BRIEFING PAPER

EMERGING GLOBAL THREATS RELATED TO THE ONLINE SEXUAL EXPLOITATION OF CHILDREN

INTRODUCTION

Information and communication technologies (ICTs) are now an integral and positive component of modern life. They are as important to the educational and social development of children and young people as they are to the overall global economy. Yet their emergence as mass consumer products has also generated a number of unforeseen and unintended consequences. Technology is evolving rapidly thereby creating a constant shift in the forms through which online sexual exploitation of children occurs.

Around the world, the rapidly expanding Internet space is making more children vulnerable to sexual exploitation and abuse. As Internet up-take rates climb in many parts of the developing world, the potential negative impact of ICTs on children could be disproportionately severe because: (i) parents, policymakers and children have less awareness of the related risks, and (ii) laws, law enforcement and social services may be lacking or scarce in comparison to more developed countries. Moreover, the nature of the Internet means that a growth in online child sexual abuse material (CSAM) anywhere can have an impact everywhere. All countries thus have a stake in controlling this spread.

THE MAJOR GLOBAL THREATS FACILITATED BY ICT EXPANSION AND INNOVATIONS ARE:

Greater circulation of child sexual abuse material, increasingly through peer-to-peer (P2P) file- sharing platforms and the Darknet: The volume and scale of CSAM on these platforms has reached unprecedented levels: many individual offenders have been found to possess millions of images.[1] The US National Centre for Missing and Exploited Children (NCMEC) received 78,946 reports from the public and 1,027,126 reports from Electronic Service Providers in 2014 related to the presence of child abuse material online and other related incidents.[2] NCMEC's Child Victim Identification Program has also reported processing over 150 million images and videos through its Child Recognition and Identification System in 2014[3] and the UK's Internet Watch Foundation processed 68,092 reports in 2015.[4] Data from INHOPE (2014) indicates that 91% of child sexual abuse materials they processed was non-commercial. Additionally, the "Darknet" and other encrypted software techniques allow users to access and disseminate CSAM anonymously. Those legitimate services and features available thanks to the advancement of technologies are challenging for specialised law enforcement units in charge of investigating CSAM cases. For example, the Onion Router (TOR) is a tool used to conceal the location and identity of the user who is sharing or accessing CSAM. A study indicated that only 2% of hidden web services on TOR hosted CAM, yet these 2% of CAM sites accounted for 80% of traffic.[5] Furthermore, "many police officers commented that TOR is probably more commonly used to share child sexual abuse material than what is reflected in the investigations".[6] Due to their hidden nature, it is impossible to accurately quantify the extent of these illegal activities; however, law enforcement agencies around the world agree that the scale is substantial. CEOP estimated that there were around 50,000 individuals in the UK involved in downloading and sharing child sexual abuse material during 2012.[7]

[1] INHOPE 2014, Facts, Figures and Trends: http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx

[2] NMEC quoted in INTERPOL: size of the problem (8 July 2015), unpublished.

[3] Jennifer Newman and Cierra Buckman, "Child Pornography Offending: Analysis of Data from the National Center for Missing & Exploited Children" (presentation at the Dallas Children's Advocacy Center 27th Annual Crimes Against Children Conference, Dallas, TX, USA, 10-13 August, 2015).

[4] Internet Watch Foundation, "Annual Report 2015", accessed 15 January 2017.

[5] Dr. Gareth Owen, "TOR: Hidden Services and Deanonymisation," (January 2015) quoted in INTERPOL: Online Child Sexual Exploitation- the size of the problem (8 July 2015), 2.

[6] NetClean (2016), "The NetClean Report 2016: Ten important insights into child sexual abuse crime", December 2016, 16, accessed 21 December 2016. http://www.netclean.com.

[7] CEOP/NCA, "Threat Assessment of Sexual Exploitation and Abuse," (2013) quoted in INTERPOL: size of the problem (8 July 2015), 2

In addition to anonymous file-sharing platforms, offenders share materials through websites, file and image hosting services and social network sites. File and images hosting only accounted for 62% in 2014 according to INHOPE while IWF confirmed that image hosts made up to 78% of all confirmed CSAM reports (2015). The UK-based hotline also noted a rise in disguised websites.[8]

Use of cloud-based services and internet-enabled mobile devices: Child sex offenders no longer have to risk carrying incriminating evidence through customs or border checkpoints. Instead, they can abuse children, document the abuse through a mobile phone camera or other easily portable video device, and upload the stills and videos to cloud services to be accessed when they return home. While discussing trends concerning the technological change to 2021 and affecting all forms of crime, the UK-based National Crime Agency emphasises that, "there will be a further substantial shift to mobile and portable computing via smart phones and tablets, and criminals –like the public at large – will adopt new methods of communications as they are developed (mirroring the rapid adoption of VoIP platforms and WhatsApp in place of telephony and SMS texting respectively)".[9]

Increase in live streaming of child sexual abuse: The increased use of live video streaming of child sexual abuse continues to be identified as a growing threat to children by EUROPOL[8] and other law enforcement agencies. This particular form of sexual exploitation transcends borders by allowing child predators to be located anywhere, while abusing their victims through a streamed live presentation. The phenomenon first received widespread public attention in South East Asia, but now appears to be spreading to other regions.[10]

Growth in the sexual extortion and coercion online and in the production of self-generated ("sexting") child sexual abuse materials: First, more and more children are being lured with money or gifts by offenders who entice them into creating and sharing indecent photos of themselves. EUROPOL notes, "Both content and financially driven extortion is based on the threat to disclose the images on the Internet and/or send directly to friends, family, schools, etc."[11] Offenders use methodologies ranging from traditional grooming techniques to more coercive techniques (e.g. sextortion). According to INTERPOL, where coercive techniques are used, an emerging trend has been identified towards more extreme, violent, sadistic or degrading demands by offenders. Often time the control over their victim is a greater driver for offenders than the pursuit of a sexual outcome.[12]

