PUBLIC VERSION
MAY 2017

Online sexual coercion and extortion as a form of crime affecting children

LAW ENFORCEMENT PERSPECTIVE

EUROPOL | EC3 European Cybercrime Centre

ONLINE SEXUAL COERCION AND EXTORTION AS A FORM OF CRIME AFFECTING CHILDREN / LAW ENFORCEMENT PERSPECTIVE

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu

PHOTO CREDITS

Europol: page 4.

Shutterstock: page 1 (cover).

CONTENTS

FOREWORD 4

ACRONYMS 5

KEY CONCLUSIONS AND RECOMMENDATIONS 6

INTRODUCTION 8

1/ DESCRIBING THE PHENOMENON 9

1.1. Current state of knowledge 9

1.2. Characteristics of online sexual coercion and extortion of children 10

1.2.1. Motivation of perpetrator 10

1.2.2. Circumstances 11

1.3. Key elements of online sexual coercion and extortion of children 12

1.3.1. Material 12

1.3.2. Threat 12

1.3.3. Value 13

1.4. Scope 14

1.5. Terminology and working definition of online sexual coercion and extortion of children 15

2/ VICTIMS AND PERPETRATORS 16

2.1. Perpetrator profile 16

2.2. Victim profile 17

3/ A RESPONSE TO THE PHENOMENON 19

3.1. Preventive response 19

3.2. Reporting and support mechanisms 21

FOREWORD

I am pleased to introduce this report addressing online sexual coercion and extortion as a form of crime affecting children. The report provides a law enforcement perspective of this online threat and recommends actions as a part of our preventive campaign on this topic.

Children are increasingly using the online environment to communicate and form relationships and this should be considered as a natural part of their development. However, it is our collective responsibility to educate them on the threats they may experience and also protect them to make the online environment as safe as possible. Where something untoward happens online we should provide clear and effective reporting and support mechanisms so they understand where to turn to for assistance.

Europol is fully committed to supporting the European Union Member States and all our partners in providing support to vulnerable members of our society in overcoming the risks posed in the online environment.

Steven Wilson
Head of Europol's European Cybercrime Centre

ACRONYMS

CSAE	child sexual abuse and exploitation
CSE	child sexual exploitation
CSEM	child sexual exploitation material
EC3	European Cybercrime Centre of Europol
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EU	European Union
IWF	Internet Watch Foundation
IWG	Interagency Working Group
NCMEC	National Center for Missing and Exploited Children
NGO	non-governmental organisation
oSCEC	online sexual coercion and extortion of children
SGSEM	self-generated sexually explicit material

KEY CONCLUSIONS AND RECOMMENDATIONS

1/ There appear to be two major motivations for the online sexual coercion and extortion of children ([1]) (oSCEC): sexual and financial. Minors are the victims of both, however the sexual gratification of a perpetrator appears to be the primary motivating factor. Financially motivated offences are predominantly carried out by organised offenders based outside of the EU.

Recommendation: Differentiated strategies reflecting the differences in perpetrators' motivation and profiles need to be created and implemented for the prevention and management of oSCEC-related behaviours.

2/ One major limitation of the current capacity to assess the true nature of and successfully combat oSCEC is the lack of a common language and understanding of this phenomenon on the part of different stakeholders, such as legal and judicial systems, law enforcement and the private sector, including the media.

Recommendation: Advocate for initiatives contributing to a multidisciplinary, comprehensive approach, essential elements of which are prevention and education, criminalisation of various forms of conduct, reporting and intervention, along with policies designed to involve representatives of different sectors.

3/ The expression 'sextortion', commonly used in public discourse, may lead to ambiguous and sometimes even paradoxical understanding of the crime affecting children. Use of this term implies equivalence with the crime affecting adults, and may lead to a failure to recognise more complex and nuanced features of the crime affecting children and its grave consequences for them.

Recommendation: Promote the use of proper terminology that exhaustively reflects the nature of oSCEC.

4/ Online sexual coercion and extortion of children, as one of the new crime phenomena of the digital age, is heavily understudied. Gaps in the research limit the capacity to develop evidence-based policies and interventions, whether at the level of identifying new instances of oSCEC, developing suitable reporting mechanisms, legislative and preventive strategies or implementing interventions that meaningfully respond to the needs of victim, perpetrator and other stakeholder populations.

Recommendation: Conduct more in-depth academic research, especially in terms of victim and perpetrator characteristics, the offence process and the supporting victim–perpetrator interrelationship. As the financial victimisation of children is a comparatively new trend in online child sexual abuse and exploitation (CSAE ([2])) further empirical work is required to identify particular factors at play that render young people vulnerable to financial exploitation.

[1] While the term 'online sexual coercion and extortion of children' is used within this report this usage is not without its limitations. For user concern on this see the section 'Terminology and working definition of online sexual coercion and extortion of children'.

[2] The phrase 'child sexual abuse and exploitation' is used within this document to maintain consistency with United Nations (UN)/United Nations Children's Emergency Fund (Unicef) policy.

5 In identifying cases of oSCEC it is a challenge to reliably discriminate between consenting and non-consenting types of behaviours related to youth-produced sexual content ([3]), such as sexting ([4]), bearing in mind that the child's own awareness of their exploitation may be compromised by deceptive solicitation strategies or simply a lack of awareness of what constitutes such practice.

Recommendation: Specific empirical focus needs to be given to how online sexual coercion and extortion offences are influenced by children and young people's behaviour online and how to indicate profiles of risk and vulnerability in their online behaviour that may render them susceptible to online sexual coercion and extortion.

6 The complex and dynamic nature of online unlawful behaviour causes shortcomings in the recording of incidents of oSCEC which creates difficulties in assessing the scope of this crime threat.

Recommendation: Further investigate the online environment to make sure that criminal actions are fully reflected in legal solutions and are categorised in a coherent way enabling accurate data retrieval. The situation at each individual national level merits auxiliary research which should explain whether the current legislation can cope with the complexities of oSCEC, whether it is complementary and whether it is sufficient to ensure appropriate prosecution.

7 In the context of preventive intervention, a lack of awareness programmes explaining characteristics of oSCEC and addressing its key elements has been observed.

Recommendation: Deliver effective, tailor-made awareness programmes to make children and young people aware of acceptable and unacceptable online communication, including the illegality of some online practices, with a particular focus on those in the peer environment. Such programmes should be included in school curricula.

8 The reporting mechanisms follow a multidisciplinary approach, in the form of cross-reporting, where different actors are represented. The differences between the goals of each of the actors, especially a disconnect between reporting mechanisms and supportive initiatives, pose challenges for coherence and effectiveness in this domain.

Recommendation: Conduct a review of solutions in this domain at national level in individual EU Member States to make sure that they reflect all scenarios of oSCEC, ensuring a potential child victim can be provided with tailor-made assistance. Prevention campaigns should be closely linked with the reporting and support mechanisms to fully achieve their goals.

9 The online environment where sexual coercion and extortion of children can be detected needs to be monitored by platform providers to find the most effective ways of eliminating that behaviour.

Recommendation: Private sector to continue efforts in enhancing detection, preventive intervention and reporting mechanisms introduced through their own services.

---

[3] 'Nude or semi-nude images or videos produced by a young person of themselves engaging in erotic or sexual activity and intentionally shared by any electronic means', Internet Watch Foundation (IWF), *Emerging patterns and trends report #1 — Youth-produced sexual content*, 2015, p. 3. Available at: https://www.iwf.org.uk/resources/research

[4] Definitions of 'sexting' were reviewed by the Interagency Working Group (IWG) on Sexual Exploitation of Children, in *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*, 2016, p. 44. Available at: http://luxembourgguidelines.org

INTRODUCTION

Aim

The aim of this report is twofold: to raise awareness of oSCEC as one of the most significant online threats against children ([5]); and to contribute to the public discourse on effective responses to it, especially in terms of reporting and support mechanisms in the EU Member States.

Methodology

The report draws heavily from the law enforcement version commissioned by experts representing the Child Sexual Exploitation European Multidisciplinary Platform Against Criminal Threats (EMPACT-Cyber-CSE) community ([6]), released in December 2016. Its objective was to increase the understanding of this crime phenomenon at the level of law enforcement agencies in order to support them in preventing and combating this crime phenomenon.

