This is an electronic reprint of the original article. This reprint may differ from the original in pagination and typographic detail.

Please cite the original version: Parviainen, J. & Rajamäki, J. (2022) Analysis of Sexual Abuse of Children Online and CAM Investigations in Europe. In Thaddeus Eze, Nabeel Khan and Cyril Onwubiko (Eds.) Proceedings of the 21st European Conference on Cyber Warfare and Security. Reading: Academic Conferences International Limited, 411-418.

doi: 10.34190/eccws.21.1.276

Available at: https://doi.org/10.34190/eccws.21.1.276

CC BY-NC-ND 4.0



Analysis of Sexual Abuse of Children Online and CAM Investigations in Europe

Johanna Parviainen and Jyri Rajamäki
Laurea University of Applied Sciences, Espoo, Finland

<u>Johanna.Parviainen@student.laurea.fi</u> Jyri.Rajamaki@laurea.fi

Abstract: Child sexual abuse or child's exploitation online as sexual violence including Child Abuse Materials (CAM/CSAM) is a global phenomenon. This case study aims to get information on the current nature of crimes by online published surveys, reports, articles, and documents as an international and cross-border cybercrime in Europe. To get information of children's own experiences of some European countries, information on how they react to sexual messages or sexual harassment online or how they recognize a threat to be a victim of sexual abuse online are important aspects to understand the phenomenon at all. The sexually motivated offenders and their behavior online conversations are also important to recognize to get more information of this criminal activity at all. If sexual abuse has been done only online, the knowledge of the current events helps law enforcement authorities (LEAs) to understand how they could find reliably the needed digital evidence for pre-trial investigations and judicial processes. The authorities' workload can be high in CAM/CSAM cases first with handling enormous digital data, but also with nature of cases which has seen widely causing different forms of stress also to professionals. From this point of view, this study also aims to describe how the different forensic tools and technological solutions would help LEAs with their jobs, for example, by classifying different materials into different categories, recognizing better victims and suspects, or winning time to investigate other crimes.

Keywords: cybercrime, child abuse, child abuse materials, sexual harassment, CAM investigation

1. Introduction

Digitalization and using the internet online is a part of our everyday life. Also, children take part in a vibrant online environment by using new tools, technology advances, infinity novelties, and opportunities. Comparing earlier generations, children as a representant of the so-called digital native generation can have already completely different skills to gather information or excellent learned multitasking skills (Pongrácz, 2019). Children's rights and their fundamental freedom as digital citizenship in free societies are important. To their fullest development, potential, and participation in the digital environment and infrastructure with communication technology devices, connectivity, services, and contents, everyone should have affordable access and the possibility to use the digital environment. It has been seen that holistic participation provides resilience and response to life both online and offline. However, it is important to ensure that digital content fits children's age and maturity as age-appropriate and child-friendly content in a different area of living also providing a plurality of high-quality information sources with different services online. Taking care of family and other social relationships online is important also to children. Council of Europe (2018) has seen that all member states must protect children in the digital environment from violence, exploitation, or abusing avoiding risks. Risks can be associated with harmful or illegal activities or events in which children should have competence wisely commitment to the digital environment. These dangers can be multiple such as extremely online recruitment to criminal offenses, extremist political or religious movements. Online can also include risks for bullying, harassment, hate speech, discrimination, racism, stalking, grooming, adult pornography, or child sexual materials. Children's needs and vulnerable settings should be able to guarantee from all these (Council of Europe, 2018).

Every environment can include harmful or potential risks because it is natural that we all can meet at the same time with good things different bad things, threats, dangers, and harmful situations there we are – in this case in the digital world online. That is why we need knowledge of individual risk online. When we are talking about children, it is necessary to notice that they can naturally have a low sense of danger or they cannot interpret something in their ages right or as a risk at all (Pongrácz, 2019). The growing concern has seen that different platforms on the internet may include individuals with a sexual interest in children (Kloess, et al., 2017), who are using the widely opened possibilities of the internet to possess, product and distribute illegal materials such as CAM/CSAM (Brown, 2017). Recognizing the current nature of these crimes can give better possibilities to understand and react to this multidisciplinary and comprehensive phenomenon (Europol, 2017).

