Tanja MILOSHEVSKA

UDK: 343.541-053.2:004.738.5]:616.98:578.834}0 36.31(100)
Review article

THE COVID-19 IMPACT ON GLOBAL POLICE RESPONSE IN RELATION TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Abstract:

In this paper we draw attention that there have been significant increases in activity relating to child sexual abuse and exploitation on both the surface web and dark web during the COVID-19 lockdown period. This paper aim is an analyse about how the COVID-19 pandemic is presently modifying the trends and threats of child sexual exploitation and abuse offences, which were already at high levels prior to the pandemic. This article highlights the trends and threats in the current COVID-19 context compared to pre-pandemic measures, what impact these are having in the short-term, and what changes we have seen when COVID-19 measures are reduced. It contributes to the space of the dark web during lockdown by manifestation on the ongoing organised business model that has evolved as technology expands and the level of threat that it poses to children. The objective is to share these trends across the global law enforcement community and science in order to improve the monitoring and detection of child sexual exploitation and abuse online, further investigations and global police response.

Keywords: *child sexual exploitation, abuse, Europol, Interpol, Dark web, Covid-19.*

Introduction

The COVID-19 pandemic and measures taken by many governments to restrict its spread are likely to have had an impact on the trends and threats of child sexual exploitation and abuse (CSEA) offences across the world.

Law enforcement agencies, government and non-government organizations (NGOs) globally have expressed concerns regarding the impact COVID-19 isolation measures may have on crimes against children (ECPAT, 2020). With the closure of schools and other support services, the likely increase in online time, and the confinement at home (UNICEF, 2020) it is considered that children may be at an increased risk of sexual exploitation both online and offline.

Online Child Sexual Abuse[1]refers to the sexual abuse and exploitation of children via the internet. Whereas the sexual abuse or exploitation very much takes place in the physical world, the subsequent sharing of images and videos depicting this abuse significantly aggravates the impact of this crime on victims. The amount of CSAM already online was staggering and it has continued to increase during the pandemic with statistics indicating that the amount of material has rapidly increased in some countries. While the number of young children accessing the internet has grown significantly over recent months, awareness of the potential risks remains low and cases of online sexual abuse and exploitation have increased significantly (Europol, 2020).

The following shifts in environmental, social and economic factors are of specific consideration in this paper:

- The closure of schools and subsequent movement to virtual learning environments;
- The increased time children spend online for entertainment, social and educational purposes;
- The restriction of international travel and the repatriation of foreign nationals;
- Confinement measures leading to increased time spent at home;
- Limited access to community support services, child care and educational personnel who often play a key role in detecting and reporting cases of child sexual exploitation.

Terminology

Online Child Sexual Abuse and Exploitation (CSAE) is used throughout this information resource to capture all types of offence. Online CSAE Offending can take a number of different forms which include:

[1]The terms child sexual abuse and child sexual abuse material includes child sexual abuse material and material that may be produced through the exploitation of a child in exchange for some material gain. It is used in this paper in accordance with the Terminology guidelines for the protection of children from sexual exploitation and sexual abuse, accessible at http://luxembourgguidelines.org/

Online Grooming - The act of developing a relationship with a child to enable their abuse and exploitation both online and offline. Online platforms, such as social media, messaging and live streaming, can be used to facilitate this offending.

Live Streaming – Live streaming services can be used by Child Sex Offenders (CSOs) to incite victims to commit or watch sexual acts via webcam. CSOs also stream or watch live contact sexual abuse or indecent images of children with other offenders. In some instances, CSOs will pay facilitators to stream live contact abuse, with the offender directing what sexual acts are perpetrated against the victim.

Online coercion and blackmail – The coercion or blackmail of a child by technological means, using sexual images and/or videos depicting that child, for the purposes of sexual gain (e.g., to obtain new IIOC or bring about a sexual encounter), financial gain or other personal gain.

Possession, production and sharing of IIOC and Prohibited Images– CSOs can use online platforms to store and share IIOC and prohibited images. Online platforms can also be used to facilitate the production of IIOC, for example screen-recording of CSEA perpetrated over live streaming.

