EUROPEAN FINANCIAL COALITION

against Commercial Sexual Exploitation of Children Online

14 months on: A combined report from the European Financial Coalition
2009-2010

An intelligence assessment on the commercial distribution of child sexual abuse images

A progress report on the work of the European Financial Coalition

With support from the Prevention of and Fight against Crime Programme of the European Union
European Commission - Directorate-General Home Affairs.
This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Contents

Overview and key findings

The European Financial Coalition against commercial sexual exploitation of children online (EFC) was formally launched on 3-4 March 2009 at the 'An Indecent Profit' conference by M. Jacques Barrot, Vice-President of the European Commission.

Major financial, internet and technology corporations have joined forces with international policing agencies, the European Commission and specialist child protection non-governmental organisations (NGOs) to track and disrupt the trade in child abuse images and eventually to confiscate the proceeds of crime of those who are engaged in the commercial distribution of child sexual abuse images on the internet.

Led by the Child Exploitation and Online Protection (CEOP) Centre – the UK's national law enforcement agency for protecting children from sexual exploitation – and funded by the European Commission, the EFC brings together stakeholders engaged in the fight against the commercial distribution of child sexual abuse images.

The EFC aims to facilitate and support pan-European police operations focused on this area of criminality by developing and supporting cross-sector solutions targeting, in particular, the electronic payment systems used to purchase child exploitation and abuse images on the internet.

This will ultimately help to:

- identify, locate and safeguard victims;
- identify, locate and arrest perpetrators[1];
- identify, trace and seize the assets of offenders[2]; and
- educate, inform and empower key stakeholders to prevent the proliferation of commercial child abuse websites and ultimately disrupt and dismantle criminal activity.

The purpose of this report is to evaluate and analyse the current intelligence available on commercial child sexual abuse websites and to evaluate the effectiveness of the pilot phase of the European Financial Coalition.

This report has been authored by the Strategic Analyst within the European Financial Coalition and has been peer reviewed by intelligence analysts within the CEOP Centre, the Behavioural Analysis Unit of the CEOP Centre, Europol AWF Twins section and members of the EFC Steering Group.

Key findings

- **There has been a significant decrease in the number of active commercial sites that can be identified.**
- **Difficulties with data gathering and differing methodologies within organisations make an accurate analysis problematic.**
- **Organisers of commercial child sexual abuse websites are distributing but not producing images.**
- **Images are generally historic and re-cycled time and time again.**
- **Not all distributors are from organised criminal networks, many of them are disorganised individuals working together and who may or may not have a personal sexual interest in children.**
- **Criminals from organised networks generally come from Eastern Europe.**
- **Commercial sites are generally not high profit; compared to other areas of online criminality online profits are actually quite low.**
- **There are numerous access points for child abuse images on the internet and offenders will adapt to the current technologies available.**
- **The producers of abuse images are likely to use small, secure areas of the internet that are password protected to share the images for free.**
- **The European Financial Coalition should expand its remit within phase II to cover all child abuse images online, whilst retaining the commercial elements.**

[1] Purchasers of child abuse images.
[2] Organisers/suppliers of child abuse images.

Part 1

The strategic intelligence picture

Part 1 The strategic intelligence picture

Methodology and limitations

A number of sources were utilised in producing this report and a full list can be found in Appendix A. This report has brought together information from qualitative and quantitative data, however, as with all intelligence reports, conclusions and recommendations are based upon the information that is available and inferences drawn from that information.

In drafting this document it is inevitable that much of the information available is widespread. Indeed whilst there are some agencies and organisations throughout Europe that do collect information about commercial child abuse websites, there has not yet been a central collection point for intelligence on these sites, making an assessment of the overall intelligence picture difficult. One of the advantages of the EFC has been its ability to consolidate that information to provide a more detailed and informed assessment.

Law enforcement case studies referred to in this report are not listed or mentioned by name unless the operations are complete and already in the public domain. All information provided in this regard has been redacted to protect the integrity of ongoing police investigations.

Definitions

The use of the word 'commercial' refers to child abuse images (CAI) that are available to purchase. This could include a website designed to provide child abuse images for a cost (normally a subscription), or uncensored newsgroups who charge a fee for membership and have child abuse images available as part of their service.

Uncensored newsgroups are very different to commercial websites: they provide access to many different online areas and the majority of these areas are legal. Newsgroup organisers can therefore claim that they were not aware that child abuse images were being accessed via their service, unless they have already been informed and have not removed access to the material.

The majority of newsgroups are actually re-sellers; they provide access via their own newsgroup to a library that is held by a 'parent' newsgroup. Parent newsgroups are normally hosted within the US and owners will strongly resist any attempts to censor their content by claiming 'freedom of speech'.

Organised criminal networks can be defined in many different ways. For the purpose of this report, the term is used to describe a structured group of criminals where members have defined roles, are highly likely to be engaged in more than one form of criminality and where their sole purpose is financial gain. Individuals who employ others, or who work with others solely to achieve a specific common goal but without any real structure are in this report classed as 'disorganised' individuals.

Security

This document is not protectively marked. Please contact CEOP for authorisation before re-producing any part of this report.

Part 1 The strategic intelligence picture

The extent of the problem

Notwithstanding the limitations highlighted in this document, this assessment attempts to qualify the true extent of commercially available child abuse images. In the past credible commentators have suggested that there are thousands of commercial websites selling child abuse images. Analysis was therefore conducted in order to identify if this is still true today and a number of different sources were utilised. One of the difficulties of conducting this analysis is that different agencies use different methodologies for counting commercial sites and they rely heavily on an analyst's interpretation of what qualifies as commercial. Consequently different agencies may well have differing views of the extent of the problem.

The US Financial Coalition Against Child Pornography (FCACP) has reported a 50% decrease in the past year of reported commercial abuse websites and this downward trend is believed to be continuing. The US Treasury has also reported a significant reduction in the money flow from child abuse images based on reports from law enforcement[3].

In their 2009 Annual Report[4], the Internet Watch Foundation (IWF – UK hotline) stated that 8,844 URLs/web pages were reported by them in 2009 containing child abuse images, worldwide. The IWF confirmed that these were not all commercial and that figure was for all websites containing child abuse images. There was no breakdown given for how many of those 8,844 were commercial sites. The IWF stated within the 2009 report that they have suggested that there has been a change in methodology by commercial distributors and are seeing more and more examples where the content sites do not take payment; instead the payment is managed by a seemingly unconnected site, usually purporting to sell legitimate goods/services (software etc). Instead of receiving the goods/services, the purchasers are provided with a link, or a membership ID with which to access the child abuse images. It may be that the content is hosted on publicly available servers (free hosts) but is 'hidden' as the content is not linked to any payment site. Information from the US FCACP[5] would appear to corroborate this as they are also reporting changes in the way payments are made, with a trend towards alternative payment schemes and the use of emails to send instructions on alternative (non-credit card) payment mechanisms. However, at this point in time this theory cannot be corroborated by evidence, therefore research needs to be conducted to identify if this suggested change is happening in reality.

Analysis of the Flagging and Co-ordination System[6] (FACS), which contains reports from the IWF and includes data from this year, demonstrates a decrease in the number of reported commercial sites in 2010 when compared to the last five months of 2009. However, it must be noted that FACS only contains sites with a payment page attached. Nevertheless taking the figures from August 2009 (the start of FACS) to July 2010, there were 276 reported commercial sites in the last five months of 2009, compared to 61 reported commercial sites in the first seven months of 2010; a 78% decrease this year of traditional payment commercial child abuse images sites.

The INHOPE database[7] of identified child abuse images sites from across European hotlines has only recently been developed, and they are therefore not in a position to make a judgement on whether there has been any significant changes in the number of commercial sites as they do not hold statistics from previous years. The data they do have however shows that commercial sites account for 22% of all reported child abuse images sites across a four month period, although it is not clear how many sites 22% equates to.

