COVID-19 AND THE SEXUAL EXPLOITATION OF CHILDREN ONLINE

The COVID-19 crisis triggered an unprecedented rise in the production and distribution of child sexual abuse material, child sexual exploitation material, live streams of child sexual abuse and, especially, self-generated sexual content involving children. During the onset of the pandemic, both children and child sex offenders were forced to stay home due to lockdown measures. More time at home led to more time spent online, which significantly increased sexual exploitation of children online.

This article analyses the different types of sexual exploitation of children online and the significant increase of cases reported during the pandemic. In addition, it cites some of the latest trends across the globe and the critical role that financial institutions play in undermining the commercialisation of online child sexual abuse and exploitation.

COVID-19 isolation abruptly pushed children's daily lives online, resulting in higher levels of emotional vulnerability as they sought alternative ways to socialise, whilst unaware of the risks associated. According to Insafe, a national helpline network that works with INHOPE through Safer Internet Centres (SICs)[1] across Europe,

European helplines had a sharp increase in calls received during the second quarter of 2020. Over 19,000 calls were for online-related issues, representing a 70% increase for the same reporting period in 2019.[2] In addition, there was an increase in the number of calls for grooming, sextortion and sexual harassment, between the third and fourth quarter of 2020.[3]

Differentiating child sexual exploitation material from child sexual abuse material

The term 'child sexual exploitation material' (CSEM) is an umbrella term that refers to all sexualised material depicting children and material that exploits a child, although it does not explicitly depict sexual abuse. The term 'child sexual abuse material' (CSAM) is a subset of 'child sexual exploitation material' and it refers to sexualised material depicting acts of sexual abuse. The main difference between CSEM and CSAM lies in the exchange of any type of benefit—including monetary gain—for the exploitation. It is worth noting that exchange is common in the context of CSAM, as it is often exchanged either for other CSAM or for financial gain. Consequently, the material may be both abusive and exploitative simultaneously.[4]

Live streaming child sexual abuse

Live streams of child sexual abuse are ephemeral video transmissions over the internet streamed in real time. The abuse can be carried out in relative secrecy leaving little or no trace of the abuse, which enables child sex offenders to avoid detection by law enforcement authorities. Unlike the commercialisation of CSAM/CSEM, live online child sexual abuse relies primarily on traditional money services businesses and banks, rather than cryptocurrency. One of the driving forces for live online child sexual abuse is poverty, especially in countries of the Global South. Liquidity is also a key factor as impoverished individuals engage in live online child sexual abuse to survive.[5]

Self-generated sexual content involving children

According to a September 2020 Interpol report, there has been an increase in self-generated sexual content from children.[6] The term 'self-generated' refers to sexualised material, which could be illegal and/or coerced, that is created by children (in particular adolescents). Some children say that 'self-produced images provide advantages in their relationships and/or increased self-esteem.'[7] It is worth noting that adults may have preconceived opinions on this phenomenon due to the media mostly relaying negative stories. Although material that is not shared beyond trusted individuals may have no negative consequences, it is important to consider the inherent risks of this phenomenon and that it can be considered a criminal offence in some countries.

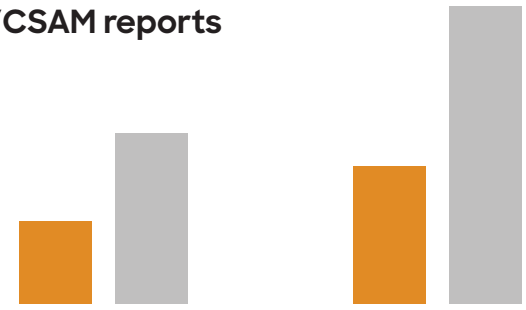
Although children may willingly produce sexual material, this does not mean they consent to or are responsible for the abusive or exploitative use and/or distribution of this material. It is important to consider the reasons behind the production of this material, such as potential grooming, coercion or extortion. It is possible that another person has dictated the sexual acts depicted, especially in cases when much younger children appear in such content.[8] As a result, it is important to emphasise that the term 'self-generated' should not stigmatise the child—implicitly or inadvertently—for the abuse and exploitation that may result from generating or sharing material against their will. The COVID-19 outbreak also led to a marked increase in 'capping', where child sex offenders capture screenshots during live streams with children. They then distribute or use these images to extort children and obtain more material.[9]