Indecent Images of Children (IIOC) are images of, or depicting, a child or part of a child which are judged to be in breach of recognised standards of propriety. Examples of images considered to be indecent are those depicting a child engaging in sexual activity or in a sexual manner, through posing, actions, clothing etc. IIOC includes photographs, videos, pseudo-photographs and tracings.

Prohibited Images of Children are non-photographic images, for example cartoons etc, which portray a child engaging in sexual activity, a sexual act being performed in the presence of a child or focus on the child's genital or anal region (National Crime Agency, 2023).

Evolution of crime trends and threats due to COVID-19

Confinement measures are increasing the amount of time children and adults spend online for educational, professional, entertainment and social purposes, and are creating an inadvertent risk of sexual exploitation by predators operating online (FBI, 2020). Information from multiple sources including INTERPOL member countries indicate a significant increase in the sharing of CSEAM through the use of peer-to-peer networks during the COVID-19 pandemic.

Viral content does not necessarily have a correlation with the number of offender's active online or the number of unique CSEAM being distributed. Nevertheless, the continuous re-victimization of the victim and the increased risk of innocent members of the public being inadvertently exposed to CSEAM means

the effective management of viral CSEAM content on the clear net is an important factor.

Besides the significant increase in viral control, several countries have reported some notable increases and trends in the distribution of CSEAM on the clear net:

• An increase in users on clear net applications discussing and sharing child abuse material;

• An increase in the distribution of self-generated material (Interpol, 2020).

Data from INSAFE, a global network of helplines against CSAM and negative online behaviours, shows the contacts made to helplines in the first quarter of 2020 saw a sharp increase compared to previous periods, resulting in the highest number of contacts in one quarter in the last four years (Europol, 2020a). The increase in contacts may reflect the figures referred to in previous Europol (2020a) and other reports (ECPAT, 2020) on the increased vulnerability and isolation of many children during this period.

Tech-facilitated CSECusually starts with grooming (establishing a relationship with a minor victim), then 'sexting' (creating and/or sharing sexually suggestive images of the victim), sextortion (blackmailing the child victim with their own images to extort sexual favours or money) or live sexual abuse (coercing a child into sexual activities) and CSAM sexualized materials depicting children (Bird at all, 2020).

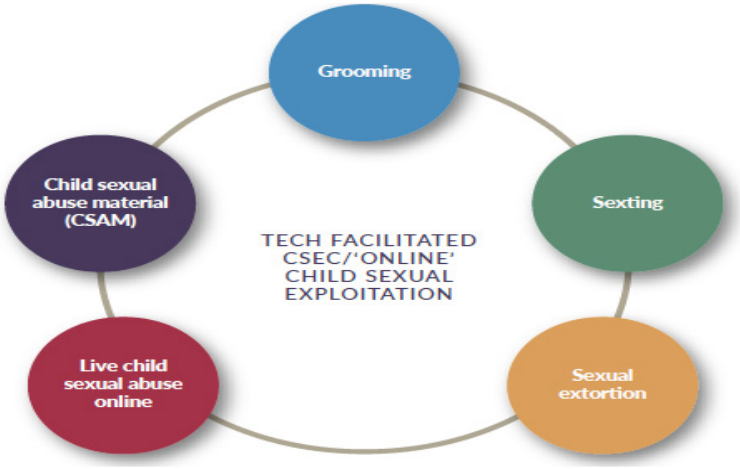

Figure 1 *Stages and elements of online CSEC (ECPAT, 2017)*

Digital and network technologies can now be found in every stage of the CSEC process:

(1) Member-only dark web forums and encrypted communication apps such as ShadowCrew and WhatsApp have reportedly been used by traffickers to securely and anonymously communicate and plan their criminal activities;