In order to gain a more comprehensive analysis of the current picture, an independent expert company[8] were asked to analyse its database of previously flagged sites suspected of linking to child abuse images. This database contains over 14,500 records and is maintained by the company in order to provide analysis to financial companies on child abuse images and the misuse of their systems. That data includes (but is not limited to) reported sites from:

- The National Center for Missing and Exploited Children (NCMEC) Cybertipline: company receives notices of reports to the cybertipline on behalf of its financial industry clients;
- IWF: company receives periodic updates of known child abuse images sites from the IWF;
- ASACP[9]: company is partnered with the ASACP and gets lead data from them; and
- Internet Crawling: company continuously crawls the Internet and monitors millions of known adult sites for any suggestion of child abuse images.

[3] Information from USFCACP.
[4] IWF Annual Report – 2009.
[5] Information from USFCACP – Backgrounder Document August 201.
[6] For an explanation of FACS see Part 2 – Pilot Project Achievements.
[7] For an explanation of the INHOPE database see Part 2 – Pilot Project Achievements FACS.
[8] Company used by financial industry to conduct analysis and are based in the US. They have requested anonymity within this report.
[9] Association of Sites Advocating Child Protection (US).

Part 1 The strategic intelligence picture

Once a site enters the database, it is reviewed to confirm its content status. An analyst reviews the content and provides one of the following categorical site labels:

Content Type	*Definition*
A	The site shows children (aged 1-16) engaging in sexual contact, nude or in sexually suggestive poses.
A1	The site shows young children in suggestive, but clothed, positions. Typically, these are labelled as child model sites.
Child Abuse Link Farm (CALF)	Advertises child abuse sites. The site contains child abuse images images and no method of payment with a primary purpose of redirecting users to other sites (including, but not necessarily A sites).
Model Link Farm (MLF)	The site advertises on child abuse images terms but has no child abuse images. The site contains a link farm of URLs that predominantly link to sites promoting models of young children in suggestive, but clothed positions (directs you to A1 sites).
Adult Content	The site has normal adult content, but may advertise on child abuse images terms.
Inactive	The link investigated is not active at the time it is reviewed. Typically returns a 404 error or Site Not Found.
Parked	The site is parked. Typically, the site has content that simply redirects users to other normal commerce sites.

Analysis conducted on the 14,579 sites over a period of five days (3-7 August 2010), identified that in this time period only 46 (0.3%) of these were actually active and showing some form of child abuse images content (including child modelling images). Analysis was then conducted on the 46 sites to identify which of these were commercial.

Of the 'A' sites identified during the August review, six of the ten did not take any payment and four purported to take payment. It should be noted that although some sites have a payment system in place, others have logos or checkout facilities advertised but cannot actually physically accept payment.

Of the six that did not take payment:

- Two are single image sites hosted on a media storage facility;
- Two are sites with suspect content and no way to pay. On checkout, both refer to a teen site that appears to have legal content;
- One is a nudist site with no way to pay e.g. young girls pictured but not actively engaged in sexual activity; and
- One is a 3D (cartoon/3D) incest site with no way to pay.

Of the four that purported to take payment, each displays the Visa, MasterCard, and Discover logos:

- Two are 3D (cartoon/3D) sites with purported payment taken by Plasmabill or SafePay. Previous research suggests these are frequently card harvesting payment sites; and
- Two are nudist sites that offer payment via Plasmabill.

Of the 23 'A1' sites identified during the August review, the breakdown shows:

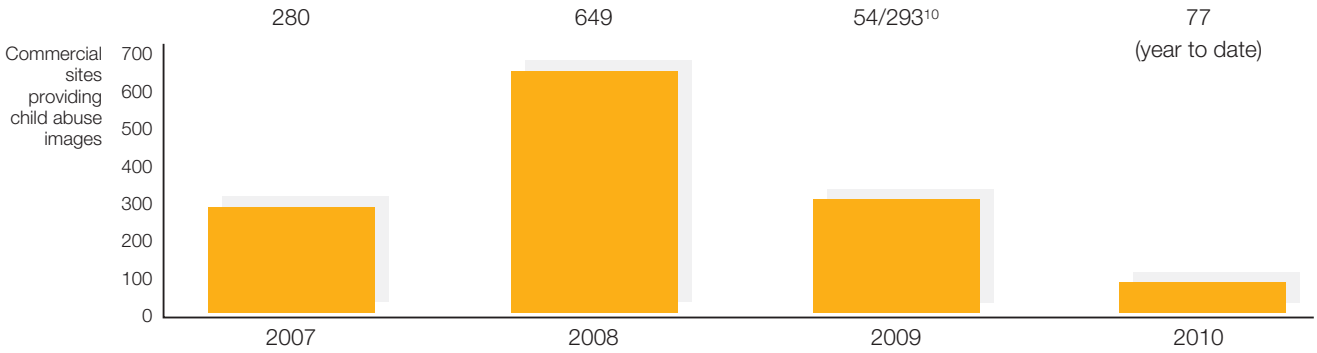
- Three do not have active payment pages;
- One offers only Western Union as a payment method; and
- Nineteen have payment with nnpay.org payment page.

Part 1 The strategic intelligence picture

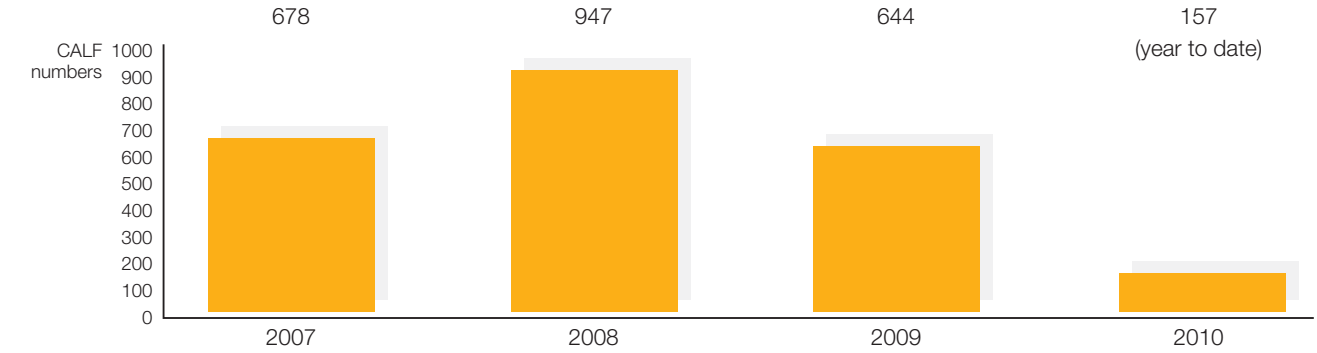
Therefore out of the 46 active sites with child abuse images content, 24 of them were confirmed as being commercial sites (or purporting to be commercial) and the vast majority of those (20 out of 24) were claiming to be child modelling sites, meaning children posing clothed, but in suggestive positions.

Perhaps the most surprising finding for the company undertaking the research was that they did not find any active 'branded sites' during this time period. Branded sites are those that are a number of seemingly different websites but are actually believed to be operating together. The IWF 2009 report identified 461 of these unique 'brands', one of which had 102 different URLs involved in the distribution of images. These branded sites are believed to make up a large percentage of child abuse images sites that are active at any one time. Therefore, the inability of the company to identify a single branded site active within the five day timeframe is significant. Although the timeframe for the analysis was very short it would be expected to find some of the branded sites active. The IWF are reporting branded sites being active this year. They are currently conducting a project to identify the number of these branded sites and so far have 10 identified.