Children have a risk of being a victim of sexual harassment or sexual abuse with sexual messages, asked for or send nude photos and CAM/CSAM materials photos or videos. The offender's intention, criminal activities, and illegal material have harmful reactions or distress to child victims internationally and cross-border. This case study, focusing on the general European context, investigates child sexual abuse or child's exploitation online including CAM/CSAM as sexual violence. The research material contains different reports, articles, documents, and common conventions behind different legislations of child sexual abuse online or child exploitation as an international cybercrime. These sources were chosen mainly from the latest year as a sample to get updated knowledge of victims, offenders, technological issues, and point of view of judicial processes as digital evidence and investigators' workload in pre-trial investigations. The study explores this complexity and widespread phenomenon as a crime against children and the dissemination of CAM/CSAM material.

2. Children's online behavior

The EU Kids Online 2020 survey, summarized in Table 1, gained results from 25 000 children aged 9-16 in 19 European countries between autumn 2017 and summer 2019. The survey mapped children's internet access, online practices, skills, risks, and opportunities by summarizing the main findings as a key topic from each area. The risks and opportunities mentioned as specific activities or experiences that could lead to harm or a positive outcome, including overall negative experiences, online aggression and cyberbullying, encountering potentially harmful content, experiencing data misuse, excessive internet use, sexting, seeing sexual images, meeting new people online and preference for online communication. In most countries, children had happened something bothered or upset in the past year online, not frequently, but a few times. Harmful content was named including, for example, cyberbullying, hate messages, requires to be very thin, personal data misuse, or get viruses or spyware. Also spending time daily or weekly online or other excessive internet use has reported in some cases to be harmful impacting to children eating, sleeping or leaving them less time to spend with friends, family or doing schoolwork but the majority of the children in all of the countries had not shared this experience. To clarify sexual messages by this survey it was first noticed that many children exchanged sexual messages with a peer or girl/boyfriend, which were seen quite normal development to be using digital environments online context day-to-day lives in every life's area considering also flirting, exploration of sexuality and the establishment. Maintenance of intimate relationships which also could be mediated via technology did not constitute a risk of serious harm. Commonly it was also reported that many can feel it be easier themselves online than meeting people face-to-face, but the majority of the children in all countries had told that they never talk about personal things online that they did not talk about face-to-face. However, eight countries reported that most of the children were talking about different things online than offline at least sometimes or more often. (Smahel, et al., 2020)

The EU Kids Online 2020 survey studied how to ensure a balanced approach to sexual images online or other media considering all kinds of media-related exposure to sexual images, not only online materials. Many children could seek sexual content by curiosity, trying to find answers for questions they have about puberty or knowledge of their own body and sexual identity. To clarify more deeply this part of images which can cause harm or potential risks as a bothering or upsetting material, children had named for example being exposed to online sexual content, aggressive content, and other types of unwanted sexual content. An average of 22 percent of children, commonly older children, reported that they had received sexual messages in the past year. Also, an average of 6 percent of children reported that they had sent sexual messages. If children were asked or to him/her had received sexual requests to exchange sexual messages or material online, they had mainly been girls between 12 to 16 years. Especially girls reported that they had felt upset, distressed, and potential harm after this. Sending sexual messages, images and videos could always have the potential to be distributed and made public without original participations control. Commonly, several children had not told harmful experiences to anyone and if, they had told to a parent, friend, teacher or to professionals who helps children. Most children say they usually know how to react to the online behaviors of others which they don't like for example coping with blocking the person, talking to other people, ignoring the problem, using technical measures, or confronting the stressor or aggressor. Complex sexting using different electronic devices could lead to grooming or sexually abusive behavior efforts by adults. These situations included also risks for sending or receiving intimate digital material (Smahel, et al., 2020).

Table 1: Examples from different European countries by a survey to get a wider approach to the experience of harmful content or risk for abuse children online (Smahel, et al., 2020)

Croatia	30 percent of children aged 9-17 had seen sexual content online in the past year
	almost two-thirds of children had seen sexual photos or films with nudity intentionally without
	any intention to see these contents
Portugal	33 percent of children and youths have reported seen sexual content online in the past year
Czech Republic	girls have more often specially asked to share intimate information
	boys have received sexually charged messages
	girls and younger children have reported being upset being attacked online
Germany	bullying, receiving, or sending sexual messages has seen being quite normal with digitally
	engaged children
	children have been also exposed to various cyber risks by many opportunities of being online,
	such as exposing also sexual, violent, or hateful content
	63 percent of children have reported that they feel pleasant experience to meet an online
	contact in real life
Switzerland	many young children have online social media profiles, and they see social media useful tool to
	find new friends
	older children have seen to be vulnerable to more risky experiences by having more skills and
	owning smartphones
	many meets with online known in real life face-to-face and mostly they have felt experiences
	enjoyed and positive