As this document addresses a heavily understudied crime area, the methodology has clear limitations. The information presented in the report is a combination of the surveyed observations of 30 experts representing the EMPACT community (child sexual exploitation (CSE) experts) ([7]), analysis of open-source case data ([8]) and explanations provided by representatives of academia. To make the response of law enforcement complete, this report also builds on expertise gathered by the members of the dedicated team, dealing with online CSAE in the European Cybercrime Centre (EC3) ([10]). Where appropriate, the answers of CSE experts have been supplemented with information originating from other specialised sources, organisations or institutions ([11]).

The report does not cover legislative responses to the crime phenomenon being examined. Related concepts such as sexting, self-generated sexual material, grooming and online solicitation, along with oSCEC in peer-perpetrated cases, are mentioned but are not studied in depth.

[5] EC3, *The internet organised threat assessment*, 2016, pp. 10 and 24. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2

[6] More information about this model of cooperation is available at: https://www.europol.europa.eu/content/eu-policy-cycle-empact

[7] The collection of responses to the survey ended in April 2015, so the situation reflected in the report refers to the 4-year period before that date.

[8] A reference is made to the outcomes of scanning of open sources for sexual coercion and extortion cases reported from 2012 until the end of March 2017 — 95 in total, 87 referring to minors as victims. Obvious limitations should be highlighted here as all the research was conducted in English.

[10] More information is available at: https://www.europol.europa.eu/ec3/child-sexual-exploitation

[11] All websites were accessed on 15 May 2017.

1/ DESCRIBING THE PHENOMENON

There is no doubt that much has recently changed in the online behaviour thanks to technological expansion offering new communication channels, growing internet coverage and the widespread availability of mobile devices. One of the new and emerging manifestations in online behaviour is a phenomenon referred to in this report as online sexual coercion and extortion. The forms of online sexual coercion and extortion have recently been reported by a number of sources, however the range of reported scenarios varied in many respects.

A comprehensive scan of open sources revealed that this very specific kind of cyber-enabled crime modus operandi — based, in simple terms, on blackmailing those individuals whose sexual photo or video was made available in an online environment — has been utilised in numerous ways, affecting victims across all demographics. Various ways of outlining the phenomenon under investigation were also found, along with a great deal of diversity in the keywords used to describe it, such as 'sextortion', 'sexual extortion', 'sexual blackmail', 'webcam blackmail', 'webcam sex scams', 'sexual harassment' and 'dating scam'. Some of these expressions were used interchangeably, even if they referred to different types of behaviour ([12]). A natural consequence of this situation was that even when some sources attempted to provide definitions of sexual coercion and extortion, their scope was also wide-ranging.

It is possible to indicate the key elements of online sexual coercion and extortion that appeared in the majority of the reported scenarios:

- material — any material (information, photo or video) the victim seeks to keep private.
- threat — what a victim would like to prevent from happening, in most cases the release of material that victim seeks to keep private.
- value — what the perpetrator demands from a victim.

The presence of these elements together in the online environment is essential for the commission of the crime ([13]). The occurrence of sexual material that can be acquired by a perpetrator is crucial to trigger the whole process. It also differentiates online sexual coercion and extortion from related concepts, such as the abuse of power to obtain a sexual benefit or advantage.

1.1. Current state of knowledge

Much of the empirical research in the domain of child sexual abuse and exploitation has focused on child sexual exploitation material (CSEM ([14])) or CSEM-related offences, variously involving acts of download, possession, distribution or production ([15]). Significant legal and media attention has been concentrated on adults who use technology to engage in sexual contact with children through processes of sexual grooming, solicitation or extortion, whereas comparatively little research attention has been given to this problem ([16]).

Online grooming and solicitation incidents are known to vary widely in their presentation. That is why both phenomena have been variously defined in national and

[12] E.g. the term 'sextortion' was used by the International Association of Women Judges in 2008 to describe corruption involving sexual exploitation. Thomson Reuters Foundation and International Association of Women Judges, *Combating sextortion — A comparative study of laws to prosecute corruption involving sexual exploitation*, 2015, p. 9. Available at: http://www.trust.org/publications/i/?id=588013e6-2f99-4d54-8dd8-9a65ae2e0802

[13] For user concern on this see also Açar, K. V., 'Sexual extortion of children in cyberspace', *International Journal of Cyber Criminology*, Vol. 10, No 2, 2016, p. 113, and Kopecký, K., 'Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors)', *Telematics and Informatics,* Vol. 34, No 11-19, 2016, p. 16.

[14] IWG, 2016, p. 38; Frangez, D., Klancnik, A. T., Karer, M. Z., Ludvigsen, B. E., Konczyk, J., Perez, F. R. and Lewin, M., 'The importance of terminology related to child sexual exploitation — Revija za Kriminalistiko', *Kriminologijo,* Vol. 66, No 4, 2015, pp. 291-299.

[15] Seto, M. C., Hanson, R. K. and Babchishin, K. M., 'Contact sexual offending by men with online sexual offenses', *Sexual Abuse: A Journal of Research and Treatment*, Vol. 23, 2010, pp. 124-145; Taylor, M. and Quayle, E., 'Internet sexual offending', in Brown, J. M. E. and Campbell, E. A. E. (eds), *The Cambridge handbook of forensic psychology*, Cambridge University Press, New York, 2010, pp. 520–526.

[16] Seto, M. C., Wood, J. M., Babchishin, K. M. and Flynn, S., 'Online solicitation offenders are different from child pornography offenders and lower risk contact sexual offenders', *Law and Human Behavior,* Vol. 36, No 4, 2012, p. 320.

international law, policy and in academic literature. Recent concerns around oSCEC have prompted renewed focus on these definitions. This is because online grooming and solicitation activities are related to and overlap with incidents of online child sexual coercion and extortion. This overlap is most conspicuous in sexually motivated, adult-perpetrated cases where strategies of overt manipulation and intimidation ([17]) are used to coerce the child into sexual conduct — whether in the procurement of CSEM or physical sexual activity.

Also, little empirical focus has been given to more recent, related concerns around children and young people's own sexualised use of technology and their role in relation to online CSAE ([18]). The sexual material and activities targeted, commoditised or procured by perpetrators through coercion and extortion have been highlighted by recent definitions of oSCEC ([19]). Therefore, consideration needs to be given to the types of youth-produced behaviours related to sexual content ([20]), such as sexting, that are implicated in these offences. It is critical to differentiate between those children and young people who sext, or produce and send self-generated sexually explicit material (SGSEM) of their own volition, and those who are coerced into such behaviours. Empirical focus needs to be given to how online sexual coercion and extortion offences are influenced by children and young people's behaviour online and indicate profiles of risk and vulnerability in their behaviour that may render them susceptible to online sexual coercion and extortion.

The above described gaps and silos in the research present a number of problems. They compromise the ability to understand 'contact' forms of online CSAE ([21]) and to keep pace with the evolving nature of these phenomena. This is particularly true given the increasing intersection between CSEM and 'contact' forms of online CSAE as present in oSCEC. Critically, they limit the capacity to develop evidence-based policies and interventions, whether at the level of identifying new instances of oSCEC, developing suitable reporting mechanisms, legislative and preventive strategies or implementing interventions that meaningfully respond to the needs of victim, perpetrator and other stakeholder populations.

[17] Sullivan, 2009.

[18] Phippen, A. and Leaton Grey, S., *Invisibly blighted — The digital erosion of childhood*, UCL Press, 2016.

[19] E.g. National Center for Missing and Exploited Children (NCMEC), 2015 and 2016; UN Office on Drugs and Crime (UNODC), 2015.

[20] E.g. IWF, 2015.

[21] Livingstone, S., and Haddon, L., 'EU kids online', *Zeitschrift Für Psychologie/Journal of Psychology*, Vol. 217, No 4, 2009, p. 236.

1.2. Characteristics of online sexual coercion and extortion of children

1.2.1. MOTIVATION OF PERPETRATOR

The majority of open-source cases of oSCEC featured activities with an apparent sexual motivation or interest, where the objective was the procurement of sexual material or activity (83 %). However, in a fraction of cases a patently economic interest prevailed. Similarly, in a handful of cases there was a mixed profile of financial and sexual interest, indicative of a more exploitative profile of sexual offender.