(2) Children are found to be groomed and manipulated via Instagram, Facebook, Snapchat and KIK; (BBC News, 2019).
(3) Minors are being coerced into CSEC via Skype, online games and virtual worlds like Second Life and VRChat; (Stop it now, 2021).
(4) Such illicit activities are then live-streamed, recorded and stored in cloud-based applications such as Dropbox, Google Drive and OneDrive, before being further distributed via peer-to-peer networks or in invitation-only forums on both the surface web and the dark web;
(5) Traffickers have reportedly 'advertised' their CSEC victims on websites such as Back page and Craigslist; (Malik, 2018).
(6) Illicit proceeds and transactions are then anonymously distributed and circulated among CSEC purchasers, traffickers and criminal networks; and lastly, this tech-enhanced criminal activity circle is then restarted at (1), or at the planning phase of the crime (Wagner at all, 2021).

Modus operandi

The nature of offences committed during the COVID-19 pandemic relating to online CSEA has not changed in relation to known modus operandi but offenders are exploiting the lockdown measures in order to carry on offending and target children online.

A series of conditions relating to changes in the social and physical environments of victims and offenders during COVID-19 has resulted in them spending an increased amount of time online. This meeting of potential victims and offenders online is one of the key factors that leads to the increased threat picture for children despite no noticeable changes in modus operandi.

Surface web

The vast majority of online CSAM is detected on image hosting websites that are accessible from the surface web and on P2P networks (Europol, IOCTA, 2019). 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 the online distribution of CSAM continues to take place via a variety of platforms, P2P network sharing remains among the most popular way among perpetrators to share CSAM. One-to-one distribution and sharing among larger groups routinely take place on social networking platforms. This harmful sharing and re-sharing of content that victimises children has been repeatedly detected at record levels during the COVID-19 pandemic within Europe. National Centre for Missing and Exploited Children (NCMEC) has stated that there has been a 106% increase in such activity across the globe (Forbes, 2020).

Such material is created through a range of means. One of the most harmful is direct contact sexual abuse of children by offenders. However, the ability of offenders to trick, coerce and sexually extort children into producing child abuse material without ever meeting them online has also prominently

featured in recent cases (Independent, 2020). The effects noted by victims in such cases are also extremely damaging.

Dark web

Dedicated bulletin boards on the dark web were popular among offenders as a channel for the distribution of CSAM during this period. Monitoring of these sites by Europol verified that there was an increase in activity from March to May 2020 on the same dark web site, particularly in relation to posts about videos captured through webcam. These videos range from children who are being forced or coerced by an offender into producing abuse material to other videos of a sexual nature produced by children for peers or for social media attention and include videos being captured without their knowledge. The categories the child abuse material is listed under include 'spycams', 'webcams' and 'live streams.

In another dark web forum, a section specifically for those capturing this live stream footage, known as 'cappers', saw the numbers of messages and threads more than triple from 500 messages from December 2019 to February 2020, to 1 500 from March to May 2020. This reinforces concerns previously expressed by Europol / IOCTA (2019) and others (IWF, 2018) about the quantity of material appearing to be self-produced by children themselves. Some of this activity may relate to annual 'competitions' organised within forums to gather and promote video captures of child sexual exploitation and abuse material.

Overall, the total number of files made available by offenders to one another across several prominent dark web forums increased significantly during the period March to May 2020. In one case, the number of files made available increased by almost 50 % and in another case, it almost doubled.

In response to law enforcement operations targeting these dark web communities and due to the need to select participants and ensure exchanges of information are strictly related to child sexual abuse, some offenders have created new forums. These forums act 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 (Europol, 2020c).

Constant monitoring of these communities has indicated that activities of child sexual abuse offenders on the dark web have been less affected by the lockdowns than those on the surface web. As previously reported by Europol, there have been numerous discussions about COVID-19 on dark web forums dedicated to child sexual exploitation, including enthusiastic messages about the opportunities provided when children will be online more than before (Europol, 2020b).

Social media applications and encrypted messaging

Messaging applications continue to be used by offenders during the COVID-19 pandemic to access children and distribute CSEAM. As with social media platforms, an increase in the circulation of viral CSEA videos via messaging applications has been reported (Interpol, 2020).