Extending the analysis over a longer time period, commercial sites providing child abuse images are showing a significant decrease across the 'A' sites:



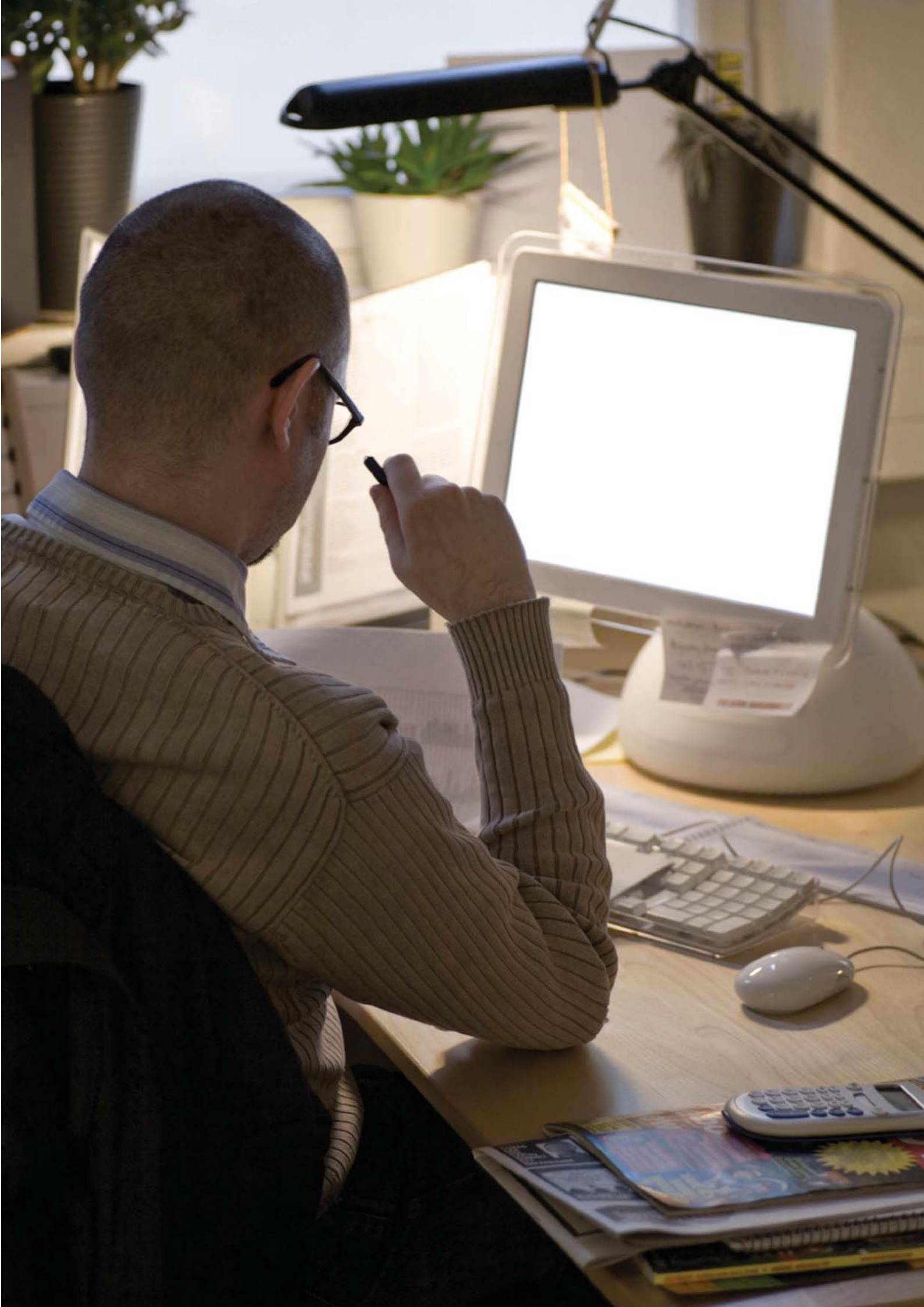
CALF (the adverts and banners for child abuse images sites) have also decreased quite dramatically as shown below:



This would suggest that commercial sites and the advertisements for them are significantly decreasing from their peak in 2008 – a drop of 88% between 2008 and 2010 for commercial 'A' sites. This analysis, however, only takes into account sites that have a payment page attached to them (whether the page is valid or not), so will not capture the sites that allegedly adopt new payment methods (the hidden sites) such as organising payment by SMS or email.

Therefore whilst there may have been thousands of commercial sites in operation previously, there is currently no available evidence to suggest that this is the case today. The analysis and data provided from a number of different sources suggest that there are only a handful of active sites at any one time. However, it must be noted that this may in part be due to differing methodologies in the way sites are counted and the suggested change change in modus operandi by the distributors. This apparent decline of commercial child abuse images websites may also be the result of a number of other factors such as: images being readily available for no cost, the development of new technologies, law enforcement action, media attention afforded to police tactics in relation to this crime and a move towards other online technologies as society becomes more comfortable with online environments and becomes more IT literate.

[10] A change in the way URLs were counted in 2009 showed less commercial sites. The new method of counting was abandoned when it was agreed it was not capturing all the sites, so although 54 were identified under the new system it was estimated there were 293 under the previously used methodology.



Part 1 The strategic intelligence picture

Commercial versus non-commercial distribution

Comparing the commercial distribution of child abuse images to other access points is difficult. The EFC has concentrated on the commercial aspect of trade in child abuse images since the project began.

Initial analysis of the INHOPE URL database that has been designed to capture information from across Europe shows that 22% of all reported child abuse image sites are commercial[11]. The INHOPE database has, however, only been designed to capture web content so it does not include internet applications such as peer to peer. It is also not clear how many they identified as figures were only given in percentages. Interestingly, the INHOPE data shows that the most reported web based tool after commercial is image hosting sites. Image hosting is a service offered by a number of providers (generally free of charge) where the public can upload their digital photos to the site and receive back a URL which they can then distribute to friends and family. Social networking sites are apparently not captured within the data.

By definition peer to peer involves agreed file sharing between computer users with the same networking programme to connect to each other and directly access files from each others' hard drives. Consequently, abuse of this is less likely to be found and brought to the attention of the authorities by concerned members of the public, as those with child abuse images on their hard drives are unlikely to agree to share with anyone else, unless they have an agreed interest in child abuse images, or they do not realise that it means others can access the child abuse images. Arguably, law enforcement activity or reports from the online industry are more likely to unearth criminal activity in peer to peer environments.

It is not therefore easy to draw direct comparisons between commercial and free access points; however it is apparent that commercial child abuse image websites and uncensored newsgroups continue to be utilised by those with a sexual interest in children. The persistent presence of commercial websites, even if they are not as prevalent as previously believed, demonstrates that there is a demand for pay per view access to images of child abuse. If demand did not exist, commercial child abuse websites would simply cease to operate. Further evidence for their continued use comes from law enforcement operations against these sites which consistently identify hundreds of 'customers'. Operation Koala[12] involved 28 countries and identified more than 650 suspects (for a full explanation of Operation Koala see Images section on page 15).

The distributors

One of the most prominent gaps in knowledge to be addressed by the EFC was the motivations of the website organisers. Whilst a number of claims have been made about organised networks operating websites selling access to child abuse images purely as a profitable criminal enterprise, it is also possible that offenders with a sexual interest in children operate such websites in order to profit from their deviant interest in children. This question is of major importance, as the strategies used to disrupt the distributors very much depends on their motivations. If the motivation for running a website is a personal sexual interest in children rather than profits, law enforcement attempts to target the flow of money is less likely to have an impact than it would if the motivation were purely financial.

Based on seven case studies from Europe and the US of distributors arrested (or being investigated) for operating commercial websites, part of the motivation does in some cases appear to be a sexual interest in children. Organisers may have realised that they can make money from their sexual interest in children; any profit is an added bonus rather than the main reason for providing images. If these offenders did not sell access to images, they may well share them via non-commercial access points such as peer to peer networks. Out of the seven case studies utilised for this report, two of them identified organisers who had a personal sexual interest in children.

Analysis of behaviour would suggest that individuals who are willing to distribute child abuse images have a personal sexual interest in children, and part of law enforcement activity should be to further develop the current understanding of this issue with effective interviews.