Comparing these findings to earlier studies, the wide view of point can have still more specific details to take consider. For example, in the Czech has been recognized that specific social networks' online blackmailing of intimate images has affected 6 to 8 percent of Czech children, which has meant more than 21,000 children (Kopecký, 2016). German survey has pointed out that parents or carers may thoughtlessly add their children's risk online publishing children's or adolescents' pictures online without their permission. It has been seen as important that parents or carers are aware of possible negative consequences, hurtful comments, or their children's right to privacy at all (Smahel, et al., 2020). In spring 2021, Save the Children Finland has surveyed grooming by children's self-reported online survey. Children mainly recognize different conversations, messages, or images which can lead to grooming quite well, but still, there can be a gap between their knowledge and real-life actions in real situations how they react to contact-making or how ready they are to tell parents at least of harmful situations online (Juusola, et al., 2021). One meaningful question is also that in general, meeting a stranger in real life after online knowing in the theme of child sexual abuse has depicted as especially risky ordering to tell someone about the meeting or meet unknown only in a public place, but a Swizz's survey also wants to consider that average 70 percent of all children in the survey reported that they were happy after the meetings which could be an opportunity and benefits for children (Smahel, et al., 2020).

3. Grooming, child sexual abuse online and CSAM

Figure 1 summarizes the phenomenon of child sexual abuse online.

Grooming Grooming occurs usually when an adult prepares a child for sexual contact (Sorell, 2016). Cyber grooming is a means and instrument to achieve the offender's primary goal, which is sexual abuse of a child victim with intimate materials, arrange a personal meeting in the real world, or get intimate materials from children (Kopecky, 2016). Hacking in this context means that perpetrators can hunt victims even months by getting children's or youths' trust for them. They cheat by appearing as the victims' peers even they are older in real life. The perpetrator's purpose is to engage children well-built relationship of trust where children do not even recognize what is happening at this game where the intent aim is sexual. In these cases, personal data may circulate uncontrolled in the virtual world including photographs voluntarily provided in a context contrary to the original purpose. (Pongrácz, 2019) Online child sexual abusing or CAM/CSAM Sexual harassment, sexting, online conversations with abusing by sexual messages, asked or sent photos, videos or live-streaming. Including also children's self-generated or create sexual materials as a response to an enticing online message. Using sexual images and/or videos depicting children. Sending erotic or pornographic, usually child pornographic material or links there to child. (Europol, 2017) Online sexual coercion and extortion of children (oSCEC) As one of the new crime phenomena of digital age as a cyber-enable crime. Means blackmailing those individuals whose information, sexual photo or video as a material has made available in an online environment self-generated for example a part of online conversations and which victims would like to keep private. In these cases, the perpetrator has value, power, benefit and advantage which gives the possibility to treat children and go still further with their intentions. (Europol, 2017) Manipulation can be defined also as blackmailing online in which threat of revealing privacy, intimacy or sexually explicit

Figure 1: Terminology definitions

Contact making to a child normally starts with a conversation on media platforms, chat applications, or online games or gaming platforms. It is quite common that conversations move from one online platform to another including social engineering methods with manipulative or threatening tactics to create an individual relationship. The perpetrators can be peer-perpetrated with harmful and bullying consequences to the victim, but most of the cases are made by sexually motivated adults who use technology to engage in sexual contact with children through processes of sexual grooming to get CSAM or meet victims for physical sexual activity. The perpetrators may also be organized groups with sexual and/or financial motivations. Financially motivated offenders' main goal is to obtain money and procurement sexual material for commercial distribution. Usually, they had been located to organized criminal groups which generally operate in teams and with contacts between countries with a common language outside of the EU both national and international levels. In these cases, perpetrators can include both genders, they do not know the victim personally and they can target widely potential victims. Usually, they have used pre-recorded footage by enticing online messages or manipulative techniques obtained from pornography and live-sex camera sites. Mainly manipulations can occur, for example, by pretending to be younger (peer), with sexual reciprocation ("I do, if you do" meanings by shared images or live streaming), assuring friendship or romantic relationship online, using multiple fake online identities (pretending to be a supportive friend or a sympathetic victim of the same offender) or offering something (e.g., money, drugs) to the child. It can be enough to threaten with messages for example to post images to a place where family and friends could see, for example, victims naked photos or threat to create sexual content of child by using digital editing tools or record child unknowingly, but in the worst cases, threats can be threatening to hurt a child or family members physically or commit suicide (Europol, 2017). However, it is quite usual in real life that those who have picked up an online investigation into child abuse images have not previously been known to the police or other authorities (Brown, 2017). In the next two chapters, couple examples of from earlier research in Europe describe closer offenders' motivation as a criminal activity.

