EUROPEAN FINANCIAL COALITION

against Commercial Sexual Exploitation of Children Online

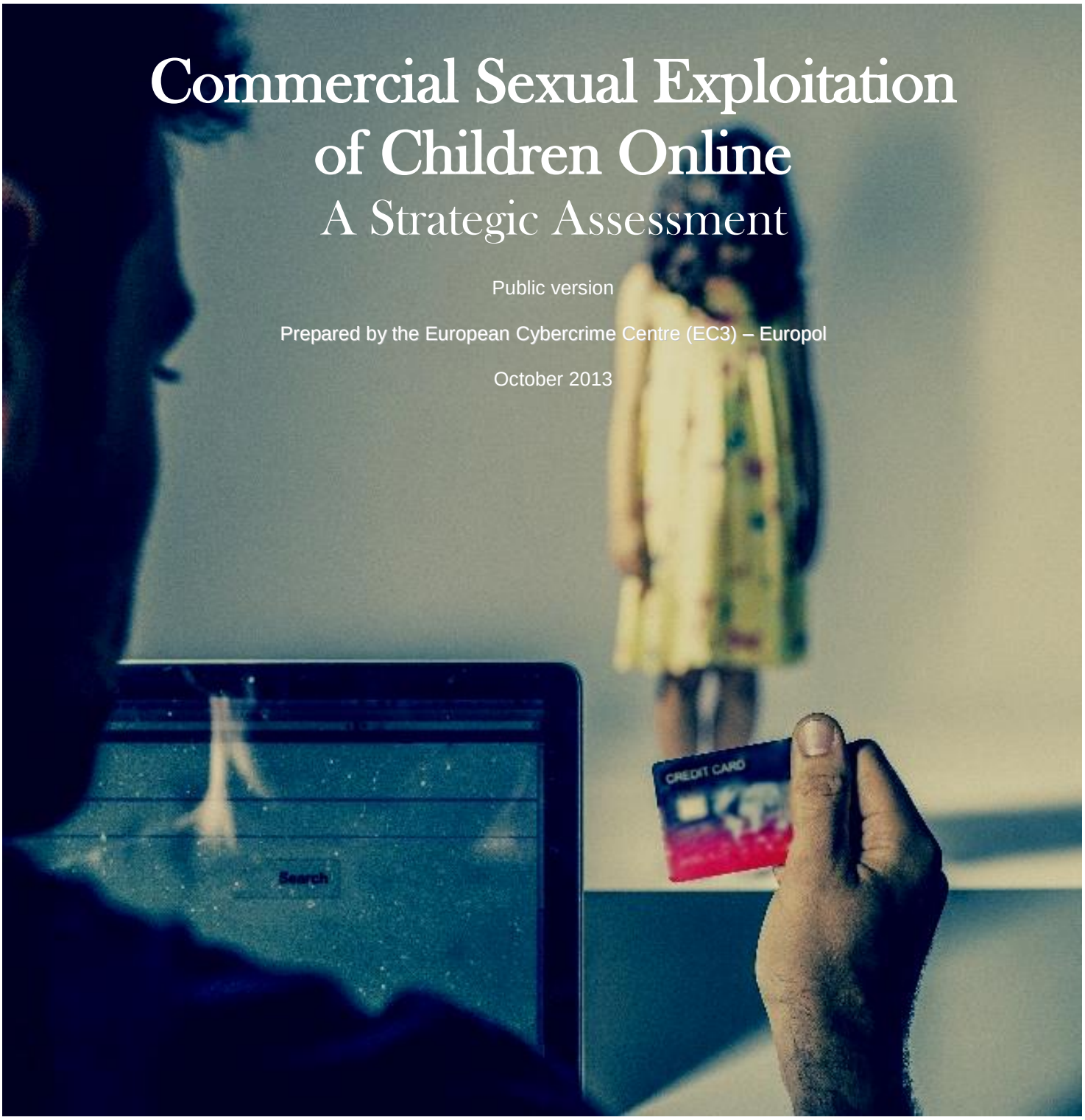
Commercial Sexual Exploitation of Children Online

A Strategic Assessment

Public version

Prepared by the European Cybercrime Centre (EC3) – Europol

October 2013



This project has been funded with the support of the European Commission. This publication reflects the views only of the author. The European Commission cannot be held responsible for any use which may be made of the information contained therein.