[11] INHOPE URL database
[12] Europol

Part 1 The strategic intelligence picture

According to the investigators of distributors based in Eastern Europe, offenders appeared to have no personal sexual interest in children. Instead, their motivation was purely financial. The distributors were part of organised criminal networks that were also using a variety of other illegal activities to make money. It must, however, be noted that the investigators did not necessarily look for any evidence of a personal sexual interest in children, as they had already obtained the evidence necessary to bring charges against the offenders for a variety of offences. It can also be extremely difficult for investigators to judge whether offenders have a sexual interest in children: even if abuse images are found on their personal computers, they could simply be collecting them for use on the website. Taking the lack of any evidence for sexual interest in children at face value, this Eastern European preference for organised criminality to be running these kinds of websites is a likely consequence of weaker regulations, controls and law enforcement which all in turn reduce the risk for distributors.

Of the seven case studies utilised within this report, only two of them are confirmed as being run by organised criminal networks, both of which are based in Eastern Europe. Of the remaining five, four were run by individuals with no identified links to organised crime and in the final case it is not yet clear who the organisers are.

The fact that organised criminal networks do not in general appear to have taken advantage of what is perceived to be a lucrative market is perhaps surprising. There are four possible explanations for this:

(i) many organised criminals have a 'moral code' and find the idea of sexually exploiting children for money morally repugnant;

(ii) the market is actually not as lucrative as supposed;

(iii) the risks are too great; and/or

(iv) the market is already flooded with free images.

Given that many child trafficking rings are run by organised criminal networks[13], it is very clear that the exploitation of children does not breach the 'moral code' of many groups and individuals to making money from child exploitation. This, in turn, suggests that there is not enough profit to be made or it does not warrant the risk, or possibly they feel that due to images being freely available there is not enough of a market to justify running a commercial site.

Early law enforcement operations, such as Operation Avalanche (Landslide website – USA, 1999) showed that millions of dollars were being made on an annual basis by a commercial adult pornography website, which also supplied access to child abuse images. It must however be noted that these profits did not derive exclusively from child abuse images. Operation Avalanche led to a number of operations around the world, with thousands of arrests of the purchasers from these websites, attracting widespread media attention. This would have had a major disruptive effect on both distributors and purchasers by creating fear amongst buyers that if they purchased images then they were likely to be caught. Fewer buyers mean less profit for organisers. This is likely to remain true today, with many offenders being extremely wary of making purchases that are known to be easily traceable.

More recent operations suggest that whilst there are still profits to be made, those profits are much lower than previously estimated. In most cases distributors are likely to make hundreds of thousands of Euros rather than millions; however if distributors can keep their website up and running for a reasonably lengthy period of time, it is feasible to make over a million Euros[14] within a few years[15]. All of the agencies[16] are reporting an increase in the cost of subscriptions for commercial sites in the past couple of years. Subscription costs are normally given in US dollars, and the price has increased from approximately $29.99 a month to generally closer to or over $100 a month. The US FCACP has reported one site asking for over $1000 a month[17]. There are two possible explanations for this. Firstly, that organisers have had to increase their costs in order to increase their profits due to a lack of demand; or secondly, that demand is high and therefore they can afford to charge more. Analysis of FACS has not identified any subscription costs of over $1,000, however, general costs would appear to be between $79.95 and $99.95.

[13] Strategic Threat Assessment – Child Trafficking in the UK April 2009 CEOP.
[14] Or any other currency.
[15] Information taken from both case studies and FACS.
[16] Expert company, USFCACP and the IWF.
[17] USFCACP Background Document.

Part 1 The strategic intelligence picture

Case studies utilised within this report are included in the chart below. The chart shows a breakdown of the case studies used and includes an estimate of profits made.

Case study	*Organised crime*	*Estimated* profit (euros)*	*Time period*	*Confirmed personal sexual interest in children*
Case study 1	Yes	Not known	Not known	No
Case study 2	No	40K	Annual	Yes
Case study 3	Yes	Not known	Not known	Not known
Case study 4	No	1.4 million**	7 years	Yes
Case study 5	Not known	Not known	Not known	Not known
Case study 6	No	55K	3+ years	Not known
Case study 7	No	8.5K	Annual	Not known

* *All profits are estimated and converted into Euros.*

** *This figure may change as the investigation continues. This case study is anomalous due to a very different operating method by organisers.*

The chart clearly shows where figures are available that the profits made are actually relatively small, particularly if you compare that to other online crimes such as internet fraud[18].

Identifying the distributors is a more convoluted process than identifying the buyers due to having to retrace payments from its source (the buyer) to its ultimate destination (the merchant) than it is to follow the simple everyday transaction of making an online purchase, especially as the distributors make every effort to hide the money flow. Nevertheless a number of high profile arrests of distributors within the last few years, clearly show the risks of distributing child abuse images. The lack of organised criminal enterprises operating child abuse images websites is therefore likely to be due to it being considered 'high-risk, low-profit' by the more sophisticated networks who prefer the 'low-risk, high-profit' approach.

[18] 'Online fraud generated £5billion worldwide in 2007' 2008 ACPO National Strategic Assessment.

Part 1 The strategic intelligence picture

The images

Evidence from victim identification experts, other law enforcement officers and agencies that study commercial websites suggests that it is very rare for new, contemporary images to appear on commercial child abuse image websites or newsgroups. The images are instead historic, meaning that they are a number of years old in most cases and are often well known to law enforcement.

This evidence of historical images on commercial sites suggests that those who are distributing the images are not responsible for their production: they are instead re-cycling old images. The reason for this is probably two-fold. Firstly, it means very little outlay for the organisers as they are not having to pay to have images produced, leaving them with only having to pay for their website and server costs; and secondly, there is less risk of a victim or abuser being identified if the images are historic.

There are of course exceptions to the rule. This was demonstrated in Operation Koala[19] (2006), with the arrest and conviction of an Italian national for producing and distributing child abuse images via a commercial website. The organiser was producing new material using children from the Ukraine by grooming the parents to get access to their children and paying them for agreeing to 'model'. The Italian national sold his illegal videos through seven websites. The main website was administered by the organiser, as he had enough IT skills to act as webmaster. This website served to advertise his products. It showed a preview of the videos of the young 'models' and through this website potential customers were able to email him in order to arrange the details of the transactions. The videos were sold either as DVDs sent via ordinary mail, or as downloadable files on the other six websites which were hosted on free web services. In this case he posted an encrypted file containing the video and communicating the relevant username and password to the ordering customer. The Italian national was also paying a Belgian national for videos of him abusing his two daughters. These videos were posted on his sites. Prior to his arrest, the material available was becoming more and more extreme and his customers were actively encouraging the offender to post more videos, escalating the abuse and exploitation of the children. A number of 'customers' to this particular website were also contact sexual offenders who, upon arrest, admitted that they had abused children in the past or that they were still abusing children, most often their own.

This particular case study is illustrative of the damaging nature of commercial child abuse sites around which networks of like-minded individuals are able to gather and to a greater or lesser extent, incite and direct further sexual abuse of children – a theme that is also evident in private sharing areas on the internet, where offenders share images for prestige over money.

Generally, the majority of new images are distributed within more secure areas of the internet, such as private social networking groups or peer-to-peer environments. These areas are often encrypted and password protected with access that is strictly controlled by a 'site controller'. Access to these areas is by invitation only and they are not simply available via the domain name of the site.

These networks will often be hierarchical in nature and involve the delegation of administrative powers to other individuals who have proved their 'worth' or their 'responsibility' and perform the role of a 'senior admin', but overall control remains with the site controller.

In terms of risk to children, those who are members of secure areas and are exchanging images for prestige rather than money, are often considered significant offenders; they produce images by abusing children themselves or inciting others to perpetrate, record and share abuse with like minded individuals. They are also knowledgeable about law enforcement tactics and will attempt to stay ahead of any initiatives which may lead to their identification and arrest.