In the Czech Republic, Kopecký (2016) surveyed children's prevalence of cyberbullying and other risky forms of communication in the years 2014-2016. He focused on specific cases of children's extortion that had been captured and dealt with by the Centre for the Prevention of Risky Virtual Communication and Police for the research. He found victims ages were 11-17 years by whom 73 percent were girls. He also stated that 15-17 years old children were in a worse situation regarding blackmail even younger children would have a lack of life experiences. Recognized techniques had focused on gaining children's confidence, luring out intimate material, and subsequent blackmailing. Kopecký identified a simplified model of blackmailing of children in five stages through the usage of ICT by specific, repetitive forms of communication within the behaviors of the offenders. First, the offender gets in touch with the child by a conversation which can typically be initiated sexually or reflect straight to exchange or have photos. After it, the offender begins to positively evaluate by flattering or praising the victim all materials sent by victims and ask smoothly for more photos or other materials to achieve children's admiration and respect. In the third stage, the offender attempts to confirm that the victim's identity leads to a real child and that the photos are authentic by commonly identifying verification photos with the note or date. After this, photos get more increasing and intensifying nature between the victim and the offender where children's participation can also imitate offenders' behavior in exchanging naked photos or sexual acts when a child can send to the offender almost anything. The offender can also send photos from erotic or pornographic websites, usually child pornographic material, to the child. At last, when the child decides to be not to respond anymore, the offender generally proceeds to blackmail either threatening to tell friends or parents on the social network. The research stated approximately 17 percent increase of exchanges after that, and the offender can also get photos that contain the child's face. In this way, the children are not able to detach or break away from the engagement of contact and because they usually do not tell any adult right after events, there are no easy ways to stop or interrupt actions. (Kopecký, 2016)

In the UK, Kloess, et al. (2017) researched criminal offenses by 2009-2012 conducted 29 transcriptions of chat logs conversations in naturally occurring interactions between offenders and victims under 16 years also using each case the whole contextual police reports had ascertained offenders underlying motivation and function to get children to engage in online interactions. In all cases, offenders approached and established initial contact with victims via public chat rooms, social networking sites, or dating websites but in a few cases, conversations were moved to instant messaging and email. The heterogeneous group of offenders had a highly sexual nature of conversational topics. The research found four specific strategies to engage victims: directness in initiating online sexual activity, pursuing sexual information, the next step, and fantasy rehearsal even if by manipulative strategies. Commonly offenders could design their communication in such a way that frequently achieved their goal of sexual arousal and gratification trying to achieve victims' compliance by overcoming victims' resistance

to incite victims into performing sexual acts on online sexual activity. Offenders can be suggestive or flattering or enquire about the victim's sexual likings, preferences, practices, or previous sexual experiences. The offenders can deal with their own experiences or use emotions such as normalizing the nature of behavior or performing playful to belittling situations. For example, repeating initial offenders' questions, requirements, or compliance, insinuating through offender's disappointment, sadness, or other feelings offenders try to find sexual arousing. It is also possible to use other victims recorded sexual behavior online encouraging victims to respond by likelihood way. Also, direct attempts to initiate sexual activity via webcam to show parts of body or genitalia, masturbation, use foreign objects to perform penetrative sexual acts or ask for arrangements for physical meetings or conduct sexual contact are usual. Mainly offenders ensure contacts continue to the future respectively even if they also consider minimizing the risk of disclosure and detection, but there can also be highly manipulative, sexual of fantasy fulfillment motivated and even aggressive directness to the victim after a few minutes' conversations. (Kloess, et al., 2017)