Colophon
Text: European Cybercrime Centre (EC3) – Europol
Print: Coyote Print
Photography: Natalie Hill Photography
Responsible editor: European Financial Coalition against Commercial Sexual Exploitation of Children Online

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

Contents

1. Introduction & Executive Summary 5

1.1 Introduction 5

1.2 Executive Summary 5

2. Trends in CAM Distribution 6

2.1 Scale and Extent of Commercial Distribution 7

2.2 Commercial Web Streaming 8

2.3 Context – Non-commercial distribution 9

2.4 "Sexting" and "Sexploitation": self-generated indecent material 10

2.5 Legislative Issues 11

3. Web Distribution and Hosting - Analysis of Commercial URL data 11

4. Analysis of Commercial CAM Brands – IWF Research 13

5. Payment Methods 15

5.1 Credit Card Payments 15

5.2 Alternative Payment Systems 15

6. Emerging Issues & Future Considerations 15

6.1 Internet Adoption and Mobile Payment Systems 15

6.2 Cyberlockers 16

6.3 Legislative Developments 17

7. Concluding Remarks & Recommendations 17

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

1. Introduction & Executive Summary

1.1 Introduction

The European Financial Coalition against Commercial Sexual Exploitation of Children Online ("EFC") brings together key actors from law enforcement, the private sector and civil society in Europe with the common goal of fighting against commercial sexual exploitation of children online. Members of the EFC join forces to take action on the payment and ICT systems used to run these illegal operations.

Within the framework of a 36-month project funded by the European Commission, the EFC focuses on five working groups ("Work Packages" or "WP"). Each Work Package is responsible for one of the five strategic objectives of the EFC. The WPs are composed by both public and private partners and meet regularly in order to implement their respective deliverables in accordance with the overall timetable of the three year project. Relevant participants are identified over time, depending on the needs of a Work Package. The five working groups will contribute to the establishment of a permanent platform and resource centre for law enforcement authorities, payment system providers and ISPs engaged in counteracting the online distribution of child abuse material.

The EFC is chaired by Europol (European Cybercrime Centre – EC3), and led by a Steering Committee composed of representatives of Europol-EC3, Missing Children Europe, INHOPE, EUROJUST, Visa Europe, MasterCard, PayPal, Microsoft, Google, CEPOL and the International Centre for Missing and Exploited Children ("ICMEC"). Its secretariat is hosted at and managed by Missing Children Europe[1].

1.2 Executive Summary

The aim of this assessment is to identify current trends in production, distribution and access to commercial child abusive material (CAM), based on the insight and expertise of EFC members, as well as observations of EU Member States law enforcement representatives. Examining offending both in terms of child exploitations and as a criminal business, it seeks to highlight opportunities for intervention, and specific gaps in the information available. It is anticipated that the findings will be used to inform further intelligence gathering, crime prevention and enforcement activities by the EFC and its member organisations.

Based on the information available to the EFC Work Package in charge of this report in June 2013, key findings are as follows:

- The vast majority of CAM is still distributed non-commercially on the open net, using

[1] More information on the EFC, its structure and objectives is available on the EFC website: www.europeanfinancialcoalition.eu

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

peer-to-peer (P2P) technologies. Commercial distribution persists, however, and is evolving, including new forms of activity on the hidden net.

- The live streaming of abuse for payment is an emerging trend of particular concern, deserving of greater enforcement attention, systematic intelligence gathering, and effective collaboration of prevention measures.
- As an increasing number of young people use Internet based services to produce sexualised content, there is a real risk that this material will find its way into commercial circulation.
- Analysis of web search terms reveals a reduction in interest in traditionally popular "series" of images, persistence in the popularity of generic keywords for child abusive material, and increased interest in "borderline" and "barely legal" material. While more sophisticated offenders use closed online networks to access CAM, web search continues to provide an "entry level" means of access.
- Web search analysis also reveals increasing interest in CAM in emerging markets such as Latin America. As Internet adoption continues to proliferate worldwide, the EFC can expect to see new material, new payment methods and greater levels of interest from previously underconnected regions.
- According to data provided by INHOPE, the top countries with the highest number of servers hosting commercially distributed CAM include the United States, the Russian Federation, Kazakhstan, Japan, The Netherlands, Ukraine, Germany, Czech Republic and Hungary. For some of these – but not all – high levels of identified commercial CAM URLs may to some extent reflect the misuse of globally popular legitimate hosting services.
- Analysis by the Internet Watch Foundation reveals that just 8 Top Level Distributors were responsible for 513 commercial CAM distribution brands in 2012, and that the 10 most prolific brands recorded in 2012 were all associated with a single Top Level Distributor.[2] This seems to indicate that while there are large numbers of URLs being used for the commercial distribution of CAM, this may be due to a small number of extremely prolific Top Level Distributors.

2. Trends in CAM Distribution

Analysts engaged in the assessment of global criminal phenomena such as online child sexual exploitation (CSE) invariably face methodological challenges regarding data collection. In the first instance, data on online sexual offences against children is not always collected at national

[2] IWF Briefing Paper – Website Brands Project, March 2013

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

level: this is particularly the case where countries lack national police intelligence and recorded crime databases. Secondly, without exception data is recorded and collected at national level according to the relevant articles of national penal codes. By this token, even where national legislations are approximate, variations in the precise previsions will mean that data collected according to these specifications will never be truly comparable to those of other countries.

While internationally comparable crime data remains an aspiration, this assessment consciously takes a more qualitative approach to identifying trends in online commercial CSE. Accordingly, the assessment of current trends is based on the observations of online child sexual exploitation investigators themselves. Between June and September 2012, interviews were conducted with 10 members of the European Union's COSPOL Internet Related Child abusive material Project (CIRCAMP).[3]

Respondents were asked to base their answers on their professional experience in the last four years, and in particular to consider what has changed in that period, and possible future developments.

2.1 Scale and Extent of Commercial Distribution

Perhaps unsurprisingly, the majority of EU law enforcement specialists have estimated that a very small amount of CAM is now paid for. Those respondents who felt able to give a percentage estimate (n=7) identified an average of 10.1% of CAM as commercial. The median value of 7.5% is perhaps more representative in this case due to the presence of an outlier value of 40% in one response. This is identical to the estimate supplied to the Virtual Global Taskforce in 2008[4]. The wide availability of free material, especially via P2P technology, is felt to be the dominant reason for such a low percentage. The higher percentage of 18% cited in INHOPE's statistics for 2012 may be explained by the fact that this data refers only to websites, and therefore does not include P2P platforms[5].

Some respondents observed that new, and therefore more coveted for offenders material is most likely to be exchanged in non-commercial environments, and that paying by credit card to download from websites – once the most popular method for accessing CAM – is now seen largely as an option for the inexperienced, not least because payment for material by credit card is often accompanied by compromise of the owner's details by organised crime groups. These views correlate with the EFC's 2010 analysis, which found a significant reduction in the number of active commercial sites identified, and that images on these sites were generally

[3] The Netherlands, Ireland, France, The United Kingdom, Denmark, Belgium, Germany, Sweden, Finland and Spain

[4] Baines, V. (2008), *Online Child Sexual Abuse: The Law Enforcement Response – a contribution of ECPAT International to the World Congress III against the Sexual Exploitation of Children and Adolescents*, p.34 - http://www.ecpat.net/worldcongressIII/PDF/Publications/ICT_Law/Thematic_Paper_ICTLAW_ENG.pdf

[5] INHOPE (2012) *Annual Report 2012*, p.18 – www.inhope.org/...reports/INHOPE_Annual_Report_2012.sflb.ashx

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

"historic and recycled"[6].

In addition, law enforcement has observed that an ever increasing demand has made new material to be a currency in itself. The value is in the novelty of the image, as a result of which images and videos have become bargaining chips. From an investigative perspective, new material means ongoing abuse and unidentified victims, and for this reason amongst others detection of non-commercial distribution has received greater priority in recent years.

But commercial distribution has evidently not been completely eradicated, and there are indications that it is evolving in response to technological developments and to meet the demand for new material. While some specialists have seen no new cases of commercial CAM distribution for some time, successful international law enforcement cooperation and information exchange can mean that a single investigation in one country can identify numerous subscribers in another. It would also appear that some so far non-commercial distributors are becoming more entrepreneurial, charging fees for privileged access to previously unseen material in environments like Tor. Moreover, there is some evidence of interaction with destinations for travelling sex offending, with offenders in South East Asia web streaming abuse to order for payment.

2.2 Commercial Web Streaming

A number of case studies relate to individuals in the EU directing child sexual abuse via live web streaming. In one recent case a perpetrator in an EU Member State, ordered child sexual abuse online in a South-Eastern Asian country, using chat services and webcam to instruct women on the particular type of abuse he wanted to watch. He paid 25-30 USD for each 30 minute session of abuse of young girl victims. He also paid an annual sum of 5500 USD for camera shots, using credit cards transfers for payment. It was later discovered that most of the women in the village where the abuse took place were involved in the crimes; sometimes they abused children who were not their own.

Of particular note is the fact that investigations in some EU Member States have resulted in the successful prosecution of EU citizens for hands on sexual offences conducted through live web streaming, and landmark rulings that the direction of CSE via the Internet is tantamount to rape of a child.

The demand for new material appears to be reflected in the prices seen by respondents. While

[6] EFC (2010) *Fourteen months on: A Combined report from the European Financial Coalition* – http://www.ceop.police.uk/documents/efc%20strat%20asses2010_080910b%20final.pdf ; cf. Wolak, Finkelhor & Mitchell (2011) 22, who found that CAM offenders using P2P possessed more extreme images (e.g., younger victims, sexual violence) and larger numbers of images than those who did not use P2P (Wolak, J. Finkelhor, D. & Mitchell, K. (2011) "Child Pornography Possessors: Trends in Offender and Case Characteristics", *Sexual Abuse: A Journal of Research and Treatment* 23.1: 22-42).

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

individual video clips can cost as little as 10 USD each, and subscriptions as little as 50 USD for 3 months, one video file of new material on demand can cost as much as 1200 USD. While payments by named and prepaid credit card are still detected, money transfer services and virtual payment systems are misused as soon as they reach the general market. It is therefore reasonable to assume that future developments in payment methods will be exploited by those engaged in commercial CAM distribution.

2.3 Context – Non-commercial distribution

EU non-commercial distribution methods largely reflect those described in the *VGT Environmental Scan 2012*[7]. Public P2P networks such as Gnutella, eDonkey and eMule are where the greatest volume of offending is identified, attributed more to the ease of detection due to the open nature of these services than to the extent of their misuse. Public P2P may also be used by more sophisticated offenders on occasion, for instance to rebuild a collection quickly after accidental loss or seizure.

Private P2P networks continue to be the platform of choice for mid-level offenders. The ability to establish closed groups of like-minded individuals for encrypted P2P transfer appeals to those with a desire for both convenience and security. Effective law enforcement activity, however, may be prompting a move to other services.

Distribution continues in closed groups on social media. Contrary to expectations that they would be entirely superseded by more recent social services, bulletin boards (BBS), newsgroups and IRC remain in use. It is thought that some offenders may see greater security in continuing to use a trusted platform and view newer untested services with suspicion. BBS, social media and closed forums serve as meeting points which facilitate a move to one-to-one communication and distribution, and to advertise links to content stored on bulletproof hosting sites or in encrypted online storage facilities, for which passwords and encryption keys will be shared directly. There also appears to be some evidence of distribution on public photo sharing sites.

There has been a marked increase in recent years in the use of hidden services like Tor and Freenet. Tor in particular is associated with the more sophisticated offender, in as much as its network of virtual tunnels is designed specifically to anonymise Internet use. A higher proportion of new, home-made material has been observed on Tor, the rationale being that the newer material, the higher the risk and the greater security required. In recent years Tor has become easier and quicker to use, and this is believed to be one reason for its increased misuse by CAM distributors. At the same time, it is believed that a wider availability of security

[7] VGT (2013) *Environmental Scan 2012* - http://www.virtualglobaltaskforce.com/wp-content/uploads/2013/05/VGT-Environmental-Scan.pdf

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

advice on online forums for those with a sexual interest in children has made even lower level offenders better informed on how to protect themselves, encouraging them to seek more secure means.

While the vast majority of CAM distribution in the aforementioned environments is non-commercial, evidence of distributors on Tor charging fees for access to new material points to the emergence of new models of commercial distribution which reflect the intrinsic value of material that is highly coveted for offenders in so far as it is previously unseen or even made to order.

This model challenges the traditional distinction between commercial and non-commercial distribution, which cast the former as largely profit driven and conducted by those with limited sexual interest in children. Rather, there is evidence to suggest that individuals with a sexual interest in children who produce and distribute CAM are becoming more entrepreneurial. Should this trend increase, it is not impossible that other forms of CAM will be commercialised, including images and video obtained through online solicitation, and self-generated indecent material.

2.4 "Sexting" and "Sexploitation": self-generated indecent material

Children and young people conduct their social lives and construct their identities online. The current trend for sexualised behaviour on randomised video chat platforms is a natural extension of their need to be seen and their sexual exploration. But this activity is now being exploited by individuals with a sexual interest in children, employing "sextortion" techniques in particular to ensure continued compliance. "Sextortion" is the popular term for the process by which young people are coerced into continuing to produce indecent material by the threat of exposure, and is one of the cornerstones of this evolved solicitation strategy.

Coercion and blackmail have been features of the online solicitation of children for some time. While some offenders continue to pose as children in order to make contact with young people, respondents have noted an increase in recent years in the use of aggression and coercive tactics to ensure victim compliance. This appears to have been accompanied by a reduction in the time taken by offenders to build an online relationship. From an offender perspective, such immediacy is more efficient, enabling them to solicit multiple victims simultaneously, and resulting in cases involving hundreds of young victims in total.

Such methods are used to commit online offences, for instance coercing children and young people to engage in sexual activity on webcam, web stream or VoIP. While the amount of such material found in offender collections is currently limited, one respondent noted that the "home made" quality of much of the material generated through online solicitation may mean that it

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

will have increasing appeal for networks of CAM distributors and downloaders. For the future, a retail market for such material cannot be ruled out. In particular, it has been suggested that young men engaged in the domestic trafficking of young girls for sexual exploitation (known in some countries as "lover boys") may see the production and commercial distribution of CAM generated online as a potentially lucrative business opportunity.

2.5 Legislative Issues

Live web streaming poses a particular challenge to traditional law enforcement investigative methods: access to streamed content does not constitute an offence of possession or making if the offender does not store a copy of the material. While the *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention) of 2007 introduced the offence of "knowingly obtaining access, through information and communication technologies, to child pornography [*sic*]"[8], and equivalent offences exist in a number of national jurisdictions, prosecutions are very rare. Awareness raising activity targeting prosecutors and judges has been identified as essential to achieving convictions and adequate sentencing for such offences. In this context, the aforementioned prosecutions of EU citizens for the direction of live streamed child sexual abuse serve as examples of good practice to be replicated throughout the European Union.

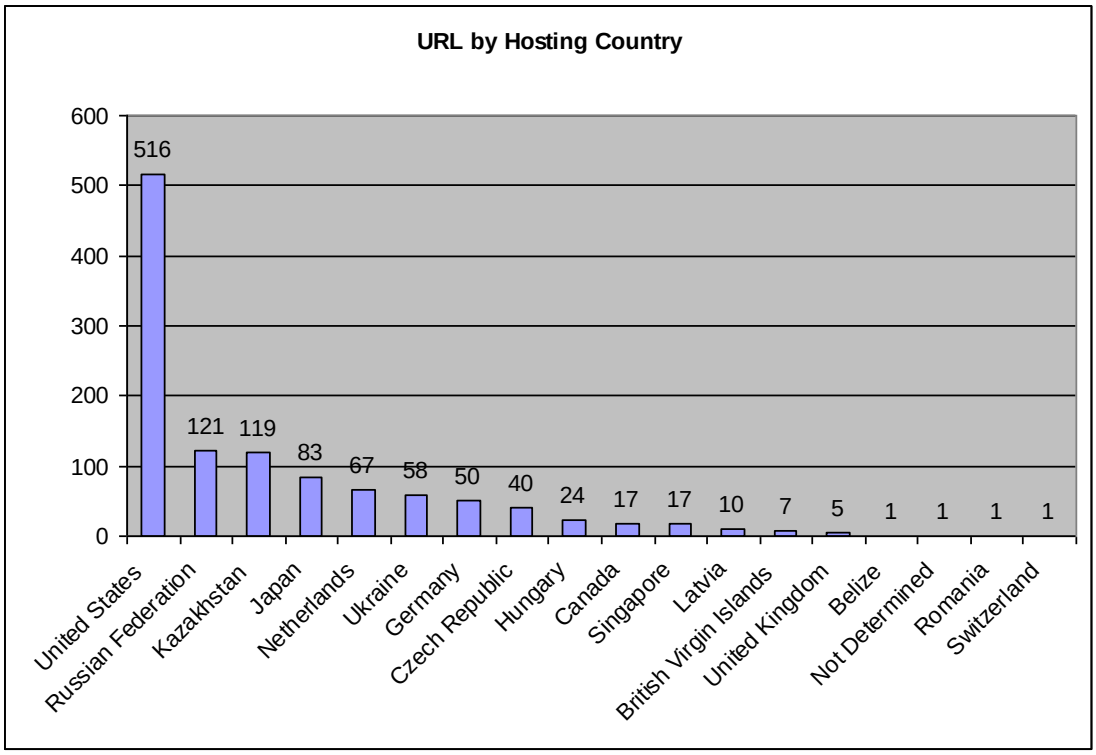
In addition, INHOPE reports inconsistency within the EU on the extent to which Internet hotlines can access – and therefore properly assess – CAM. In some Member States, the strict provision that law enforcement alone can access CAM without fear of prosecution arguably hampers the effectiveness of law enforcement agencies by adding to their administrative burden. In such cases, hotlines are unable to determine the veracity, seriousness or urgency of a report before referring it to the police. In contrast, in countries where assessment of CAM by the designated national hotline is permitted by law, the hotline can provide a comprehensive intelligence package which not only saves law enforcement time by providing more accurate information, but also helps them prioritise.

3. Web Distribution and Hosting - Analysis of Commercial URL data

A total of 1138 URLs suspected of the commercial distribution of CAM were registered by INHOPE in the last quarter of 2012 and referred to Europol for further analysis. It is important to emphasise that the countries mentioned below are merely those in which the host servers are located.

[8] CETS No. 201, Article 20.1

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs



This distribution is broadly similar to INHOPE's statistics for 2012 as a whole[9].

At the same time, it is evident that a number of domains have used multiple hosting services. Those occurring most frequently include:

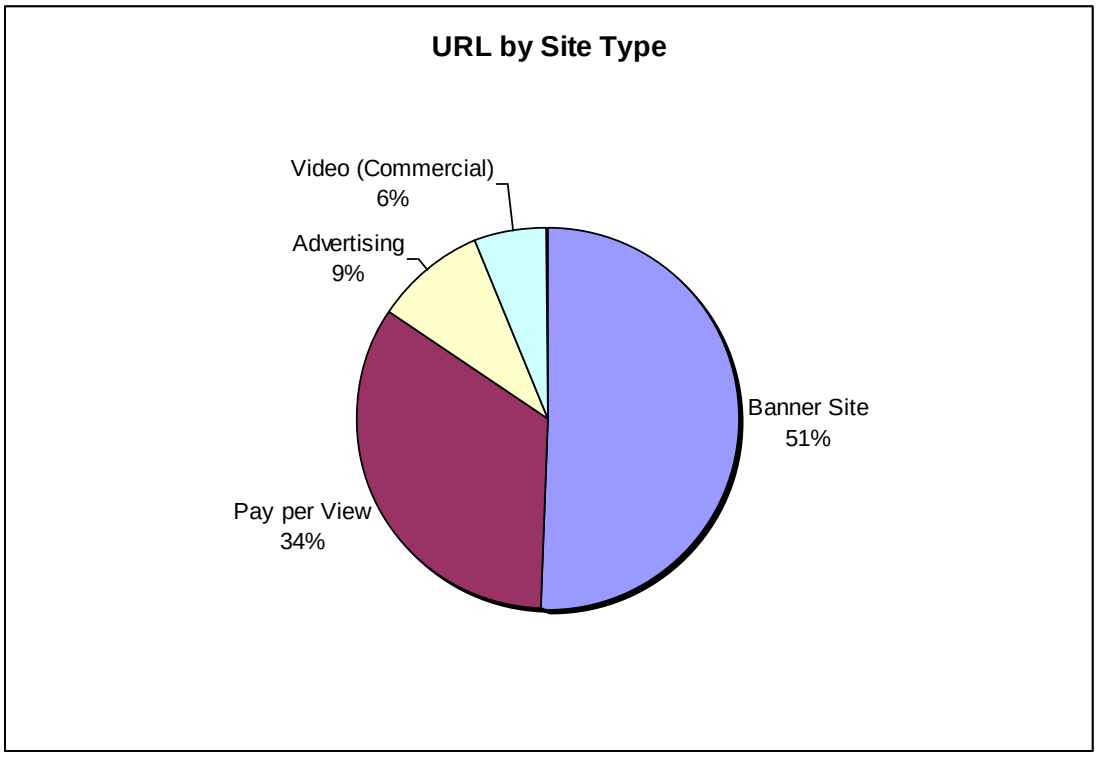
- **cu.cc** and **cz.cc**, officially operating under the Top Level Domain of the Cocos Islands, an Australian territory. cu.cc and cz.cc are domain name registration services which permit the registration of up to 100 domain names for free, or up to 1000 domain names for a premium. A Whois lookup tool on the site enables open searching and (in theory) identification of those who have registered specific domains.

  uni.me, officially operating under the Top Level Domain of Montenegro. uni.me is a successor to cu.cc which provides unlimited free domains.

- Other hosting services such as **bufsiz.jp** were also prominent in the data. According to the below presented chart, "banner sites" or free hosting services account for just over half of all URLs reported as suspected of the commercial distribution of CAM:

[9] INHOPE (2013) *Annual Report 2012: Making a Real Difference* – http://cdn.pressdoc-static.com/33629/documents/19230-1369212176-INHOPE_Annual_Report_2012.pdf

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs



The biggest number of the banner sites were hosted in the US – 42,5%, the Russian Federation – 12,5% and Kazakhstan – 12,2%.

In addition, just over a third of commercial URLs were identified as "pay per view". 52% of pay per view URLs were hosted in the US, 11% in Kazakhstan, and 9,8% in the Russian Federation.

4. Analysis of Commercial CAM Brands – IWF Research[10]

In 2012, the IWF Hotline processed 39,211 reports of which 9,550 website URLs were actioned for containing child sexual abuse material. Of these 9,550 URLs, 2,587 (27%) appeared on commercial websites.

IWF Analysts had observed that the same websites would often appear on multiple URLs over a period of time. Therefore the number of URLs actioned for containing commercial child sexual abuse material was not necessarily an accurate reflection of the number of commercial websites which may actually be in operation.

Additionally, when recording additional information regarding these commercial websites it became apparent that there were numerous links between the different sites which suggested

[10] Analysis taken from IWF Briefing Paper – Website Brands Project, March 2013

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

that groups of brands may be operated by single overarching entities.

The most significant indicator of a potential connection between sites is the use by multiple websites of the same payment mechanism. In cases where a common payment mechanism exists, websites are considered part of the same Top Level Distributor group. It is important to clarify that this does not mean use of the same payment *type* – i.e. digital wallet operators, credit card, SMS, paid call – but rather that the sites all point to identical merchant accounts with the same provider, use the same email addresses for contact/payment, or utilise the same web payment form on the same URL, for example.