CSAM is increasingly distributed via social media applications. The self-destruct function of some of these applications makes investigations particularly complicated. In some cases, this is the result of self-generated material being shared with peers, after which it is further distributed via social media and eventually ends up on CSAM platforms. There are also instances where fake social media accounts are created in order to spread private pictures and videos of underage victims together with their personal information. Although such accounts are often quickly deleted, it is easy for perpetrators to simply create a new account. Encrypted messaging can also be used by those exchanging child abuse material, even allowing them to form communities and groups in order to do so (Europol, 2019).

According to child safety experts and law enforcement," distributors of child sexual abuse images are trading links to material in plain sight on platforms including YouTube, Facebook, Twitter and Instagram using coded language to evade the companies' detection tools "(Solon, 2021).

Gaming platforms continue to be used for the distribution of CSEAM and as a means for offenders to make contact with children.

Impact on policing

Countries have reported increased obstacles for victims to report offences and seek medical treatment and other forms of support. This has resulted in under-reporting of certain types of offences during the COVID-19 pandemic. A delay in reporting is expected until schools are reopened and / or access to social services returns to normal. There are concerns that some offending may never be reported if the delay in access to services is too long.

Countries have also reported difficulties in contacting victims through conventional means during this period making it difficult to move forward with existing investigations.

Law enforcement personnel working on online child sexual exploitation have been affected by the introduction of work-from-home policies across the world. This, along with shifting priorities due to COVID-19 tasks, has had an impact on the use of the INTERPOL International Child Sexual Exploitation (ICSE) database. 60 per cent of member countries who regularly use the ICSE database have either not accessed the database or have seen a significant reduction in their activities during the COVID-19 pandemic.

Countries have reported some impact on technical resources due to work from-home policies such as no ability to connect remotely to police networks.

Recommendations include the acquisition of secure VPN connections for remote working and the use of alternative worksites that may be vacant due to non-critical operations (Interpol, 2020).

The World Health Organization (WHO) has called for technology companies and telecoms providers to do everything they can to keep children safe online given the heightened risks of online harm. "They must do more to detect and stop harmful activity against children online, including grooming and the creation and distribution of child sexual abuse images and videos." These efforts will be hampered as social media providers (YouTube, Facebook and Twitter) have warned they are increasingly reliant on artificial intelligence and automated tools for the detection of illegal content on their platforms due to staff facing restrictions whilst working from home. Such software has limitations and may not be as accurate as human review.

CyberTipline is a hotline receiving reports about multiple forms of online child sexual exploitation, operated by the NCMEC. In 2020, the total number of reports received by CyberTipline increased by 28% from 2019, with 21.7 million reports (NCMEC CyberTipline, 2021). However, in March 2020 alone, NCMEC had recorded a 106% increase in CyberTipline reports of suspected child sexual exploitation – rising from 983,734 reports in March 2019 to over 2 million (Solon, 2021). The number of reports was even higher in April 2020 (4.2 million reports according to press releases) (Alfonso, 2021). The majority of reports received in 2020 in general (99.6%) were related to suspected CSAM and included 65.4 million images, videos, and other files, including 33.6 million images, of which 10.4 million were unique, and 31.6 million videos, of which 3.7 million were unique (NCMEC CyberTipline, 2021).

The COVID-19 impact on policing has varied by country but some key issues identified include:

- ✓ a reduction or delay in reporting of CSEA offences as normal reporting channels are affected;
- ✓ a reduction in the use of the INTERPOL ICSE database by member countries;
- ✓ a reduction in the availability of specialist law enforcement human resources that support CSEA investigations;
- ✓ changes in processes and efficiency due to technical constraints of working-from home which has impacted both law enforcement and electronic service providers reporting to law enforcement;
- ✓ Delays or closures in courts leading to delays in processing cases.
- ✓ An increase in online CSEA activity on both the Dark net and clear net but there is no information at this stage to indicate an increase in new CSEAM in circulation;
- ✓ A significant increase in the sharing of CSEAM through the use of peer-to-peer networks;

- ✓ A significant increase in viral content shared through both social media platforms and messaging applications resulting in repeat victimization of victims and exposure to innocent bystanders;
- ✓ An increase in the self-generated material distributed on the clear net;
- ✓ No significant changes in the volume of offences using online gaming platforms but certain games have been identified as having a potential risk interest;
- ✓ Early indications that CSEAM for payment may be an emerging trend in certain countries.