4. CAM/CSAM investigation methods

The purpose of digital forensic investigations is to get digital evidence of a specific criminal event. In these cases, in which offenders have operated in illegal activities through their digital devices, by seized devices appropriate analysis of digital examination is a possibility to get needed information for this evidence, find information of victims, other offenders, or CSAM. These digital traces with every single item of digital evidence of different events will guarantee both victim's and suspect's rights in the judicial process by presenting admissibility and incriminating evidence to a court and other legal liabilities. Forensics needs are challenged also by the development of technology. It is not only a question of new possibilities or threats, even if it is a question about day-to-day practices. Data per person on average has increased enormously and it leads to the continuous growth of data scales in examinations which has quite commonly used for data storage terabyte-sized hard disks and cloud services by high capacity and low costs. It is quite normal that almost everyone has a large amount of digital information spread throughout separate personal devices and cloud-based personal accounts. This also means an ever-growing workload to online child abuse investigators and criminal technicians. All of this can cause also delays first for investigations and all trial processes. (Acar, 2018)

In contexts of cybercrimes, digital pieces of evidence of the crime can even itself be enough for prosecution and conviction in the trial (Denk-Florea, et al., 2020) or they are important with other pieces of evidence by side with child's interview or other's interrogations. For example, two studies in the last years have examined law enforcement professionals' workload and distress with CSAM investigation. A survey from the UK has shared the professionals' negative emotions like shock, anger, desensitization to material, desire not to look at the material, physical responses of sickness or empathy feelings for the victims, or feelings of inadequacy. Many events of cases have been named as a highly disturbing material, but also the duration and frequency of viewing materials and the uniqueness of each criminal case can affect distress. For example, especially audio or written information included videos were recognized to be highly distressing by their way to witness and recollect victims' traumatic event experience again. In the CSAM context, all indications include abuse and contents can at least be so raw with intrusive images, unwanted thoughts, or flashbacks that there can be hard to find resilience or psychological safety to professionals heightened rationale to do their job even they have commitment and motivation to important jobs to seek norm violations or illegal practices as their job (Denk-Florea, et al., 2020). A survey in the US has researched that there is an increased risk for experiencing psychological distress, different transforms or stress symptoms with can occur as emotional stress by indirectly stressful experiences without non-specific traumatic events; such as compassion fatigue. Especially situations can be stressful for those investigators who have the overlap dual roles as both duties in smaller units; duties as a digital forensic examiner and a case-investigators even in each case meeting also in face-to-face interaction with interrogations the child victims, parents or family members and offender or offenders. (Seigfried-Spellar, 2017)

Images depicting children in sexual acts are under criminal offense mainly around the world their possession, production, or distribution, which means that law's everywhere should intervene, reinforce and reflect unwanted events. By continuing growth of digital materials has indicated that also image-related offenses would come to be increasingly challenging technological solutions to identify illegal materials and that still demanding also more forensic examinations of seized equipment or devices and setting new requirements to all of them who are working with these cases (Brown, 2017). As an international and cross-border crime, child sexual abuse online and CAM/CSAM means that in many cases the offender, victim, and data can all relate to different

countries. Usually challenges to forensic issues has associated with the locality with legal frames to get data from countries where the some company's headquarter or operational center is located to technological possibilities and capabilities particularly or to anonymization technologies, encryptions or peer-to-peer structures, real possibilities to victim and offender identifications, particularly to the actual current legal issues or all these issues limitations together (Acar, 2017). It has also been recognized that in a few cases, the offenders have used sophisticated computer programs which have allowed the users to remotely control a PC or laptop webcam to record or acquire intimate materials without the victim's knowledge (Kopecký, 2016). Internet anonymity has been seen as one of the key risk factors for harmful harassment, abuses or uncontrolled behavior at all no matter if there is a question of individual or organized crimes because of hiding your real name and identity that perpetrator who has a sexual desire for children as a personality disorder can cause many risks to keep their experiences and activities secret by transferring child pornographic or child sexual abuse materials or images anonymously through the network or seeking for victims (Pongrácz, 2019). In Dark Web's different platforms, anonymity can protect perpetrators online without risks of being caught and they can form groups of hundreds or thousands of members scattering all over the planet to deal individual's sexual interest in children or an interest in child abuse images production, distribution or exchange (Brown, 2017).