During the life of its research project on brands (June 2009 to December 2012), IWF has identified 1,292 individual unique website templates being used for the commercial distribution of CAM. Analysis and categorisation with reference to the Key Identifiers indicates that since 2009 there have been a total of 13 Top Level Distributors in operation.

513 individual brands were active during the course of 2012. During the course of the year, 268 new brands were created. This trend is broadly consistent with that observed in 2011 in that approximately 50% of the templates were either previously unseen or had been sufficiently altered to qualify as “new” brands. Analysis and categorisation of these 513 brands indicates that 8 Top Level Distributors were active during 2012.

Since June 2009 only one new Top Level Distributor has been identified. This Top Level Distributor was active during the period January – May 2012; however, only two further reported incidences of the payment site associated with this Top Level Distributor were recorded in the latter part of 2012 and there have been no recorded instances of this group of sites so far in 2013.

The 10 most prolific brands recorded in 2012 were all associated with a single Top Level Distributor, accounting for 15.26% of commercial sites actioned by IWF during this period. 3 Top Level Distributors accounted for the top 30 most prolific brands actioned by IWF in 2012 and of that top 30, a total of 16 were associated with the same Top Level Distributor which also occupies the top 10 positions.

This seems to indicate that while there are large numbers of URLs being used for the commercial distribution of child sexual abuse material, this may be due to a small number of extremely prolific Top Level Distributors. It is not possible to state whether what has been identified represents a small number of payment proxies providing “routes to market” for this distribution and/or whether payments are then being redistributed.

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

5. Payment Methods

5.1 Credit Card Payments

While law enforcement specialists in the EU currently have limited contact with commercial distribution, some have been able to identify alternative payment systems as the most prominent payment methods for CAM. The vast majority agreed on a continued downturn in payment for CAM by credit card.

Proactive approaches by payment processors, including the engagement of third parties to conduct monitoring and test purchasing exercises – appear to have been effective in reducing the number of sites able to take payments.

5.2 Alternative Payment Systems

With regard to the emerging trend for live streaming of child sexual abuse for payment, alternative payment system providers have been cited as used payment methods. As highlighted by the Financial Coalition Against Child Pornography (FCACP) in 2011, the non-bank status of many emerging alternative payment systems enables them to bypass compliance rules on knowledge of payer and payee identities[11].

The continued evolution of alternative payment systems has resulted in the emergence of distributed digital currencies like BitCoin. While at the time of writing there is insufficient information to identify BitCoin as a prominent payment method for CAM in the EU, concern has been expressed in the wider international environment that the relative anonymity afforded by the service will prove attractive to CAM distributors and purchasers[12].

Digital currencies are already the dominant method of payment on Silk Road, a Tor forum which has become notorious for the retail of illicit drugs. The distribution of CAM is currently banned on Silk Road, but this does not preclude other entrepreneurial criminals replicating its business model specifically for CAM – complete with most popular digital currencies.

6. Emerging Issues & Future Considerations

6.1 Internet Adoption and Mobile Payment Systems

At the time of writing just over one third of the world is connected to the Internet. A high level of Internet adoption in the European Union (73%) is in stark contrast to those of Africa and Asia,

[11] FCPAP (2011) *Report on Trends in Online Crime & Their Potential Implications in the Fight Against Commercial Child Pornography*, p.2 – available from ICMEC on request

[12] See for instance, Washington Post 17 June 2013, "Can Bitcoin make peace with Washington?" - http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/17/can-bitcoin-make-peace-with-washington/

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

where Internet adoption currently stands at 15.6% and 27.5% respectively[13]. Considerable growth is anticipated in these regions in the next few years: by analogy with the experiences of regions such as Latin America and the Middle East who have seen massive increases in Internet adoption in recent years, this growth is likely to bring new victims, new offenders and new criminal methods to light[14].

Methods of CAM distribution will continue to develop in line with technological adoption. Increased bandwidth is already cited as a reason for much larger amounts of video material seized in recent years, the analysis of which puts considerable pressure on the resources and psychological well-being of law enforcement units. Further bandwidth increases around the world are naturally expected to result in even larger numbers of investigations involving even larger amounts of video, but also in the amount of web streamed abuse to order.

With regard specifically to commercial CAM distribution, it is of note that some of the most rapidly connecting areas of the world are also hubs for innovation in mobile payment systems, often leapfrogging levels of adoption in more developed regions. These factors may combine to create opportunities for CAM distribution that is entirely facilitated by mobile connectivity – from image and video capture to storage and payment. Moreover it is anticipated that domestic variants of mobile payment systems will become increasingly popular in the EU. As a result, those charged with combating commercial CAM distribution will be required to focus greater attention on these payment methods.

