tools and reigniting old techniques, and targeting more vulnerable victims.

Different types of attacks witnessed

Private sector and Member States respondents observed several phenomena relating to DDoS attacks over the past year. Private sector respondents reported seeing an increase in massive and simple DDoS attacks. European law enforcement did not witness significantly impactful attacks in 2019 but reported two kinds of attacks: targeted attacks which aim to damage specific industries or information systems; and crimes using automated tools. Automated attacks have been growing over the past year and are likely connected to CaaS. Threat actors can purchase pre-existing automated tools and deploy them for their own purpose, which makes conducting a DDoS attack a relatively cheap and easy way of carrying out an attack for threat actors who may have limited skills or experience in engaging in cybercrime. Moreover, criminals can use DDoS as a decoy or smokescreen for a more targeted attack.

Additionally, old DDoS methods are still prevalent. European law enforcement observed attacks targeting telecommunications and technology firms, where, in some cases, DDoS attackers threatened companies with reputational harm and extorted them for payment. Law enforcement agencies also came across cases where threat actors engaged in small attacks against larger organisations, extorting them for money with the threat of conducting larger attacks. Some threat actors targeted public systems and websites with DDoS attacks, however, these attacks were difficult to attribute to anyone specifically. One reason for the change in DDoS attacks could be the increase in protective measures used by organisations against them.

With respect to 2020, Amazon said its Amazon Web Services Shield service mitigated the largest DDoS attack ever recorded, stopping at 2.3 terabyte attack in February 2020[31].

DDoS has become increasingly adaptive

Cybercriminals who engage in DDoS attacks have adapted against increasingly robust protection measures. Instead of targeting high-value targets with massive volume attacks, attackers have shifted their focus on smaller organisations with less mature security apparatus. Downscaling their targets enable attackers to utilise volume more efficiently, and ensure maximum payout when the attacks are financially motivated. For example, private sector respondents reported smaller volume attacks which are capable of blocking smaller data centres. Small requests from 700 IP addresses make it difficult to block against a DDoS attack, and difficult for investigators to trace the attacker responsible as the attack comes from multiple IP addresses. These attacks incorporated additional methods which allowed the attackers to bypass the firewall's operational capacity.

Law enforcement case study

Law enforcement caught wind of a DDoS attack targeting a Finnish-based company. When approached by law enforcement, however, the company did not agree with the assessment, denying they were under attack. The attackers had used network mirroring DDoS via the Finnish company to amplify their attack on a major casino service in Southern Europe, which was the real target of the attack. Law enforcement thought that the Finnish company was the target, however attackers were only utilising the company's large network for mirroring and thus adding more volume to their actual DDoS attack. This is an old technique which has resurfaced after a few years, however with increased volume and capabilities. European law enforcement observed a couple of these cases.

IoT and DDoS

Connected devices, also known as the Internet of Things (IoT), are an additional avenue for DDoS attacks. According to private sector respondents, connected devices which run on legacy operating systems or which have weak or non-existent password protection could be vulnerable to DDoS attacks or for criminals wanting to provide DDoS services for other criminals, particularly as connected devices could be used for lateral movement to infiltrate networks. Private sector respondents also observed IoT botnets emerging, and while these have been mostly experimental, not yet witnessed in use for specific scenarios, criminals may advertise these for DDoS attacks.

The threat potential of DDoS attacks is higher than its current impact in the EU

Private sector respondents raised the concern of threat actors targeting third-party service providers with their attacks, for example energy and telecommunication providers. If attackers managed to bring down organisations in these sectors, criminals could potentially gain access to other valuable targets. Third-party service provider targeting could have other significant knock-on and cascading impacts in the supply chain. For example, the high level of interconnectivity in the financial industry also makes it vulnerable to disruptions.

3

CRIME PRIORITY

Child sexual exploitation online

KEY FINDINGS

- The amount of online CSAM detected continues to increase, further exacerbated by the COVID-19 crisis, which has serious consequences for the capacity of law enforcement authorities.
- The use of encrypted chat apps and industry proposals to expand that market, pose a substantial risk for abuse and make it more difficult for law enforcement to detect and investigate online CSE activities.
- Online offender communities exhibit considerable resilience and are continuously evolving.
- Livestreaming of child sexual abuse continues to increase and became even more prevalent during the COVID-19 crisis, a recent case shows CSAM production also takes place in the EU.
- The commercialisation of online CSE is becoming a more widespread issue.

3.1 INTRODUCTION

The main threats related to online CSE have remained relatively stable over recent years and throughout 2019. However, the COVID-19 pandemic has somewhat shifted this assessment. Detection of online CSAM was already increasing on a year-to-year basis, but saw a sharp spike during the peak of the crisis. A surge in the exchange of online CSAM occurred during the contact and travel restrictions and the consequences of this may have a long-term impact on CSE in general.

3.2 THE AMOUNT OF ONLINE CHILD SEXUAL ABUSE MATERIAL CONTINUES TO INCREASE

The year-on-year increase of detected online CSAM has continued. Law enforcement authorities in the EU see themselves confronted with an overwhelming amount of online CSAM to the extent that it becomes unmanageable for many of the units dealing with this crime. This includes regular complaints requiring investigation, including production of CSAM through rape and sexual assault, possession of that material, grooming, sexual coercion and extortion, but also referrals from the National Center for Missing and Exploited Children (NCMEC), ISPs, and hotline reports. This ongoing increase reflects a continuous distribution and redistribution of CSAM content. The effect of this on victims is significant and ongoing[32]. An international survey carried out by the Canadian Centre for Child Protection revealed that 70% of victims feared being recognised in public as a result of their involuntary participation in the offences against them[33].

The COVID-19 crisis revealed an extra surge in online distribution of CSAM. Referrals from the public, and industry in third-party countries reached record highs during the peak months of the pandemic. EU Member States also reported an increase in the number of blocked attempts to access websites featuring CSAM during their lockdowns. Moreover, several EU Member States have reported an increase in detected CSAM activity on Peer-to-Peer (P2P) networks especially in the second half of March, when lockdowns in EU Member States started materialising[34].

The increase in online CSAM has serious consequences for the capacity of law enforcement authorities to follow up and investigate reports of online CSE. Many investigators in EU Member States are faced on a daily basis with the task of making impossible choices between investigating one report instead of another.

There might be several reasons behind the growing amount of detected CSAM, including more offenders or better detection mechanisms. At least some of the CSAM is being repeatedly uploaded and widely distributed. However, the harm resulting from being a victim of this is severe, as victims experience repeat victimisation every time a picture or video is shared[35].

One of the drivers of the continuous growth of online CSAM is the growth in self-produced material. Especially during COVID-19 related lockdowns, children spent more time online, sharing images and videos that subsequently ended up with CSE offenders.

3.3 CRIMINALS INCREASINGLY ENCRYPT THEIR COMMUNICATIONS COMPLICATING INVESTIGATIONS

Offenders keep using a number of ways to disguise online CSAM, making it more complicated for law enforcement authorities to detect such images and videos. Although P2P network sharing remains among the most popular ways for perpetrators to share CSAM, it appears to be declining in popularity. The use of proactive EMPACT preventive and educative campaigns such as Police2Peer[36] seem to have had a continuing impact on reducing demand through these networks over time. One-to-one distribution and sharing among larger groups routinely takes place on social networking platforms and widely used encrypted communication applications such as WhatsApp, a trend reflected by the increasing number of referrals from US service providers via NCMEC[37].

Increased encryption of many digital communication channels means it is becoming more and more challenging for law enforcement agencies to investigate these crimes. There is increased activity on encrypted communication platforms beyond Tor, making it difficult to detect and investigate online CSE activities, including the creation and distribution of material, online grooming, sexual coercion and extortion.

Perpetrators have been using encrypted communications for a long time, but now even less tech-savvy offenders can easily use encryption. While the development of encrypted messaging platforms is not something bad in itself, it does raise significant obstacles for investigations in this crime type. Additionally, the conversion of popular unencrypted chat applications to encrypted status poses a substantial risk of increased abuse of those platforms for the exchange of CSAM and communication between offenders[38]. Several platforms including Facebook have reported a significant amount of CSAM. If these platforms move to implement end-to-end encryption for their messenger, concerns will rise over their continued ability to identify CSAM on their own platforms.

International police cooperation leads to the arrest of a Darkweb child sex abuser in Spain

The operation to bring down a child sex abuser, who had made explicit videos of an underage boy, owes its success to international cooperation. Information from Queensland Police – Australia's Taskforce Argos sent via Europol's secure communication channel – allowed Europol experts to carry out operational analysis, which revealed that a video from 2015 found in Belgium and France may have been filmed in Spain.

The analysis of the images and video – which showed how the suspect abused a boy who was under five years old at the time – led the Spanish National Police to locate the suspect. When looking into the message published with the video, officers noticed that the suspect used words and phrases from Spain and not from a Latin American country.

Using operational analysis, open-source enquiries and cross-checking information, Europol experts found that the suspect was registered on several websites and boards dedicated to child sexual abuse and exploitation on the Darkweb. The investigation revealed that the suspect was also using a social media network where he was in touch with a woman who shared the same surname as the one in the title of the sexual abuse video.

Once the abuser was located in Barcelona, cybercrime experts from the Spanish National Police Central High-Tech Crime Unit located in Madrid moved to Barcelona. Due to the lockdown in Spain, they were assisted remotely by other experts in Madrid. The material seized showed how the arrested suspect was using several email addresses and Darkweb access points to commit this crime[39].

3.4 DARKWEB OFFENDER COMMUNITIES ARE CONTINUOUSLY EVOLVING

Online offender communities exhibit considerable resilience in response to operational activities carried out by law enforcement agencies, attacks by unidentified actors and losses of staff and platforms. Their reactions include resurrecting old communities, establishing new communities, and making strong efforts to organise and administer them.

Parallel to the activity of large offender communities through Darknet forums is a development involving smaller communities sharing CSAM directly with each other via encrypted messaging platforms. Following several high-profile law enforcement operations on the Darkweb, many offenders seem to believe they are more secure in such small networks, sometimes based on invite-only. Offenders are also known to have used encrypted communication channels to infiltrate existing child-aged groups and form break-off groups involving children and adults[40].

In response to law enforcement operations targeting these Darkweb communities and due to the need to select participants and ensure exchanges of information are strictly related to child sexual abuse, offenders tightly control their communities. They use Darkweb forums as meeting places where participation is structured similarly to criminal organisations, with affiliation rules, codes of conduct, division of tasks and strict hierarchies. The purpose of the structure is to enforce rules and promote individuals based on their contribution to the community, which they do by recording and posting their abuse of children, encouraging others to abuse and providing like-minded, technical and practical support to one another.

Administrators require strict observance of the rules to avoid being banned from the forum. In addition, compliance with the rules and active participation can lead to a progressive increase in rank. Users regularly publish information and safety manuals aimed at avoiding detection by law enforcement authorities. Some users are also attentive to law enforcement operations and regularly publish news articles or even summary reports of the techniques used during successful operations. Cross-posting of such advice across various boards and forums highlights a collective approach to improve operational security for all. Some of these communities also meet offline, sometimes travelling great distances and bringing physical hard drives as storage media with them. Whereas Darkweb communities and real-life child sexual abusers used to be relatively separate, there appear to be more hands-on abusers – including individuals travelling for live distant child abuse – who are also very active on the Darkweb. Some law enforcement agencies have had cases where offenders keep material they produced themselves with them for many years before uploading it to the internet, hoping to avoid victim identification. This illustrates the crucial importance of victim identification efforts by law enforcement agencies, such as the Victim Identification Taskforce (VIDTF) organised on a regular basis by Europol.