Conclusion

Although it is still too early to estimate the impact of COVID-19 on child sexual exploitation and abuse online, it has no doubt increased the vulnerability of children to tech-enabled sexual exploitation. School closures forced children into the digital sphere unprepared, without adequate knowledge of how the digital sphere works or what risks it entails. Online gaming and chat groups became key meeting places for interactions among children, thus raising the risk of commercial sexual *exploitation*of children. Indeed, since early 2020 there has been a rapid increase in digitalization of society at all levels.

Online gaming, chat groups, phishing email attempts, contact through social networks and educational applications became the main places for encounters between children and sex offenders. Unsupervised time online also increased the risk that underage individuals could produce and distribute self-generated indecent material.

As technological advancements are continuously converting the global economy, they have directed to the appearance and increase of several cyber-enabled offences, containing online child sexual exploitation. Child sexual exploitation and abuse online is reportedly one of the crimes adapting most quickly to and capitalizing on the opportunities offered by technology.

Europol (2020b) and Interpol (2020) report that government-imposed restrictions affected trends and threats of commercial sexual exploitation offences across the world. They observed a spike in demand for child trafficking for online sexual exploitation and distribution of online child sexual exploitation material in many parts of Europe as more predators and potential perpetrators were confined at home during pandemic.

In fact, security assessments from Europol and Interpol predict that there will be a sharp increase in the amount of self-produced indecent material in next years, which could lead to a corresponding increase in online solicitation and exploitation.

REFERENCES

1. Alfonso III F. (2021). The pandemic is causing an exponential rise in the online exploitation
2. of children, experts say. Available at: https://www.cnn.com/2020/05/25/us/child-abuse-online-coronavirus-pandemicparents-investigations-trnd/index.html. [Accessed 10 May 2023].
3. BBC News. (2019). Instagram biggest for child grooming online – NSPCC finds, 1 March. Available at: https://www.bbc.com/ news/uk-47410520. [Accessed 5 May 2023].
4. ECPAT International. (2017). Online child sexual exploitation: A common understanding. Available at: https://www.ecpat.org/wp-content/uploads/2017/05/SECO-Booklet_ebook-1.pdf.[Accessed 10 February 2023].
5. ECPAT International. (2020). Why children are at risk of sexual exploitation during COVID-19. Available at: https://ecpat.exposure.co/covid19?utm_source=Website&utm_campaign=Hero.[Accessed 10 May 2023].
6. EUROPOL. (2019). IOCTA 2019. Available at: https://www.europol.europa.eu/sites/default /files/documents/iocta_2019.pdf. [Accessed 7 March 2023].
7. EUROPOL. (2019). Operation Chemosh: How encrypted chat groups exchanged emoji 'stickers' of child sexual abuse. Available at: 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. [Accessed 10 May 2023].
8. EUROPOL. (2020a) Beyond the pandemic: How COVID-19 will shape the serious and organised crime landscape in the EU. Available at: https://www.europol.europa.eu/publications- documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu.
9. EUROPOL. (2020b). Catching the virus cybercrime, disinformation and the COVID-19 pandemic. Available at: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrimedisinformation-and-covid-19-pandemic. [Accessed 10 May 2023].
10. EUROPOL. (2020c), Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. for Law Enforcement ration20
11. FBI. (2020). School Closings Due to COVID-19 Present Potential for Increased Risk of Child Exploitation. Available at: https://www.fbi.gov/news/pressrel/press-releases/school-closings-due-to-covid-19-present-potential-for-increased-risk-of-child-exploitation. [Accessed 10 April 2023].
12. Forbes. (2020). Child Exploitation Complaints Rise 106% To Hit 2 Million In Just One Month: Is COVID-19 To Blame? Available at:https://www.forbes.com/ sites/thomasbrewster/2020/04/24/child-exploitation-complaints-rise-

106-to-hit-2-million-in-just-one-month-is-covid-19-to-blame/#71cff86e4c9c. [Accessed 9 May 2023].