6.2 Cyberlockers

CAM distributors have been making use of online personal file storage for some years. Often known as “cyberlockers”, personal file storage services range from those hosted by multi-service providers to dedicated storage providers. Available information indicates that the majority of CAM distributed by this means is done so non-commercially. In light of rapid developments in payment technologies, however, it is not impossible that access to CAM in cyberlockers will increasingly be given in return for a fee. Further information gathering and direct liaison with online storage providers is now required to determine whether this is the case.

Those cyberlocker services that charge a fee for premium membership profit indirectly from the storage and distribution of child abusive material – knowingly or otherwise. And since many online storage services use mainstream processors for payments, there is inevitably some concern among processors about levels of CAM distribution in these environments.

---

13 Internet World Stats (June 2012 figures), accessed 21/06/13 – http://www.internetworldstats.com/stats.htm
14 VGT (2013) *Environmental Scan 2012* p.21 - http://www.virtualglobaltaskforce.com/wp-content/uploads/2013/05/VGT-Environmental-Scan.pdf

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

6.3 Legislative Developments

The 2011 EU Directive on Combating the Sexual Abuse and Sexual Exploitation of children and Child Pornography obliges Member States to provide for criminal penalties in their national legislation in the form of "effective, proportionate and dissuasive" penalties for the online solicitation of children for sexual purposes[15]. Also of note, the Directive requires that rules on jurisdiction be amended "to ensure that sexual abusers or sexual exploiters of children from the Union face prosecution even if they commit their crimes outside the Union, in particular via so-called sex tourism"[16].

Member States have until December 2013 to transpose the Directive. A review conducted in June 2012 by a coalition of NGOs active in the field of child right protection found that at that stage a number of Member States still reported shortcomings in these areas in their national legislations[17].

In states that are yet to criminalise online solicitation or extend their territorial jurisdictions, it is anticipated that this transposition will result in increased workload for law enforcement units – especially where public reporting mechanisms are introduced – and may demand new skills from investigators. Additionally, the global nature of online CSE means that an increased investigative focus on online solicitation and extra-territorial prosecution in one country is likely to result in an increase in the number of referrals to law enforcement partners in others. By this token, the transposition of the Directive will not only bring more offences to light, but may also have an impact on investigative capacity worldwide.

7. Concluding Remarks & Recommendations

A general recommendation is that the findings of this report should inform the activities of the other EFC Work Packages, and of the European Commission's EU/US Global Alliance against Child Sexual Abuse Online. More specific recommendations are as follows:

Distribution Methods

- Investigation into live web streaming for payment to be prioritised by law enforcement, in so far as this form of CAM distribution is directly responsible for new instances of hands on child sexual abuse.

[15] Directive 2011/92/EU of the European Parliament and of the Council, Article 6, Recital 12 &19
[16] Ibid. Article 17 & Recital 29
[17] Missing Children Europe, eNACSO, NSPCC & Save the Children (2012) *Survey & Workshop reviewing the Transposition of Directive 2011/93/EU in 11 Member States*, available on request.

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs

- Engagement with the most popular video chat and VoIP providers – including mobile applications – to determine the extent to which they are able to proactively identify and mitigate live streaming of child sexual abuse.
- Engagement with legitimate "Cyberlocker" providers, to establish the extent to which CAM is distributed commercially in these environments, and company procedures for identifying and mitigating material.
- Further exploration of commercial distribution models in hidden services.

Web Hosting

- Engagement with top non-EU hosting countries via the European Commission's EU/US Global Alliance against Child Sexual Abuse Online.
- Engagement with domain name registrars and similar US legitimate services, either through EFC members or the Global Alliance, to determine the extent to which they have built the removal of CAM into their standard operating procedures.
- Direct engagement with hosting services based in the EU with the aim of improving the hygiene of their services.

Payment Methods

- Data gathering from alternative payment systems providers as a priority, to determine the extent and nature of payment for CAM via virtual payment and money transfer services.
- Further analysis (with Work Package 3, if appropriate) to determine the extent to which financial service providers operating in the EU comply with the EFC's good practice on the prevention and detection of CAM.
- Information gathering on the misuse of mobile payment systems in the commercial distribution of CAM; direct engagement with leading EU and non-EU providers, with a view to anticipating changes in the methods of commercial CAM distributors and purchasers.

Legislative Issues

- EFC via Work Package 4 to promote good practice amongst the judiciary on prosecutions for live web streaming and knowing access to CAM.
- In accordance with Article 17 of Directive 2011/92/EU, EFC to promote legislative change and good practice in legislative interpretation in those EU Member States that do not currently allow Internet hotlines to assess CAM.

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate-General Home Affairs