Ninety suspects identified in major online child sexual abuse operation

Police around the world have taken down a global child abuse ring with links to over forty countries through a Belgian investigation supported by Europol. Four suspects have been convicted by a Belgian court.

This case was sparked by the Belgian East Flanders Federal Judicial Police, after more than nine million pictures and videos of the abuse of thousands of children from around the world were found there during a house search.

The vast majority of this footage had never been seen in circulation before by law enforcement. Suspecting they were producing their own, the Belgian investigators launched operation Gargamel together with Europol across Europe and beyond. The image and video data seized during this investigation has been used for Victim Identification Task Forces hosted by Europol, through which seventy children and thirty suspects have been identified. The Belgian Federal Judicial Police succeeded in identifying 60 suspects (of which 24 in Belgium) and 40 victims, which brings the actual total to ninety suspects and 110 victims.

Some suspects have already appeared before court in a number of other countries. In Australia, a suspect was sentenced to 15 years in prison.

More arrests and rescues are expected globally as police in over 40 countries examine the intelligence packages compiled by Europol and information from the Belgian Federal Judicial Police[43].

3.5 LIVESTREAMING IS BECOMING MAINSTREAM

Livestreaming of child sexual abuse continues to increase, becoming even more popular than usual during the COVID-19 crisis, when travel restrictions prevented offenders from physically abusing children[41]. As offenders had fewer opportunities to engage in physical CSE, live streaming emerged as a viable alternative to hands-on child sexual abuse. In some cases, video chat applications with built-in payment systems are used. This is a complicated area for law enforcement investigations, as usually none of the material is recorded, except for occasional chat conversations.

The Philippines remains the main country where live distant child abuse (LDCA) takes place. Cases of online CSE in the Philippines surged during the COVID-19 crisis, as the lockdown meant already poor families struggled to generate income and children did not go to school[42]. However, this year has further confirmed that this type of online CSE is not limited to Southeast Asian countries. A large operation in Romania uncovered significant levels of livestreaming taking place within the country, demonstrating that the EU is not immune to this threat.

In some cases, those seeking live streams of CSE are deceived: they pay for a live stream, but never receive anything.

3.6 COMMERCIALISATION OF ONLINE CSE IS AN EMERGING THREAT

Last year's IOCTA reported that commercialisation of CSAM remained limited to LDCA[44]. However, the past year has brought to light a number of indications that the commercialisation of online CSE is becoming a more widespread issue. For a long time, online CSE was one of the few crime areas Europol focused on that was not primarily driven by financial gain. Although offenders are still primarily driven by a desire to obtain more CSAM, in some cases they do seek to profit from online CSE. The emergence of a profit-driven model in this crime area is a worrisome development.

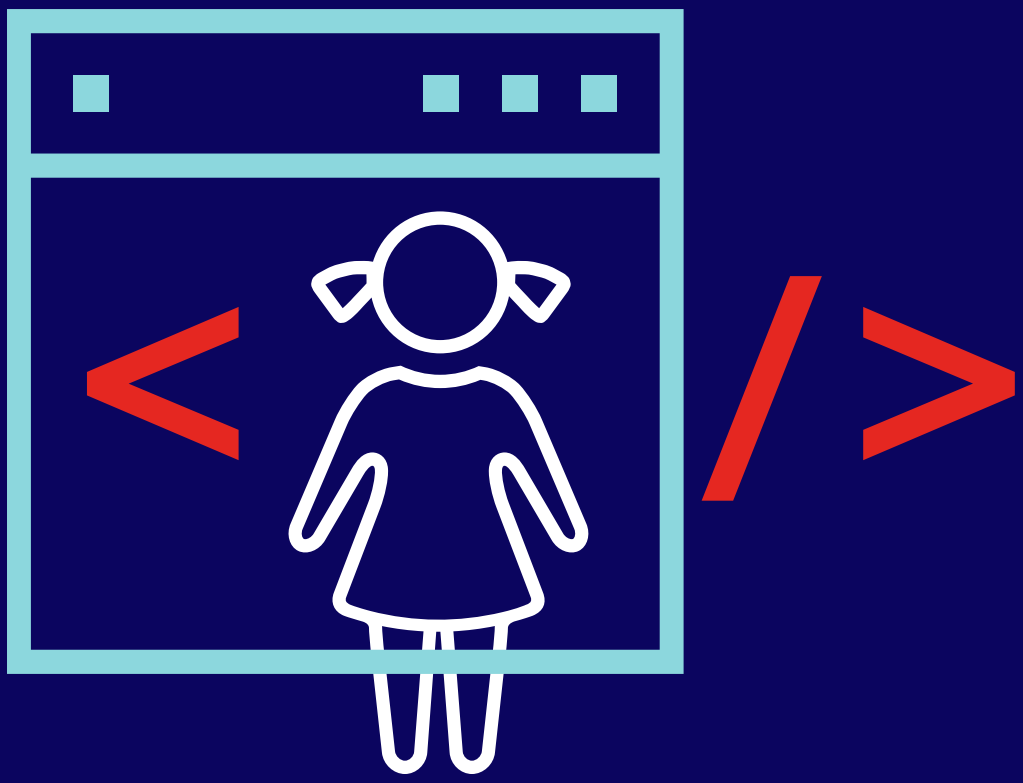
The monetisation of content has been seen on both the Clearnet and the Darknet, with many links on the dark web referring to Clearnet resources. Individuals monetise CSAM by uploading material to hosting sites (including legitimate hosting services) and subsequently acquiring credit on the basis of the number of downloads. This credit can be used to pay for additional hosting or in some instances can be cashed out, either in cryptocurrencies or other means. LDCA has had a commercial element for a longer time, as offenders frequently pay to watch parents, carers and offenders abuse children remotely to order. Uploading CSAM to legitimate hosting services is another method of monetising CSAM. The platform used to download this material may not be aware of the content or can claim not to be aware. The hosting site's advertising and the potential profits per click are also increased through such models.

3.7 ONLINE CHILD SEXUAL ABUSE TO REMAIN SIGNIFICANT THREAT

Online child sexual abuse remains a significant threat. The situation with COVID-19 has increased the time people spend online, whether it is for remote working, remote schooling or spare time. Children who spend a lot of time online unsupervised are therefore much more exposed to potential offenders through online gaming, the use of chat groups in apps, phishing attempts via email, unsolicited contact on social media as well as through less secure online educational applications[45]. Additionally, unsupervised time online further increases the risk of producing and distributing self-generated indecent material among underage individuals, which could also eventually reach child sex offenders. Furthermore, child sex offenders could take advantage of lonely and isolated children online, connecting with them to produce explicit material or to arrange a meeting in real life[46]. The current situation regarding COVID-19 creates considerable levels of uncertainty and unpredictability for the foreseeable future. The developments around the pandemic and related lockdowns and travel restrictions will have a big influence on the developments regarding online CSE.

The growth in CSAM being detected is showing no signs of stabilising, let alone decreasing. The end of the current health crisis and the lifting of lockdown measures may result in an increased number of reports of CSE, as abuse that occurred during the COVID-19 pandemic may be reported to law enforcement or other authorities after the fact. It is highly likely that in the upcoming year there will be a sharp increase in the amount of self-produced indecent material, which might also lead to a corresponding increase in online solicitation and exploitation.

Travel restrictions and other measures during the pandemic have likely prevented offenders from travelling and so have shifted their focus further to the exchange of CSAM online. A relaxation of travel restrictions and opening up of air travel will likely lead to an increase in transnational offenders seeking out CSE in certain countries and regions. If air travel remains limited for the foreseeable future however, or becomes more expensive, it is also possible we will see an increase in proxy offending both with surrogates such as childlike sex dolls or via live streaming.



4

CRIME PRIORITY

Payment fraud

KEY FINDINGS

- SIM swapping is a key trend that allows perpetrators to take over accounts and has demonstrated a steep rise over the last year.
- BEC remains area of concern as it has increased, grown in sophistication, and become more targeted.
- Many law enforcement agencies and financial services identified online investment fraud as one of the fastest-growing crimes, generating millions of losses and affecting thousands of victims from all EU countries.
- CNP fraud continues to increase as criminals diversify in terms of target sectors and e-skimming modi operandi.

4.1 INTRODUCTION

While the majority of fraud types are well known, they enjoy continued success due to insufficient cybersecurity measures and an overall lack of awareness. Fuelled by a wealth of readily available data, as well as a CaaS community, it has become easier for criminals to carry out attacks. As a result, law enforcement and industry continue to identify well-established frauds such as BEC, as a major threat but also witnessed new key trends such as SIM swapping emerge.

4.2 INCREASE IN SIM SWAPPING AND SMISHING

SIM swapping is one of the new key trends in this year's IOCTA. This modus operandi garnered considerable attention over the past twelve months, as law enforcement agencies noticed a significant increase with a growing number of cases in Europe.

SIM swapping is a type of account takeover and refers to the circumvention of SMS-based 2FA to access sensitive user accounts. Criminals fraudulently swap or port the victim's SIM to one in the criminal's possession in order to intercept the one time password (OTP) step of the authentication process. Since this typically requires detailed information on the victim, SIM swapping attacks are highly targeted. This also means that the overall volume of cases differs from Member State to Member State, leading to SIM swapping cases causing significantly higher losses in some jurisdictions while it is barely present in others.

Overall, SIM swapping poses a significant concern and huge potential danger and risk. A successful SIM swapping attack can lead to criminals gaining complete control over a victim's bank, email or social media account, and as a result, enable a number of serious follow-up crimes.

Operation Quinientos Dusim[47]

In January 2020, investigators from the Spanish National Police together with the Civil Guard and Europol targeted suspects across Spain believed to be part of a hacking ring which stole over €3 million in a series of SIM swapping attacks. Law enforcement arrested 12 individuals in Benidorm (5), Granada (6) and Valladolid (1).

Composed of nationals between the ages of 22 and 52 years old from Italy, Romania, Colombia and Spain, this criminal gang struck over 100 times, stealing between €6 000 and €137 000 from bank accounts of unsuspecting victims per attack.

The modus operandi was simple, yet effective. The criminals managed to obtain the online banking credentials from the victims of the different banks by through the use of banking Trojans or other types of malware. Once they had these credentials, the suspects would apply for a duplicate of the SIM cards of the victims, providing fake documents to the mobile service providers. With these duplicates in their possession, they would receive the 2FA codes directly to their phones send by the banks to confirm the transfers.

The criminals then proceeded to make fraudulent transfers from the victims' accounts to money mule accounts used to hide their traces. All this was done in a very short period – between one or two hours – which is the time it would take for the victim to realise that his/her phone number was no longer working.