Second, the phenomenon of "sexting" has increased among adolescents, who willingly produce erotic/pornographic images of themselves, typically to share with their current "partner." These partners, however, often disseminate the images, which then end up in the possession of child sexual abuse material collectors. Some of the key findings of a study with a sample of 3,803 youth-produced images and videos conducted by the Internet Watch Foundation in 2015 reveal that:

- 17.5% of content analysed depicted children aged 15 years or younger;
- 85.9% of content depicting children aged 15 or younger was created using a webcam;
- 93.1% of the content depicting children aged 15 or younger featured girls;
- 89.9% of the total images and videos assessed as part of the Study had been harvested from the original upload location and were being redistributed on third party websites.

In line with this, another research shows that 88% of self-generated, sexually explicit content online was taken from its original location and uploaded to a different Internet site.[13]

[8] Internet Watch Foundation Annual and Charity Report 2015, p.18, https://www.iwf.org.uk/assets/media/annual-reports/IWF%202015%20Annual%20Report%20Final%20for%20web.pdf

[9] National Crime Agency (2016), "National Strategic Assessment of Serious and Organised Crime 2016", September 2016, accessed 2 November 2016, http://www.nationalcrimeagency.gov.uk/publications/731-national-strategic-assessment-of-serious-and-organised-crime-2016/file.

[10] EUROPOL, "Internet Organised Crime Threat Assessment (IOCTA) 2016", accessed 21 November 2016, p.26, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

[11] Ibid.

[12] CEOP/NCA, "Threat Assessment of Sexual Exploitation and Abuse" (2013) quoted in INTERPOL: size of the problem (8 July 2015).

[13] Study on the Effects of Information and Communication Technologies on the Abuse and Exploitation of Children, United Nations Office on Drugs and Crime, 2015, https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf

Exploitation of young children: The primary trend among abusers is to target infants and pre-pubescent children. The 2015 report by Internet Watch Foundation noted that children assessed as being aged 10 years or under represented 69% of the victims, whereas Canada's tipline for reporting the online sexual exploitation of children early 2016 shared that 78.3% of the children in the images and videos they analysed were estimated to be younger than 12 year old.[14] Statistics on online child abuse material published by INHOPE in 2014 revealed that 7% of the victims were infants, compared to 6% in 2011.[15] In 2013 a number of business websites in the U.K. were hacked to show images of extreme sexual abuse of children under two years old; 227 reports of this practice were made within a six-week period.[16] As of 1 June 2015, the International Child Sexual Exploitation database (ICSE) held images of 6,672 unique identified victims in different age ranges. Unfortunately, there are still some 40,000 victims[17] in the database waiting to be identified, among whom there are very young children.

Use of the virtual currency Bitcoins to purchase CSAM: Various parties, including the FBI and Europol warn about the risks of virtual currencies, particularly crypto currencies such as Bitcoin, being an attractive payment system for those trying to trade illicit goods including child sexual abuse material. There are known instances of child sexual abuse material being exchanged via anonymous platforms in exchange for Bitcoins.[18] According to EUROPOL, a continued increase in the use of payment systems that offer more anonymity than traditional payment methods is to be expected and they may become the currency of choice for various manifestations of child sexual exploitation online, including financially drive sexual extortion of children and live online child sexual abuse.[19] Law enforcement agencies are clear that these mechanisms pose an ongoing, but as of yet unquantifiable, threat in the context of child sexual abuse.

Background information about ECPAT International

ECPAT is a network of 95 national or local member organisations in 86 countries, of which many are national coalitions. The ECPAT Network aims to build collaboration among local civil society actors and the broader child rights community to form a global social movement for protection of children from sexual exploitation. Its membership reflects the richness and diversity of experience, knowledge and perspectives that arise from working in widely different contexts. ECPAT member organizations are involved in implementing a range of initiatives to protect children.

The ECPAT International Secretariat, based in Bangkok Thailand, serves the Network. It provides technical support and information and organises learning events to extend and exchange the knowledge of its members. The Secretariat also represents and advocates on key issues at the international and regional levels on behalf of the Network.

For more information, please visit www.ecpat.org.

[14] Internet Watch Foundation Annual and Charity Report 2015, op.cit. and Child Sexual Abuse Images on the Internet, A Cybertip.ca Analysis, January 2016, https://www.cybertip.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf

[15] INHOPE, op. cit.

[16] Internet Watch Foundation, 2013, 'Websites hacked to host "the worst of the worst" child sexual abuse images. http://www.iwf.org.uk/about-iwf/news/post/367-websites-hacked-to-host-the-worst-of- the-worst-child-sexual-abuse-images

[17] INTERPOL, "Online Child Sexual Exploitation – the size of the problem" (8 July 2015), 2.

[18] European Banking Authority (2014), "EBA Opinion on virtual currencies", https://www.eba.europa.eu/documents.10180/657547/EBA-Op-201-08+Opinion+on+Virtual+Currencies.pdf

[19] EUROPOL, Commercial Sexual Exploitation of Children Online, European Financial Coalition, Oct. 2013, p.15. http://www.europeanfinancialcoalition.eu/private10/images/document/5.pdf and Internet Watch Foundation, Briefing Paper – Preliminary Analysis of New Commercial CSAM Website Accepting Payment by Bitcoin, January 2014. https://www.iwf.org.uk/assets/media/Briefing%20Paper%20-%20Preliminary%20Analysis%20into%20Commercial%20CSAM%20Distributor%20Accepting%20Bitcoin%20Payment%20Sanitised%20Not%20Restricted.pdf