13. Independent. (2020). Matthew Falder: One of Britain's most prolific paedophiles challenges 32-year prison sentence for 'sadistic' crimes, Available at: https://www.independent.co.uk/news/uk/crime/matthew-falder-paedophile-appeal- prison-sentence-blackmail-cambridge-a8585881.html. [Accessed 10 May 2023].
14. Internet Watch Foundation. (2018). Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse. Available at: https://www.iwf.org.uk/sites/default/files/inline-files/Distribution
15. %20of%20Captures %20of%20Live-20Sexual streamed%20 Child%
16. %20Abuse%20FINAL.pdf. [Accessed 21 March 2023].
17. INTERPOL. (2020). Threats and trends: child sexual exploitation and abuse, COVID-19 impact. Available at: https://www.INTERPOL.int/en/News-and-Events/ News/ 2020/ INTERPOLreport-highlights-impact-of-COVID-19-on-child-sexual-abuse. [Accessed 21 March 2023].
18. Lucia B. et al. (2020), Transformative technologies: How digital is changing the landscape of organized crime, Global Initiative against Transnational Organized Crime. Available at: https://globalinitiative.net/wp-content/uploads/2020/06/Transformative-Technologies-WEB.pdf. [Accessed 21 March 2023].
19. Malik N. (2018). When it comes to Child Sexual Exploitation, we cannot ignore the Dark net, Forbes, 4 September 2018. Available at: https://www.forbes.com/sites/nikitamalik/2018/09/04/when-it-comes-to-child-sexual-exploitation-we-cannotignore-the-darknet/#62708606de6a. [Accessed 21 March 2023].
20. NCMEC CyberTipline. (2021).Available at: https://www.missingkids.org/gethelpnow/cybertipline.[Accessed 21 March 2023].
21. Solon, O. (2021). Child sexual abuse images and online exploitation surge during pandemic. Available at: https://www.nbcnews.com/tech/tech-news/child-sexual-abuse-images-online-exploitation-surge-duringpandemic-n1190506. [Accessed 11 April 2023].
22. Stop It Now. (2021). How People Use the Internet to Sexually Exploit Children and Teens. Available at: https://www.stopitnow.org/ohccontent/how-people-use-the-internet-to-sexually-exploitchildren-and-teens. [Accessed 21 March 2023].
23. UNICEF. (2020). COVID-19: Children at heightened risk of abuse, neglect, exploitation and violence midst intensifying containment measures. Available at: https://www.unicef.org/press-releases/covid-19-children-heightened-risk-abuse-neglect-exploitation-and-violenceamidst. [Accessed 15 March 2023].

24. Wagner L. at all. (2021). Exploited in Plain Sight-An assessment of commercial sexual exploitation of children and child protection responses in the Western Balkans, Global Initiative against Transnational Organized Crime's Observatory of Illicit Economies in South Eastern Europe (SEE-Obs), Geneva, Switzerland.

25. Wagner L, Thi Hoang. (2020). Aggravating circumstances: How corona virus impacts human trafficking, Global Initiative Against Transnational Organized Crime. Available at: https://globalinitiative.net/analysis/humantrafficking-covid-impact/.[Accessed 17 January 2023].

26. WHO (2020). Joint Leader's statement - Violence against children: A hidden crisis of the COVID-19. Available at: https://www.who.int/news-room/detail/08-04-2020-joint-leader-s-statement---violence-against-children-a-hidden-crisis-of-the-covid-19-pandemic. [Accessed 21 March 2023].