These findings are consistent with recent data published by specialised sources. To review this increasing form of sexual victimisation in greater depth, the National Center for Missing and Exploited Children ([22]) (NCMEC) analysed a subset of sexual coercion and extortion-related CyberTipline reports ([23]) received from October 2013 until April 2016, reclassified by CyberTipline analysts as online enticement blackmail ([24]). Based on the information that was indicated or known when the CyberTipline report was made ([25]), offenders appeared to have committed oSCEC with one of three primary objectives:

- to acquire increasingly more explicit sexual content (photos/videos) of the child (78 % of reports);
- to have sex with the child (5 %); or
- to obtain money or goods from the child (7 %).

Coercion and/or extortion which centres around financial benefit, rather than sexual gratification for the perpetrator, is a comparatively new trend in online CSAE. A general observation based on the collected information is that minors are not primary targets of financially motivated perpetrators ([26]). They are, however, among the victims of this criminal activity. One of the well-known cases of this

[22] The National Center for Missing & Exploited Children is a non-profit corporation, the mission of which is to help find missing children, reduce child sexual exploitation and prevent child victimisation. More information is available at: http://www.missingkids.com/About

[23] The CyberTipline provides public and electronic service providers (ESPs) with the ability to report online (and via freephone numbers) instances of online enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names and misleading words or digital images on the internet.

[24] NCMEC, 2016. Available at: http://www.missingkids.org/sextortion

[25] In 2 % of these reports multiple objectives were indicated; in 11 % of reports the objective could not be determined.

[26] For user concern on this see also. http://www.nationalcrimeagency.gov.uk/news/960-help-available-for-webcam-blackmail-victims-don-t-panic-and-don-t-pay; https://scamalytics.com/wp-content/uploads/2015/02/GDI-Scammers-Online-Dating-Fraud-Scamalytics.pdf

kind was the suicide of a 17-year-old boy from Scotland, who died having been targeted by a group operating from the Philippines and after being tricked into taking part in an explicit Skype chat. He believed that he was talking to a girl of the same age in the United States. He was then blackmailed by the offender demanding money, and threatened that if he failed to pay his naked images would be posted on social networking sites ([27]).

It also seems that there are certain differences in how the scope of criminal activity is defined by the offender's language skills. In general, an offender speaking widely known languages is able to reach more potential targets, whereas an offender speaking a language which is not widespread will not extend beyond the national level ([28]). However, in the case of financially motivated perpetrators, criminal groups will generally operate between countries with a common language. To date, the majority of countries where victims have been targeted are those where English is a primary internet language, such as the United Kingdom, United States, Australia, Singapore, Hong Kong, Indonesia and Malaysia. Similar crimes emerging in French-speaking Africa, targeting France, have also been seen ([29]).

The phenomenon of oSCEC should always be looked at from the victim's perspective while acknowledging differences in perpetrators' motivations and, as a consequence, in their profiles. In this context approaches excluding the remote extortion of money using sexual images ([30]) unless the perpetrator also demands the production of further sexual images or videos from the scope of the oSCEC threat may not necessarily be appropriate, as they miss a sexual crime context. Sexual material created by a minor as a response to an enticing online message can be categorised as CSEM. The risk to a victim extends beyond the initial exploitation and includes revictimisation due to its online posting. Once in worldwide circulation the sexual material may trigger the attention of people who are sexually interested in children and in grooming or online solicitation. Financially motivated perpetrators may consider the commercial distribution of the sexual material gained through remote coercion of money as an opportunity for gaining additional revenue. In the future, a retail market for CSEM produced in the process of sexual coercion or extortion cannot be ruled out, although this observation is still anecdotal.

1.2.2. CIRCUMSTANCES

In describing the ways children are approached, CSE experts referred to both the environments where the suspect contacted the minor and the means of communication which were used for this purpose. The most common answers were: 'social media', 'chat applications' and 'webcam'. Only one expert mentioned online games. According to them, while some platforms were more likely to be used to approach victims than others, there is little evidence to suggest there is anything specific to these platforms that encourages coercive and exploitative behaviour. They are simply platforms used by a high volume of young people, which provides a viable opportunity to those wishing to contact them for potential abuse.

National differences applicable in relation to targeting potential victims are also worth highlighting in this context. Services with largely domestic markets will for the most part enable potential victims to be targeted only by fellow nationals. In contrast, services with a global reach can facilitate such activities by both local perpetrators and those in a different country. This is an important distinction, implying as it does that globally popular services are likely to give rise to (and indeed report) more internationally complex cases ([31]). The use of gaming platforms that allow the user to communicate with many other players with similar interests have a strong potential for abuse, including coercion and extortion.

Some differences have been observed in the targeting of potential victims. There are indications that organised crime groups target a broad spectrum of individuals, and send out bulk requests to groups of potential victims rather than targeting them on an individual basis. This seems not to be the case for sexually motivated perpetrators, who use social engineering methods and apply manipulative tactics aimed at establishing more individual relationships. In both cases offenders will often have used the same social media platform through which contact was initially made to obtain lists of their victim's contacts to target other victims.

The experiences of CSE experts are consistent with the outcomes of NCMEC's analysis where the use of multiple platforms was indicated in 42 % of the reports. When communication occurred across multiple platforms, the offender would intentionally and systematically move the communication with the child from one online platform type to another. Typically the offender approached the child on a social networking site where they learned personal information about the child and then switched to an anonymous messaging app or live-stream video chat where they obtained sexually explicit content from the child ([32]).

Little is known in terms of how long the process of online coercion and extortion lasts. CSE experts indicated that the shortest period observed by them was a few hours whereas the longest one was 'many years', and suggested that differences in the length of this process may depend on the perpetrator's motivation. Examples of cases supporting this observation can be retrieved from open-source data, however empirical evidence is needed before any judgement can be made.

[27] http://www.bbc.com/news/uk-scotland-edinburgh-east-fife-27251900

[28] EC3, *The internet organised threat assessment*, 2014, p. 30. Available at: https://www.europol.europa.eu/ec3/strategic-analysis

[29] https://www.interpol.int/Crime-areas/Cybercrime/Online-safety/Sextortion

[30] E.g. Brookings' report, *Sextortion: Cybersecurity, teenagers, and remote sexual assault,* 2016, p. 11. Available at: http://www.brookings.edu/~/media/Research/Files/Reports/2016/05/sextortion/sextortion1.pdf?la=en

[31] Virtual Global Taskforce, *Environmental scan 2012*, p. 18. Available at: http://www.virtualglobaltaskforce.com/wp-content/uploads/2013/05/VGT-Environmental-Scan.pdf

[32] NCMEC, 2016.

The time factor plays also a significant role in terms of a waiting period between the time the offender acquires the sexual material of the child and the time when coercion and extortion begins. The NCMEC data indicates that, where the waiting period could be determined ([33]), in 80 % of the cases the blackmail appeared to occur the same day. In financially motivated cases this period can be very short, which may cause extreme distress and pressure to the victim, posing challenges to finding the most efficient forms of intervention.

While recognising that a comprehensive picture of oSCEC is still developing it is clear that, regardless of motivation of the perpetrators, the online environment does expand opportunities for the perpetrator in the following areas:

- perceived anonymity and use of manipulative techniques;
- elimination of geographical barriers — opportunity for abuser to receive funds regardless of location;
- high number of potential victims;
- management — in terms of actions to be performed, such as creation of sexual material, photos or videos, participation in tailor-made live-streaming of child abuse;
- lowering risk — in terms of prohibiting disclosure or discovery of the engagement;
- level of threat to victims — ease of distribution of material.

The facilitating role of online technologies and environments, however, needs to be understood not only for offender facilitation. Online technology can have a part to play in the victimisation process with regard to how children and young people's behaviour in online platforms can increase their vulnerability to oSCEC ([34]).

1.3. Key elements of online sexual coercion and extortion of children

1.3.1. MATERIAL

The CSE experts reported that sexual material was recorded by both victim and offender. The images/videos were created by minors for private purposes and then got into unwanted circulation (accidentally or by use of malware or hacking ([35])), or they were created during a deceptive conversation with a perpetrator. The choice of manipulative tactics, often used in combination, depends on the characteristics of both the perpetrator and the victim.