Security measures vary according to the technical ability and paranoia of those involved and provide challenges to law enforcement in terms of investigation and infiltration. That said, with the development of law enforcement techniques, the use of advanced technology and the use of legislation[20] against those who fail to provide passwords when required during investigation, more and more individuals, who deemed themselves too clever to be caught, are being held to account for their actions.

[19] Information from Europol.
[20] Regulation of Investigatory Powers Act, Part III in the UK – will vary across Europe.

Part 1 The strategic intelligence picture

A recent example of such a group operating is Operation Enrack[21] which involved a network sharing child abuse images via the social networking site Facebook. The images were shared for free. The senior administrator, a registered sex offender from the UK, was in charge of a number of private groups on Facebook containing thousands of images of children suffering abuse. Investigators infiltrated the network and discovered that the offender was enabling carefully selected contacts to access up to three of these private groups. At the point at which contacts were able to demonstrate their trustworthiness, usually through adding their own child abuse images, the administrator would facilitate access to the next group. Each group contained more extreme images and films of child sexual abuse. He was charged with making (producing) and distributing child abuse images and in August 2010 was given an indeterminate public protection sentence. Two children in the UK have been safeguarded.

The victims

It is essential to remember that technology is the medium through which images are shared and that in the production of these images real children are abused or exploited in the offline world. The victims of indecent images which are distributed for wider consumption not only have to deal with the ramifications of the original abuse, but also their continued and constant re-victimisation, possibly for the rest of their lives. Once uploaded to the internet, these pictures cannot be removed. Victims are fully aware that their images are still accessible to those with a sexual interest in children. They live with the knowledge that their abuse will continue to be viewed. In the case of older children, the victims may be recognisable as adults.

There is also the possibility that some victims were groomed by being shown pictures of other children being abused. Offenders use this tactic to convince victims that abuse is 'normal'. The victim then also has to live with the knowledge that their images may be used to groom other children. Evidence suggests that the recording of the abuse aggravates and prolongs the victimisation of the child and can increase their sense of complicity[22].

This cycle of re-victimisation, the fear and shame of being identified and the knowledge that images of their abuse may be used to groom others, will in many cases have a significant impact on victims that will follow them well into adulthood.

[21] CEOP press release 26 August 2010.
[22] Information from USFCACP – Backgrounder Document August 2010.

Part 1 The strategic intelligence picture

The 'customers' and purchasers

One obvious question often posed when discussing this type of criminal behaviour is why someone would spend money buying child abuse images when nowadays there are a growing number of images available for free, for example, via peer to peer networks.

Without conducting major de-brief interviews of convicted purchasers, it is not possible to answer this question with any quantifiable evidence, however, consultation with a behavioural psychologist and practitioners within this field has led to a number of possible theories and these are explored below.

Buyers are 'new' to looking for child abuse images on the internet: it is suggested that if buyers are not regular users of the internet for this purpose, they will not be aware that child abuse images are available via other avenues for free. Once they are more experienced and confident they will move on to the free avenues. This theory may well have some merit; it is not particularly difficult for buyers to find commercial sites while browsing the internet. Searches on simple and logical keywords can also find commercial sites. Forums and newsgroups are also used to advertise such sites. An advanced understanding of the online environment is therefore not required to find commercial websites.

Buyers are frequently collectors: many buyers of child abuse images are also collectors. They wish to collect as many images as possible and look to collect full series' of pictures. There are many known and infamous series of child abuse images and buyers will pay to ensure that they obtain the complete set of images. So whilst they may have obtained some images from free access points, they may well then turn to commercial websites and pay for images to complete the series. Evidence from arrests of purchasers has demonstrated that many offenders keep and very carefully organise all of the images they have collected, suggesting that there is an element of obsession with gaining full collections.

Buyers believe they are safer using commercial avenues: buyers believe that peer to peer (the most popular method of gaining free images) is heavily monitored and regulated because of level of media attention afforded to illegal music sharing and copyright issues. Therefore, they may believe that they are actually less likely to be caught if they use commercial avenues instead. Many may also believe that utilising access points like peer to peer may leave their security compromised on their own computer as it allows sharers access to their personal folders.

Buyers want new images: buyers are looking to find new images that they have not previously seen. Although commercial sites do not generally supply new images, they do advertise their images as new and previously unseen. By the time the buyer has paid the money for access and realised that they are once again viewing historic images, it is too late – they are unlikely to make a complaint that they have been defrauded.

Overall, the reason for buying rather than acquiring images for free probably resides in a mixture of the theories described above. It is equally possible that there are additional motivations that have not been explored within this assessment. The only way to improve understanding of the motivation of buyers is to undertake a detailed programme of offender debriefs, preferably as part of a comprehensive research project.

Financial processes

Criminals who sell child abuse images on the internet use a number of different methods for collecting payments, ranging from traditional banking methods, to newer, less conventional e-commerce options. Many of them use reputable financial companies, hence the need to have the financial industry fully involved in the EFC and in the development of strategies to prevent the abuse of their payment systems.

As a result of national and international legislation and regulation, alongside a desire to protect their brand, many financial companies have systems and protocols in place to help identify illegal activity, although some will occasionally fall under the radar. Reputable financial companies can withdraw services to a customer if they identify that child abuse images have been purchased; however, financial companies do not share this information with other financial service providers, leaving the criminals free to move from one to another, in one case changing suppliers up to three times in their operating lifetime. Members of the EFC Payments Industry Working Group are actively attempting to identify ways of legally sharing this information to frustrate child abuse images sellers' ability to move between financial service providers.

Part 1 The strategic intelligence picture

The funds generated by the sexual exploitation of children are laundered in many different ways, utilising both traditional and less conventional methods.

As this is an unclassified document the methods used cannot be detailed within this report, although they are included within the restricted version for law enforcement use. The financial industry must continue to work closely with law enforcement to ensure that new methods are quickly identified and opportunities for their abuse by criminals are prevented.

The US FCACP has reported a trend in websites directing buyers away from traditional payment tools and methods, such as credit cards, and toward multi-layered, alternative payment schemes[23]. For example, a website may purport to offer the traditional credit card payment methods on a webpage but, after attempting to use a credit card, a purchaser is instructed to send an email to a specified email account. The sellers will then reply with instructions on how to send money through alternative payment (non-credit card) mechanisms.

The use of 'middle men' to collect payments is fairly common for child abuse images distributors. These middle men act as a barrier between the organisers and law enforcement. The use of 'mules' is also fairly common, particularly with regards to offline payments, for example, Western Union. The mules are paid to collect the money and there is a reasonable chance that these mules have no idea of the source of these payments.

Analysis of the FACS database shows that the most widely used of the payment processors (when specified) are Western Union. Out of 337 reports (August 2009-July2010), Western Union accounted for 24% of advertised payment methods. 69% of sites simply stated payment by credit card, with no type specified. Visa and MasterCard are specified in 11% of identified commercial sites. The chart below shows all payment methods listed that were mentioned more than four times. It must be remembered that these are the advertised payment methods and an attempt to actually use those methods may re-direct to alternative payment systems (for a full list of payment methods identified please see Appendix B).

Payment method	*Accepted to gain access to website*	*%*
Credit card (type not specified)	*234*	*69%*
Western Union	*80*	*24%*
Visa	*37*	*11%*
MasterCard	*37*	*11%*
Delta	*8*	*2%*
Egold	*16*	*5%*
PayPal	*12*	*4%*
JCB	*9*	*3%*
Wire transfer	*8*	*2%*
Cash	*7*	*2%*
Maestro	*8*	*2%*
Discover	*8*	*2%*
Money order	*8*	*2%*
Bank transfer	*8*	*2%*

It is important to bear in mind that not all commercial child abuse images sites that are advertised actually supply child abuse images. Fraudulent sites exist that are purely designed to capture credit or debit card details that can then be used to commit fraud; no child abuse images is supplied in many of these cases. Other commercial child abuse images sites do supply the images as promised but will also capture the card payment details and use these to again commit fraud.

[23] Information from USFCACP – Backgrounder Document August 2010.