In Europe

Europe has become the largest host of CSAM/CSEM. In 2019, the Internet Watch Foundation (IWF) found that 89% of the 132,676 reported web addresses containing CSAM/CSEM content were hosted in Europe.[10] Moreover, the European Commission highlighted that the number of reports in relation to CSAM/CSEM concerning Europe has dramatically increased over the last decade.[11]

Whilst it is not considered to be primarily driven by financial gain, Europol expressed concerns about the emerging threat of CSAM/CSEM commercialisation.[12] In July 2020, the European Commission highlighted that the demand for CSAM/CSEM increased by 25% in some EU member states as a result of the COVID-19 outbreak.[13]

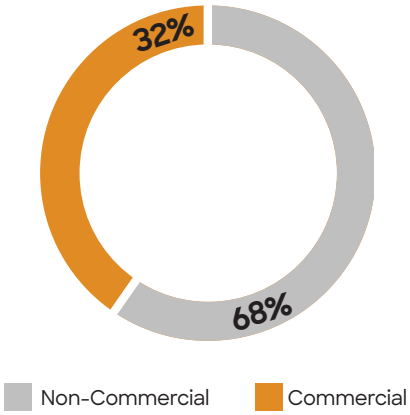
Figure 1: **CSEM/CSAM reports**



	CSEM/CSAM reports	Confirmed CSEM/CSAM
2017	87,930	148,041
2019	183,788	320,672

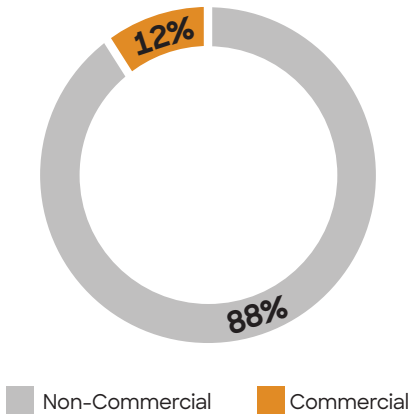
Source: INHOPE, 2019 Annual Report

Figure 2: **Hidden services hosting CSEM/CSAM (2019)**



Source: Internet Watch Foundation

Figure 3: **Webpages hosting CSEM/CSAM (2019)**



Source: Internet Watch Foundation

The dark web

The majority of CSAM/CSEM is exchanged, bought and sold online. Consequently, the online dimension of this crime is almost omnipresent. Today, using the internet to commit sexual offences against children is easier than ever, whether it is used to get in contact with children or to find like-minded offenders. The internet makes it easier to produce, access and distribute CSAM/CSEM through open networks as well as over the dark web and peer-to-peer networks.[14]

INHOPE traced CSAM/CSEM in more than 60 countries worldwide and highlighted that the number of anonymous reports to its hotlines doubled from 2017 to 2019. In 2019, 183,788 reports were submitted, and 320,672 illegal images and videos were processed (see Figure 1).[15]

On the other hand, IWF has observed a rising trend in commercial hidden services on the dark web since 2016. These hidden services offer CSAM/CSEM for sale and often contain hundreds or thousands of links to CSAM/CSEM hosted on cyberlockers. In 2019, IWF noted a 238% increase of these hidden services, compared to the previous year and highlighted that 68% of the 288 newly identified hidden services were for commercial use (see Figure 2). In addition to hidden services, IWF found a 7% increase in webpages containing CSAM/CSEM and highlighted that 12% of the 132,676 webpages identified were commercial in nature (see Figure 3).

Cryptocurrency

Due to their anonymous nature, these hidden services and websites only accept payments in cryptocurrency. Although anonymity may be useful for legitimate technological purposes, especially in a hyperconnected world, anonymity is also appealing to perpetrators of sexual crimes against children. According to ECPAT International, 'There is an apparent migration of online child sexual exploitation from more traditional payment systems (such as credit cards) to anonymising tools and (pseudo) anonymous payment systems including virtual currencies."[16] In 2019, Chainalysis reported that less than 930,000 US dollars' worth of bitcoin and Ethereum payments went to addresses associated with CSAM/CSEM providers. However, it still represents a 212% increase over 2017, mainly attributed to the rising adoption of cryptocurrency.[17]

In order to evade detection, perpetrators of sexual crimes against children may need to find alternatives that offer additional layers of anonymity, such as altcoins like Monero, or anonymising tools and platforms such as mixers/tumblers and

peer-to-peer exchangers. It is important to point out that the volume of CSAM/CSEM is such that child sex offenders may simply not pay for it and rather exchange CSAM/CSEM within networks of like-minded individuals at no cost. Therefore, CSAM/CSEM has an exchange value that can be considered a currency itself.