Operation Smart Cash[48]

An eight-month-long investigation between the Romanian National Police and the Austrian Criminal Intelligence Service with the support of Europol has led to the arrest of 14 members of a crime gang who emptied bank accounts in Austria by gaining control over their victims' phone numbers.

Law enforcement arrested the suspects earlier in February in Romania in simultaneous warrants at their homes in Bucharest (1), Constanta (5), Mures (6), Braila (1) and Sibiu (1).

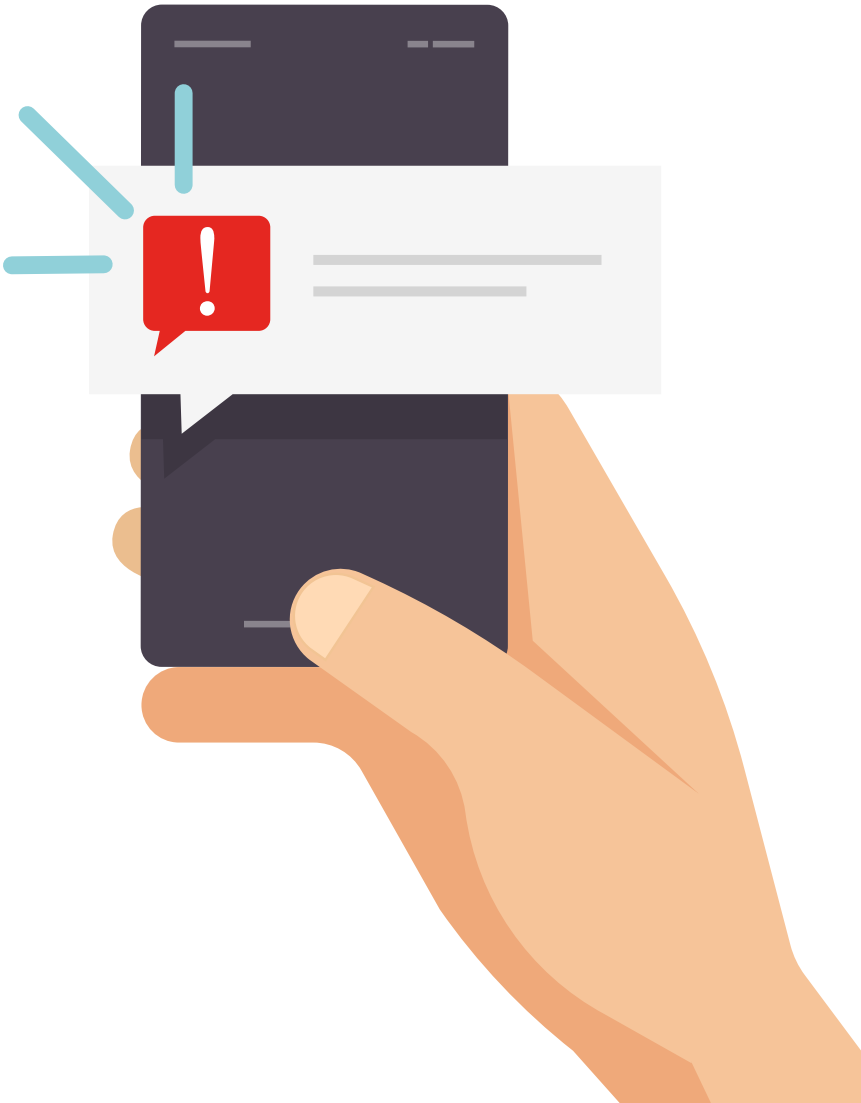
The gang perpetrated the thefts, which netted dozens of victims in Austria, in the spring of 2019 in a series of SIM swapping attacks.

Once having gained control over a victim's phone number, this particular gang would then use stolen banking credentials to log onto a mobile banking application to introduce a withdrawal which they then validated with an OTP sent by the bank via SMS allowing them to withdraw money at cardless ATMs.

It is estimated that this gang managed to steal over half a million euros this way from unsuspecting bank account owners.

Similar to SIM swapping, SMishing has seen an increase over the past twelve months. SMishing refers to the sending of fraudulent text messages purporting to be from trusted senders, typically targeting financial institutions and their customers.

SMishing is a lucrative alternative to phishing by email for a number of reasons. As most bank customers receive the advice to be suspicious of emails, customers do not yet have the same level of scepticism towards potentially fraudulent text messages. In addition, it is difficult to impossible for banks to protect their customers from SMishing attacks, as criminals aim to abuse the Alpha Tag of the SMS thread and Signaling System 7 (SS7) vulnerabilities.



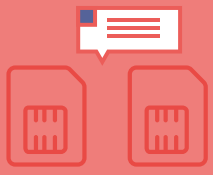
SIM SWAPPING – A MOBILE PHONE SCAM

SIM swapping occurs when a fraudster, using social engineering techniques, takes control over your mobile phone SIM card using your stolen personal data.

HOW DOES IT WORK?

A fraudster obtains the victim's personal data through e.g. data breaches, phishing, social media searches, malicious apps, online shopping, malware, etc.

With this information, the fraudster dupes the mobile phone operator into porting the victim's mobile number to a SIM in his possession



The fraudster can now receive incoming calls and text messages, including access to the victim's online banking

The victim will notice the mobile phone lost service, and eventually will discover they cannot log in to their bank account

WHAT CAN YOU DO?

- Keep your software updated, including your browser, antivirus and operating system.
- Restrict information and show caution with regard to social media.
- Never open suspicious links or attachments received by email or text message.
- Do not reply to suspicious emails or engage over the phone with callers that request your personal information.
- Update your passwords regularly.
- Buy from trusted sources. Check the ratings of individual sellers.
- Download apps only from official providers and always read the apps permissions.
- When possible, do not associate your phone number with sensitive online accounts.
- Set up your own PIN to restrict access to the SIM card. Do not share this PIN with anyone.
- Frequently check your financial statements.

ARE YOU A VICTIM?

- If your mobile phone loses reception for no reason, report it immediately to your service provider.
- If your service provider confirms that your SIM has been swapped, report it to the police.

Exploitation of 2FA behind smart ID

Three EU Member States reported cases of SMishing. Criminals used SMishing to bypass the 2FA mechanism offered by national smart IDs. Criminals aiming to attack bank accounts and the respective national banking infrastructure targeted these national Smart ID solutions through social engineering. Abusing alphanumeric SMS threads, criminals sent SMS appearing to come from the bank. These text messages prompted the recipients to log in to their online bank accounts using their smart ID, for instance to change their bank information. Following the link, they were then directed to fake bank log in account pages, which would verify a fraudulent transaction initiated by the criminal after they attempted to log in. Alternatively, threat actors would use this modus operandi to create a new Smart ID account under the victim's name, but under full criminal control.

4.3 BUSINESS EMAIL COMPROMISE REMAINS A THREAT AND GROWING AREA OF CONCERN

BEC remains a main and further growing threat for law enforcement and private industry. BEC is a sophisticated scam targeting businesses and organisations, whereby criminals employ social engineering techniques to gain access to an employee's or executive's email account to initiate bank transfers under fraudulent conditions, i.e. by pretending to be the CEO and asking the employee to carry out a payment.

BEC causes enormous losses and disruption to livelihoods and business operations[49]. Often following spear phishing emails, BEC is highly tailored and very effective with targets ranging from governments, international organisations, small to large businesses and individuals.

The two most common types of BEC are CEO fraud (criminals impersonating a high-level executive requesting urgent bank transfers) and invoice fraud (criminals impersonating suppliers asking for legitimate payments to be directed to a bank account under the criminal's control, or creating new, fraudulent invoices).

According to interviews with Member States, in many cases, BEC is carried out through a compromise of email accounts hosted by Office 365, access to which is typically gained through credential phishing in advance to the fraud. This is often possible due to limited security measures, such as a lack of 2FA; as well as a lack of awareness regarding spear phishing attempts. These type of attacks are still mostly originating from Eastern Europe, Nigeria and other African countries. The most sophisticated threat actors come from Israel.

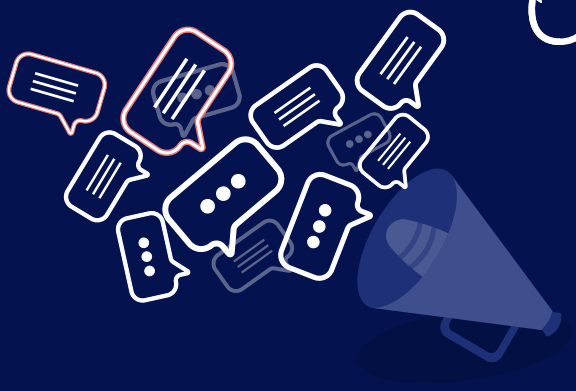
BEC has increased, grown in sophistication, and become more targeted

Over the past twelve months, BEC has increased across most EU Member States, with an additional increase as a result of the global outbreak of COVID-19. This increase in volume coincides with a growing sophistication and a more targeted approach. Criminals make use of technically advanced measures, such as compromising bank accounts, identifying the ideal time to strike, managing email conversations with complex man-in-the-middle attacks or even using Artificial Intelligence (AI) to mimic the voice of a company's CEO[50]. The growing sophistication of BEC is also reflected in the establishment and use of complex criminal networks, which are used to launder the proceeds of the fraud. Additionally, criminals have become better at local languages and the exploitation of local contexts.

While criminals target all kinds of organisations and businesses, there is an increased focus on smaller companies, rather than just large corporations. As a result, even cybersecurity companies not usually dealing with BEC have been receiving requests for technical assistance, for instance to conduct forensic investigations on the servers.

BANK SMISHING SMS

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.



HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account. But...the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

WHAT CAN YOU DO?

- Don't click on links, attachments or images that you receive in unsolicited text messages without first verifying the sender.
- Don't be rushed. Take your time and make the appropriate checks before responding.
- Never respond to a text message that requests your PIN or your online banking password or any other security credentials.
- If you think you might have responded to a smishing text and provided your bank details, contact your bank immediately.

Industry case study

A private sector partner reported a case in which a threat actor used social engineering and blended attacks to target the bank and its corporate clients simultaneously. The fraudster, having gained access to the client's email network, contacted the bank to request a change of the client's beneficiary account. The perpetrator subsequently managed the conversation and information exchange between the bank and the corporate client at the same time. Through this, the perpetrator showed a thorough understanding of the bank's processes and knowledge of who to speak to in order to change the account.

Industry case study

One private sector partner reported a case in which a criminal impersonated its CEO while at a conference. The threat actor made initial contact through WhatsApp, using a spoofed ID account and picture of the CEO and subsequently sent a forged email from the CEO about an urgent acquisition. Using information taken from open sources, the attack was highly targeted and convincing, demonstrating detailed knowledge about the CEO's current whereabouts. The fraud – the payment of an invoice, which never existed – was stopped only at the last moment, when a missing purchase order number raised a red flag.

Criminals likely to abuse voice biometrics

In the future, law enforcement and industry expect to see an increased use of voice biometrics to commit impersonation fraud. While biometrics are currently working well, attempts to compromise them to get access to bank accounts for BEC are expected to proliferate as additional security measures are being implemented.