Information collected by NCMEC ([36]) provides more details on the manipulation tactics that were used by offenders:

- reciprocation: 'I'll show you if you show me';
- developing a bond by establishing a friendship/romantic relationship online;
- using multiple online identities against a given child, such as the person coercing or extorting for sexual content as well as pretending to be a supportive friend or a sympathetic victim of the same offender;
- pretending to be younger;
- pretending to be female when they are really male;
- accessing the child's online account (e.g. social media) without authorisation and stealing sexual content involving the child;
- recording the child unbeknownst to them while on a video chat;
- initially offering something to the child, such as money or drugs, in exchange for sexually explicit material;
- pretending to work for a modelling agency.

In the case of financially motivated perpetrators sexual material is, in most cases, created on a consensual basis, as a response to an enticing online message and manipulative techniques. This includes use of the pre-recorded footage, often created by specialised software or obtained from pornography and live-sex camera sites.

1.3.2. THREAT

The tactics used to obtain primary sexual material from a child need to be differentiated from those that a perpetrator uses to ensure their compliance. The most common ones reported by both CSE experts (19 out of 22 answers) and NCMEC (67 %) ([37]) were offenders threatening to post previously acquired sexual content online and, often, specifically threatening to post it in a place for family and friends to see (29 %). Other tactics used by the offenders included:

- physically threatening to hurt or sexually assault the child or family members;
- threatening to commit suicide themselves;
- threatening to create sexual content involving the child by using digital editing tools;
- creating a fake profile as the child and threatening to post sexual content involving the child;
- saving sexually explicit conversations with the child and threatening to post them online ([38]).

[33] 39 % of incidents.

[34] Ybarra, M. L. and Mitchell, K. J., 'How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs', *Pediatrics*, Vol. 121, No 2, 2008, pp. 350-357.

[35] https://www.fbi.gov/file-repository/stop-sextortion-brochure.pdf/view

[36] NCMEC, 2016.

[37] Ibid.

[38] Ibid.

In addition, some CSE experts referred to incentives or particular deceptive practices, that is, when the perpetrator introduced him/herself as representing some kind of authority.

It is worth noting that the majority of perpetrators' threats are based on the sexual nature of the victim–perpetrator relationship. The sensitivity of this relationship, especially in the child's case, is a factor that strengthens the impact of these threats, as the victim would like to prevent it from being revealed. Additionally, the child's distress may be greater if they believe they are participating in illegal activity. In many cases the coercive strategies employed to support the procurement of sexual or financial gains may conform to profiles of cyberharassment and cyberstalking behaviour.

Open-source data shows examples of very specific kinds of threats. In one case a perpetrator who used the internet to meet young girls on modelling and pro-anorexia websites manipulated the girls by acting as an anorexia coach who encouraged them to starve themselves. He also requested that they send him sexually explicit photos. If the girls did not do it, he threatened not to coach them and he ridiculed them (*).

* http://tucson.com/news/local/man-sentenced-to-years-in-federal-sextortion-case/article_8bddebfc-ef26-11e6-b2fa-2b533309c8fd.html

1.3.3. VALUE

In indicating what was most demanded from children in oSCEC schemes the responses of the CSE experts are consistent with the previously cited NCMEC data. When questioned about the proportion of solicitations related to demands for money the majority of the CSE experts assessed it as '10 % or less' and explained that the biggest bulk of the demands were for more CSEM. In their opinion sexual coercion and extortion targeting children is, in the majority, content driven.

This aspect is worth exploring further by making a reference to other observations by NCMEC ([39]). When sexually explicit content was the apparent objective, offenders commonly escalated their demands, both in the quantity of images/videos and/or in the level of seriousness. It was of course not uncommon for children to believe that complying would make the blackmail stop. In some extreme instances, reports indicated that the child was coerced or extorted to provide videos of a certain length while performing specific sexually explicit behaviours, and sometimes even to include other children, such as siblings or peers, in the images/videos.

The demand to include other children requires particular attention, as it seems to be a newly observed trend in oSCEC. In such cases perpetrators leverage control over an established victim to gain access to other children, who are family members or friends. Even children who use safe practices in the online environment or younger children who may not use the internet yet can be targeted this way. According to NCMEC ([40]), in 24 % of the reports retrieved reporters mentioned that they suspected or knew that additional children were targeted by the same offender.

A majority of respondents (21 out of 30) to the question of whether the offender attempted to convince or succeeded in convincing the child to create more sexual material replied in the affirmative. The numbers reported by the experts in terms of the proportion of SGSEM that appeared to have been produced specifically for the suspect under investigation varied from 12 % to 100 %, and the average was 72 %. Some experts (nine) have not determined a percentage but mentioned that this occurred in 'the majority' of or 'almost all' cases. Six experts did not provide or possess such information. These numbers are important indicators (notwithstanding the small sample) that the content-driven type of online sexual coercion and extortion affecting children can significantly increase the amount of CSEM in circulation. The newly produced CSEM can be commoditised by likeminded distributors and downloaders.

In terms of non-content-driven perpetrators' demands the experts that provided information (n = 17) were divided. Eight reported demands for offline encounters with the victims, four reported demands for money and two referred to demands to provide more contacts — from the child's peer group. A single expert reported both money and offline encounters and three experts did not report any further demands. It is worth noting, that when money/goods were the apparent objective, the CSE experts indicated that the money was to be sent via a money transfer service or online payment system. One expert reported that offenders tried to get credit card information from a child, either directly or by having the child sign up for a particular website that required that information.

[39] NCMEC, 2016.

[40] Ibid.

1.4. Scope

The task of collecting information to support an assessment of the scope of online sexual coercion and extortion affecting children is challenging. It is crucial to consider that its incidences may be heavily underreported. Victims can be reluctant to come forward to law enforcement about their victimisation due to embarrassment regarding the material provided to the perpetrator, or may be unaware of the fact that they have been the subject of a criminal offence.

Since oSCEC occurs at the intersection of a number of criminal behaviours, including the grooming and online solicitation of children and the sexual coercion and extortion of adults, it bears the hallmarks of these offences. This overlap can give rise to conceptual confusion regarding the nature of online child sexual coercion and extortion and the criminal offences that may be involved. These factors heavily influence the process of data collection. Additionally, the very complex nature of this crime phenomenon and the different ways of reporting its instances raise challenges beyond the sort of data that is collected, including which organisation (or part thereof) should be targeted in this data-collection process.

Some of the recently published reports can, however, be helpful in shaping a picture of oSCEC. The authors of the Brookings report, who aimed at defining the remote coercion of sexual material or activity and focused on 78 cases involving at least 1 397 victims, stated that in their opinion this was undoubtedly just the tip of the iceberg. According to them, if the prosecutorial estimates in the various cases are to be believed, the number of actual victims probably ranges between 3 000 and 6 500 ([41]). They also noted that 55 of those cases (71 %) involved only minor victims and an additional 14 (18 %) involved a mix of minor victims and adult victims. In nine cases (12 %), all identified victims were adults ([42]).

At the time of writing this report every attempt at determining the scope of the crime threat based on statistical data is close to speculation, as there are no data sets which could be used for comparison. Some assumptions may, however, be drawn from the data collected by NCMEC. The total number of sexual coercion and extortion-related CyberTipline reports received from October 2013 until April 2016 by NCMEC was 1 428. According to NCMEC, since the CyberTipline began tracking this phenomenon in October 2013 these reports have been on the rise. In just the first two full years, between 2014 and 2015, there was a 90 % increase in the total number of reports. This pattern has continued, with oSCEC reports up 150 % within the first several months of 2016 compared to the number of reports in that same time frame in 2014 ([43]). Still, the increasing numbers of the reported cases can also be interpreted as an outcome of raising awareness about the problem rather than growth of the crime threat itself.

Information provided by CSE experts for the purpose of this research also had obvious limitations due to different classification of oSCEC cases. The reasons for this are the nature of the case and the stage when coercion and/or extortion takes place, as an investigation may be launched into grooming cases or online CSEM distribution, and at a later stage it may be determined that elements of coercion or extortion are part of it. On top of that, cases of financially motivated sexual coercion and extortion may be conducted outside of units dealing with CSAE ([44]). All of this makes the collection of information very complicated and, in most cases, not retrievable in an automated way. Additionally, data on online sexual offences against children is not always collected at the national level.

Internationally comparable information remains an aspiration. This is because when the data is recorded and collected at the national level, and where national legislation is approximate, there are variations in the precise provisions for data collection that make national data sets not directly comparable to those of other countries. The use of a mix of legislation regarding sexual abuse and exploitation together with the 'regular' law for extortion was pointed out by some respondents.

Questions regarding the number of cases of oSCEC with which their units dealt in the last 4 years and the number of cases that concluded with the successful prosecution of a suspect or suspects were the most problematic for the experts. Some of them had nothing to report due to the lack of statistical data, and explained this by making a reference to one or more reasons explained above. This, in addition to significant discrepancies in the numbers provided by other experts, did not allow any observations to be made.

At the request of EC3, NCMEC retrieved CyberTipline reports on oSCEC concerning EU Member States (as a possible location of either a victim or an offender) received from October 2013 until April 2016. The total number of reports was 123, and they were sent to the following countries: United Kingdom, Italy, Germany, Sweden, Ireland, Romania, Finland, Belgium, Spain, Portugal, the Netherlands, France, Estonia, Denmark, Bulgaria and Austria. In the vast majority of reports the offender's motivation was sexual: the demands were for sexually explicit content (98) or to have sex with a child (four). Demands of a financial nature were expressed in five cases.

On a final note, it is worth referring to the statistics collected by the UK National Crime Agency's Anti-Kidnap and Extortion Unit (AKEU), which during 2016 received 1 247 reports of offences assessed as cyber-enabled blackmail, more than triple the figure for the whole of the previous year (386) ([45]). Where the demand indicating the

[41] Brookings' report, p. 4.

[42] NCMEC, 2016.

[43] Ibid.

[44] As is the case with the UK National Crime Agency's Anti-Kidnap and Extortion Unit (AKEU).

[45] Information partially available at: http://www.nationalcrimeagency.gov.uk/news/960-help-available-for-webcam-blackmail-victims-don-t-panic-and-don-t-pay. Additional information on 2016 case data was shared with EC3 upon request.

offender's motivation was specified (738), the majority of cases (665) were financially motivated.

1.5. Terminology and working definition of online sexual coercion and extortion of children

The vague or absent definitions of the concept of online sexual coercion and extortion across open sources surveyed for this report may be a possible explanation for the broad use of seemingly self-explanatory terms, such as 'sextortion'. However, its usage in public discourse can be questioned. Unqualified use of this term — an amalgam of 'sexual' and 'extortion' — can be problematic, as it can promote reductionist thinking around the problem of oSCEC, suggesting an overly simplistic image of what is in effect a damaging and complex phenomenon. The unqualified use of this term, along with other terms of a similar nature, can also lead to the development of ambiguous and sometimes even paradoxical concepts ([46]). This confusion could be mitigated by legal definitions or examples of the context in which they are used in legislative instruments, but neither international conventions nor EU legislation define these terms.

Since most national legislation already covers the criminal offence of extortion the phrase 'sexual extortion' would seem to be more relevant, however the correctness of this approach can still be questioned. Some legislation ties the concept of 'extortion' inextricably to the taking of money or property through use of violence or threats ([47]), whereas the purpose of sexual extortion is to obtain sexually explicit material or sexual favours. The term 'sexual extortion' is therefore not broad enough to cover the full variety of online manifestations.

'Coercion' might therefore be a more relevant word, as its meaning is broader and can also be used in connection to any other type of act the victim might be forced to commit, such as acts with sexual connotations. It is worth mentioning that both the Lanzarote Convention ([48]) and the EU directive ([49]) use the word 'coercion' but not 'extortion'.

Acknowledging all of the aspects presented above, the term 'sexual coercion and extortion' is used within this report, however this usage is not without its limitations. For instance, the word 'sexual' defines the concept as sexual in nature, when in some cases the primary motivation or objective for the extortive exchange is social gain or malice (as may occur in peer-perpetrated cases). Similarly, some children may be entirely unaware of the acquisition or procurement of their image and in those cases the defining characteristic is deception rather than coercion.

The use of the term 'sexual coercion and extortion' can also be problematic in the context of financially motivated procurements involving children, as the primary motivation for such offences is not sexual. However, given the sexual nature of the conduct and/or material that is targeted or procured in the exchange, this use may be justified. Alternative terminology such as 'economic sexual extortion' or 'commercial sexual extortion' may also be appropriate for use in public discourse, as it directly refers to the financial nature of unlawful behaviour and the motivation of its perpetrators.

The open-source searches returned few documents which contained a definition of online sexual coercion and extortion ([50]). In terms of oSCEC most of the documents originating from specialised sources referred in the first place to related concepts in online behaviour, such as sexting, grooming and solicitation. On limited occasions they introduced elements of online sexual coercion and extortion as their escalated form ([51]). Some other proposals were retrieved from websites of organisations or institutions dealing with combating CSAE ([52]). The majority of them, however, used the term 'sextortion' in their definitions, which suggests that more efforts are needed in promoting the use of proper terminology.

Bearing the previously described characterising features and key elements of the phenomenon under investigation in mind, in broad terms oSCEC may be defined as the targeting and commoditisation of a child, or the visual depiction of that child, by technological means, using sexual images and/or videos depicting that child, through coercion or extortion for the purposes of sexual gain (for example new CSEM or a sexual encounter), financial gain or other personal gain (such as psychosocial gain, e.g. popularity or malicious satisfaction).

[46] For user concern on this see also IWG, 2016, p. 53.

[47] E.g. German Criminal Code, Section 253, Extortion.

[48] The Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse.

[49] Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography.

[50] E.g. Brookings' report, p. 10; https://www.wearethorn.org/sextortion/; https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-sextortion-in-the-far-east.pdf

[51] E.g. UN Office on Drugs and Crime (UNODC), *Study on the effects of new information technologies on the abuse and exploitation of children,* 2015, p. 12. Available at: https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf

[52] E.g. https://www.interpol.int/Crime-areas/Cybercrime/Online-safety/Sextortion; http://virtualglobaltaskforce.com/resources/faqs/

2/ VICTIMS AND PERPETRATORS

2.1. Perpetrator profile

While the primary motivators for online child sexual coercion and extortion behaviours appear to be resolvable to sexual and financial interests, it is important to consider that the motivations for sexually exploitative behaviours are rarely limited to one of these factors. Existing sexual offence research indicates that motivations for such behaviours are typically multidimensional. In the case of offenders with exploitative profiles, the sexual coercion and extortion offence may be both financially and sexually motivated. These motivations and offence-related inclinations can extend to a range of other factors, such as antisocial tendencies and socioemotional influences such as deficits in intimate relationships ([53]) and aggressive or violent dispositions ([54]).

Additionally, existing polar conceptualisations of sexually motivated solicitation offenders are rather static. They offer little insight into the dynamic nature of the supporting offence process, or the factors that may support offending onset and persistence, particularly those factors that influence the escalation of offending behaviour. Perpetrator motivations and objectives in solicitation processes are dynamic and responsive to situational influences, changing as a function of technology use and in response to the variable dynamics of victim–offender interactions ([55]). More robust empirical understanding of the offender's behavioural profiles is required, with attention to the dynamic influence of victim behaviours, responses, online contexts and other situational factors relating to offence progression.

The task of determining the profile of a perpetrator in oSCEC cases is additionally challenging due to the variety of tactics and deceptive strategies that are used. For this reason information retrieved from CyberTipline reports may not be helpful, as it reflects only the perspective of the victim or of someone who reports on the victim's behalf. In financially driven incidents the victims usually interact with a female, or someone who pretends to be female, so victims perception of the situation may not be reliable.

In answer to the EMPACT survey question about the typical profile of the offender behind oSCEC, the most apparent finding was that of all the experts surveyed (n = 24), only two reported both males and females as being commonly implicated in these offences. None of the CSE experts reported that only females typically perpetrated online sexual coercion and extortion offences, and the great majority of them (22) reported that males were most commonly responsible for these offences. While the information about the gender of the most common

OFFENDER PROFILE SEXUAL MOTIVATION

- Male.
- Operates alone but shares / exchanges the acquired content.
- May act on both international or national level.
- Activity driven by knowledge of languages.
- Targets female victims.
- May know the victim in person.
- Main goal: to obtain sexual material and/or sexual favours offline.

[53] Seto et al., 2012.

[54] Wolak, J., Finkelhor, D. and Mitchell, K., 'Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study', *Journal of Adolescent Health*, Vol. 35, No 5, 2004, pp. 424.e11-424.e20.

[55] E.g. Kloess, J. A., Beech, A. R., and Harkins, L., 2014. Online Child Sexual Exploitation Prevalence, Process, and Offender Characteristics. *Trauma, Violence and Abuse, 15(2),* pp. 126-139.

perpetrator in oSCEC cases was precise, the reported age range was dispersed. The experts reported perpetrators between 14 and 70 years old, the average age being 34 years old. It is assumed that the experts described perpetrators of sexual rather than financial procurements.

The motivation behind criminal activity also seems to define some further characteristics of the phenomenon under investigation: oSCEC is to be considered a global phenomenon, however when it is driven by sexual interest in children it does not appear to bear hallmarks of organised crime, as seems to be the case for its financially driven form.

Some recent initiatives undertaken by Interpol are worth mentioning here. In 2014 Interpol coordinated two operations — Operation Strikeback 1 and 2 — in the Philippines. Apart from the successful neutralisation of a few criminal groups based there, this intervention also highlighted some methodologies used by those groups. Operating on an almost industrial scale from call centre-style offices, cyber-blackmail agents were provided with training and offered bonus incentives such as holidays, cash or mobile phones for reaching their financial targets ([56]).

The problem has not been eradicated. Both increased reporting by law enforcement and media highlighted other key source countries. Besides the Philippines, criminals demand that money be remitted to Côte d'Ivoire and Morocco. To determine any potential way forward in dealing with the crime threat, the current efforts of law enforcement should focus on an assessment of its true scale and on further understanding the methodologies used in its furtherance.

OFFENDER PROFILE FINANCIAL MOTIVATION

- Both genders.
- Members of an organised criminal enterprise.
- Operates in teams based in developing countries.
- May act at both international and national level.
- Targets male victims in countries linked by language.
- Does not know the victim in person.
- Main goal: to obtain money.

2.2. Victim profile

The literature does not provide much insight into whether there is a 'typical' victim for sexual coercion and extortion and therefore, until more evidence is gathered, opinion-based judgements should be avoided. There is certainly some evidence to suggest ([57]) that as young people get older they are more likely to become victims, but without a greater understanding of causation it would be difficult to draw conclusions. There may for example be a higher probability of coercion purely as a result of more unsupervised internet access and, in teen years, a failure to perceive risk given their developmental stage and associated vulnerability.

Gender distinctions are also difficult to determine from studies. It has been empirically established, for example, that girls are more likely to experience coercion to participate in SGSEM-related activities ([58]). It is, however, unclear whether this vulnerability extends to online sexual extortion experiences, and whether girls are particularly vulnerable to coercive forms of online sexual extortion. While organisations such as the Internet Watch Foundation (IWF) generally report that a higher prevalence of female SGSEM is collected, methodologies in such studies are not sufficiently complex to make inferences regarding whether this is due to a higher level of female victims or simply that such images are more likely to be found on the open internet.

In light of the above observations, NCMEC's ([59]) analysis of a subset of sexual coercion and extortion-related CyberTipline reports may again be helpful in providing additional information on the subject matter:

- 78 % of the reports involved female children and 15 % involved male children (in 8 % of reports, child gender could not be determined);
- male and female children each ranged in age from 8 to 17 and had an average age of 15; however, compared to female children, it was less common for male children to be on the younger end of the spectrum.

Further important observations regarding gender distinction were also made:

- female children were blackmailed significantly more often for sexually explicit content (84 %) compared to male children (53 %);
- male children were blackmailed significantly more often

[56] https://www.interpol.int/en/News-and-media/News/2014/N2014-075

[57] E.g. IWF, 2015.

[58] Daphne III research report, *Safeguarding teenage intimate relationships (STIR): Connecting online and offline contexts and risks*, 2015, Bristol, United Kingdom. Available at: http://stiritup.eu/wp-content/uploads/2015/06/STIR-Exec-Summary-English.pdf

[59] NCMEC, 2016.

for money/goods (32 %) compared to female children (2 %).

While the majority of these manipulation tactics were used equally against male and female children, there were significant differences in the use of certain methods. More specifically, when child victims were male offenders were significantly more likely to pretend to be younger and/or a female; offer to engage in sexual reciprocity through shared images or by live-streaming; and record the child unknowingly and then threaten to post the images/videos so family and friends could see. In contrast, when child victims were female, offenders were significantly more likely to offer something to get initial sexually explicit content from them, such as money or drugs ([60]).

In terms of the most common victims of online sexual coercion and extortion based on the CSE experts' experience of the last 4 years, 14 out of 24 experts reported more female victims. Eight reported both male and female victims, while two also stressed that there was a greater number of female victims. One expert reported only male victims. The reported minimum age was 7 and the maximum 18. Only one expert reported an age range of 15 to 25, suggestive of the broader scope of this crime phenomenon and the fact that it affects adults as well as minors. The average of the minimum reported ages was 11.2. The average of the maximum reported ages was 15.3 (without the outlier value of 25).

Additional observations can be drawn from the already referenced data collected by AKEU in the United Kingdom. The majority of victims in cyber-enabled blackmail cases (1 247) reported to the AKEU in 2016 were male (1 107) and ranged in age from 8 to 82, with the largest number of victims in the 18-24 age range (443), however the total number of victims under 18 was 123. Female victims were significantly more likely to be targeted by solely sexually motivated offenders, with demands for further images or sexual contact made in 46.56 % of cases featuring female victims.

VICTIM PROFILE

- **Any person whose sexual material could be acquired by a perpetrator.**
- **Usually female in case of sexually motivated perpetrators.**
- **Usually male in case of financially motivated perpetrators.**

In terms of the question about the number of victims of oSCEC that were identified (both in the country of the expert and other countries), many CSE experts could not provide a total number, stressing again that there were no separate statistics to determine whether the child was a victim of online sexual coercion and extortion or another sexual offence. Those that have provided numbers reported between 40 and 300, with an average of 80 victims identified.

The experts had difficulties in answering the question on the average number of victims per case. Some of them mentioned one to two victims per case, while others reported 20 to 50 victims. The rest used descriptive phrasing in their responses instead of numbers, and such expressions as 'a lot' or 'many'. One expert stressed the fact that even though he only mentioned an average of one victim per case the trend is up to five or six per case. Conclusions could not be drawn from such diverse information, which only stresses a need for further research in this domain.

Experts pointed out the following victim characteristics in cases of online sexual coercion end extortion affecting children:

- naivety of the victims, either on a relational level or on a technical level;
- absence of parental control;
- willingness to share self-generated sexual content;
- significant amount of time spent online each day;
- use of social networks and other ways of online communication, especially through mobile devices;
- befriending strangers (unknowns);
- sexualised conversations with strangers;
- lack of technical knowledge.

These data, however, do not necessarily provide an empirical rationale for the resulting coercion or abuse, as this is an interpretation by the survey respondent. While the reporting officers might suggest these are 'reasons' for the crime, without far more in-depth exploration of cases it is very difficult to prove this is the reason for the offence. For example, 'absence of parental control' or spending a lot of time online a lot are not necessarily causes of a young person becoming a victim of coercion. The responses may be a useful interpretation by those involved in the investigation of such crimes while highlighting the need for objectivity when interpreting victim motivations.

The two most emphatic risk factors for victimisation reflected in the answers of CSE experts related to a lack of knowledge about the dangers of the internet, along with a lack of parental control and the victim's adverse personal situation or psychological state. Parental control should be considered here as meaning parental engagement, where young people are willing to discuss their online behaviour and any concerns they might have about the people they meet, and to disclose such in the event of upset or harm. In terms of the second category of low self-esteem, experiencing difficulties at school or with friends or family were most commonly mentioned as causation factors.

[60] NCMEC, 2016.

3/ A RESPONSE TO THE PHENOMENON

3.1. Preventive response

The significance of prevention at different levels to effectively reduce CSAE has been highlighted in the existing international legal instruments ([61]). Some of these provisions are echoed to some extent by national legislation, organisational solutions and academic literature. However, the development of a 'culture of prevention' around CSAE at the EU level is still ongoing, and Member States' practices vary considerably in this field ([62]).

The development of successful preventive or awareness-raising campaigns related to CSAE is not always simple. The CSAE crime phenomenon is multifaceted, with intricate subtleties; hence, crime-prevention campaigns often face challenges that can only be overcome through the combination of theory-based models with existing practical knowledge. The latest research highlights that the prioritisation of intervention and prevention in this domain must be on the basis of a multidisciplinary, public health approach in which all agents involved standardise their approaches, with clear and coherent primary aims and objectives ([63]).

An extensive online search was carried out in order to describe efforts to prevent oSCEC ([64]). The different types of initiatives that address the prevention of risky online behaviour in general were grouped into different categories. To better understand the different types of initiatives found the categories chosen according to the content and/or action plan of these initiatives were then divided into subcategories according to their content and form.

The first category groups together the initiatives that related to a more technological feature, such as guidelines for the IT industry or existing software that claims to prevent hazardous online behaviour ([65]). The items in the second category relayed a more academic background — studies and published articles of different sorts that provide a better understanding of the online behaviour of children and perpetrators. The third category was based on approaches coming from the law enforcement environment or other organisations/institutions dealing with CSAE-related complaints ([66]). Finally, the fourth category was the most 'hands-on', including actions to raise awareness or to

[61] Lanzarote Convention, Chapter II, 'Preventive measures'; paragraph 34 of the recital, Article 23 of the EU directive.

[62] *Combating sexual abuse of children Directive 2011/93/EU — European implementation assessment*, 2017, p. 28. Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/598614/EPRS_STU%282017%29598614_EN.pdf

[63] Key finding of the EU-funded report exploring policing and industry practice in the prevention of online child sexual abuse and the experience of young people online, including the experience of victimisation. *EU Child Online Safety Project — Enhancing police and industry practice, 2016,* p.8. Available at: http://www.mdx.ac.uk/__data/assets/pdf_file/0017/250163/ISEC-report-FINAL.pdf

[64] Although the aim of the search was to cast as wide a net as possible in order to have a better understanding of the international and national prevention of oSCEC, obvious limitations should be highlighted here. All the research was conducted in English, which undoubtedly excluded a certain number of other initiatives. Additionally, the analysis of the programmes was done only with the information available through open sources, possibly biasing how they were developed and their contents.

[65] An interesting example of a technological feature is a model originating in Norway which has been successfully used in several other countries. When a user with a Bulgarian IP address wants to access a sexual coercion and extortion-dedicated online platform he/she is redirected to the website of the Bulgarian Cybercrime Unit where it is possible to report a crime (http://www.cybercrime.bg).

[66] E.g. https://ceop.police.uk/ceop-reporting/

educate parents and children on the topic of unsafe online behaviour ([67]).

The main conclusion was that there were several programmes that addressed potentially unsafe online behaviour including sexting and phenomena like grooming or cyberbullying, but very few of these programmes directly and solely targeted oSCEC ([68]). These were presented either in a cartoon-type format or as short videos. Additionally, the initiatives found seemed not to fully comply with the theory behind effective prevention programmes ([69]), as only some of them incorporated some of what are considered the essential principles ([70]) of effective prevention programmes.

One issue with a number of prevention programmes in this domain was that they are 'pull'-based in nature: the end user has to have at least a passing interest in the topic to access the materials. Empirical work ([71]) shows that while preventive programmes targeting such behaviours as sexting are often established, when they are delivered poorly it is unlikely that young people will view them favourably. Preventive programmes can lay the foundations and provide materials for effective learning, but they need to be integrated into broader education content, with appropriate levels of discussion and follow-up support for young people.

Effective preventive programmes should ideally result in a mix of the different existing types of interventions using various methods. In terms of the CSAE domain there is a need to develop education programmes that acknowledge that sometimes something wrong happens, and to provide more of an empathetic or incident-response approach. Encouraging young people to be more critical in their online interactions rather than attempting to prevent them engaging in behaviours which enact the exploration of their sexual identities is essential to this approach. Some research findings focusing exclusively on oSCEC suggest ([72]) that it is important to base preventive programmes in case studies.

TECHNICAL FEATURE

- Guidelines for IT industry.
- Prevention software.
- Safer internet policies.

ACADEMIC APPROACH

- Comparative law studies.
- Studies on offenders in the virtual world/ grooming.
- Virtual- versus real-world studies.
- Evaluation of national strategies.
- Focus on the importance of prevention.

LAW ENFORCEMENT-ORIENTED ACTIONS

- Websites for the online reporting of CSAE-related crime.
- Police advice/warnings on newspapers.

EDUCATION AND AWARENESS RAISING

- Advice for parents/children on online behaviour.

[67] E.g. http://swgfl.org.uk/products-services/esafety/resources/So-You-Got-Naked-Online/Content/Sexting-Toolkit; https://www.facebook.com/help/726709730764837/?helpref=hc_fnav

[68] E.g. http://www.missingkids.org/sextortionpsa; http://www.sextorsion.es/; http://ow.ly/ePX9306ESpR

[69] Nation, M., Crusto, C., Wandersman, A., Kumpfer, K. L., Seybolt, D., Morrissey-Kane, E. and Davino, K., 'What works in prevention: Principles of effective prevention programs', *American Psychologist*, Vol. 58, No 6/7, 2003, pp. 449-456. Available at: http://www.ncdsv.org/images/AmPsy_WhatWorksInPrevention_6-7-2003.pdf

[70] Ibid. Principles related to programme characteristics: comprehensive, varied teaching methods, theory driven, positive relationships. Principles related to matching the programme with a target population: appropriately timed, socioculturally relevant. Principles related to implementation and evaluation of prevention programmes: outcome evaluation, well-trained staff.

[71] E.g. Phippen, A., 2012. *Sexting: An Exploration of Practices, Attitudes and Influences.* Available at: https://www.nspcc.org.uk/globalassets/documents/research-reports/sexting-exploration-practices-attitudes-influences-report-2012.pdf; Ringrose, J., Gill, R., Livingstone, S., Harvey, L., 2012. *A qualitative study of children, young people and 'sexting'* – A report prepared for the National Society for the Prevention of Cruelty to Children.

[72] Kopecký, 2016, p. 20.

The added value of this method is a higher level of influence on the child, and at the same time they are trained on how to react if they ever face a similar situation ([73]). On a final note, the preventive programmes addressing threats in the online environment should be included in national school curricula.

The massive importance of prevention can be supported by information originating from a number of sources on the consequences of oSCEC ([74]), including cases of self-harm or even suicide ([75]). Among CSE experts who felt able to provide feedback on the question of whether the child's experiences led to them threatening or engaging in self-harm, including sexual self-harm or even suicide (n = 20), 12 replied affirmatively and four reported suicide or suicidal behaviours. Eight experts replied in the negative. This small sample, even if very limited by the source data, stresses the value of prevention in responding to the crime threat.

According to the outcomes of NCMEC's study, child victims commonly experienced a range of negative outcomes, including hopelessness, fear, anxiety and depression. Overall, it was indicated in 13 % of CyberTipline reports focusing on oSCEC that the child victim had experienced some type of negative outcome. Of those reports with some type of negative outcome, it was indicated that about one in three children (31 %; 4 % of all oSCEC reports) had engaged in self-harm, threatened suicide or attempted suicide as a result of the victimisation. There were no child gender or age differences in regard to negative outcomes. It was also common that concern was expressed for other potential victims, and was a likely reason for making the report ([76]).

Without any doubt the key message which should be conveyed by prevention and awareness-raising interventions targeting the phenomenon under investigation is that oSCEC is a crime and perpetrators will be prosecuted. It is also essential that such interventions focus on the key elements of oSCEC: material, threat and value and align particular actions around them. Furthermore, since the occurrence of sexual material that can be acquired by a perpetrator is crucial to triggering the process of oSCEC, specific attention should be given to 'material'-oriented interventions. It seems that applying the knowledge already gathered within the research on the types of youth-produced sexual content-related behaviours ([77]), such as sexting, to initiatives aiming at preventing the irresponsible sharing of sexual material is to be considered a starting point. To make such an intervention complete and address instances of technically assisted coercion, continued efforts aiming at raising awareness of safety features that could be applied to prevent use of hacking or malware are needed.