Social media and online gaming

As part of the online grooming process, child sex offenders can make payments to children to gain their trust and/or convince them to share sexualised material of themselves. The extortion process may be financially driven as child sex offenders can pressure victims into paying money by threatening to disclose this material to their peers or relatives if they do not pay. These payments can be conducted with both fiat currencies and cryptocurrencies. The grooming process may be initiated via social media platforms, which are not necessarily anonymous, as well as gaming platforms, where child sex offenders may use virtual currencies in online games.[18] Child sex offenders may then suggest migrating to more anonymous platforms where extortion begins.

In 2020, the global games market generated 159.3 billion US dollars in revenue, and the number of gamers worldwide is expected to exceed three billion by 2023.[19] Social interaction is at the core of these platforms as users or players seek to build virtual relationships, which are often paramount in the context of online gaming. In fact, some gaming platforms are growing into full-fledged social networks. Even with the large appeal of online gaming for child sex offenders, the largest electronic service providers' reports on child sexual abuse/exploitation to the US' National Center for Missing & Exploited Children's CyberTipline include social media platforms.[20]

The role of financial institutions

The financial sector plays a critical role in the global fight against online sexual exploitation of children. Money transfer services, online payment services and cryptocurrency providers must be involved to undermine the commercialisation of online child sexual abuse and exploitation. Only 22% of bankers and financial investigators feel confident in detecting crypto-related payments.[21] Therefore, it is necessary to understand the use of cryptocurrencies and the true extent to which these facilitate online sexual exploitation of children to impede payments for this crime, especially since Europe has become the largest host for CSAM/CSEM. Some reports with further information include 'The Chainalysis 2021 Crypto Crime Report',[22] the 'Cryptocurrency Crime and Anti-Money Laundering Report'[23] and the 'Cryptocurrency and the BlockChain: Technical Overview and Potential Impact on Commercial Child Sexual Exploitation.'[24]

In addition, Europe has the highest count of virtual asset service providers (VASPs) with weak know your customer (KYC) procedures.[25] Thus, collaborating with companies focused on blockchain analytics and forensics may raise awareness and leverage expertise as they play an indispensable role to de-anonymise cryptocurrency, which may result in successful investigations and prosecutions.[26]

Implementing effective KYC protocols for VASPs, which are crucial for any anti-money laundering (AML) regime, can help identify individuals engaged in online sexual exploitation of children and report these payments. VASPs can also reference the Financial Action Task Force's 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' for recommendations.[27] In addition, suspicious activity reports and suspicious transaction reports constitute valuable intelligence that may lead to successful investigations and prosecutions.

It is extremely difficult to detect live online child sexual abuse, which makes it a severely underreported crime. In addition, it occurs through private communications, which are increasingly using end-to-end encryption and child sex offenders themselves may use additional defensive methods. Nevertheless, live online child sexual abuse is primarily driven by financial gain and the flow of money may be the evidence that links perpetrators to this crime.

Conclusion

According to the EU strategy for a more effective fight against child sexual abuse, "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."[28] The cooperation between all stakeholders such as law enforcement, civil society and the private sector, as well the adoption of a multi-disciplinary approach, are essential to deliver a suitable response to this crime. Therefore, it is time to break the business model of online child sexual exploitation and disrupt the supply chain and demand for CSAM/CSEM. It is necessary to act on behalf of the innocent children who have endured appalling suffering and hold perpetrators of sexual crimes accountable to prevent other children from suffering the same horrible fate in the future.

Jonathan Dupont, analyst, financial intelligence unit, Lithuania, jonathandupont@protonmail.com

1 "Insafe and INHOPE," *Better Internet for Kids*, https://www.betterinternetforkids.eu/policy/insafe-inhope

2 "Latest helpline trends: Quarter 2, 2020," *Better Internet for Kids*, 25 September 2020, https://www.betterinternetforkids.eu/practice/helplines/article?id=6473739

3 "Latest helpline trends: Quarter 4, 2020," *Better Internet for Kids*, 30 March 2021, https://www.betterinternetforkids.eu/practice/helplines/article?id=6806753

4 "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse," *Interagency Working Group in Luxembourg*, 28 January 2016, https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf

5 "Online Sexual Exploitation of Children: A Crime with a Global and an Evolving Transnational Threat," *Republic of the Philippines Anti-Money Laundering Council*, http://www.amlc.gov.ph/news-and-announcements/16-news-and-announcements/238-amlc-study-on-online-sexual-exploitation-on-children

6 "INTERPOL report highlights impact of COVID-19 on child sexual abuse," *Interpol*, 7 September 2020, https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse

[7] "The Circulation of Sexual Images Taken by Children Themselves on the Rise amongst Offenders," *ECPAT International*, 18 November 2020, https://ecpat.exposure.co/end-child-sex-abuse-day-2020

[8] "'Deeply dark criminal activity' drives rise in child abuse images online," *The Guardian*, 3 December 2020, https://www.theguardian.com/global-development/2020/dec/03/deeply-dark-criminal-activity-drives-rise-in-child-abuse-images-online.