Recognizing illegal material by technological ways would get advice and help for all actors. Attempts to reduce or eliminate the traffic images online can start from to use of known URLs with illegal contains to block them by lists or restrict access to certain pages. The hashes can help to develop PhotoDNA which is meant for imagematching technology as a unique signature for a digital image. By this signature, it would be easier to identify, report, eliminate and find copies of images or material of CSAM online (Brown, 2017). In the latest years, the discussion of different possibilities which technologies can occur to the offender, but also current technologies or future's new technologies which can or could be helpful or advancing to authorities' jobs in prevention or detection. For example, Acar (2017) has seen that applying web cameras and video streaming through Voiceover-IP (VoIP) applications with audio and video communications can be one of the emerging forms of online child sexual abusing between the offenders and victims as an efficient, fast, cheap and private technology without no clue to the real world. Acar has mentioned that discussion of new or better practical solutions needs to solve cases with a technical and legal debate together, also with private sectors entities or as a public-private partnership. Video chats, for example, could enable access to the third part in real-time communications considering issues such as privacy, needed information to protect children but also to get solid evidence of recordings of criminal activities for the legal processes. According to Acar (2017), fully automated chatbots with text-to-speech recognition and big data analysis of metadata (attributes of a resource such as a date, creator, and location of IP addresses) including content data (communications texts, audio and video files) by VoIP companies could be helpful items to get the situation to better. In particular, crime prevention needs technology considering effective but also cost-efficient strategies. Technological capabilities should be taken into consideration proactively, considering that offenders will always apply new technologies for criminal activities too. (Acar, 2017) Maybe, automated methods are not adequate alone for current practical needs and measures of digital forensic investigations, but for example, automated triage system including time-consuming report writing could be quicker and easier for investigators workload as a job but also by a psychological way without seeing distressing materials. They could help to allocate LEAs' limited resources, for example, for quicker identification of victims. (Acar, 2018)

5. Discussion

Child sexual exploitation is one of the EU's priorities in the fight against serious and organized crime (Europol, 2022). Commonly, cybercrimes are expected to come agile exploiting new technologies fast and tailoring their attacks using new methods and cooperating in new ways. This requires LEAs to have capabilities and possibilities for how to fight cybercrime (Interpol, 2022). The phenomenon was recognized already at the beginning of century 2000. There are different conventions or recommendations which have had impacts on domestic legislation in European countries or impacts to different measures or interventions as a co-operation between each other.

Criminal policy and protection for society against cybercrimes including child depicting material and electronic evidence

- Need of a common criminal policy and protection for society against cybercrime by adopting appropriate national legislation and efficient international
 co-operation and co-operations between states and private industry to legitimate interests in the use and development of information technologies
 taking care of specific requirements of the fight against cybercrime.
- Necessary to every member states to have domestic legislative and other measures to prevent all materials in every stages that visually depicts all persons under 18 years or not less than 16 years of age engaging in sexually explicit conduct.
- The effective collection of evidence in electronic form of a criminal offence to facilitate criminal offences detection, investigation and prosecution at the
- Requirement to states to offer a holistic response to sexual violence against children by prevention, protection, prosecution and promotion of national and international co-operation (Convention of Lanzarote, 2007).

Guidelines to respect, protect and fulfil the rights of the child in the digital environment

- One measure to prevent child sexual abuse material is that every state should continually monitor with their own jurisdiction how child sexual abuse or child depicted materials are hosted, give highest priority to victim-focused material and require law-enforcement authorities identify, locate and protect children subjected to sexual exploitation or abuse.
- The materials databases including "hashes" as a important tool to find perpetrators or represents illegal materials with rapid analysis of large quantities of data without need to examine every picture by picture.
- Importance to law-enforcement authorities to have connect to the INTERPOL database that deals with child sexual abuse material
- Council of Europe has also recommended that states should also actively engage with the Internet Corporation for Assigned Names and Numbers (ICANN)

Common challenge to answer and try to solve

- Recommendation that private sectors and platforms providers should find the most effective ways of preventing, reporting and eliminating crimes against children online environment through their own services considering technological expansion with new communication channels, growing internet coverage and the widespread availability of mobile devices (Europol, 2017).
- Relevant public and private authorities, educational and child protection and care systems, public institutions, stakeholders, specialised public agencies
 and civil society organisations can together create, implement and monitor sharing strategies, action plans, good practices and programmes to reduce or
 remove risks of violence, exploitation and abuse against children by quarantee their well-being in virtual world (Council of Europe, 2018).
- Business enterprises should also co-ordinate their actions effectively with law-enforcement authorities providing assistance such as a technical support
 and equipment to to identify perpetrators and collect evidence for criminal proceedings by available technologies or make easily availability of metadata
 concerning any child sexual exploitation and abuse material found on local servers on their platforms (Council of Europe, 2018).