4.4 ONLINE INVESTMENT FRAUD DRAWS IN VICTIMS ALL OVER EUROPE

Another relative 'newcomer' in this year's IOCTA is online investment fraud. Many law enforcement agencies and financial services identified online investment fraud as one of the fastest-growing crimes of the past twelve months, generating millions of losses and affecting thousands of victims from all EU countries. Many Member States witnessed this type of fraud for the first time.

Online investment fraud refers to a fraud type whereby criminals aim to lure their victims into transferring them money with appealing get-rich-quick schemes. Offering commodities such as cryptocurrencies, diamonds, or gold, criminals promise victims extraordinary financial returns on their investments, while criminals keep victims engaged through websites showing fake investment returns. While online investment fraud usually accounts for mid-level money losses, some victims have lost their entire life savings before realising that they had fallen victim to a scam.

Online investment fraud demonstrate high level of complexity

A number of online investment fraud cases have shown a significant level of complexity, with large networks of shell companies and call centres behind these schemes, as well as the development of software and communication tactics to systematise the exploitation of victims to their last cent.

In some cases, criminals have asked victims to install RATs to take control over the target computer, to initiate money transfers to criminals through full control over the computer and bank account. In addition to eliciting money transfers from their victims, criminals have also been seen to combine this type of fraud with phishing and the theft of credentials to be used subsequently for additional fraud.

Criminals usually target victims through social media, using celebrities and fake versions of news outlets, or come across the fraudulent investment web sites via search engines. Criminals have also been seen employing blended social engineering, with a mix of SMishing, cold calling and other techniques. Often these targets include older victims, who are less technologically savvy.

Online investment fraud is difficult to investigate, as criminals set up complex international schemes of companies with legal appearance, spanning across several legal jurisdictions. The groups behind these schemes are difficult to identify, due in part to their use of anonymisation tools, spoofed phone numbers and legitimate-looking websites.

Given the fast rise of investment fraud in many EU Member States, law enforcement agencies expect this type of fraud is to continue to increase and appear in so far unaffected countries, too. Perpetrators generally seem to originate from Russia, Ukraine and other Eastern European countries

4.5 CARD-NOT-PRESENT FRAUD CONTINUES TO INCREASE AS CRIMINALS DIVERSIFY

CNP fraud, such as carding and e-skimming, has increased over the past twelve months, with criminals shifting to new sectors and employing novel modi operandi.

Carding refers to the use of stolen card data to purchase goods or services. While carding has increased, criminals have moved away from targeting the airline industry towards the accommodation and rental sectors. The reduction in airline fraud is a direct result of successful public-private cooperation, which reduced the overall losses by nearly 50% and pushed criminals to other sectors. This is in addition to the purchase of goods such as mobile devices, phones and electronics, which criminals bring in from other countries using compromised card details.

Criminals take the stolen card details from dark web marketplaces (such as the Joker's Stash[51]), which make it increasingly easy to obtain stolen credentials from specific forums. Since these Darkweb forums typically require payment or some kind of interaction in order to gain entry, access is often difficult for law enforcement to obtain.

E-commerce/digital skimming a low risk and high-value modus operandi

The compromise of card data through e-skimming (also referred to as digital skimming) has increased, with technically knowledgeable organised criminal groups targeting e-commerce merchants with weak security measures. While sometimes criminals are seen targeting bigger companies when they see the opportunity, e-skimming mostly affects smaller to medium-size merchants, who do not have the capabilities to put into place sufficient protection and who, as a result, are often compromised without being aware of the criminal activity taking place on their sites.

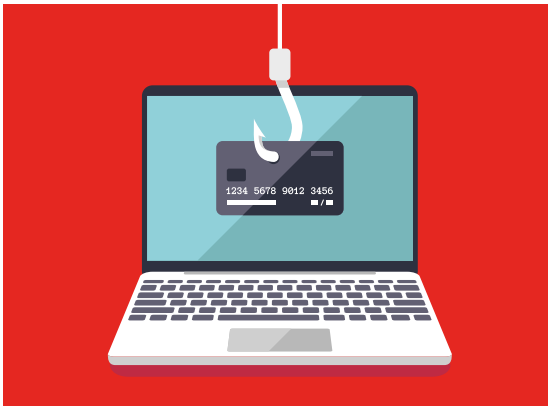
In an e-skimming attack, criminals inject malicious JavaScript code into the merchants' checkout pages, which allows them to capture personal data

Investigating carding on the dark web

During the Carding Action Week at the end of 2018, the Hungarian police launched an investigation into a vendor who was active on various markets offering card details from Hungarian cardholders.

The vendor was using different Pretty Good Privacy (PGP) public keys on the various market places but the police were able to decode these keys. This made it possible to identify the vendor's primary e-mail address used for registration on these market places.

During the investigation, the police were able to link the vendor's activities offering 400 account details from various financial institutions including 198 Visa accounts. Visa provided the necessary evidence and law enforcement arrested the vendor, and he is currently in custody waiting for his trial. The cooperation between the Hungarian Police and Visa resulted in the saving of €227 286 of potential fraud losses.



and credit card credentials. The malicious code typically checks the various customer and payment account number inputs, exfiltrates the data to an attacker-controlled C&C server, following which criminals can use this information to commit other crimes. Criminals commonly exploit for example improperly configured cloud data repositories, occasionally utilising automated processes to target vulnerabilities. Other entry points that criminals have increasingly been targeting include e-commerce merchants directly, or their service providers, which are supplying solutions ranging from analytics and advertisements to other general IT services.

The most common type of e-skimming activity, which interviewees mentioned, relates to the use of Magecart malware by organised criminal groups. This type of digital skimming has proven to be so lucrative that many established cybercriminals have moved into conducting such attacks, with JavaScript-based skimming now considered one of the main threats to financial institutions.

Private sector respondents have seen different variants of point of sale (POS) malware, including PwnPOS, AlinaPOS, and POSeidon / Backoff. FIN7 and FIN8 have been active threat actors in this area. FIN8 has also been observed using new malware toolsets to target POS environments.

As with other cybercrime areas, e-skimming, too, has seen criminals coming up with novel technical ways to execute their attacks, such as the Pipka malware.

Spotlight: FIN6

FIN6 is a prolific group of criminals, which has been targeting merchant point of sale (POS) systems to gather payment account data. In 2019, they expanded their attacks to e-commerce merchants, which represents a merger between CNP fraud and e-commerce breaches. The attackers injected malicious code into the merchant's websites, which would gather payment account number inputs and gather these account numbers into an attacker-controlled C2 server. Other skimmers have been observed gathering more input data than payment account numbers, which puts users' data at risk.

Spotlight: Pipka

Pipka is a new form of JavaScript skimmer which allows cybercriminals to configure which form fields the programme will parse and extract, including payment account numbers, expiration data, card verification values and the payment cardholder's name and address. Pipka has the added feature of being able to remove its malicious JavaScript component from the Hypertext Markup Language (HTML) code after successful execution. This is a new development in JavaScript skimming, and it adds interesting new layers to the malware. The Pipka skimmer reflects advancements made in e-skimming, and it goes to show that criminals targeting e-commerce will continue to develop innovative approaches to gather sensitive payment account data.

Darkweb marketplaces enable increase of e-skimming

Dedicated forums give cybercriminals the possibility to offload their stolen credit card data in a relatively low risk and efficient way. The forums also provide user-friendly interfaces for fraudsters seeking to buy them. At the same time, CaaS has created a competition between various underground forums, where cybercriminals are offering their sniffers and skimmers with constantly improved capabilities.

E-skimming poses a significant challenge to law enforcement and industry

While it is an increasing threat causing significant losses, detection of e-skimming is often difficult. Merchants do not necessarily realise that they have been infected, as it is the card-issuing banks that notice the frauds first. Reporting back to the merchant does not always take place, especially if the bank and the merchant are in different countries, in which case it can be difficult to determine who is liable for covering the losses: the bank or the merchant. In addition to the difficulty of timely detection, there are currently no anticipated technological or legal drivers to deter criminal groups conducting Magecart-style attacks, which is likely going to lead to a further increase in these types of attacks.

Digital fingerprints for sale

Continuing innovative developments of recent years, criminals are offering full digital user profiles in order to bypass advanced fraud prevention tools. In keeping up with e-commerce merchants increasingly employing analytics checking a user's identity against device fingerprints and several other metrics, criminals have moved to obtaining and selling these digital profiles to commit fraud. Taken from machines compromised in a botnet, they are used in order to make purchases using the compromised computer pretending to be a returning customer, using the same browser settings and victim's card credentials. After the fraud, many victims erase the evidence themselves, following Windows security guidance to restore to the last known configuration after having been compromised by the botnet, effectively removing all traces of the intrusion. This use of botnets to bypass sophisticated fraud prevention tools reflects a recurrent theme in the fight against cybercrime – as security measures are heightened, criminals come up with novel ways to continue their illicit activities.

4.6 TERMINAL ATTACKS INCREASE AS POPULARITY OF BLACK-BOX ATTACKS SOARS

Logical attacks on ATMs and POS devices remain a threat and have increased across most Member States. Among these, especially black-box attacks have proven popular, as organised criminal groups successfully manage to extract large amounts of cash in short periods of time. Black-boxing involves the installation of an external device connected to the cash dispenser in order to bypass the need for a card authorisation to dispense cash. Typically, the actual installation of the black box requires little technical knowledge besides the provision of the device and instructions. With cybercriminals remotely sending instructions to jackpot the ATMs, itinerant criminal networks are able to operate across several locations in different countries within a few days, requiring quick law enforcement response and international cooperation in order to stop them. These criminal groups are often Russian-speaking and with links to Eastern Europe, actively targeting ATMs across Europe.

Criminals are targeting mostly older ATM models, for which security measures and software have not been updated. While the modi operandi here remain largely the same; with occasional developments taking place in accordance with improved ATM security measures, law enforcement agencies noticed some changes in modi operandi over the past twelve months. As such, one Member State respondent saw a particularly ingenious criminal group using a new type of modus operandi for each attack, including a malware to check the balance of an ATM before deciding to attack it.

CRIME PRIORITY

5 The criminal abuse of the darkweb

KEY FINDINGS

- The Darkweb environment has remained volatile, lifecycles of Darkweb market places have shortened, and no clear dominant market has risen over the past year compared to previous years to fill the vacuum left by the 2019 takedowns.
- The nature of the Darkweb community at the administrator level shows how adaptive it is under challenging times, including more effective cooperation in the search for better security solutions and safe Darkweb interaction.
- There has been an increase in the use of privacy-enhanced cryptocurrencies and an emergence of privacy-enhanced coinjoin concepts, such as Wasabi and Samurai.
- Surface web e-commerce sites and encrypted communication platforms offer an additional dimension to Darkweb trading to enhance the overall business model.

5.1 INTRODUCTION

In 2019 and early 2020 a high level of volatility on the Darkweb was witnessed. Following protective measures, which multiple marketplaces have implemented, the situation has calmed down considerably. Nevertheless, the Darkweb environment remains difficult to disrupt as developments are often challenging to anticipate. This adds to the law enforcement challenges with respect to this growing threat, which continues to function as a key facilitator for many other forms of crime.

5.2 MARKETPLACE DEVELOPMENTS

More marketplaces based on purchased scripts have launched over the past twelve months, but some of these disappeared due to hacking or exit scams. The decrease in large-scale marketplaces has led to an increase in smaller marketplaces, in some cases catering to specific users or needs. Some of these markets are growing and as they gain positive feedback from users, they are becoming increasingly stable. Users are monitoring ratings and usually tend to keep to stable markets and vendors with high ratings. The market community has engaged in new ways of building trust with its users by developing cross-cutting solutions on information and reliability. A new site called DarkNet Trust has emerged which verifies vendors' reputations by searching through usernames and PGP fingerprints and it is able to search over ten thousand profiles from marketplaces[52].

After the takedown of DeepDotWeb mentioned in the IOCTA 2019[53], centralisation of information on Darkweb markets has stabilised and even increased. DeepDotWeb was a popular information service which made it easier for users to navigate the Darkweb ecosystem. Users are now looking to set up information hubs to increase user-friendliness in the Darkweb environment and sites such as dark.fail and darknetlive.com have taken over DeepDotWeb's role as information hubs. Dread, a popular Darkweb forum found on The Onion Router (Tor), continues to operate, having been around for approximately three years. The administrators of Dread additionally produced a DDoS protection solution (nicknamed Endgame Filter), which is free to use for other marketplaces, therefore expanding their role beyond a traditional information hub. Developers have also produced a Darkweb search engine termed Recon, a service allowing users to see what kind of drugs are for sale on the Darkweb, what vendors there are and what ratings they have. Another example of a Darkweb search engine is Kilos, which emerged in November 2019 reportedly as a potential follow up of Grams. Grams was a Darkweb search engine which ceased operations in 2017[54]. Since going online Kilos seems to have adopted the objective of indexing more platforms and adding more search functionalities than Grams. Moreover, Digital Shadows describes how "Kilos has introduced updates, new features, and services that aim to ensure security and anonymity for its users and also add a more human element to the site not previously seen on other prominent Darkweb-based search engines."[55]

Even though marketplaces continue to appear and disappear, an increasing number of operationally secure marketplaces, such as wallet-less and user-less markets, have emerged. Additionally, some marketplaces have intentionally relatively short lifecycles, which pose a challenge to law enforcement investigations. Short life cycles are making it difficult for law enforcement to investigate criminal cases. Administrators seem to want to stay under the radar of law enforcement by knocking down markets and keeping market lifecycles low.

Darkweb child abuse: administrator of Darkscandals arrested in the Netherlands

Early in March 2020, Europol announced the successful takedown of DarkScandals, a website which hosted videos of non-consensual and violent sex videos, including elements of rape, torture, human trafficking and CSE. The website had claimed it hosted thousands of videos of this kind of footage from all around the world. The Dutch law enforcement authorities and national prosecutor's office cooperated with German authorities, US law enforcement authorities and US Department of Justice and Europol in an operation to arrest the administrator and takedown the DarkScandals website. The administrator, a Dutch national, had allegedly received over 2 million dollars in exchange for selling the content on the website. The offender was charged with several counts of distribution of CSAM, production and transportation of obscene matters for sale or distribution, engaging in the business or selling or transferring obscene matter, and laundering of money instruments[59].

5.3 ADMINISTRATORS AND USERS ADAPT AS THEY AIM TO ENHANCE SECURITY AND RESILIENCE

Furthermore, Darkweb administrators have been observed pulling together and showing a collaborative spirit to maintain the environment under challenging circumstances. When faced with similar challenges, forum and service administrators have been seen working more closely together over sharing code and security methodologies (i.e. anti-DDoS measures, avoiding scams, creating trust-building sites to help users navigate vendors across different marketplaces, etc.). The Darkweb is essentially shaping into a 'business sector' in itself. There are also differences in the way administrators conduct their business on the Darkweb. Some are presenting to have a moral compass, banning items relating to the COVID-19 pandemic crisis, for example. This is not typical across the Darkweb, but it is an indication that some administrators differ in their approaches to conducting illicit trade.

Administrators are also looking to upgrade their security apparatus with other new features. Some marketplaces are already shifting to wallet-less and user-less markets, adopting multi signatures on Bitcoin and Monero, lacking registration requirements and enacting no JavaScript policies. Monopoly is also a wallet-less market in which payment occurs directly between buyer and vendor, and instead of enacting transaction fees, the market receives a monthly commission. Marketplaces were observed using multi signature wallets in their transactions[56].

Users have also opted to use safer communications methods. The reputation of Protonmail, an encrypted email service considered to be a former favourite among Darkweb users[57], has suffered after accusations that it has been helping law enforcement. Due to this, Darkweb users are shifting to new emerging encrypted email services such as Sonar and Elude[58].

In addition to encrypted email services, Darkweb users are relying increasingly on popular digital communication channels such as Discord, Wickr and Telegram. As these offer some degree of anonymity to the users, criminals consider it a safe place. This has introduced new initiatives, such as the Telegram vending service bot.

5.4 INFRASTRUCTURE PREFERENCES REMAIN STABLE, BUT CRIMINALS DO USE ALTERNATIVES

In terms of the Darkweb infrastructure, Tor remains the preferred option. As a result, criminal usage of Tor continues to be the primary focus. However, criminals have started to use other privacy-focused, decentralised marketplace platforms, such as OpenBazaar and Particl.io to sell their illegal goods. The emergence of decentralised privacy-oriented platforms is not a new phenomenon in the Darkweb ecosystem but they have started to increase interest over the last year. OpenBazaar in particular is noteworthy as certain high priority threats have emerged on the platform over the past year. These include those banned by some of the other Tor market-based administrators such as weapons and fentanyl. Even though the numbers may be considered limited, the nature of these items means the focus ought to be on impact rather than volume. COVID-19 related items also emerged on OpenBazaar during the pandemic. OpenBazaar has advertised a mobile platform Haven and has seen thousands of downloads on Android[60].

5.5 PRIVACY ENHANCING WALLETS EMERGE AS A TOP THREAT, AS PRIVACY ENHANCING COINS GAIN POPULARITY

With respect to cryptocurrency on the Darkweb, privacy-enhanced wallet services using coinjoin concepts (for example Wasabi and Samurai wallets) have emerged as a top threat in addition to well established centralised mixers. Apart from expected functionality including advanced decentralised coin mixing or integration of Tor these offer additional features. Samurai, for example, offers remote wipe SMS commands when under distress. These wallets do not necessarily remove the link between the origin and destination of the funds but certainly make cryptocurrency tracing much more challenging. Some administrators of underground markets are trying to apply these wallets to their payment systems. Threat actors have also been witnessed increasingly using hardware wallets, a separate physical device, which securely store seeds and private keys for a wide range of cryptocurrencies.

Initially, Darkweb markets relied solely on Bitcoin. However, over the past few years this has changed. An increasing number of markets are recognising the benefits of offering multiple coin alternatives, including Litecoin, Ethereum, Monero, Zcash, and Dash. While Bitcoin still remains the most popular payment method (mainly due to its wide adoption, reputation and ease of use), the use of privacy-enhanced cryptocurrencies has somewhat increased albeit not at the rate expected by their proponents. Monero is gradually becoming the most established privacy coin for Darkweb transactions, followed by Zcash and Dash. All these privacy coins may present a considerable obstacle to law enforcement investigations, despite the competing altcoin communities uncritically favouring their implementation over the others.

5.6 SURFACE WEB PLATFORMS OFFER AN ADDITIONAL DIMENSION TO DARKWEB TRADING

Some platforms existing on the clear web (or surface web) are also catering Darkweb goods and services, which offers additional benefits for criminals' business models. A number of cybercriminals are relying on surface-level e-commerce platforms for increased visibility, posting links to their online digital goods stores. One case involved an e-commerce platform registered to a company based in the Middle East, hosting online stores selling malicious digital tools from Arabic, Russian, and English language-based underground forums (links were found to underground forum administrators including cracked.to and nulled.to). Stores on the platform also offered stolen accounts, databases, carding, crypters, banking malware, ransomware and variants of the Mirai botnet. This platform allowed sellers to accept payments through PayPal and cryptocurrencies[61]. Surface e-commerce sites are useful for cybercriminals, as they allow them to showcase their products and services and they are legitimately registered businesses. Law enforcement also found cybercrime tools available on other clear web sites.

5.7 STEADY SUPPLY OF DIVERSE DARKWEB MARKET ITEMS

There has been an increase in the provision of digital and cybercrime elements on the Darkweb. Personal data, access to compromised systems (e.g. through RDP application), as well as services catering malware, ransomware and DDoS attacks, are all elements prevalent for the facilitation of cybercrime. Document and proof of identity services have also increased on the Darkweb. Perpetrators generally use identity and document services to support citizenship claims and other applications, obtaining lines of credit to set up a business, open untraceable bank accounts, proof of residence, to commit insurance fraud, purchase illicit items and other uses. There has been a shift in the offering of legitimate-looking counterfeit passports to "legal or registered" passports, which can pass several authentication tests, with criminals offering registered passport services. Trend Micro Inc. explains that the increase of global immigrants and the increasing adoption of e-passports is a likely driver behind this trend[62]. Additionally, some Darkweb sites also promote money laundering and instructions for users on how to use cryptocurrencies for money laundering.

Users can find drug listings in massive volume on the Darkweb; however, these do not necessarily reach priority-levels in terms of impact. More impactful, dangerous drugs, such as fentanyl, opioids and heroin are still significantly present on the Darkweb, although listings are smaller in number. Europol has observed an increasing trend of top organised crime groups having a presence on the Darkweb dealing drugs, which is likely due to an effort to expand their distribution mechanisms. As noted in IOCTA 2019, drug dealers may also be running multiple monikers on the Darkweb, which makes it difficult to prioritise within the drug topic. Additionally, the COVID-19 pandemic crisis seemed to have the most effect on the supply chains regarding drug trade compared to other crime. This has now stabilised and the situation has returned to normal, with an anticipated growth on the horizon.

Finally, the distribution of firearms has become significantly more fragmented. After the takedown of the Berlusconi marketplace by Italian law enforcement, which used to be the go-to place for firearms on the Darkweb, firearms have emerged on different marketplaces. Firearms are also available on OpenBazaar, although the scale of supply is unconfirmed. Some shops are also selling firearms from the United States. The ability for individuals to purchase firearms on the Darkweb has become increasingly difficult, due to recent law enforcement successes in catching individuals purchasing firearms illegally.

The diverse products and services vary in their level of impact and their ability to facilitate more serious forms of crime. The supply of these goods on the Darkweb poses a significant threat in the EU. Furthermore, the geographic nature of the threat is also diversifying. The Hydra market – the largest darknet marketplace serving Russia and neighbouring countries – has recently advertised an impending publication of a new, secure encrypted market platform, which they aim to open to the English-speaking community. Such a development would arguably make Darkweb investigations more difficult for law enforcement in the future and poses a significant threat to the EU.

Recommendations

The following section consists of highlights from this year's Member State and partner interviews combined with Europol insights. The majority of the responses resonated with previously reported recommendations focusing on recurring themes, such as:

» coordination and cooperation;

» information sharing
(removing practical obstacles, enhance judicial cooperation, reduce time, foster a culture of transparency and trust);

» enhancing the legal framework;

» prevention and awareness;

» capacity building.