[9] "Child abuse predator 'handbook' lists ways to target children during coronavirus lockdown," *The Guardian*, 13 May 2020, https://www.theguardian.com/society/2020/may/14/child-abuse-predator-handbook-lists-ways-to-target-children-during-coronavirus-lockdown

[10] "IWF 2019 Annual Report Zero Tolerance," *Internet Watch Foundation*, 27 April 2020, https://www.iwf.org.uk/report/iwf-2019-annual-report-zero-tolerance

[11] "EU strategy for a more effective fight against child sexual abuse," *European Commission*, 24 July 2020, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf

[12] "Internet Organised Crime Threat Assessment (IOCTA) 2020," *Europol*, 5 October 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[13] "Delivering on a Security Union: initiatives to fight child sexual abuse, drugs and illegal firearms," *European Commission*, 24 July 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1380

[14] "Why Children are at Risk of Sexual Exploitation during COVID-19," *ECPAT International*, 7 April 2020, https://ecpat.exposure.co/covid19?utm_source=Website&utm_campaign=Hero

[15] "INHOPE Launches 2019 Annual Report," *INHOPE*, 22 July 2020, https://www.inhope.org/EN/articles/inhope-launches-2019-annual-report

[16] "Online Child Sexual Exploitation: An analysis of Emerging and Selected Issues," *ECPAT International Journal*, Issue 12 April 2017, https://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf

[17] "Making Cryptocurrency Part of the Solution to Human Trafficking," *Chainalysis Insights*, 21 April 2020, https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020

[18] "The Rising Danger of Child Trafficking in Online Gaming," *ECPAT USA*, 23 December 2019, https://www.ecpatusa.org/blog/2019/12/11/the-rising-danger-of-child-trafficking-in-online-gaming

[19] "Newzoo Global Games Market Report 2020, Light Version," *Newzoo*, https://newzoo.com/insights/trend-reports/newzoo-global-games-market-report-2020-light-version/

[20] "2019 Reports by Electronic Service Providers (ESP), *National Center for Missing and Exploited Children*, https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf

[21] Pamela Clegg, "Only 22% of Bankers and Financial Investigators Feel Confident Detecting Crypto-Related Payments," *CipherTrace*, 10 December 2020, https://ciphertrace.com/only-22-percent-of-bankers-feel-confident-detecting-crypto-related-payments/

[22] "The Chainalysis 2021 Crypto Crime Report," *Chainalysis*, 2021, https://go.chainalysis.com/2021-Crypto-Crime-Report.html

[23] "Cryptocurrency Crime and Anti-Money Laundering Report, February 2021," *Ciphertrace*, 2021, https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/

[24] Eric Olson and Jonathan Tomek, "Cryptocurrency and the BlockChain: Technical Overview and Potential Impact on Commercial Child Sexual Exploitation," *International Centre for Missing & Exploited Children*, May 2017, https://www.icmec.org/cryptocurrency-and-the-blockchain-technical-overview-and-potential-impact-on-commercial-child-sexual-exploitation/

[25] "2020 Geographic Risk Report: VASP KYC by Jurisdiction," *CipherTrace*, https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/

[26] Kelly Phillips Erb, "IRS Followed Bitcoin Transactions, Resulting In Takedown Of The Largest Child Exploitation Site On The Web," *Forbes*, 16 October 2019, https://www.forbes.com/sites/kellyphillipserb/2019/10/16/irs-followed-bitcoin-transactions-resulting-in-takedown-of-the-largest-child-exploitation-site-on-the-web/?sh=7ec05ecb1ed0; "US law enforcers partner with cryptocurrency tracking firm to fight financial crime," *Thomson Reuters*, 23 December 2020, https://www.thomsonreuters.com/en-us/posts/corporates/cryptocurrency-financial-crime/

[27] "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," *Financial Action Task Force*, 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

[28] "EU strategy for a more effective fight against child sexual abuse," *European Commission*, 24 July 2020, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf