EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Combating child online sexual abuse

VIRTUAL GLOBAL TASKFORCE

Virtual Global Taskforce Child Sexual Exploitation Environmental Scan 2015

Public version
October 2015

The VGT aims to make the Internet a safer place, identify, locate and help children at risk and hold perpetrators appropriately to account.
The Report Abuse button on the VGT website is an effective way to report suspicious online behaviour.

www.virtualglobaltaskforce.com

Table of contents

1. Executive summary

Key findings are as follows:

- Online child sexual exploitation (CSE) methods of operation continue to develop in line with the adoption of technology. CSE offenders will exploit current and emerging technology, coupled with anonymous networks.
- Greater levels of Internet adoption, both in terms of territorial coverage and increased bandwidth, as well as further expansion of mobile connectivity, remain key factors that are constantly reshaping online offending.
- The live streaming of child sexual abuse is no longer an emerging trend but an established reality. The technology that enables the streaming of live images and video is being exploited by perpetrators with a sexual interest in children as well as by those interested in the monetisation of live-distant child abuse (LDCA)[1].
- The prevalence of online distribution of self-generated sexually explicit material (SGSEM) is a phenomenon requiring additional research due to its unclear relationship with CSE.
- Children remain at risk of harm through online grooming and solicitation for sexual purposes, which in the most serious cases can turn into sexual coercion, where victims are threatened with the dissemination of sexually explicit material depicting them, and they have to comply with offenders' demands.
- Peer-to-peer (P2P) file sharing methods remain the main platform to access child sexual abuse material (CSAM) and the means for non-commercial distribution.
- The use of The Onion Router (Tor) in the proliferation of CSAM remains a key threat. Restricted areas of Tor pose the highest risk to children as it is likely that more CSAM of an extreme nature, often created on demand, is being requested and shared there.
- Commercial CSE has not been eradicated but has evolved into new forms of criminal activity. The dynamic nature of this crime area dictates that emerging

1 Live-distant child abuse (LDCA) is a term suggested by specialists to underline the fact of sexual abuse even if physical contact between an offender and a victim does not take place

trends should always be taken into consideration whenever questions about the current scale of this phenomenon arise.

- CSE offenders continue to misuse legitimate hosting possibilities to store and distribute CSAM. The marked increase in the abuse of image hosting sites was reported by INHOPE[2].

2 International Association of Internet Hotlines (INHOPE) is an active and collaborative network of 51 hotlines in 45 countries worldwide, dealing with illegal content online and committed to stamping out child sexual abuse from the Internet; http://www.inhope.org

2. Introduction

The Virtual Global Taskforce (VGT) is a collaborative partnership of law enforcement agencies, who have come together across the digital divide to combat online child sexual abuse worldwide.

This environmental scan has been commissioned by the VGT Board of Managers to set its strategic priorities for the next four years. It is a public version of an assessment by and for law enforcement (LE).

The assessment builds on and updates the document published in May 2013[3], and should be considered as an interim product, primarily focusing on developments in the child sexual exploitation phenomenon in the last two years. Following the example of the 2013 assessment, this report consciously follows a more qualitative approach to analysing aspects of CSE. However, careful attention was also paid to quantitative data whenever available.

In qualitative terms this research draws heavily on the observations of 35 online CSE investigators themselves representing VGT member agencies, expressed in a thematic questionnaire addressed to them[4].

Additional information was taken from responses to questionnaires by LE partners of the European Cybercrime Centre (EC3-Europol)[5] which helped produce the 2014 Internet Organised Crime Threat Assessment (iOCTA)[6] and the updated 2015 iOCTA[7]. The iOCTA examines and reports on the current threat landscape across the whole of the European Union (EU) for all cyber-dependant and cyber-enabled crime areas.

Additionally, to make the response of law enforcement complete, in many instances this assessment refers to expertise gathered by the members of Focal Point (FP) Twins[8].

---

3 http://www.virtualglobaltaskforce.com
4 Responses provided by LE agencies in Australia, Switzerland, United Kingdom, Canada and the US Homeland Security Investigations (HSI)
5 https://www.europol.europa.eu
6 https://www.europol.europa.eu
7 https://www.europol.europa.eu
8 The team of experts and analysts dealing with CSE in the European Cybercrime Centre (EC3-Europol)

The first part of the environmental scan sets out current trends in CSE as reported by LE representatives. In some instances their answers have been supplemented by information originating from other specialised sources, organisations or institutions. The second section focuses on future developments (social, technical, legislative and organisational) which may influence the CSE area in four years' time. This part draws on the responses of both LE and VGT partners[9] as well as comprehensive scanning of open source material.

EC3-Europol would like to express its thanks to all members of the international community for their cooperation in preparing this document.

3. Law enforcement trends

This part of the report aims to highlight obvious trends that have been indicated by law enforcement representatives in their responses to the questionnaires mentioned in the introduction. As the majority of respondents referred to online CSE, this document consequently refers to contact offending to a very limited extent. The trends will be further elaborated in parts 3 and 4 of the report, focusing specifically on both victim and offender environments.

As expected the range of answers was very broad. Many of the respondents indeed referred to global trends, whereas others tended to make only a reference to characteristics of them, or pointed out particular environments or even specific examples relating to both offender and victim. There were also significant differences in the way that changes – either increases or decreases - were reflected, and in particular trends. The diversity of the respondents' functions undoubtedly enriched the set of responses, although it could also be why some participants did not answer all questions.

Also of note, respondents were additionally asked to rank the current trends in order of importance. The very subjective, diverse approach of respondents, which is believed to reflect investigative priorities of individual law enforcement agencies, made analysis

9 Responses provided by ECPAT International, International Centre for Missing and Exploited Child (ICMEC), Kids Internet Safety Alliance (KINSA) and NetClean

of this part of the survey very challenging. That led to ranking the responses not by importance but by frequency. Careful attention has also been given to any reported changes referring to the scale of a specific trend.

3.1 Current trends in child sexual exploitation

The majority of respondents noted a general trend, which is a steady increase in cases of online offences resulting from the increased and widespread use of and access to the Internet and technology. At the same time respondents identified growth in specific areas of concern in that general trend such as online grooming and solicitation, including sexual extortion, the live streaming of child sexual abuse, as well as the spread of self-generated sexually explicit material on social media.

Some respondents observed that children are becoming more daring and explicit, and often more complicit in terms of self-generated sexually explicit images.

The live streaming of child sexual abuse is no longer an emerging trend but an established reality.

It is of particular concern in the context of emerging markets due to Internet adoption there.

Concerns were expressed regarding an increased use of social networks in child sexual exploitation. This use was primarily to set up initial contacts with potential victims, which is then followed by virtual, 'face-to-face' chats with sexual intent.

Where coercive techniques were adopted in online solicitation of children for sexual purposes, an emerging trend towards more extreme, violent, sadistic or degrading demands by offenders were mentioned.

Respondents were asked how increasing Internet coverage in developing countries has impacted online CSE in their jurisdictions. Interestingly, the majority of them clearly indicated the consequences of such developments in both the victim and offender environments. They mainly referred to the increase in the live streaming of child sexual abuse to their nationals from developing countries, although this type of crime was also reported as being committed on a national level. They also referred to the increased targeting of children for online CSE by offenders located in such countries. In their

opinion more leads have been generated in both areas mentioned above. Some answers alluded to more images of unknown victims and more production of material apparently sourced in developing regions.

According to respondents, child sexual offenders exploit technology that enables live streaming of images and video in many different ways. The relatively high financial rewards available to organisers of live-distant child abuse in developing countries were indicated as a significant driver contributing to its widespread proliferation. In addition some evidence was found of the facilitated planning of transnational child victim sexual offending, referred to as 'high risk travels', including where details of abuse are arranged prior to travel[10]. On a contrary note, instances of non-commercial streaming of contact abuse among members of closed networks were also reported.