Coordination and cooperation remain critical

There is little doubt that cybercrime requires more effective cooperation between private and public sector parties. Attackers use a coordinated approach and share infrastructure, which makes a broad and cohesive response to the criminal developments even more important. This also requires the engagement of multiple levels of collaboration.

More taskforce-like approaches, which has worked especially well in the Netherlands and the UK, would be beneficial. Considering the global nature of the Darkweb ecosystem and cross-border interaction of its users, the key recommendation is to establish a dedicated multinational Darkweb task force to approach the problem. This would help address legal jurisdiction challenges and obstacles hindering coordination.

Pre-investigative actions and information sourcing should be enabled with a dedicated centralised approach in the EU. This would help identify firstly priority cases and criminals, and secondly, appropriate jurisdiction over cases and highlight the most efficient ways of cooperating over specific cases and operations.

There is a persistent need for better cooperation with hosting services, social media platforms, and ISPs. Companies need to be more proactive in illegal content and activity and blocking it as soon as they detect it. One way of improving this is to invest in technologies that make sure their platforms are clean. They should also be able to demonstrate more willingness to assist law enforcement agencies to deal with, for example, CSE, and show improved openness and transparency.

Information sharing becomes even more crucial to offer timely response to cybercrime

Efficient and timely information gathering, analysing and sharing is crucial for fighting cybercrime. To this end, information sharing should be harmonised (what information can be shared between parties) and institutionalised. Structured efforts need to be put into place, increasing trust among the parties sharing information.

We must develop a culture of acceptance and transparency, and incentives for victims to bring their incidents to light and not fear penalties and re-victimisation for being targeted by cyber-attacks.

Considering the fast nature of cybercrime, it is important to make the exchange of information in light of international cooperation faster by implementing channels with, for example, the relevant ISPs at the European level (VPN, anonymisers, anonymous email providers, cryptocurrency exchanges, etc.).

Enhancing the legal framework

International law and national legislation should be better aligned with investigation practices in cybercrime. The link between legislation and investigative practices requires more focus.

There should be more relevant and focused legislation addressing bulletproof hosts and registrars, with which voluntary cooperation varies with law enforcement.

Darkweb threat actors increasing reliance on encrypted email services, privacy-enhanced cryptocurrencies and BPH providers pose a substantial problem to law enforcement. This calls for increased KYC type policies.

Prevention and awareness as well as crisis management

As indicated in many parts of the IOCTA, criminals remain successful because of inadequate cyber hygiene and an inability of victims to detect cybercriminal activities. This inability often stems from a lack of awareness on the side of the victim. This returns in many different forms of crime, including social engineering and phishing, as well as investment fraud. A lack of knowledge and awareness of the risk related to online CSE is also one of the drivers behind the increase in online CSAM. This highlights the need to continue promoting preventive and educational initiatives in a coordinated and structural manner across Europe.

In addition to raising awareness, there are calls for more effort on improving general cyber preparedness, including crisis management, exercises and disaster recovery plans. This is a recommendation which Europol in cooperation with its partners has responded to through its efforts with respect to the Law Enforcement Emergency Response Protocol (LE ERP). Developing evaluation schemes to assess and test IT security with infrastructure and devices, establishing rules and setting guidelines could increase resilience against cybercrime.

Capacity building

Cyber elements are becoming more and more visible in other areas of criminality and increasing numbers of these criminal activities are becoming cyber-enabled. This trend requires increased capacity among law enforcement to deal with this evolving challenge. Integrating cyber elements into law enforcement readiness already at the police academy level would enable educating and facilitating individuals who want to specialise in cybercrime. Effective investigations require technical expertise (civilian) and experience in criminal cases (law enforcement). Every police force should be responsible for developing knowledge within their units.

References

1 Durbin, Steve, "The Future's Biggest Cybercrime Threat May Already Be Here", https://www.darkreading.com/vulnerabilities---threats/the-futures-biggest-cybercrime-threat-may-already-be-here/a/d-id/1338439, 2020

2 Europol, "Staying Safe During COVID-19: What you need to know", https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know, 2020

3 The European Union External Action Service (EEAS), "A Europe that Protects: Countering Hybrid Threats", https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en accessed 27 July 2020 , 2020

4 Europol, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, 2020

5 Wolford, Ben, "Does the GDPR apply to companies outside the EU?", https://gdpr.eu/companies-outside-of-europe/, 2020

6 Palmer, Danny, "GDPR: 160,000 data breaches reported already, so expect the big fines to follow" https://www.zdnet.com/article/gdpr-160000-data-breaches-reported-already-so-expect-the-big-fines-to-follow/, 2020

7 Schwab, Pierre-Nicolas, "European GDPR statistics: evolution of the number of complaints per country", https://www.intotheminds.com/blog/en/gdpr-statistics-europe/ , 2019

8 Verizon, *2020 Data Breach Investigations Report*, 2020

9 Many interviewees used the term sophistication in connection to a variety of threats. The widespread use of the term, however, also makes its value as a descriptor limited. Certain sources aim to further unravel the answer to what makes a particular tactic or modus operandi sophisticated. See DePaula, Nic & Sanjay Goel, "A Sophistication Index for Evaluating Security Breaches", *11th Annual Symposium on Information Assurance*, 2016, and Buchanan, Ben, "The Legend of Sophistication in Cyber Operations", https://www.belfercenter.org/publication/legend-sophistication-cyber-operations, 2017

10 Europol, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, 2020

11 See IIJ America, "Allow / Deny List (Domain Policy Set Level)", https://iijasd.zendesk.com/hc/en-us/articles/206289805-Allow-Deny-List-Domain-Policy-Set-Level-, 2015 and the UK National Cyber Security Centre, "Terminology: it's not black and white", https://www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white, 2020

12 Chainalysis, "The Chainalysis Crypto Crime Report is Here. Download to Learn Why 2019 Was the Year of the Ponzi Scheme", https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report, 2020

13 Paquet-Clouston et al., "Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem", *Advances in Financial Technology (AFT19)*, https://arxiv.org/pdf/1908.01051.pdf , 2019

14 BBC, Coincheck: World's biggest ever digital currency 'theft', https://www.bbc.com/news/world-asia-42845505, 2018

15 At the time of writing – August 2020.

16 European Commission, "February infringements package: key decisions", https://ec.europa.eu/commission/presscorner/detail/en/inf_20_202 , 2020

17 Coin ATM Radar, https://coinatmradar.com/, 2020

18 European Commission, "Protecting victims' rights", https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights_en#:~:text=The%20European%20Commission%20presented%20on,fully%20rely%20on%20their%20rights, 2020

19 See for example https://twitter.com/EC3Europol activities.

20 For more information see Europol and Eurojust's reports on the Observatory Function.

21 Alrwais, Sumayah et al., *Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider*, IEEE Symposium on Security and Privacy, 2017

22 State Criminal Police Office Rhineland-Palat-

inate, https://www.presseportal.de/blaulicht/pm/29763/4387169, 2019

23 Chainalysis, "Ransomware Attackers Aren't Sparing Anyone During Covid-19", https://blog.chainalysis.com/reports/ransomware-covid-19 , 2020. Also see BBC News, "NHS 'could have prevented' WannaCry ransomware attack", https://www.bbc.com/news/technology-41753022, 2017, and Winder, Davey, "Infection Hits French Hospital Like It's 2017 As Ransomware Cripples 6,000 Computers", https://www.forbes.com/sites/davey-winder/2019/11/20/infection-hits-french-hospital-like-its-2017-as-ransomware-cripples-6000-computers/#5db5ae55576e, 2019

24 Krebs, Brian, "REvil Ransomware Gang Starts Auctioning Victim Data", https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/, 2020

25 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, 2018

26 Krebs, Brian, "REvil Ransomware Gang Starts Auctioning Victim Data", https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/, 2020

27 Goodin, Dan, "LockBit Is the New Ransomware for Hire", https://www.wired.com/story/lockbit-is-the-new-ransomware-for-hire/, 2020

28 Virsec, "Maze & Other Ransomware Groups Say They Won't Attack Hospitals During COVID-19 Outbreak-But How Trustworthy Is Their Word?", https://virsec.com/maze-and-other-ransomware-groups-say-they-wont-attack-hospitals-during-covid19-outbreak-but-how-trustworthy-is-their-word/, 2020

29 Hammersmith Medicines Research, "HMR targeted by cyber criminals", https://www.hmrlondon.com/hmr-targeted-by-cyber-criminals, 2020

30 Intel 471, "Understanding the relationship between Emotet, Ryuk and Trickbot", https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/, 2020

31 AWS Shield, "Threat Landscape Report – Q1 2020", https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf, 2020

32 European Commission, "Preventing and Combating Child Sexual Abuse and Exploitation: Towards an EU Response", https://audiovisual.ec.europa.eu/en/video/I-191928, 2020

33 Canadian Centre for Child Protection, "International Survivors' Survey", https://protectchildren.ca/en/programs-and-initiatives/survivors-survey/, 2017

34 Europol, "Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic", https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic, 2020

35 Canadian Centre for Child Protection, "International Survivors' Survey", https://protectchildren.ca/en/programs-and-initiatives/survivors-survey/, 2017

36 Europol, "Partners & Agreements – Police2Peer: Targeting file sharing of child sexual abuse material", https://www.europol.europa.eu/partners-agreements/police2peer, 2020

37 Europol, "Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic", https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic, 2020

38 BBC News, "NSPCC urges Facebook to stop encryption plans", https://www.bbc.com/news/technology-51391301, 2020 and Musil, Steven, "Facebook urged to halt encryption push over child abuse concerns", https://www.cnet.com/news/facebook-urged-to-halt-encryption-push-over-child-abuse-concerns/, 2020

39 Europol, "International police cooperation leads to arrest of Darkweb child sex abuser in Spain", https://www.europol.europa.eu/newsroom/news/international-police-cooperation-leads-to-arrest-of-dark-web-child-sex-abuser-in-spain, 2020

40 Europol, "Operation CHEMOSH: how encrypted chat groups exchanged Emoji 'stickers' of child sexual abuse", https://www.europol.europa.eu/newsroom/news/operation-chemosh-how-encrypted-chat-groups-exchanged-emoji-%E2%80%98stickers%E2%80%99-of-child-sexual-abuse, 2020

41 Europol, "Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic", https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic, 2020

42 Wongsamuth, Nanchanok, "Online child sexual abuse cases triple under lockdown in Philippines", https://news.trust.org/item/20200529090040-3ejzo/ , 2020

43 Europol, "90 suspects identified in major online child sexual abuse operation", https://www.europol.europa.eu/newsroom/news/90-suspects-identified-in-major-online-child-sexual-abuse-operation, 2020

44 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2019*, 2019

45 Europol, "COVID-19: Child Sexual Exploitation", https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation, 2020

46 Europol, "COVID-19: Child Sexual Exploitation", https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation, 2020

47 Europol, "The SIM hijackers: How criminals are stealing millions by highjacking phone numbers", https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers, 2020

48 Europol, "The SIM hijackers: How criminals are stealing millions by highjacking phone numbers", https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers, 2020

49 Cimpanu, Catalin, "FBI: BEC scams accounted for half of the cyber-crime losses in 2019", https://www.zdnet.com/article/fbi-bec-scams-accounted-for-half-of-the-cyber-crime-losses-in-2019/, 2020.