Part 1 The strategic intelligence picture

Recommendations

Based on these findings the following recommendations are made for further action.

Recommendations

Recommendation 1	In-depth de-brief interviews of convicted purchasers across Europe should be commissioned to understand the motivations behind the purchases of child abuse images.
Recommendation 2	Convicted distributors of child abuse images should be de-briefed in order to identify their motivations, the systems utilised and the payment processes used.
Recommendation 3	A central European database should be held of identified child abuse image sites, preferably by a central European law enforcement agency (Europol).
Recommendation 4	Hotlines throughout Europe should be encouraged to share their data with Europol as well as INHOPE.
Recommendation 5	A clear definition of what constitutes a commercial site providing child abuse images is required so that different agencies can utilise the same methodology.
Recommendation 6	A more in-depth understanding of other access points is required in order to understand the relations between commercial and other access points and the effect targeting commercial sites may have on these other areas, and offender behaviour.
Recommendation 7	Further research should be conducted into the 'hidden' commercial sites to identify if anecdotal evidence that the modus operandi of distributors has changed, can be converted into quantifiable evidence.

Part 2

A progress report on the work of the European Financial Coalition

Part 2 A progress report on the work of the European Financial Coalition

Introduction and background

Led by the UK law enforcement agency, the Child Exploitation and Online Protection (CEOP) Centre and funded by the European Commission, the European Financial Coalition (EFC) brings together a multitude of financial, online, law enforcement, governmental and non-governmental stakeholders in Europe engaged in the fight against the commercial distribution of child sexual abuse images.

Launched in March 2009, the EFC aims to facilitate and support pan-European police operations focused on this area of criminality by developing and supporting cross-sector solutions targeting, in particular, the electronic payment systems used to purchase child exploitation and abuse images on the internet.

The European Commission (EC) has funded a 14 month pilot project which began on 1 July 2009. Depending on the success of the pilot project, EC funding may be extended for a further three years.

This section of the report is to identify the progress of the EFC within the pilot period. Recommendations for further action will be based on this evaluation.

Aims and objectives of the pilot

The main aim of the pilot project was to facilitate and support pan-European police operations focused on this area of criminality, with cross-sector solutions targeting, in particular, the electronic payment systems used to purchase child exploitation and abuse images on the internet.

This will ultimately help to:

- identify, locate and safeguard victims;
- identify, locate and arrest perpetrators[24];
- identify, trace and seize the assets of offenders[25]; and
- educate, inform and empower key stakeholders to prevent the spread and ultimately disrupt and dismantle this crime once and for all.

In order to achieve this, the EFC objectives were to:

- gather and analyse intelligence on commercial websites selling child abuse images; individuals and/or groups behind commercial websites; payment systems utilised and purchasers of such material;
- prevent by means of education, dissemination of best practice, suggestion for legal changes, awareness raising and implementation of identified strategies;
- reduce/eradicate supply by means of enforcement, disruption and confiscation and influence demand by means of disruption and enforcement; and
- encourage co-operation and co-ordination between law enforcement, Industry and non-government organisations across Europe.

[24] Purchasers of child abuse images.
[25] Organisers/suppliers of child abuse images.

Part 2 A progress report on the work of the European Financial Coalition

The structure of the EFC

The EFC consists of a Steering Group (the main decision making body of the Coalition) and five distinct working groups:

The Law Enforcement Co-operation Working Group (LECWG) is chaired jointly by CEOP and the Italian Postal and Communication Police. Members are drawn from law enforcement agencies and authorities. The primary aim of this working group is to ensure the co-operation and co-ordination of law enforcement agencies across Europe. This co-ordinated approach facilitates pan-European targeting of commercial websites and the individuals or networks behind them. It must be noted that the LECWG can only share sanitised strategic intelligence with the other working groups and the Steering Group.

The Payments Industry Working Group (PIWG) is chaired jointly by VISA Europe and MasterCard. Members are drawn from major financial institutions. The primary aim of this working group is to ensure the financial industry is more resilient by identifying common working practices, detailing best practice and encouraging greater participation by the industry across Europe. The production of a best practice document will identify the payment mechanisms used for the exchange or sale of child abuse images and identify opportunities to improve law enforcement and payment processor co-operation. This group works closely with the Law Enforcement Co-operation Working Group in order to identify current trends and the payment mechanisms involved.

The Internet and Technology Working Group (I&TWG) is chaired by Microsoft and has members drawn from industry, law enforcement and non-governmental organisations. The main aim of this working group is to identify technological solutions to disrupt commercial websites that trade in child abuse images, beginning with initiatives aimed at companies or organisations hosting such websites. In the longer-term the aim is to incorporate technical expertise in programming and development. This working group also provides advice to law enforcement.

The Legal Working Group (LeWG) is chaired by Eurojust and comprises members of legal authorities, the legal industry and NGOs. The main aim of this working group is to identify the legal restrictions that prevent co-operation between law enforcement, the private sector and NGOs concerning the production and commercial distribution of child sexual abuse images on the internet. This working group also seeks to identify the main differences in criminal legislation of the EU Member States in this field and to identify how and to what extent information may be exchanged between law enforcement and non-law enforcement bodies.

The Awareness Raising and Prevention Working Group (ARWG) is chaired by Missing Children Europe and has members from industry and NGOs. The main aim of this working group is to utilise their influence to reach out and engage a broader community of participants and supporters across Europe. For example, convincing politicians of the value their influence could have for prioritising child abuse agenda items. Members of the ARWG also reach out across sectors to raise awareness of the commercial sexual exploitation of children, and synthesise examples of best practice to facilitate the development of robust prevention strategies.

Part 2 A progress report on the work of the European Financial Coalition

The pilot project achievements

The Coalition

The EFC commenced on 1 July 2009 with 11 organisations signed as members, drawn from law enforcement, industry and non-governmental organisations (NGOs). EFC membership currently comprises 29 organisations (for a full list of partners please see Appendix C). This number has increased on a monthly basis and the expanded membership has brought diverse expertise to the Coalition and ensures European-wide coverage. The EFC has become a true coalition with stakeholders working closely together to combat commercial child exploitation and to increase our knowledge and understanding in this area.

Intelligence sharing

One of the key aims of the pilot project was to allow the EFC to gain an in-depth understanding of commercial child abuse websites; how they operate, the motivation of organisers, the financial processes used and the extent of the problem. Only by developing this understanding can we hope to have a true impact on these websites by ensuring the most effective strategies are utilised against them.

The EFC has successfully negotiated the sharing of intelligence with both EFC members and non-members, including the US Financial Coalition. This has allowed the EFC to begin to build a more accurate picture of commercial child abuse image websites via a Flagging and Co-ordination System (FACS).

Flagging and Co-ordination System (FACS)

The Flagging and Co-ordination System is a database of identified commercial child abuse image websites currently held and operated by the EFC Secretariat at CEOP.

One of the main issues quickly identified when the EFC first started to operate was the lack of a central holding point for identified commercial websites. Each European state tends to have at least one hotline, generally run by an NGO which acts as the reporting centre for that state. Many of these hotlines are members of INHOPE. (For a full list of hotlines under the INHOPE umbrella please see Appendix D). INHOPE has recently commenced the collection of data from each of the umbrella hotlines and are operating a similar system to FACS; however INHOPE is simply attempting to identify the number of websites selling access to child abuse images, and how many of those are duplicate (branded) sites.

FACS is designed to answer those same questions but also seeks to establish:

- which payment systems are most likely to be used by website organisers;
- which payment methods are likely to be used;
- extrapolating from the data how much money organisers are likely to be making; and
- identifying the way in which payments are routed through to the organisers.

As an added benefit, FACS is also designed to ensure co-ordination in law enforcement operations against commercial sites by flagging those that are already the subject of ongoing investigation, and identifying those that are not. This will promote the effective use of law enforcement resources.