In the answers related to particular online environments, peer-to-peer (P2P) has been commonly mentioned as the main platform to access CSAM, invariably attractive for CSE offenders. Although some specialists describe the material which is being shared there as known and often dated, P2P is an important part of a possible offending pathway, from open searching using search engines, via exchanges on the open Internet to the hidden services in the Darknet[11]. The overall impression of respondents was that P2P cases still constitute the significant part of investigations conducted by specialised units.

Surprisingly, answers directly indicating criminal activities in the Deep Web[12] and the Darknet as an obvious trend were quite limited. Rather, general references were made, pointing out the general need of offenders to remain anonymous, their move to closed networks or use of new technologies offering more anonymity and encryption. This could be explained by the fact that the experience of LE agencies in conducting investigations in those environments differs significantly.

Many respondents made a reference to third party storage, indicating this shift in hosting trend as one of the obvious ones in online CSE in recent years. It presents an additional

---

10 *2014 iOCTA, P.56; https://www.europol.europa.eu*
11 *The Darknet –'A collection of networks and technologies used to share digital content. The Darknet is not a separate physical network but an application and protocol layer riding on existing networks. Examples of Darknets are peer-to-peer file sharing, CD and DVD copying and key or password sharing on email and newsgroups'. Definition provided by Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman in 'The Darknet and the Future of Content Distribution'; http://crypto.stanford.edu. For the purpose of this assessment the term Darknet will be used, and it should be understood as 'web communications and technologies most commonly associated with illegal or dissent activity, where connections and sharing are anonymous'*
12 *Deep Web – World Wide Web content that is not part of the Surface Web*

challenge for the successful combating of online distribution of CSAM, especially in the light of additional features which allow offenders to store CSAM remotely.

As evidenced by INHOPE, CSE offenders continue to misuse legitimate hosting possibilities to store and distribute CSAM. In 2014 image hosting sites were identified as hosting 42% of the reported URLs (an increase from 22% in 2013), followed by website hosting at 30% (37% in 2013) and file hosting sites 20% (29% in 2013)[13].

Special attention should be given to file hosting sites that are often referred to as cyberlockers[14]. The Internet Watch Foundation[15] reports that as new cyberlocker services come online, they continue to be highly vulnerable to being abused to store CSAM. This can be reinforced by evidence that there has been a marked increase in the use of cyberlockers to host CSAM, from 649 instances in 2012, to 1400 in 2013[16], and to 5582 in 2014[17].

Analysis conducted by G2 Web Services[18] on a specific set of 16-21 cyberlockers over 15 weeks identified that 25% of them contained CSAM, and that such material is most likely to be hosted on cyberlockers that offer some sort of premium upload/download service. Additionally, both so-called Pay-for-Premium Services[19], as well as Affiliate/Rewards programs[20] possess vulnerabilities, which can be misused by offenders interested in the distribution of CSAM for financial gain[21].

Among responses related to commercial CSE, some made reference to a general downward trend in the number of dedicated pay-per-view websites, and a shift from traditional credit card payments to the ones offering the most anonymity, namely alternative payment options including virtual currency. Although this seems to be a

---

13 *INHOPE 2014; http://www.inhope.org*
14 *'Cyberlocker' in this report should be understood as a third-party online service that provides file-storing and file-sharing services for various types of media files and data, including a service that requires a premium account to download either faster or simultaneously. Such services are also called 'one-click hosters'*
15 *Internet Watch Foundation (IWF) is the UK hotline belonging to INHOPE's network for reporting criminal online content (child sexual abuse content hosted anywhere in the world, criminally obscene adult content hosted in the UK, non-photographic child sexual abuse hosted in the UK); https://www.iwf.org.uk*
16 *IWF 2013 annual report, P.12; https://www.iwf.org.uk*
17 *IWF 2014 annual report, P.10; https://www.iwf.org.uk*
18 *G2 Web Services is a provider of payment risk management solutions in due diligence, compliance, and fraud protection*
19 *Premium Services offer their users additional features, such as increased download/upload speeds, simultaneous downloads, etc. Access to certain files could also be limited unless a user pays for a premium service*
20 *Affiliate/Rewards Programs allow users who upload content to earn a portion of the revenue their uploads generate*
21 *Contribution from G2 Web Services to the EFC report as explained further in the references 22 and 23*

globally recognised trend, additional context is required to support this observation, especially in light of the recent research conducted by EC3-Europol under the umbrella of the European Financial Coalition (EFC)[22]. An in-depth examination of the scale and extent of the most recent developments presented in the 'Strategic Assessment on Commercial Sexual Exploitation of Children Online'[23] provides a complete picture of commercial CSE and proves that it has not been eradicated but has evolved into new forms of criminal activity.

3.2 Online victim environment

3.2.1 Self-generated sexually explicit material

The future of SGSEM appeared to be highly unpredictable in the previous report. There was some inconsistency in responses about the distribution of such material by young people, and uncertainty in both the academic and law enforcement communities on how problematic behaviour of this nature should be identified and categorised. The aim of this part of the document, therefore, is to report any developments in this area, focusing on its interactions with other forms of online CSE.

The term 'sexting' is mistakenly used by the public and media as a synonym for 'self-generated sexually explicit material'.

In the last few years SGSEM has been closely associated with the phenomenon of 'sexting' in public and media attention, therefore it was crucial to determine if there is common understanding of both terms, and the reasons for this relationship.

The majority of respondents who answered the question of what they understand by 'sexting' indicated similar elements, and described it as the production and distribution of sexual text, images or video by young people. According to those respondents sexting is usually addressed to peers, and considered by its authors to be a 'harmless fun' element

22 http://www.europeanfinancialcoalition.eu
23 The Strategic Assessment of Commercial Sexual Exploitation of Children Online (also called 'The EFC report') was produced with invaluable contributions from the European law enforcement community and EFC members: INHOPE, IWF, CEOP, VISA, MasterCard, PayPal, Western Union, Web Shield, G2, GSMA, Google, Microsoft, ICMEC, Missing Children Europe, Eurojust, and CEPOL; https://www.europol.europa.eu

to gain the acceptance of a person they may or may not know, usually of the opposite sex, or 'normal behaviour' in a relationship between teenage peers.

Only one respondent generally stated that sexually explicit material is distributed 'from people to people', whereas the vast majority referred to children, teenagers, minors, underage persons or explicitly to children under the age of 18.

The fact that respondents indicated a peer as a recipient of self-produced sexually explicit material distributed in the process of sexting, adds a valid point to a broader discussion on the SGSEM phenomenon. Sexting needs to be considered as just one of the processes of producing SGSEM, therefore this term should not be used as its synonym. There are other circumstances where such material is produced, which differ remarkably from the ones associated with 'sexting'. What does significantly matter is the recipient of this material: a peer in case of sexting, and an offender in case of grooming and online solicitation, including sexual extortion. Also, persuasive influences or coercive measures apparent in the process of producing such content should be taken into consideration.

The recent IWF paper on online-produced sexual content[24] brings to the readers' attention the need to change their own definition of SGSEM. In their earlier study carried out in 2012, IWF described such content as "nude or semi-nude images of a young person knowingly engaging in erotic or sexual activity".

The need for change became apparent on analysis of the new data[25] when the following key findings of the study were formulated:

- 17.5% of content depicted children aged 15 years or younger, with 42.9% of these depicting children assessed as being 10 years and younger;
- 85.9% of content depicting children aged 15 or younger was created using a webcam;
- 93.1% of the content depicting children aged 15 or younger featured girls;
- 46.9% of content depicting children aged 15 years or younger was Category A or B[26] compared to 27.6% of content in the 16-20 years age range;

24 *IWF in partnership with Microsoft: Emerging Patterns and Trends Report#1, Online-Produced Sexual Content, 10 March 2015; https://www.iwf.org.uk*
25 *The findings of the study are based on a snapshot of the distribution of youth-produced sexual content featuring young people during a three month period from September – November 2014*

- 89.9% of the total images and videos assessed as part of the study had been harvested from the original upload location and were being redistributed on third party websites[27].

According to IWF both the scope of the 2012 study and the definition of SGSEM were inadequate in describing the observed trends. This was particularly the case in relation to the methods of creation of the content and the age of many of the individuals depicted.

The study highlights an increasing trend in the distribution of sexually explicit content produced by younger children using laptop webcams which, due to the nature of the technology used, they are aware is being shared with at least one other party.

Accordingly, to reflect recent findings a new definition of self-generated sexually explicit material is proposed by IWF in their report, introducing important elements such as the one that this content is produced by a young person of themselves, and that it is intentionally shared by any electronic means[28].

Findings of the study leave a lot of room for further exploration of this area, especially as some seem to question traditional understanding of the situation. For example, it is believed that SGSEM is created and distributed via mobile phones or other mobile devices, yet the IWF report that 85.9% of content depicting children aged 15 or younger is created using a webcam in a home environment, most commonly a bedroom or bathroom[29]. Further questions which should be raised refer to the notion of 'intentional sharing' used in the IWF's definition, and different motivations behind the production of sexually explicit content by young people.

The picture presented below summarises what is currently believed to be known about the origins of self-generated sexually explicit material and should be considered as a starting point for further discussion[30]. It builds on the assumption that SGSEM is not only produced by peers as a part of sexting but can also be produced and distributed as a part of grooming and online solicitation, including sexual extortion.

---

26 *Under the Guidelines laid down by the UK Sentencing Guideline Council. Category A: images involving penetrative sexual activity; images involving sexual activity with an animal or sadism. Category B: Image involving non-penetrative sexual activity*
27 *Emerging Patterns and Trends Report#1, Online-Produced Sexual Content, P.3 and 16; https://www.iwf.org.uk*
28 *Emerging Patterns and Trends Report#1, Online-Produced Sexual Content, P.3; https://www.iwf.org.uk*
29 *Emerging Patterns and Trends Report#1, Online-Produced Sexual Content, P.17; https://www.iwf.org.uk*
30 *Contribution from FP Twins team; K.Staciwa*

Equally, a widening understanding of the SGSEM phenomenon would have an impact on the victim identification process. A large number of cases in which an adult male poses as a young female to elicit the production of material were reported by respondents. Also, sexually explicit material originally produced for a peer as a part of sexting, which has found its way into circulation, may trigger further processes of grooming or online solicitation. All of the above requires even more careful consideration of whether the child depicted in material falling under the category of self-generated needs to be identified and located.

Difficulties in gathering multi-sided data focusing on the online availability of SGSEM is a reason why determining any change in this area remains an aspiration. Participants of the survey were therefore asked about the proportion of the child abuse material they

have seen in the last two years which appears to have been produced by the victims themselves.

Those respondents (n=17) who felt able to give a percentage estimate of the child abuse material which has been seen in the last two years identified that 5-25% of it was produced by the victim themselves, of which 25-50% was estimated to be produced specifically for the suspect under investigation. These findings are especially interesting as – following the graphic presented above – they suggest that in such cases production of SGSEM is related to the processes of grooming and online solicitation.

The previous report highlighted limited evidence that such material was starting to appear in CSAM collections and be circulated online. LE specialists were, for that reason, asked this time to explain how this material is finding its way into such collections.

The general understanding of the situation is that if sexually explicit photos or videos are placed on the open Internet there is the potential for it to be captured and distributed amongst CSE offenders. Few respondents mentioned hacking methods being used for this purpose. Many answers referred to a process of CSAM production for the person who misrepresented themselves or coercion by an offender, and emphasised the fact that SGSEM is now the commodity of 'newly produced never before seen' CSAM to be used as a currency in further trade. The overall impression is that investigators are seeing an increased amount of this type of material within CSAM collections, although the limited scope of the survey must be borne in mind.

An increase in the number of websites which had apparently been created specifically to display self-generated sexually explicit images and videos featuring young people had been seen by IWF for some time. However, in 2013 the IWF saw a commercial child sexual abuse website offering the sale of self-generated sexual images and videos of young people[31].

Varying responses were received regarding the trend foreseen in the development of the self-production and distribution of such material in the next 2-4 years. It was possible to group these responses in three scenarios.

The majority of respondents indicated that it will continue to increase and explained that this is because of the increased activity of children in online environments, facilitated by

31 *IWF contribution to the EFC report; https://www.europol.europa.eu*

ever-increasing access to more sophisticated mobile technology. Others stated that the trend may not change: children and young people have moved their social lives online and they will continue to construct their identities there. The third scenario foresees a downward trend and this is explained by educational undertakings combined with greater awareness of online identities.

It is important to mention that the Directive 2011/93/EU[32] introduced provisions on solicitation of children for sexual purposes (Article 6), including an attempt by means of information and communication technology to commit offences such as 'acquisition or possession of child pornography' or 'knowingly obtaining access'. However, prosecution of such offences very much depends on the age of sexual consent, which varies in the EU MS from 14 to 18. In particular cases this variation may be seen as leaving a gap for more SGSEM generated through online solicitation to go into worldwide circulation.

On a contrary note, in some jurisdictions it continues to be the case that the minor who generated the picture and distributed it is guilty of producing and disseminating CSAM[33].

3.2.2 Online solicitation for sexual purposes - victim's perspective[34]

Regarding the gender of the victims of online solicitation, respondents continue to identify either a female or both genders, targeted in relatively equal measure. This distribution is in line with previous reporting and suggests that law enforcement continue to see greater gender balance in terms of offence reporting over the last few years.

A slight difference was observed in terms of the ages of victims. The majority of respondents indicated the victim as being between the ages of 10 and 17. This suggests that they have observed solicitation of younger children (the age limit of 12 was reported in 2012) in the last two years.

In terms of patterns of Internet usage, social media and chat sites together with online game environments were indicated as 'meeting points' where a casual, seemingly harmless, chat may start. The chat may take place regularly each day or several times a

32 Directive of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA
33 Crofts, Thomas and Lee, Murray (2013), Sexting, children and child pornography, Sidney Law Review
34 Additional information regarding notion of online solicitation is provided in the section 2.3.2

week, often late at night, behind the closed doors of a bedroom. Such processes appear to have been facilitated by easy access to and unsupervised use of mobile devices.

Observations of LE experts are supported by some recent research studies performed at national level. In the case of the UK it has been found that four in ten 5 to 15 year olds own a mobile phone, with this figure rising to almost eight in ten children aged 12-15. Children in each age group are now more likely than in 2013 to use a mobile phone to go online (36% vs. 27% for 5-15s). This varies significantly according to age, with 59% of 12-15s going online using a mobile phone. This coincides with a big increase in smartphone ownership at 13, when ownership jumps from four in ten for 12 year olds (41%) to almost seven in ten for 13 year olds (67%). Among 12-15s the mobile phone is the second most likely device to be 'mostly' used to go online, after laptops/netbooks, with tablets coming third.

Answers on risk factors for victimisation confirmed a previously reported observation that it is difficult to indicate a single dominant factor. Some participants of the survey reflected on children's emotional vulnerability and propensity to take risks, as the two broad factors[35] that place them at greater risk.

According to those respondents, children with low self-esteem or those desiring emotional attention are at an increased risk of becoming victims of online sexual exploitation. In some cases, this vulnerability may be the result of loneliness or of difficult home lives and family relationships. Others may be seeking love online and believe that they are entering into real relationships.

In terms of risk takers, this would apply to confident or outgoing children who may seek adventure or risk. This group often believes that they are in control of a situation and may be encouraged to partake in low level sexual activity before being coerced and blackmailed, with the offender using the child's initial complicity as leverage.

Attention was also given to some other external risk factors, and among them respondents indicated a level of sexualisation in society surrounding children and young people everywhere, which in their opinion led to the fact that the boundaries for decency have changed and more sexualised behaviour is viewed as acceptable. In short, those

35 *Ofcom, Children and Parents: Media Use and Attitudes Report, P.5; http://stakeholders.ofcom.org.uk*

children are constantly exposed to mainstream sexualised content which reduces inhibitions.

In the opinion of respondents, shortcomings in both children's and parents' cyber education should also be considered a risk factor. Children and young people are lacking education as to the risks of online activity. Together with a lack of awareness of the potential dangers, such as not realising that the people they are communicating with may be misrepresenting themselves, online predators might easily target children. Adults who don't have a grasp of the technology their children are using, a lack of parental guidance, and inadequate supervision of online activities, were commonly mentioned. Asking children for some information about their online behaviour was at the same time considered as proof of paying attention and facilitating imperative conversation.

On the issue of online solicitation for sexual purposes, the majority of specialists interviewed agreed that greater levels of Internet adoption in previously under connected regions of the world resulted in the increased visibility of new victims from those areas. The most common explanation was that it is one of the factors enabling live web streaming of CSAM worldwide. Respondents supported this assumption by evidencing a slight increase in images of victims from the so-called developing countries.

3.2.3 Prevention/awareness-raising measures

Raising awareness seems to be a very important preventive measure for tackling online solicitation. Participants of the survey underlined that such initiatives should be in line with understanding of the children and young people's vulnerabilities to sexual exploitation and abuse, and should address specific characteristics of this crime type. This opinion has even greater value in the light of recent changes in online solicitation, such as a reduction in the time taken by offenders to build an online relationship, and an increase in the use of aggression and coercive tactics to ensure victim compliance, of which sexual extortion is the most relevant example.

Early implemented cyber education seems to be crucial to help children understand the online world. The role of parents or caretakers is an additional key factor in this process. Firstly as they are the ones who should be able to support young Internet users in their

education, and secondly as they are the ones who can monitor their children's use of mobile devices and the Internet, acknowledging that any restrictions in this area may bring an opposite desired effect.

With the new and younger Internet users such preventive measures should also be sustainable, expanding their reach when necessary, and redesigning their scope for new age groups. At the same time the view was expressed that awareness raising measures should be present in environments where children and young people are active and become victims of online solicitation.

Key factors identified by the respondents relating to desired changes in awareness raising measures included increased resourcing and greater accessibility to increase their effectiveness. In their opinion discussions on acknowledgement of best practices should be launched in the near future. Such discussions should additionally reflect the lack of consistency across not only the EU MS but also internationally.

Difficulties were expressed in answering the question about the success rate of such preventive measures. For some specialists just the fact of their existence was enough to consider them successful. Other answers referred to statistics of particular programmes, the number of children and young people to whom sessions were delivered, registered professionals or ambassadors of particular initiatives, as well as the numbers of visitors on dedicated websites.

3.3 Online offender behaviour

3.3.1 Access to and storage of child sexual abuse material

There should be no doubt that the evermore user-friendly Internet-related technologies appear to support the pursuit of online CSE. With such a variety of choices, offenders with a sexual interest in children use services they are comfortable with and feel secure with, depending on their needs. It is likely that some offenders will make use of more than one route of access simultaneously. This approach could explain differences in the ranking of answers to survey questions about the main ways of accessing non-commercial CSAM.

Some specialists noted that some users of hidden services were turning to P2P environments as a result of recent successful LE interventions on the Darknet. While it is impossible to confirm such observations by reliable quantitative data, it perfectly supports an assumption that current online distribution of CSAM is very dynamic, and the operations of LE agencies inevitably influence it.

In light of the above it would be very helpful to refer to comprehensive, *post factum* analysis of the situation when the popular CSAM host Freedom Hosting[36] was taken down.

An article in Dailydot[37] speculates that a full backup of Lolita City, the message board which hosted well over one million images and videos of underage children, was available as a torrent if the customer knew where to look for it. It also suggests that in an attempt to circumvent the need for hosting, some of the biggest 'child pornography' websites online were encouraging users to store image and video files on the Surface Web - normal websites accessible to everyone - such as Anonfiles.com. Also of note, a move towards contemporary anonymous networks such as I2P and Freenet was mentioned, as safer alternatives to Tor. The sources for this article cannot be verified but it sheds light on what is believed to have happened in the wake of Freedom Hosting becoming unavailable.

Although comparable crime data sets indicating an increase in the use of hidden services are very limited, it is possible to indicate the reasons why this increase seems to be happening.

Hidden services have definitely become more 'user friendly' in recent years, easier and quicker to use and therefore more accessible by non-IT-savvy customers. Using such services proves attractive by masking a user's network identity but also by providing access to additional services that can facilitate other criminal activity. Respondents note no apparent loss of confidence in this network while allowing that considerable periods of down time, cyber-attack or law enforcement interventions during 2013 and 2014 might have worsened the user experience. As a consequence of the latter, various forums contain discussion threads on I2P distribution and also how to host content on Freenet.

---

36 *http://www.bbc.com*
37 *http://www.dailydot.com*

Those respondents who felt able to make an assessment agreed in describing Tor as the most popular Darknet platform among CSE offenders. An estimation of the proportion of directly connecting users that are associated with child sexual exploitation still remains one of the challenges, although some attempts have been recently undertaken[38].

Recent investigative efforts of the law enforcement community afforded it the ability to review Tor hidden services dedicated to the advertisement and distribution of CSAM. A review of 40 Tor hidden services providing CSAM identified more than 300 000 possible users. This revealed present and past access to children, commission of sexual contact offences against children, as well as production of CSAM. One of the largest CSAM hidden services on the server accumulated a collection of more than 1.4 million CSAM images during its estimated two years of operation.

Apart from the fact that these numbers are very significant, they support the assumption that hidden services on Tor are evolving in ever more dangerous directions. Presumption of the greater level of anonymity to the publisher, viewer and server hosting material should be considered as one of the factors driving constant demand for newly produced material and satisfying the sexual urges of the offender which would not be revealed in a less anonymous environment.

Special attention should be given to restricted areas in hidden services. It is suspected that these areas hold a more sophisticated cohort of offenders who are involved in commissioning contact child sexual abuse. It has been observed that these restricted forums contain material which has not been circulated before, indicating that they are likely to have been produced and uploaded by members.

Changes in commercial CSE online have already been highlighted in the section on trends. The dynamic nature of this crime area dictates that emerging trends should always be taken into consideration whenever questions about the current scale of this phenomenon arise. It is therefore necessary to broaden the definition to include all forms of commercial distribution of CSAM, such as 'disguised websites', dissemination through cyberlockers, live streaming of child sexual abuse for payment as well as instances of commercial CSE in the Darknet[39].

---

38 *For user concern on this, see http://www.wired.com (study) as well as http://www.wired.com (tor traffic)*

39 *2015 iOCTA, P. 30; https://www.europol.europa.eu*

Regarding the situation on the Surface Web in the past three years, INHOPE member hotlines registered a downward trend in the number of reports that they classified as commercial, with 18% in 2012, 13% in 2013 and only 9% in 2014[40]. INHOPE reports however that the lack of consistent and generally accepted terminology is a global issue, therefore different interpretations of 'commerciality' are used by organisations dealing with CSAM.

Given the fact that the activities of INHOPE member hotlines span many jurisdictions, collection of information will also largely be affected by the legal or procedural ability of the hotline analyst to navigate through the page to determine the payment method. This depends on the national law, on the mission statement of a hotline, as well as the collaboration agreement between the hotline and national law enforcement agency (LEA)[41].

Some important findings were also revealed by IWF under the Website Brands Project (WBP)[42]. The IWF's analysis suggests that the same websites would often appear on multiple URLs over a period of time. Therefore the number of URLs actioned for containing commercial CSAM is not necessarily an accurate reflection of the number of commercial websites which may actually be in operation. Additionally, there were numerous links between the different sites which suggested that groups of brands may be operated by single overarching entities (top-level domains). A general observation of the IWF is also that the vast majority of dedicated websites distributing CSAM are operated by a small core group of criminal entities.

Since 2011, IWF have observed an increased use of 'disguised websites'[43] to distribute CSAM. This technique represents a challenge to successful content removal as hotlines are not able to proceed with the notice and takedown without knowledge of the referring URL. INHOPE reports that this challenge can become even greater with referrers sometimes expiring after a certain period of time. When dealing with multiple time zones as the INHOPE network does, it may be that even if the referrer is reported to another

40 *INHOPE 2014; http://www.inhope.org*
41 *Contribution from INHOPE*
42 *The Website Brands Project (WBP) was initiated by IWF in 2009 in order to attempt to quantify the true volume of commercial websites in operation, and by extension the number of Top Level Domains which may be responsible for the creation and operation of the websites*
43 *These websites present different content depending on the route the user takes to reach them. When the URL is loaded directly into the browser, the page which loads contains legitimate adult content. However, when accessed via a particular gateway site (referrer), the page displays child sexual abuse content. For user concern on this, see also research paper https://www.iwf.org.uk*

hotline or to law enforcement for investigation, it may have expired and a new referrer URL is necessary to display the content. IWF continues to see this technique being used to distribute CSAM and also provide direct access to the most prolific commercial CSE websites which have been identified as part of the WBP[44].

Developments such as profit driven blackmailing of young people to disseminate sexually explicit photos or videos depicting themselves, as well as the commercial distribution of images and videos obtained as SGSEM, should also be taken into consideration to make the current picture of commercial CSE complete. In addition, there are new instances of commercial distribution in the Darknet that may challenge the so far known characteristic of users of the Darknet as like-minded offenders, interested in posting and viewing CSAM both securely and for free.

As has been concluded by the International Centre for Missing and Exploited Children (ICMEC)[45] "there is apparent migration of commercial child sexual exploitation, along with other criminal enterprises, from the traditional payments system to a new, largely unregulated digital economy made up of hosting services, anonymising Internet tools, and pseudonymous payment systems"[46].

The evolution of commercial distribution which has been observed for some time, seems to challenge the traditional distinction between commercial and non-commercial distribution, which branded the former as largely profit driven, and conducted by those with limited sexual interest in children. It is now understood that this is because both individuals with a limited sexual interest in children as well as those having such interest, who produce and distribute CSAM, are becoming more entrepreneurial and are exploiting technological developments to satisfy their commercial needs.

---

44 *IWF Annual Report 2014, P. 17; https://www.iwf.org.uk*
For user concern on this, see also https://www.iwf.org.uk
45 *The International Centre for Missing & Exploited Children (ICMEC) is a private, nongovernmental, non-profit organisation. It is the leading agency working internationally to combat child abduction and sexual abuse and exploitation*
46 *ICMEC, The Digital Economy: Potential, Perils, and Promises, P.11; http://www.icmec.org*

3.3.2 Grooming and online solicitation of children

Although the majority of respondents confirmed the provision in their national criminal legislation for offences equivalent to grooming or online solicitation in the previous report, it is important to mention some recent developments in this area.

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) of 2007[47] introduced Article 23, describing the solicitation of children for sexual purposes, also known as 'grooming'. In the process of monitoring the effective implementation of its provisions several Committee[48] members voiced some difficulties.

A major issue which was raised referred to the fact that the text of Article 23 of the Lanzarote Convention seems to be limited to the situation of an adult intending to materially meet with the child, whereas the definition outlined in the Explanatory Report to the Lanzarote Convention seems to be wider and covers the issues surrounding the exposure of a child to online sexually explicit material. Therefore the Committee launched the process of drafting an opinion on Article 23, which was finalised in June 2015. The document aims at encouraging the Parties to the Convention to extend the interpretation of its scope so as to also cover cases when the sexual abuse does not result in a real life meeting but remains online.

In the EU, grooming legislation is introduced in the provisions of Directive 2011/93/EU, which was expected to be transposed into national law by December 2013. At the moment of writing this report a Project Survey on the transposition of the Directive, jointly commissioned by Missing Children Europe (MCE), ECPAT International and the NGO Alliance on Child Safety Online (eNACSO) is about to be published. Following an analysis of the 27 national reports covering the EU MS bound by the Directive, the findings have revealed that they interpret the Directive's provisions on grooming in various ways[49].

---

47 *To date, it has been signed by all 47 Council of Europe member states and ratified by 38 (Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Finland, France, Georgia, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Lichtenstein, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovenia, Spain, Sweden, Switzerland, former Yugoslav Republic of Macedonia, Turkey, Ukraine)*

48 *The Convention provides for the establishment of a Committee of the Parties to monitor its implementation. The Committee of the Parties shall be composed of representatives of the Parties to the Convention*

49 *Contribution from Missing Children Europe and eNACSO*

When looking at the implementing options regarding Article 6 it can be concluded that some MS have opted for the introduction of a *sui generis* (specific) criminal offence. Others preferred to incriminate online grooming as a preparatory act or an attempt at already existing criminal offences, such as sexual harassment and indecent assault.

Some MS require a material meeting to take place in order for the online grooming offence (Article 6 (1)) to be committed. This seems to be a restrictive interpretation of the provision on online grooming since the initial idea lying behind introducing this offence was to prevent the actual abuse taking place. Usually if a meeting between the child and the potential perpetrator already took place, it is likely that more serious offences such as contact sexual abuse had already been committed.

Such interpretation may seem to be insufficient in the light of trends in online CSE and the fact that sexual abuse can occur without a real-life meeting, i.e. when a child is groomed online to provide child abuse material depicting that child. In such cases, there is no need for material acts leading to a meeting to take place, as the sexual abuse itself is undertaken online.

Analysis of reports also identified the lack of criminalisation of grooming when a proposal is made by the child (as a consequence of intense solicitation of the child) as a legal gap not covered under Article 6 (1) of the Directive. Furthermore, the failure to penalise the mere sexual chatting (sexting) with a child (for the purpose of sexual exploitation of the child) in the majority of the MS was noted as well.

Another challenge seems to be the incrimination of online grooming for the purpose of both 'engaging in sexual activities' with the child being groomed and 'the production of child pornography'. A number of MS only link the grooming offence to the former, or do not clearly cover both aspects. However, some MS opted for the implementation of more favourable provisions whereby the mere making of sexual proposals to children under the age of sexual consent suffices in order for online grooming to be committed. This means that the intention of the perpetrator does not have to cover engaging in sexual activities nor the production of CSAM. It is important however to again highlight the great disparities among national legislations in the ages of consent in relation to sexual activities.

The implementation of Article 6 (2) in national legislations differs from one Member State to another as this particular provision is interpreted in different ways. This can be explained by the fact that this provision is a result of a compromise reached in the discussion between the Council and the Parliament and leaves room for various interpretations. This confusion originates from the fact that, on the one hand Article 6 (2) refers to the online grooming of a child in order to obtain pornographic material depicting that child while, on the other hand it refers to the online 'attempt' to commit the offences such as acquisition or possession of child pornography and knowingly obtaining online access to child pornography.

Regarding the environments in which children and young people are subject to online solicitation, no significant changes were observed. The statement that environments popular among young users of the Internet are preferred by those with a sexual interest in them is still valid, therefore the attention of LE should follow the latest trends in this area both in national and international markets.

Whereas environments facilitating online solicitation may change in line with their popularity, the methodology seems to be consistent, and usually builds on well-known factors of romantic or friendly relationships. Pretending to be teenagers, befriending, conversations relating to supporting and encouraging the child, understanding the child where they perceive their parents do not, are typical examples.

Some respondents pointed out that with male homosexual communications, the move to sexual mode is almost instant in many cases, and the sexual content of the chats is more intense from the beginning and throughout. On the contrary, with female victims, the grooming process is more targeted, gradual and measured, including instances of the offer of gifts for sexual activity. One specialist observed that males tend to be enticed and females tend to be sexually extorted.

Case study: In July 2013 a 17 year old boy died when he threw himself from a bridge near Edinburgh. He had been targeted online by an offender who posed as a teenage girl and with whom he shared sexually explicit images of himself. The victim was then blackmailed by the offender demanding money. If he failed to pay he would post the victim's naked images on social networking sites.

The use of coercive techniques, including aggression and blackmail to ensure victim compliance, has been a feature of online solicitation for some time. The majority of

respondents agreed on the increasing use of them, including more extreme, violent, sadistic or degrading demands by offenders. Both tactics are cornerstones of the sexual extortion phenomenon which, according to LE experience, has been evolving and including new forms of criminal activity.

Sexual extortion usually involves the process whereby young people are coerced into continuing to produce sexually explicit material by the threat of exposure. While in-depth analysis of the background of sexual extortion goes beyond the scope of this research, it is worth mentioning that in some instances such processes may be triggered by SGSEM which is in circulation on social media. The novelty of 'home-made' material again seems to be a crucial factor.

In some severe cases, it appears that an element of power over the victim is what progresses the abuse, with some children or young people being told to perform distressing acts. In some instances the abuse spirals so out of control that victims have attempted to self-harm or commit suicide as the only way of escaping the abuse.

It is worth highlighting that the scope of criminal activity is defined by the offender's language skills. An offender speaking widely known languages is able to reach more potential victims, whereas the one speaking a language which is not widespread will not extend his operating field beyond the national level[50].

Sexual extortion as a modus operandi may also attract individuals looking for an easy way to obtain financial gain. This can take the form of either blackmailing of victims by demanding money for not distributing the sexually explicit material depicting them, or even commercial distribution of material obtained through online solicitation. Such a trend shapes a somewhat different understanding of the scope of this phenomenon than the one known so far, and points to the need for a new term such as 'commercial sexual extortion'.

Some interesting differences have been observed between cases of non-commercial sexual extortion and the ones where online coercion was driven by financial gain. While the first kind of such criminal performance will be more likely a one-man activity, the latter one can be considered as a potentially lucrative business opportunity, in which large-scale sexual extortion schemes would be applicable.

50 *Contribution from FP Twins team*

A good example of large-scale commercial sexual extortion is a combination of web cam scamming with blackmail which usually takes place on dating sites, in chat rooms, or on social networks. Once a contact is established it is moved towards web cam contact where the contacts are secretly filmed engaging in sexual practices. The victims are then blackmailed and forced to make money transfers to the perpetrator to prevent the videos from being distributed. The scale of these purely profit driven sexual extortion networks is tremendous. No attention is given to victims, who are only a means to collect more money in this semi-automated process. Operating on an almost industrial scale from call centre-style offices, such cyber-blackmail agents are provided with training and offered bonus incentives such as holidays, cash or mobile phones for reaching their financial targets[51].

One recent international operation coordinated by Interpol led to the identification of between 190 and 195 individuals working for organised crime groups operating from the Philippines and resulted in the arrest of 58 individuals. Close cooperation of the international LE community led to the identification of sexual extortion victims in Indonesia, the Philippines, Singapore, the United Kingdom and the United States. Potential victims were also traced to Australia, South Korea and Malaysia in addition to the hundreds of individuals in Hong Kong and Singapore already reported as victims (http://www.interpol.int).

There is some evidence pointing to a ring of African states, in addition to the south-east Asia based networks, targeting victims throughout Europe.

Research paper 'Sextortion in the Far East'[52] published recently revealed the move of commercial sexual extortion modus operandi to mobile device environments. Gangs that operate in east Asia (South Korea and Japan) have been employing an improved modus operandi with the potential to do more damage as the cybercriminals can directly contact the victim's family and friends. The victim is asked to download and install an Android application that is actually a data stealer that collects and sends the victim's entire saved contact information to the cybercriminal. Finally, the cybercriminal blackmails the victim to pay

51 http://www.interpol.int
52 http://www.trendmicro.com

an amount or the former will reveal the recorded video to everyone on the victim's contact list[53].

It is important to underline that commercial sexual extortion schemes seem to be applicable in the case of adults although children (below 18 years of age) may also be among the victims. According to some respondents this process is more likely in the case of young males who exchange self-generated sexually explicit material with a female or person pretending to be a female as a part of sexualised online chat.

3.3.3 Offender networking and forensic awareness

LE specialists were able to indicate different forms of offender networking in their responses and linked particular services to each of them. According to them the means of networking varies, depending on individual preferences and needs at each stage of offending.

The majority of respondents agreed that, apart from normalising or legitimising the sexual interest, online networks currently contribute to the facilitation of offending. This is achieved through a far greater level of advice than has been seen before in terms of technical solutions or security, access to children or online locations where CSAM can be found.

Peers inside those closed communities instruct each other, not only on 'How to practice child love'[54], but also provide detailed technical instructions to advise like-minded individuals on how to protect anonymity and sanitise CSAM to evade detection by law enforcement. The less experienced ones posting new material may become subject to criticism by community members for not undertaking security measures. Some solutions go beyond advice and form more stable, well-organised structures serving the broader anonymous Internet community. The currently vacated Hidden Wiki portal could be an adequate example of such organisational solutions, providing both introductory instructions to Tor and search engines for Tor hidden services. However, there are examples of even more tailor made ones, specifically for those with a sexual interest in children and teenagers.

---

53 *http://www.trendmicro.com*
54 *Document circulated in the Darknet*

Forensic awareness of CSE offenders can still vary considerably, from the skills of the uninitiated viewer to very advanced, professional ICT and information security experts who interact with the environments used for CSAM distribution. On the basis of responses provided it was possible to indicate three loosely defined categories of CSE offender, associated as a consequence of their forensic literacy with either public or private P2P networks or hidden services in the Darknet.

Regardless of environmental differences, there is enough evidence to suggest that overall forensic skills are on the rise. This can be attributed to the greater level of advice spread across the platforms where CSE offenders are active, as well as their broader awareness of improved detection and forensic investigation methods. In addition, some respondents explained such a situation by making a reference to the general trend of younger age demographics in online criminality.

Analysis of responses regarding forensic awareness of CSE offenders indicates a model of an offender posing the greatest challenge to law enforcement when attempting to identify users and decrypt computer systems and devices during investigations. Such an offender is one who combines anonymity networks with dual or multiple layers of encryption to enhance security and privacy and uses alternative payment systems in the commercial distribution of CSAM.

4. Future developments

This section focuses on some future oriented developments in the area of CSE and draws on open source scanning and responses of both LE specialists as well as representatives of VGT partners. As it cannot hope to be exhaustive it aims at highlighting some of these aspects from the perspective of technology, human behaviour, legislation and procedures as well as organisational initiatives. Concerns expressed by the LE community are presented separately.

4.1 Technology

The use of cloud services is predicted to increase in the short term as connection speeds increase. As indicated by the European Union Agency for Network and Information Security (ENISA)[55], the adoption of cloud computing solutions continues to grow, although it has been put under massive pressure due to the Snowden revelations, in particular regarding data protection issues of stored information. It is not surprising then that security solutions including anonymity in the cloud and the uptake of encryption practices are still the subject of discussions. Emergence of multi-cloud strategies should also be noted[56].

More anonymity and encryption in online behaviour are undoubtedly among the most important future challenges in establishing the traditional link between online content and user. In particular, users will soon not require very sophisticated knowledge but just easily used and widely available hardware.

Decision makers and LE specialists all over the world should focus their attention on the latest discussions regarding default encryption. Such technological developments could pose a threat to lawful access to evidence and, together with anonymity tools like Tor, have already been described in public discussions as potentially leading to the creation of a 'zone of lawlessness'[57].

'End-to-end' encryption makes it more difficult for private information to be hacked but may also prevent it from being legitimately handed over to law enforcement agencies. The companies themselves will not be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mails, and recordings stored on the devices[58]. The growing use of 'end-to-end' encryption may also mean that the Internet industry will soon struggle to identify CSAM held on its servers.

The protection of privacy and free speech offered by strong encryption and anonymity technologies continue to be promoted by civil society organisations and independent

55 *ENISA threat landscape 2014, P.65-66; https://www.enisa.europa.eu*
56 *Ibid, P.66-67*
57 *http://motherboard.vice.com*
58 *https://www.fbi.gov*

experts. Those bodies urge states to revise any laws or regulations that can restrict the use of such technologies[59].

Recognition of hidden services is expected to grow within the next few years and attract more users due to improvements in their functionality and easier means of accessing them. It is expected that developments which establish links between the Surface Web and hidden services make the latter even more popular.

Following the implementation of 4G it is envisaged that Tor users will also be in favour of accessing the network through mobile devices in the future. This will serve as an extra level of anonymity to mobile Internet connections.

In opposition to technical developments which could potentially strengthen CSE-related criminal activity online, attention should be given to several projects related to scanning the Deep Web. They are currently being undertaken by representatives in different sectors, along with developing online tools to detect and identify sex traffickers that target a key vulnerability, which is the need to advertise[60]. More discussions of this kind can be expected in the near future.

4.2 Human behaviour

Technological expansion, growing Internet coverage, and the widespread availability of mobile devices, are all factors constantly transforming our society into a digital one. Without doubt, no-one had prepared society and its children to cope with these challenges, therefore any trends in society reflecting this change, which may serve as crime facilitating factors, should never be neglected.

Young people who nowadays have become members of a digital society by default experiment with relationships, intimacy and identity online. Sharing sexualised content online seems to be a part of this adolescent development and of the sexual exploration processes but its consequences can be unpredictable. Material originally produced for private consumption end up in unwanted circulation and happen to attract the attention of people with a sexual interest in children, or profit oriented individuals who may use

59 https://cdt.org; http://www.ohchr.org
60 For user concern on this see http://www.ibtimes.com, http://www.cmu.edu as well as http://www.wired.com

them as part of grooming or extortion processes. The currently observed trends are worrying and allow speculation that this risky sexually-precocious behaviour will increase in the near future.

Open sources bring to public attention a problem of the hyper-sexualisation of young girls, representatives of the age 'tween'[61]. As reported by them "over the past two decades, the rise of the Internet and social media initiated a dramatic shift in popular culture: almost everything that could be sexualised has been sexualised, producing a new generation of girls racing toward womanhood before even finishing puberty"[62].

More sexualised behaviour has also been reflected in the language of young Internet users. Research shows that a majority of teens believe that their parents are starting to keep tabs on their online and social media lives. With that, acronyms can be used by them to hide certain parts of their conversations from attentive parents. Abbreviated words used for this purpose could potentially raise some red flags for aware parents, due to their sexualised context[63].

Some examples of risky behaviour following the worrying phenomenon of objectification of children and redefinition of morals refer to adults who create social network profiles such as 'The most sexy 4, 5, 6 year olds', not taking into account that photos of people's offspring from their own profiles can be used for less than innocent purposes. Such opportunism on the part of those operating those profiles emphatically proves that there is a great need to educate not only children but also their parents, and suggests an even greater challenge for nuanced approaches in awareness campaigns.

The general trend of Internet users being younger may have future implications for both offenders and victims of CSE, bringing younger victims of online grooming and solicitation to light and creating more tech savvy offenders, reaching straight for the most up-to-date and covert networks and extreme content. The latter trend should be considered as even more alarming as it is likely to increase the risk to children due to their potentially higher exposure to networks of sophisticated offenders and the normalisation effect this creates.

---

61 *The term 'tween' references a vaguely defined life stage (somewhere between childhood and adolescence); http://www.newsweek.com*
62 *Ibid*
64 *http://edition.cnn.com*

After successful LE actions more care is given to avoid unwanted attention, therefore even greater efforts in exploring technological solutions offering anonymity and encryption should be expected, together with more careful behaviour and additional precautionary measures. A greater level of anonymity enabling more open discussions may also stimulate some particular areas of CSE offending in the near future. A combination of technology, such as hidden services and alternative payment methods, has already been influencing communities of CSE offenders in the Darknet.

Some changes in the response to the phenomenon of CSE by representatives of society are also worth highlighting in this section. This has additional value, especially in light of recent actions aimed at assisting in combating the threat posed by CSE offenders to children, such as 'Sweetie', undertaken by the NGO Terre des Hommes to address the problem of live web streaming[64]. Such initiatives require early engagement by LE as in particular cases they may jeopardise ongoing covert law enforcement operations and intelligence gathering.

Crucially, in light of daily life examples of the objectification of children and increasing acceptance towards sexualisation of their behaviour, any undertakings which may bring changes in the perception and proper recognition of the CSE phenomenon by society should be carefully noted. One of them is the initiative of ECPAT International to set up an Interagency Working Group composed of key international organisations – both intergovernmental and nongovernmental to address the terminology and semantics relative to the sexual exploitation of children. The overall objective of this collaboration is to overcome confusion and common misconceptions, and to foster a consensus among key stakeholders on terminology to be used in programming, legislation, policy, and advocacy regarding the sexual exploitation of children. This project is also expected to influence the use of the term 'child pornography' which, as explained in the previous VGT report, may be assisting offenders in distancing themselves from the abusive and criminal nature of their involvement in online CSE.

64 *http://terredeshommesnl.org*

4.3 Law enforcement concerns

Law enforcement's capacity remains unsurprisingly the greatest concern for the future. The majority of respondents mentioned this problem when answering the question about the one thing they would change to improve law enforcement's fight against online CSE.

Increasing amounts of identified online CSE cases and the complexity of cases pose constant challenges for the prioritisation of tasks. As new forms of online offending come to light, expectations of the already limited resources grow significantly, causing additional pressure.

Consequently, a lack of proper resources leads to the situation where certain areas of CSE, which require conducting more technical or sophisticated investigations, may be out of reach. The unavoidable outcome of such shortcomings is an inaccurate risk assessment of the scope and risk posed by this crime area.

The demand for modifications to investigative techniques, including the use of covert/undercover techniques with the aim of infiltrating networks, was already mentioned in the previous report, together with the lack of applicable legislation in some jurisdictions.

4.4 Legislation/procedures

This section aims to highlight some vital discussions relating to legislation and procedures which may influence the public-private response to the child sexual exploitation phenomenon in the near future.

In that regard impact of the judgement of the European Court of Justice against the Data Retention Directive (DRD) made in April 2014 - which mandates that telecoms operators must retain all their customers' communications data for up to two years[65] - should be highlighted. The court declared the Directive invalid, taking the view that it interferes in

65 *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54)*

a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data[66].

The decision of whether or not to introduce national data retention laws is therefore a national decision. As it was expressed by the European Commission in the absence of EU rules, Member States are free to maintain their current data retention systems or set up new ones, providing that they comply with basic principles under EU law[67].

At the moment of writing this report, the transposing of the DRD has been struck down in at least 11 Member States. Without any doubt the fragmented regulation in place - or even a lack of a legal data retention framework, as is the case in several States - influence the effectiveness of LE and judicial authorities. It is worth noting though that there are also examples of moves by several European countries to expand electronic surveillance capabilities and create new legal bases for conducting bulk data collection and interpretation. Such an approach is part of an ongoing discussion on the European level about the balance between limits that are necessary to guarantee national security and sacrificing human rights at the same time.

The European Parliament took part in this discussion and in October 2015 voted on a resolution[68], following up on the one adopted in April 2014, calling for EU Member States as well as the US, to bring surveillance laws and practices in line with human rights standards[69]. Similar discussions are also taking place outside the EU[70].

Recent discussions at EU level also concern another area of high importance in CSE investigations, especially the ones focused on transnational sex offenders. In July 2015 the European Parliament's Civil Liberties, Justice and Home Affairs Committee approved the first EU Passenger Name Record (PNR) bill, two years after that same committee rejected an earlier draft of the data-sharing law for flight passenger information[71].

Under the amended rules, PNR data could be processed "only for the purposes of prevention, detection, investigation and prosecution of terrorist offences and certain types of serious transnational crime". The list approved by MEPs includes, for example,

---

66 *Court of Justice of the European Union, Press Release No 54/14 Luxembourg, 8/04/2014; http://curia.europa.eu*
67 *European Commission statement on national data retention laws, 16 September 2015; http://europa.eu*
68 *http://www.europarl.europa.eu*
69 *http://www.europarl.europa.eu*
70 *http://www.zdnet.com*
71 *http://www.euractiv.com; http://www.europarl.europa.eu*

trafficking in human beings, sexual exploitation of children, drug trafficking, trafficking in weapons, munitions and explosives, money laundering and cybercrime. At the moment of writing this report the bill is being negotiated further in so-called trialogue talks between the Parliament, the European Commission and the Council.

The near future will determine to what extent the LE agencies will be able to rely on both communication data and passenger movement-related intelligence which make up a vital part of criminal investigations in the CSE area.

In terms of cooperative mechanisms, some recent developments in the joint initiative by the EU and 55 countries around the world coming together in the Global Alliance against Child Sexual Abuse Online[72], should be reported.

A first report summarising the commitments that participating countries have undertaken in order to reach the four political targets was produced in December 2013[73]. The proposed actions placed a strong emphasis on cooperation, capacity building and training, as well as making sure that the right tools are available to both law enforcement and the private sector.

In September 2014 global decision-makers met in Washington for the second Ministerial Conference of the Global Alliance to assess the progress in the first two years and how to expand the fight against the global proliferation of child sexual abuse online in the future. In the Ministers' Declaration[74] summarising the outcome of the conference, they agreed to pursue the following actions in full respect of due process and fundamental rights requirements:

- Enabling law enforcement among Global Alliance countries to gain timely access to electronic information and evidence held by Internet service providers (ISPs) and other repositories of electronic information that is material to the investigation and prosecution of child sexual abuse offences through central

72 The Alliance was launched on 5 December 2012 and unites Ministers of the Interior and of Justice behind four shared policy targets: enhancing efforts to identify victims whose sexual abuse is depicted in child pornography, and ensuring that they receive the necessary assistance, support and protection; enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders; increasing public awareness of the risks; and reducing the availability of child pornography online and the re-victimisation of children
73 http://ec.europa.eu
74 http://ec.europa.eu

authorities and other legally authorised channels, so that no nation becomes a safe haven for such information;

- Facilitating prompt and comprehensive exchange among law enforcement of information and evidence pertinent to child sexual abuse offences featuring transborder offence conduct, victims, co-conspirators, or evidence repositories;
- Enabling Internet service providers and other repositories of electronic information to provide information pertinent to the identification, apprehension, and ultimate prosecution of online child sexual abuse offenders to law enforcement pursuant to legal process in a manner and time frame consistent with reasonable investigative and prosecutorial demands;
- Augmenting existing, collaborative and transborder efforts to identify and rescue victims of online child sexual abuse.

The next reporting round is foreseen for 2016. The reports will describe the state of implementation of the measures announced, assess progress made to reach the goals of the Global Alliance and to pursue the shared policy targets, and indicate specific actions that each participant will be undertaking as a follow-up.

Development of national and international responses to the threat of online CSE is also expected as an outcome of the UK's WePROTECT initiative[75], designed to build and improve upon existing undertakings across governments, law enforcement, industry and NGOs. At the first summit in London in December 2014 some 50 countries and international organisations committed to strengthening their efforts to tackle online CSE worldwide[76]. A further summit, which took place in November 2015 in the UAE, was expected to put concrete plans in place to deliver on those commitments.

In public-private discussion on combating CSE, the Joint Motion for a Resolution on Child Sexual Abuse Online[77], which was set by the European Parliament in March 2015, should also be perceived. Although resolutions are not binding and only suggest a political desire in a given area, it is worth noting that its content is in line with strategies already supported by the LE environment.

75 https://www.gov.uk
76 https://www.gov.uk
77 http://www.europarl.europa.eu

The motion highlighted that the fight against child abuse on the Internet should be integrated into a wider strategy addressing the overall phenomenon of child sexual abuse and exploitation, and that it requires a comprehensive approach covering the investigation of criminal offences, the successful prosecution of offenders, the effective protection of child victims and an increase in prevention activities.

Addressing the new challenges in combating CSE, including the existence of anonymous communities, the increased use of encryption, as well as the latest trends such as live web streaming of abuse for payment or sexual extortion, the motion stresses the need for a coordinated approach. This will ensure consistency in policymaking and the resulting action, encompassing the fight against crime together with fundamental rights, privacy, data protection, cyber security, consumer protection and e-commerce.

The document requests that Member States' law enforcement authorities and Europol are provided with the necessary funds, human resources, investigative powers and technical capabilities to effectively pursue, investigate and prosecute offenders. These developments should include appropriate training to build capacity in both law enforcement and the judiciary.

Furthermore, the European Parliament calls for an effective partnership in combating the commercial CSE online, especially with representatives of alternative payment systems, in order to identify opportunities for better cooperation with law enforcement authorities.

5. Concluding remarks and opportunities

- CSE in its current form is a worldwide, dynamic phenomenon. Changes in one of its areas affect the others. A coordinated approach for major operations, together with global initiatives in specialised training, should always be taken into consideration in terms of LE interventions.
- There is a need to continue looking at online CSE from the international perspective. This does not mean abandoning the prioritisation of cases according to local conditions. Rather, it requires constant reflection of the global context in national approaches.

- Careful monitoring of any developments in CSE-related trends, especially emerging technologies and software, additional forms of online and virtual currencies, new methods by which CSE offenders meet and act online, should be undertaken as a shared responsibility of all the stakeholders.

- Discussions on applying the horizontal model in tackling online CSE is vital. This model is based on the four 'P's *(Pursue – Prevent – Protect – Prepare)* and should be applied to each identified trend, followed by working rules involving all relevant stakeholders.

- Experience sharing, and close cooperation with the private sector and academia, seem to be mandatory in determining a successful response to this type of crime. Closer engagement with global services, which due to its nature can give rise to more internationally complex cases, should be considered as vital.

- The involvement of LE representatives in crucial discussions on such topics as data retention, encryption, third party hosting and collecting of Passenger Name Record data is essential for successfully tackling CSE-related forms of offending.

6. Acronyms and abbreviations

CSAM - child abuse material

CSE - child sexual exploitation

EC3 - European Cybercrime Centre

ECPAT - End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes

EFC - European Financial Coalition

eNACSO - NGO Alliance on Child Safety Online

ENISA - European Union Agency for Network and Information Security

EU - European Union

FP - Focal Point

I2P – Invisible Internet Project

ICMEC - International Centre for Missing and Exploited Children

ICT - information & communications technology

INHOPE - International Association of Internet Hotlines

IOCTA - Internet Organised Crime Threat Assessment

IP - Internet protocol

ISP - Internet service provider

IT – information technology

IWF – Internet Watch Foundation

KINSA - Kids Internet Safety Alliance

LDCA – live-distant child abuse

LE – law enforcement

LEA – law enforcement agency

MCE – Missing Children Europe

MEP - Member of the European Parliament

MS – Member States

NGO - non-governmental organisation

P2P – peer-to-peer

PNR – Passenger Name Record

SGSEM - self-generated sexually explicit material

TLD - top-level domain

Tor – The Onion Router

URL - uniform resource locator

VGT - Virtual Global Taskforce