50 Stupp, Catherine, "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case", https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, 2019

51 Krebs, Brian, "Wawa Breach May Have Compromised More Than 30 Million Payment Cards", https://krebsonsecurity.com/tag/jokers-stash/, 2020

52 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

53 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2019*, 2019

54 Digital Shadows, "Darkweb Search Engine Kilos: Tipping the Scales In Favor of Cybercrime", https://www.digitalshadows.com/blog-and-research/dark-web-search-engine-kilos/ , 2020

55 Digital Shadows, "Darkweb Search Engine Kilos: Tipping the Scales In Favor of Cybercrime", https://www.digitalshadows.com/blog-and-research/dark-web-search-engine-kilos/ , 2020

56 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

57 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

58 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

59 Europol, "Darkweb child abuse: administrator of Darkscandals arrested in the Netherlands", https://www.europol.europa.eu/newsroom/news/dark-web-child-abuse-administrator-of-darkscandals-arrested-in-netherlands, 2020

60 Europol, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, 2020

61 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

62 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

EUROPEAN
COMMISSION

Brussels, 10.9.2020
COM(2020) 568 final

2020/0259 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Objectives of the proposal

Directive 2002/58/EC ("ePrivacy Directive")[1] ensures the protection of private life, confidentiality of communications and personal data in the electronic communications sector. It implements Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("**Charter**") in secondary Union law.

On 21 December 2020, with the entry into application of the European Electronic Communications Code ("EECC")[2], the definition of electronic communications services will be replaced by a new definition, which includes number-independent interpersonal communications services. From that date on, these services will, therefore, be covered by the ePrivacy Directive, which relies on the definition of the EECC. This change concerns communications services like webmail messaging services and internet telephony.

Certain providers of number-independent interpersonal communications services are already using specific technologies to detect child sexual abuse on their services and report it to law enforcement authorities and to organisations acting in the public interest against child sexual abuse, and/or to remove child sexual abuse material. These organisations refer to national hotlines for reporting child sexual abuse material, as well as organisations whose purpose is to reduce child sexual exploitation, and prevent child victimisation, located both within the EU and in third countries.

Child sexual abuse is a particularly serious crime that has wide-ranging and serious life-long consequences for victims. In hurting children, these crimes also cause significant and long-term social harm. The fight against child sexual abuse is a priority for the EU. On 24 July 2020, the European Commission adopted an EU strategy for a more effective fight against child sexual abuse[3], which aims to provide an effective response, at EU level, to the crime of child sexual abuse. The Commission announced that it will propose the necessary legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and oblige them to report that material to public authorities by the second quarter of 2021. The announced legislation will be intended to replace this Regulation, by putting in place mandatory measures to detect and report child sexual abuse, in order to bring more clarity and certainty to the work of both law enforcement and relevant actors in the private sector to tackle online abuse, while ensuring respect of the fundamental rights of the users, including in particular the right to freedom of expression and opinion, protection of personal data and privacy, and providing for mechanisms to ensure accountability and transparency.

The providers of electronic communications services must comply with the ePrivacy Directive's obligation to respect the confidentiality of communications and with the conditions for processing communications data. The current practices of some number-

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

[2] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (OJ L 321, 17.12.2018, p. 36–214).

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM(2020) 607 final.

independent interpersonal communications services to detect child sexual abuse online could interfere with certain provisions of the ePrivacy Directive. The ePrivacy Directive does not contain an explicit legal basis for voluntary processing of content or traffic data for the purpose of detecting child sexual abuse online. Therefore, for the services falling within scope of the ePrivacy Directive, providers will be able to continue to apply such measures only if Member States adopt legislative measures justified on the grounds laid down in Article 15 of that Directive and meeting the requirements of that provision. In the absence of such national legislative measures and pending the adoption of the long-term legislation announced in the Commission Strategy of 24 July 2020, providers of number-independent interpersonal communications services would lack a legal basis for continuing to detect child sexual abuse on their services. Those voluntary activities play a valuable role in enabling the identification and rescue of victims, and reducing the further dissemination of child sexual abuse material, while also contributing to the identification and investigation of offenders, and the prevention of child sexual abuse offences.

The Commission considers that it is essential to take immediate action. The present proposal therefore presents a narrow and targeted legislative interim solution with the sole objective of creating a temporary and strictly limited derogation from the applicability of Articles 5(1) and 6 of the ePrivacy Directive, which protect the confidentiality of communications and traffic data. This proposal respects the fundamental rights, including the rights to privacy and protection of personal data, while enabling providers of number-independent interpersonal communications services to continue using specific technologies and continue their current activities to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services, pending the adoption of the announced long-term legislation. Voluntary efforts to detect solicitation of children for sexual purposes ("grooming") also must be limited to the use of existing, state-of-the-art technology that corresponds to the safeguards set out. This Regulation should cease to apply in December 2025. In case the announced long-term legislation is adopted and enters into force prior to this date, that legislation should repeal the present Regulation.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The relevant legal bases are Article 16 and Article 114 of the Treaty on the Functioning of the European Union ('TFEU').

Given that this Regulation provides for a temporary derogation from certain provisions of Directive 2002/58/EC, which was adopted on the basis of Article 95 of the Treaty establishing the European Community, it is appropriate to adopt this Regulation on the basis of the corresponding provision of Article 114 TFEU. In addition, not all Member States have adopted legislative measures in accordance with Article 15(1) of the ePrivacy Directive concerning the use of technologies by number-independent interpersonal communications service providers for the purpose of combatting child sexual abuse online, and the adoption of such measures involves a significant risk of fragmentation likely to negatively affect the internal market. Therefore, it is appropriate to adopt this Regulation on the basis of Article 114 TFEU.

Article 16 TFEU introduces a specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, by Member States when carrying out activities falling within the scope of Union law, and rules relating to the free movement of such data. Since an electronic communication involving

a natural person will normally qualify as personal data, this Regulation should also be based on Article 16 TFEU.

- **Subsidiarity (for non-exclusive competence)**

According to the principle of subsidiarity, EU action may only be taken if the envisaged aims cannot be achieved by Member States alone. EU intervention is needed to maintain the ability of providers of number-independent interpersonal communications services to voluntarily detect and report child sexual abuse online and remove child sexual abuse material, as well as to ensure a uniform and coherent legal framework for the activities in question throughout the internal market. Lack of Union action on this issue would risk creating fragmentation should Member States adopt diverging national legislation. In addition, such national solutions would most probably not be able to be adopted by 21 December 2020 in all Member States. Moreover, a Union wide derogation from the application of provisions of the ePrivacy Directive for certain processing activities can only be adopted by Union legislation. Therefore, the objective cannot be effectively reached by any Member State acting alone, or even Member States acting collectively.

- **Proportionality**

The proposal complies with the principle of proportionality as set out in Article 5 of the Treaty on European Union as it will not go beyond what is necessary for the achievement of the set objectives. It introduces a targeted and temporary derogation as regards certain aspects of changes to the current framework in order to ensure that certain measures remain permissible to the extent that they currently comply with Union law. In particular, the proposal creates a temporary and strictly limited derogation from the applicability of Articles 5 (1) and 6 of the ePrivacy Directive, with the sole aim of enabling providers of number-independent interpersonal communications services to continue using specific technologies and continue their current activities to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services, pending the adoption of the announced long-term legislation. This derogation from the revised scope of the ePrivacy Directive has to be interpreted narrowly, in particular as number-independent interpersonal communications services will remain subject to the e-Privacy Directive with regard to all their other activities. The proposal therefore contains safeguards to ensure that technologies benefitting from the derogation meet the standards of the best practices currently applied, and thereby limits the intrusiveness to the confidentiality of communications and the risk of circumvention. The derogation is limited to technologies regularly used by number-independent interpersonal communications services for the purpose of detecting and reporting child sexual abuse online and removing child sexual abuse material before the entry into force of this Regulation and ensures that the types of technologies used are the least privacy-intrusive in accordance with the state of the art in the industry. The providers should also publish annual reports on the undertaken processing. The duration of the derogation is limited to a time period strictly necessary to adopt the long-term legislation.

- **Choice of the instrument**

The objectives of the present proposal can best be pursued through a Regulation. This will ensure direct applicability of the provisions and ensure a uniform and coherent approach throughout the internal market. This is of particular importance as companies' actions to combat child sexual abuse online are applied in a uniform manner across their entire service; diverging national transposition measures might provide a disincentive when it comes to continuing the voluntary engagement. Moreover, only a Regulation appears to be able to meet the date of 21 December for entry into application.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

Not applicable

- **Stakeholder consultations**

Not applicable

- **Collection and use of expertise**

Not applicable

- **Impact assessment**

In view of the policy objective and the time-sensitive nature of the issue, there are no other materially different policy options available, and thus no impact assessment appropriate. In particular, the measure intends to introduce an interim and strictly limited derogation from the applicability of Articles 5(1) and 6 of the ePrivacy Directive to ensure that number-independent interpersonal communications service providers can continue to voluntarily using specific technologies to detect and report child sexual abuse online and to remove child sexual abuse material on their services after 20 December 2020, pending the adoption of long-term legislation. The long-term legislation will be proposed in the second quarter of 2021 as announced in the EU strategy for a more effective fight against child sexual abuse and will be accompanied by an impact assessment.

- **Fundamental rights**

The proposal takes full account of the fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union. In particular, the proposed measures take into account Article 7 of the Charter of Fundamental Rights of the European Union protects the fundamental right of everyone to the respect for his or her private and family life, home and communications, which includes the confidentiality of communications. In addition, the proposal takes into account Article 24(2) of the Charter which 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, to the extent that processing of electronic communications by number-independent interpersonal communications services for the sole purpose of detecting and reporting child sexual abuse online and removing child sexual abuse material falls into the scope of the derogation created by this proposal, the General Data Protection Regulation, which implements in secondary legislation Article 8(1) of the Charter, continues to apply to such processing.

4. BUDGETARY IMPLICATIONS

This proposal has no implications for the EU budget.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

Not applicable

- **Detailed explanation of the specific provisions of the proposal**

Article 1 defines the objective of the proposal to create a temporary and strictly limited derogation from the application of certain obligations of Directive 2002/58/EC, with the sole objective of enabling providers of number-independent interpersonal communications services to continue the use of technologies for the processing of personal and other data to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services.

Article 2 refers to the definition of number-independent interpersonal communications services in Directive (EU) 2018/1972 (European Electronic Communications Code) and to certain definitions in Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

Article 3 sets the scope of the derogation by creating a limited exemption to the obligations set by Articles 5(1) and 6 of the ePrivacy Directive for the processing of personal and other data in connection with the provision of number-independent interpersonal communications services necessary for the use of technology, including, where necessary, any human review directly relating to the use of the technology, for the sole purpose of detecting or reporting child sexual abuse online to law enforcement authorities and to organisations acting in the public interest against child sexual abuse as well as removing child sexual abuse material, and sets a list of conditions for such a derogation to apply.

Article 4 sets the dates for entering into force and into application of the Regulation and when or under which conditions the Regulation shall cease to apply.