In any preventive undertaking the key elements of oSCEC should be explained in the context of offence processes ([78]). Providing adequate advice and tools reflecting victim and abuser behaviour at each stage of such processes can reinforce the victim's position and disrupt the victimisation process. As indicated in the NCMEC's survey it was not uncommon for children to believe that complying would make the blackmail stop. This would suggest that given a proper explanation on the consequences of complying or not with a particular perpetrator's demands, a victim could be in a better position to effectively counteract those demands. An additional example of tailor-made advice can be found in the bullet points of the Federal Bureau of Investigation's leaflet 'Defence against sexual extortion', where it is stated that: 'it is not a crime for a child to send sexually explicit images to someone if they are compelled to do so, so victims should not be afraid to tell law enforcement if they are being sexually exploited' ([79]). This knowledge may be crucial for a child victim, not only in terms of disclosure but also in responding to some manipulative strategies used by perpetrators.

The analysis of the present preventive and awareness-raising initiatives in the context of the characteristics of oSCEC, especially its impact on victims, indicated a clear need for a specific kind of preventive intervention, which would be closely linked with the existing reporting and victim-support mechanisms. Such an intervention has been included in the operational action plan 2017 of the Child Sexual Exploitation European Multidisciplinary Platform Against Criminal Threats, and will be explained in the next part of the report.

3.2. Reporting and support mechanisms

Embarrassment regarding the material provided to the perpetrator or lack of awareness by potential victims that they have experienced a criminal offence have already been mentioned as the main reasons for heavy underreporting of cases of oSCEC. Additionally, it seems to be the case that some legislation may treat the victims as offenders, comparing the actions of a child taking a nude photograph and sending the media over the internet to that of producing CSEM. This shaming of the victim perpetuates the child's victimisation and creates a culture that is not-conducive to disclosing victimisation.

According to the CSE experts, notifications about cases of oSCEC were received by their respective units via multiple

[73] E.g. http://virtualglobaltaskforce.com/resources/case-studies/

[74] E.g. https://www.fbi.gov/news/stories/sextortion

[75] At least four suicides in the United Kingdom, including minor victims, have been linked to this form of criminal activity; e.g. http://www.bbc.com/news/uk-38150313

[76] NCMEC, 2016.

[77] E. g. Project Spirto: *'Self-produced images — risk taking online'*. Available at: http://www.spirto.health.ed.ac.uk/

[78] For user concern on how oSCEC takes place from the research that directly deals with this crime phenomenon see Kopecký, 2016, p. 16.

[79] http://www.westwarwickpd.org/Other/Sextortion_Affecting_Thousands_of_US_Children.pdf

sources. Around 70 % were reported directly by the victims, family members or teachers. Some experts mentioned proactive investigations online and international police channels, including Interpol, when the investigation is conducted outside of the country and a victim is a citizen of that country. The third category was reporting by the private sector and non-governmental organisations (NGOs), acknowledging the role of INHOPE's hotlines ([80]) and NCMEC in this process.

Although the answers given by the CSE experts were rather broad, they already indicate a very important characteristic of the existing reporting mechanisms: they follow a multidisciplinary approach, in a form of cross-reporting, where different actors are represented. While this approach seems to be appropriate, there are some challenges that arise from the goals of each of the actors that may influence the coherence and effectiveness of both national and international reporting mechanisms. It is therefore essential that those actors work together to minimise the duplication of efforts and provide optimal input into the whole process.

NCMEC pointed out ([81]) important child gender and age differences among those who made the reports. While male children were significantly more likely than female children to self-report, female children were significantly more likely than male children to have internet companies and peers report on their behalf. Parents/guardians and other authority figures were equally likely to report for male and female children. Furthermore, while self-reports and reports by internet company were more likely among older children, reports by parents/guardians, authority figures and online strangers were more likely among younger children. Peers were equally likely to report for older and younger children.

Child victims disclosing their victimisation is a vital element in the disruption of the offending and victimisation processes. It is therefore of utmost importance to deepen the above-presented findings, aiming at indicating factors favourable to disclosing victimisation. These factors should then be reflected in features of the reporting mechanisms and their tools to make them adequate and clear. The role of the private sector and its gatekeeper responsibilities need to be stressed here, especially in the light of the previously referenced key findings of the EU-funded research on policing and industry practice in the prevention of online child sexual abuse ([82]). According to them, with regard to industry safety practice some young people complained that safety procedures and report mechanisms were too complicated to follow, and there were also a number of misconceptions about reporting inappropriate material which stopped individuals from acting.

More detailed information on those who report incidents of oSCEC can be retrieved from the NCMEC study (*). Overall, internet companies were the most common reporters of oSCEC to the CyberTipline (33%), followed by the child victims (24%) and parents/guardians (22%).

The high percentage of reporting by internet companies should, however, be interpreted in the light of the specificity of CyberTipline reporting mechanism, which offers a practical solution to the duty provided for in US law for the reporting of incidents of CSAE by online platforms. Interestingly, almost half of internet company reports made to the CyberTipline were known to have originated as self-reports, making the child victims the most common direct or indirect reporter of oSCEC incidents that were ultimately processed by the CyberTipline (38%).

Other reporters to the CyberTipline included peers (e.g. friends, romantic partners, siblings; 7%), authority figures (e.g. police, teachers, counsellors; 5%) and online strangers to the child (3%).

* NCMEC, 2016.

[80] INHOPE is an active and collaborative global network of hotlines dealing with illegal content online and committed to stamping out child sexual abuse from the internet. More information is available at: http://www.inhope.org/gns/who-we-are/at-a-glance.aspx

[81] NCMEC, 2016.

[82] *EU Child Online Safety Project*, 2016, p. 10.

Bearing in mind the complexity of oSCEC and its impact on the victims, however, the challenge is not only to make those who want to report its incidents aware of the available reporting mechanisms, but also to provide a child victim with support that may be needed in particular circumstances, including very dynamic scenarios. Characteristics and key elements of the phenomenon under investigation should again serve as a basis to indicate the most effective methods of support. Organisations acting in this domain should evaluate their procedures and resources in the context of what community support may be available to victims of oSCEC, including immediate interventions. Support for victims should also be ensured at every stage of the oSCEC process, to help them in overcoming negative outcomes. The long-term goal is to create a supportive society response, which would reduce the persistence of victim blaming in relation to sexual offences. The importance of the role of professionals in close contact with children, along with helplines, should be underlined here ([83]).

As was already mentioned, a unique preventive campaign ([84]) has been developed as one of the activities of the Child Sexual Exploitation European Multidisciplinary Platform Against Criminal Threats, aiming at awareness raising and strengthening reporting and support mechanisms as a response to the threat of oSCEC. The campaign builds on global and universal features of oSCEC, and provides tools that, with minor modifications reflecting sociodemographic differences, can be easily adopted on a national level in every EU Member State and beyond.

The awareness-raising goal of this undertaking is to be achieved by explaining key elements of oSCEC and its characteristics, especially two main motivations of perpetrators, in a short video ([85]) translated into all EU languages, along with additional informative content broadcast through the websites of EC3, law enforcement agencies and other stakeholders who have decided to support this initiative.

To achieve the second goal of the campaign, the CSE experts have focused on strengthening the cooperation among the relevant stakeholders in their respective countries to work out the most effective way of handling notifications about incidents of oSCEC and providing the necessary support to victims at the same time. The contact details of these actors are to be communicated in numerous ways as a part of the campaign.

[83] For user concern on this see also *Combating sexual abuse of children Directive 2011/93/EU — European implementation assessment*, p. 51.

[84] www.europol.europa.eu/sayno

[85] EC3 would like to acknowledge the support of the students of The International School of The Hague in The Netherlands, who were very helpful in consulting both the script of the video and its draft.

ONLINE SEXUAL COERCION AND EXTORTION AS A FORM OF CRIME AFFECTING CHILDREN

Law enforcement perspective

EUROPOL
EC3 European Cybercrime Centre

Eisenhowerlaan 73, 2517 KK
The Hague, the Netherlands

www.europol.europa.eu
Follow us