Figure 2: Approaches for preventing children online sexual abusing

Many sources consider the phenomenon is a collective problem. As Figure 2 presents, many challenges exist for dealing with the problem with significant technological players. Some players have already reunited for developing systems to locate contents of CSAM by applying publicly available information, announcements, and warnings to commit a criminal offense or to help sites visitors to find potential sources to get help if they were worried about their behavior (Brown, 2017). Former legislations and authorities' jurisdictions have placed requirements to different actors use their possibilities by side authorities work in societies. Combining earlier and future approaches together, a good possibility exists for handling the phenomenon better at the European level considering also different actors' possible interventions widely in every stage of every society.

Recent studies recognize offenders' manipulative ways of finding child victims which it is important to take also consider these children's self-reported information of various situations online. Possible harmful situations also require awareness of possible new developing ways to these contact makings and how different actors can follow and prevent these situations even if different obstacles for getting better results to prevent, detect or solve cases are quite well known. New legislation and wide co-operation at all societies levels are needed for offering better safety in the digital environment also for children. Technological issues are both possibilities that the offenders can apply, but technology also provides possibilities to protect children online. The development should take consider also possible forensic tools and these technological solutions which could help LEAs' workload to clarify possible crimes effectively. Further research is needed to focus on almost every aspect of this phenomenon considering time preference; for example, possible new technological developmental issues, by following possible changes in victims and offenders' behavior or different interventions impacts to phenomenon would be important examine.

References

Acar, K. V., 2017. "Webcam Child Prostitution: An Exploration of Current and Futuristic Methods of Detection", International Journal of Cyber Criminology 11(1):98-109. DOI:10.5281/zenodo.495775

Acar, K. V., 2018. "OSINT by Crowdsourcing: A Theoretical Model for Online Child Abuse Investigations", International Journal of Cyber Criminology 12(1):206-229. DOI:10.5281/zenodo.1467897.

Brown, J., 2017. Online Risk to Children: Impact, Protection and Prevention, John Wiley & Sons, Ltd.

Council of Europe, 2001. Convention on Cybercrime.

Council of Europe, 2007. Lanzarote Convention.

Council of Europe, 2018. Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Recommendation CM/Rec (2018) of the Committee of Ministers, Council of Europe.

Denk-Florea, C.-B. et al., 2020. *Understanding and supporting law enforcement professionals working with distressing material: Findings from a qualitative study*, San Francisco: PLoS One; San Francisco.

Europol, 2017. Online sexual coercion and extortion as a form of crime affecting children - Law enforcement perspective, Europol, EC3, European Cybercrime Center.

Europol, 2022. Crime Areas; Child Sexual Exploitation.

- Interpol, 2022. Crimes; Crimes against children.
- Interpol, 2022. Crimes; Cybercrime.
- Juusola, A. et al., 2021. "Grooming lasten silmin selvitys 11-17-vuotiaiden lasten ja nuorten kokemasta groomingista netissä", Pelastakaa Lapset ry.
- Kloess, J. A. et al., 2017. "A Qualitative Analysis of Offender's Modus Operandi in Sexually Exploitative Interactions with Children Online", Criminology & Criminal Justice, 29(6): 563-591. DOI:10.1177/1079063215612442
- Kopecký, K., 2016. "Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors)", Telematics and Informatics, 34(1): 11-19. DOI:10.1016/j.tele.2016.04.004
- Pongrácz, I., 2019. Children, Online Dangers and Solutions.
- Seigfried-Spellar, K. C., 2017. "Assessing the Psychological Well-being and Coping Mechanisms of Law Enforcement Investigators vs. Digital Forensic Examiners of Child Pornography Investigations", Society for Police and Criminal Psychology.
- Smahel, D. et al., 2020. EU Kids Online 2020: Survey results from 19 countries. DOI: 10.21953/lse.47fdeqj01ofo Sorell, T., 2016. "Online Grooming and Preventive Justice", Criminal Law and Philosophy 11:705–724. DOI: 10.1007/s11572-016-9401-x.