2020/0259 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online

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 16(2), in conjunction with Article 114(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],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Directive 2002/58/EC of the European Parliament and of the Council[2] lays down rules ensuring the right to privacy and confidentiality with respect to the processing of personal data in exchanges of data in the electronic communication sector. That Directive particularises and complements Regulation (EU) 2016/679 of the European Parliament and of the Council[3].

(2) Directive 2002/58/EC applies to the processing of personal data in connection with the provision of publicly available electronic communication services. The definition of electronic communication service is currently to be found in Article 2, point (c), of Directive 2002/21/EC of the European Parliament and of the Council[4]. Directive (EU) 2018/1972 of the European Parliament and of the Council[5] repeals Directive 2002/21/EC with effect from 21 December 2020. From that date, the definition of electronic communications services will be replaced by a new definition, in Article 2(4) of Directive (EU) 2018/1972, which includes number-independent interpersonal

[1] OJ C , , p. .

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[4] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33).

[5] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

communications services as defined in Article 2(7) of that Directive. Those services, which include, for example, voice over IP, messaging and web-based e-mail services, will therefore fall within the scope of Directive 2002/58/EC, as of 21 December 2020.

(3) 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. Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications, which includes the confidentiality of communications. Article 8 of the Charter contains the right to protection of personal data. Article 24(2) of the Charter 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.

(4) Sexual abuse and sexual exploitation of children constitute serious violations of human rights, in particular of the rights of children to be protected from all forms of violence, abuse and neglect, maltreatment or exploitation, including sexual abuse, as provided for by the 1989 United Nations Convention on the Rights of the Child and by the Charter. Digitisation has brought about many benefits for society and the economy, but also challenges including an increase of child sexual abuse online. The protection of children online is one of the Union's priorities. On 24 July 2020, the Commission adopted an EU strategy for a more effective fight against child sexual abuse[6] ("the Strategy"), which aims to provide an effective response, at Union level, to the crime of child sexual abuse.

(5) Certain providers of number-independent interpersonal communications services, such as webmail and messaging services, are already using specific technologies to detect and report child sexual abuse online to law enforcement authorities and to organisations acting in the public interest against child sexual abuse, or to remove child sexual abuse material, on a voluntary basis. Those organisations refer to national hotlines for reporting child sexual abuse material, as well as to organisations whose purpose is to reduce child sexual exploitation, and prevent child victimisation, located both within the Union and in third countries. Collectively, those voluntary activities play a valuable role in enabling the identification and rescue of victims, and reducing the further dissemination of child sexual abuse material, while also contributing to the identification and investigation of offenders, and the prevention of child sexual abuse offences.

(6) Until 20 December 2020, the processing of personal data by providers of number-independent interpersonal communications services by means of voluntary measures for the purpose of detecting and reporting child sexual abuse online and removing child sexual abuse material is governed by Regulation (EU) 2016/679.

(7) Directive 2002/58/EC does not contain any specific provisions concerning the processing of personal and other data in connection with the provision of electronic communication services for the purpose of detecting and reporting child sexual abuse online and removing child sexual abuse material. However, pursuant to Article 15(1) of Directive 2002/58/EC, Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in, inter alia, Articles 5 and 6 of that Directive, which concern confidentiality of communications and traffic data, for the

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM(2020) 607 final.

purpose of prevention, investigation, detection and prosecution of criminal offences linked to child sexual abuse. In the absence of such legislative measures, and pending the adoption of a new longer-term legal framework to tackle child sexual abuse effectively at Union level as announced in the Strategy, there would be no legal basis for providers of number-independent interpersonal communications services to continue to detect and report child sexual abuse online and remove child sexual abuse material in their services beyond 21 December 2020.

(8) This Regulation therefore provides for a temporary derogation from Article 5(1) and Article 6 of Directive 2002/58/EC, which protect the confidentiality of communications and traffic data. Since Directive 2002/58/EC was adopted on the basis of Article 114 of the Treaty on the Functioning of the European Union, it is appropriate to adopt this Regulation on the same legal basis. Moreover, not all Member States have adopted legislative measures at national level to restrict the scope of the rights and obligations provided for in those provisions in accordance with Article 15(1) of Directive 2002/58/EC, and the adoption of such measures involves a significant risk of fragmentation likely to negatively affect the internal market.

(9) Given that electronic communications involving natural persons will normally qualify as personal data, this Regulation should also be based on Article 16 of the Treaty, which provides a specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions and by the Member States when carrying out activities which fall within the scope of Union law, and rules relating to the free movement of such data.

(10) To the extent that processing of personal data in connection with the provision of electronic communications services by number-independent interpersonal communications services for the sole purpose of detecting and reporting child sexual abuse online and removing child sexual abuse material falls within the scope of the derogation provided for by this Regulation, Regulation (EU) 2016/679 applies to such processing, including the requirement to carry out an assessment of the impact of the envisaged processing operations where appropriate pursuant to Article 35 of that Regulation prior to the deployment of the technologies concerned.

(11) Since the sole objective of this Regulation is to enable the continuation of certain existing activities aimed at combating child sexual abuse online, the derogation provided for by this Regulation should be limited to well-established technology that is regularly used by number-independent interpersonal communications services for the purpose of detecting and reporting child sexual abuse online and removing child sexual abuse material before the entry into force of this Regulation. The reference to the technology includes where necessary any human review directly relating to the use of the technology and overseeing it. The use of the technology in question should therefore be common in the industry, without it necessarily being required that all providers use the technology and without precluding the further evolution of the technology in a privacy-friendly manner. In this respect, it should be immaterial whether or not a particular provider that seeks to rely on this derogation itself already uses such technology on the date of entry into force of this Regulation. The types of technologies deployed should be the least privacy-intrusive in accordance with the state of the art in the industry and should not include systematic filtering and scanning of communications containing text but only look into specific communications in case of concrete elements of suspicion of child sexual abuse.

(12) In order to ensure accuracy and reliability as much as possible, the technology used should, in accordance with the state of the art in the industry, be such as to limit the error rate of false positives to the maximum extent possible and, where necessary, to rectify without delay any such errors that may nonetheless occur.

(13) The personal and other data used when carrying out the activities covered by the derogation set out in this Regulation, as well as the period during which the data is subsequently retained in case of positive results, should be minimised so as to ensure that the derogation remains limited to what is strictly necessary.

(14) In order to ensure transparency and accountability in respect of the activities undertaken pursuant to the derogation, the providers should publish reports on an annual basis on the processing falling within the scope of this Regulation, including on the type and volumes of data processed, number of cases identified, measures applied to select and improve key indicators, the numbers and ratios of errors (false positives) of the different technologies deployed, measures applied to limit the error rate and the error rate achieved, the retention policy and the data protection safeguards applied.

(15) This Regulation should enter into force on the third day following that of its publication in the *Official Journal of the European Union*, in order to ensure that it is applicable as from 21 December 2020.

(16) This Regulation restricts the right to protection of the confidentiality of communications and derogates from the decision taken in Directive (EU) 2018/1972 to subject number-independent interpersonal communications services to the same rules as all other electronic communications services as regards privacy. The period of application of this Regulation should, therefore, be limited until 31 December 2025, that is to say for a time period reasonably required for the adoption of a new long-term legal framework, with more elaborate safeguards. In case the long-term legislation is adopted and will enter into force before that date, that legislation should repeal this Regulation.

(17) Providers of number-independent interpersonal communications services should be subject to the specific obligations set out in Directive 2002/58/EC with regard to any other activities that fall within its scope.

(18) The objective of this Regulation is to create a temporary derogation from certain provisions of Directive 2002/58/EC without creating fragmentation in the Internal Market. In addition, national legislation would most probably not be adopted in time in all Member States. As this objective cannot be sufficiently achieved by the Member States, but can rather 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 Regulation does not go beyond what is necessary in order to achieve those objectives. It introduces a temporary and strictly limited derogation from the applicability of Articles 5 (1) and 6 of Directive 2002/58/EC, with a series of safeguards to ensure that it does not go beyond what is necessary for the achievement of the set objectives.

(19) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[7] and delivered its opinion on […],

HAVE ADOPTED THIS REGULATION:

Article 1
Subject matter

This Regulation lays down temporary and strictly limited rules derogating from certain obligations laid down in Directive 2002/58/EC, with the sole objective of enabling providers of number-independent interpersonal communications services to continue the use of technologies for the processing of personal and other data to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services.

Article 2
Definitions

For the purpose of this Regulation, the following definitions apply:

(1) 'number-independent interpersonal communications service' means a service as defined in Article 2(7) of Directive (EU) 2018/1972;
(2) 'child sexual abuse online' means:

(a) material constituting child pornography as defined in Article 2, point (c), of Directive 2011/93/EU of the European Parliament and of the Council;

(b) solicitation of children for the purpose of engaging in sexual activities with a child or of producing child pornography by any of the following:

(i) luring the child by means of offering gifts or other advantages;

(ii) threatening the child with a negative consequence likely to have a significant impact on the child;

(iii) presenting the child with pornographic materials or making them available to the child .

(c)'pornographic performance' as defined in Article 2(e) of Directive 2011/93/EU.

Article 3
Scope of the derogation

The specific obligations set out in Article 5(1) and Article 6 of Directive 2002/58/EC shall not apply to the processing of personal and other data in connection with the provision of number-independent interpersonal communications services strictly necessary for the use of technology for the sole purpose of removing child sexual

[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ C 20, 21.1.2019, p. 1).

abuse material and detecting or reporting child sexual abuse online to law enforcement authorities and to organisations acting in the public interest against child sexual abuse, provided that:

(a) the processing is proportionate and limited to well-established technologies regularly used by providers of number-independent interpersonal communications services for that purpose before the entry into force of this Regulation, and that are in accordance with the state of the art used in the industry and are the least privacy-intrusive;

(b) the technology used is in itself sufficiently reliable in that it limits to the maximum extent possible the rate of errors regarding the detection of content representing child sexual abuse, and where such occasional errors occur, their consequences are rectified without delay;

(c) the technology used to detect solicitation of children is limited to the use of relevant key indicators, such as keywords and objectively identified risk factors such as age difference, without prejudice to the right to human review;

(d) the processing is limited to what is strictly necessary for the purpose of detection and reporting of child sexual abuse online and removal of child sexual abuse material and, unless child sexual abuse online has been detected and confirmed as such, is erased immediately;

(e) the provider annually publishes a report on its related processing, including on the type and volumes of data processed, number of cases identified, measures applied to select and improve key indicators, numbers and ratios of errors (false positives) of the different technologies deployed, measures applied to limit the error rate and the error rate achieved, the retention policy and the data protection safeguards applied.

As regards point (d), where child sexual abuse online has been detected and confirmed as such, the relevant data may be retained solely for the following purposes and only for the time period necessary:

– for its reporting and to respond to proportionate requests by law enforcement and other relevant public authorities;

– for the blocking of the concerned user's account;

– in relation to data reliably identified as child pornography, for the creation of a unique, non-reconvertible digital signature ('hash').

Article 4
Entry into force and application

This Regulation shall enter into force on the third day following that of its publication in the Official Journal of the European Union.

It shall apply from 21 December 2020 until 31 December 2025.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*