Unfortunately, at this point in time FACS only includes data from the UK hotline (the IWF), although the US data will also shortly be added. There has been difficulty in gaining data from the European member states (even the EFC members), at least in part due to fragmented and inconsistent methods for gathering and recording data. It would appear that even national law enforcement agencies do not hold a database of sites identified. For the database to be effective it requires

Part 2 A progress report on the work of the European Financial Coalition

every European member state to send data on identified sites into FACS. The simplest way to achieve this would be for the national hotlines to forward their data, however not all of the hotlines are willing to share information, and INHOPE have guaranteed its members that information sent to them will not be shared in its raw format. To gain a full understanding of commercial sites a central searchable database is essential to allow for a true analysis to take place. Europol have expressed an interest in taking the FACS database and may well have more influence to facilitate data sharing across Europe.

Financial Industry Best Practice Document

The Payments Industry Monitoring and Detection Working Group have produced a best practice document to be shared across the financial industry in Europe. Representatives from major financial institutions came together to develop a document that is relevant across European industry. The best practice document is intended to ensure that common standards are met across industry to prevent the misuse of payment systems by the organisers of commercial child abuse websites. Financial institutions with European interests will be actively encouraged to sign up to the best practice document and amend their policies and procedures where necessary. The effectiveness of the best practice document will be measured by the number of financial organisations agreeing to sign up to the best practice.

Law Enforcement Best Practice Document

The Law Enforcement Co-operation Working Group of the EFC quickly identified that the standards of investigation across Europe into commercial child abuse images varies depending on resources and levels of expertise within law enforcement agencies. A decision was therefore made to produce a guidance document for investigations into commercial sites that could be sent to every national law enforcement agency in Europe to improve the standards of investigation. The intention is to produce this document in a variety of languages.

The guidance document includes sections on; how to run a financial investigation; signposting to relevant organisations throughout Europe that can be utilised for their expertise; a full child protection strategy and covert internet investigation techniques. This document is only available to law enforcement and legal authorities due to its restricted content.

After the document is widely disseminated and national law enforcement agencies have signed up to it, the levels of investigations across Europe should begin to meet a common standard and improve the success rates for investigators. It will also ensure that a solid child protection strategy is at the heart of any investigation. A proposal for a Directive[26] on sexual abuse, sexual exploitation of children and 'child pornography' was submitted to the European Parliament by the Commission in March 2010. If accepted it may have a significant impact on the way child abuse and exploitation is investigated by allowing all EU member states the option to conduct covert investigations. A number of EU member states do not currently have the legislation in place to allow for covert investigations, and this is a vital tool in combating online child abuse. The LECWG guidance document provides advice on conducting such investigations.

To ensure the effectiveness of the guidance document, training must also be provided to European law enforcement agencies alongside the documentation to further develop understanding of the investigative processes and to encourage development of the essential skill sets, including financial and covert investigations, within national agencies.

[26] Council Framework Decision on combating the sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA.

Part 2 A progress report on the work of the European Financial Coalition

EFC website

The official EFC website is available on www.europeanfinancialcoalition.eu and has been designed with three major objectives in mind:

1. to act as the public face of the EFC;
2. to encourage organisations to join the EFC; and
3. to act as a deterrent for the distributors and purchasers of child abuse images by re-directing online searches for child abuse images to the EFC website.

In the first month of being live, there were 800 hits on the website and since then the number of hits has risen to over 1,000 per month.

The website is managed by the EFC Secretariat at CEOP and is regularly updated to ensure the latest progress and news is readily available to both members and the public.

Law enforcement operations

The first EFC law enforcement operation targeting a commercial website selling child abuse images is ongoing. The operation is being run by members of the Law Enforcement Co-operation Working Group of the EFC, and being led by CEOP.

These types of operations involve long-term investigations, accumulating a substantial quantity of data for analysis. Consequently, results will not be available until the operation is complete. The aim of this operation is to identify the distributors behind a website selling access to child abuse images, those making purchases and to identify the victims. A full child protection strategy is included within the operational plan.

Part 2 A progress report on the work of the European Financial Coalition

Progress to date

The pilot phase of the EFC was designed to build a coalition of cross-sector organisations to develop the knowledge and understanding of this area in order to allow the EFC to develop effective strategies to eradicate commercial child abuse image websites in the next phase.

The real success of the EFC lies in the building and development of a true coalition involving disparate (and frequently competitive) organisations working together for a common goal – the eradication of commercial child abuse websites. The experience of the EFC has shown that people from different backgrounds, with different priorities and agendas can work together for a common purpose, and that working together can make a real difference by utilising experience and expertise from across sectors. There have however been difficulties in gaining the necessary commitment to the EFC from members. The commitment has so far been sporadic, due mainly to individuals being solely responsible for giving their time and efforts and having to fit it in with other priorities rather than it being an organisational strategic commitment.

Utilising this experience and knowledge has allowed the EFC to begin to build a much clearer understanding of commercial child abuse websites and this in turn has led to the development of disruption strategies, that it is believed will have a major impact on commercial sites given enough time.

The EFC has also been successful in building relations with other organisations working within this field, such as: CIRCAMP[27], the US Financial Coalition, national financial coalitions and the Virtual Global Taskforce. The development of strong relationships underpins a dialogue between EFC members for the sharing of ideas for best practice and building a global picture for a global problem. It will also allow Europe and the rest of the world to ensure a truly co-ordinated approach to commercial sites. Having a co-ordinated approach for both law enforcement and industry, that covers large areas of the globe, means that the organisers and the purchasers will have few places left to hide.

Issues arising

The primary difficulty experienced by the EFC has been encouraging organisations to join. Although membership has risen from 11 organisations at the beginning of the project to 29, difficulties have been experienced in gaining law enforcement participation. Although there are 28 EU member states, there are only seven European countries represented on the Law Enforcement Co-operation Working Group of the EFC.

There are two reasons for the lack of European law enforcement agencies joining the EFC. Firstly, the travel and subsistence costs of attending meetings can be a barrier for some agencies and secondly, they are reluctant to commit to dedicating their limited resources to the EFC, especially if they are already members of CIRCAMP.

Furthermore, no Internet Service Providers (ISPs) have officially joined the EFC, although several have attended working group meetings and plenary sessions. ISPs might suspect that involvement in the EFC will impact upon their commercial activities. Some are misdirected by the word *financial* in the EFC, claiming that their input in a financial coalition is unnecessary.

Suggested areas for development

Membership

Should the EFC continue for a further three years, a determined effort will be necessary to persuade more law enforcement agencies to join. A European coalition can only be truly effective if there is participation from the majority of European member states, in particular Eastern European states; and intelligence, as well as best practice, is shared effectively.

The EFC also requires greater participation from the financial industry across Europe. ISP membership is also important to the development of the EFC. This will allow for the development of increasingly effective strategies that reduce opportunities across the online environment for both purchasers and distributors of child abuse images.

The EFC will continue to build on its existing relations with relevant organisations from around the world, ensuring that communication is open and relevant and that effective strategies and best practices are shared.

[27] CIRCAMP = COSPOL Internet Related Child Abuse Material Project.

Part 2 A progress report on the work of the European Financial Coalition

Disruption strategies

Disruption strategies will also be progressed and measures put in place to define their effectiveness. The first EFC law enforcement operation will be completed in the next phase of the project and learning from that operation will improve future operations and best practice.

Technical and financial solutions

Long-term technological solutions will continue to be developed and assessed by working closely with IT companies. In addition, existing technologies will be evaluated to assess their possible use in preventing child abuse sites from reaching servers.

Further work will continue on identifying methods for the prevention of payment collection by distributors, by mapping and understanding the payment processes and money flow and working with the financial industry to prevent the abuse of their systems. Financial institutions from across Europe will be encouraged to adopt the best practice guidance and to improve their relations with local law enforcement.

Increasing knowledge

A debrief of convicted purchasers across Europe will be conducted, with advice from psychologists, to enable the EFC to determine the motivation of buyers. A debrief of convicted distributors should also be conducted in order to gain a clearer picture of their motivations, how they operate and which financial processes they are likely to utilise.

The use of cross-sector training within phase II of the EFC will help to build knowledge of the relevant issues across industry, law enforcement and NGOs, which will in turn lead to more effective targeting of child abuse images sites and processes put in place to prevent the sites appearing, or payments from being made.

Work is also required to develop the understanding of other access points, how they relate to commercial and the extent of their use when compared to commercial sites. It is absolutely essential that we understand how evolving technologies impact on the online behaviour of offenders, and where production of images are taking place and being shared, in order to identify the most dangerous offenders (those who are actually producing images).

Emerging threats

As technology is constantly evolving so is the criminal use of those technologies. Many criminals are adept at quickly finding ways to exploit technology for their own ends and this is also true of those with a sexual interest in children. As law enforcement and industry target specific areas in an attempt to prevent the abuse, offenders will move to other areas or technologies in order to stay ahead of efforts to stop them.

The introduction of mobile technologies and games consoles connected to the internet means that offenders have more access to the internet and therefore more options to exploit the different technologies that exist.

The developing use of different online payment methods will also offer more opportunities to offenders as may the introduction of the e-money directive as the market becomes more open.

Part 2 A progress report on the work of the European Financial Coalition

The way forward

Should the EFC continue?

The continued development of expertise and understanding among EFC members should not be allowed to stagnate. There is an opportunity to capitalise on the momentum developed by the EFC and it is feasible that EFC solutions will have a major impact on the ability of criminals to operate websites offering child abuse images on a commercial basis.

What impact could the EFC have in the future?

The EFC was originally set up to eradicate commercial child abuse image sites from the internet. This is a difficult challenge. Based on the understanding developed by the EFC of the way in which these sites operate and the motivations of those who operate them, it is possible that commercial child abuse websites can be eradicated, though this will be a significant challenge for all stakeholders involved. It will require a European platform, working in co-operation with global partners across industry and law enforcement, and with NGO support and assistance, to target:

- the financial processes (stop the money flow);
- service providers (stop the service);
- the buyers (stop the demand);
- the distributors (stop the supply); and
- technology (stop the ability).

It is possible to have a major disruptive effect on commercial sites by developing strategies in only one or two of these areas, however, in order to eradicate commercial websites selling access to child abuse images, all of these aspects must be targeted with effective strategies in order to make the internet a truly hostile environment for those willing to sell and buy images of children being sexually exploited and/or abused.

The remit of the EFC in the future

The work done so far by the EFC has clearly identified that although financial processes are important for the prevention and disruption of commercial websites, targeting the finances alone will not eradicate these sites. This requires a more holistic approach. The financial dimension should remain a vital component of the EFC, but cross-sector strategies must also be developed. The EFC should therefore continue to consider all effective strategies, including working towards technological solutions.

Given that accessing child abuse images via commercial sites can either be the start of an online journey by someone who has a sexual interest in children, or it can be integrated with other *modus operandi* of child sexual offenders, the likelihood is that by tackling all commercial avenues for accessing these images will simply displace the problem elsewhere online.

In this respect, consideration should be given as to whether a major impact on commercial distribution will unwittingly encourage distribution via alternative means, such as peer to peer, as organisers alter their distribution methods to include free access points. By covering all of the avenues through which child abuse images are accessed, the EFC could prevent this outcome. Previous experience in this area has identified that if law enforcement targets one area of the internet, distributors will simply move to another, thereby staying one step ahead of preventative measures.

Commercial child abuse images are intrinsically linked to the free access points, as is demonstrated by commercial images also being available via peer to peer. By targeting all online access to abusive images, the EFC can also identify and target the more secure areas on the internet that are used to distribute recently produced images, thereby identifying and protecting children that are currently being abused, and arresting those responsible.

In addition, the learning gained and relationships built by the EFC can also be utilised to target other non-commercial access points to child abuse images online. Limiting the EFC remit to commercial only could mean that opportunities to reduce the threat of on and offline child sexual abuse could be missed.

Consideration should therefore be given toward expanding the remit of the EFC to cover all child abuse images online.

Part 2 A progress report on the work of the European Financial Coalition

Conclusion and recommendations

The findings of this report show a marked decline in the number of active commercial sites, as well as a decrease in profits for the offenders behind them. This is highly likely to be due to new technologies and the general population becoming more IT literate, as well as successful law enforcement and industry efforts against distributors and viewers of child abuse images.

However it may also be due to commercial distributors changing their methods to hide the sites more effectively, thereby attempting to thwart law enforcement attempts to target them. The eradication of commercial child abuse images sites has not been achieved and commercial child abuse images is still a problem. The market has not gone away but has simply been displaced to more secure areas of the internet where images are distributed on a non-commercial basis, or may have been better hidden. It is therefore vital that a greater understanding of evolving technologies and how they impact on offenders is developed in order to put in place effective strategies to prevent those with a sexual interest in children from accessing child abuse images online, regardless of the route they use.

Commercial sites must be targeted with cross-sector solutions. Continuing to work with the financial industry as well as gaining support from ISPs and technology companies is essential in being able to achieve the eradication of these sites, and to continue to develop the required knowledge and experience on a global level to allow for targeted and coordinated action.

Although the EFC has had some success in developing the intelligence picture and producing best practice, more work needs to be done. The coalition approach is important in allowing different sectors the opportunity to work together and learn from each other.

Recommendations

Recommendation 1	The EFC should continue to operate after the pilot project to allow further development of the knowledge and understanding gained so far.
Recommendation 2	Considerations should be given to expanding the remit of the EFC to include all child abuse images online in phase II.
Recommendation 3	Phase II of the EFC should include a cross sector training schedule.
Recommendation 4	Determined efforts should be made to encourage more organisations to join the EFC, allowing for greater sharing of knowledge and expertise.

Appendices

A-E

Appendix A

Bibliography

Academic References

Bourke, Al and Hernandez AE, 2009 *'The Butner Study Redux: a report of he incidence of hands-on child victimisation by child pornography offenders'* Journal of Family Violence, 24 (3), 183-191.

Csáky, C No One to Turn To, *the under-reporting of child sexual exploitation and abuse by aid workers and peacekeepers* Save The Children UK, 2008.

Endrass J, Urbaniok F, Hammermeister L, Benz C, Elbert T, Laubacher A, Rosegger A, *The consumption of Internet child pornography and violent and sex offending* BMC Psychiatry July 2009.

Guðbrandsson, B *Sexual Abuse in Iceland and the 'Barnahús Project'.*

Hernandez, *A Psychological and Behavioral Characteristics of Child Pornography Offenders in Treatment*, Global Symposium: Examining the relationship between online and offline offenses and preventing the sexual exploitation of children, University of North Carolina, April 2009.

Quayle E, in collaboration with Lars Loof and Tink Palmer *Child Pornography and Sexual Exploitation of Children Online, a contribution of ECPAT International to the World Congress III against Sexual Exploitation of Children and Adolescents*, Rio de Janeiro, Brazil, 25-28 November 2008.

Quayle E, Taylor M, *Paedophiles, Pornography and the Internet: assessment Issues*, British Journal of Social Work, 2002.

Save The Children Europe Group *Position paper on child pornography and Internet-related sexual exploitation of Children*, Save the Children Europe, June 2003.

Save The Children Europe *Child Pornography on the Internet: Legislation, policies and practice in six selected countries – submission to the Special Rapporteur on sale of children, child prostitution and child pornography Save The Children:* Denmark, Finland, Iceland, Italy, Norway, Sweden, October 2004.

Save the Children Europe Group *Visible Evidence – Forgotten Children, the need for a child protection and children's rights focus in identifying children who have been sexually abused for the production of child abuse images*, Save The Children Europe Group, Brussels, 2006.

Seto, M *Assessing The Risk Posed By Child Pornography Offenders*, Paper prepared for the G8 Global Symposium, University of North Carolina, March 2009.

Seto, M and Eke, *A Sexual Abuse: A Journal of Research and Treatment – The Criminal Histories and Later Offending of Child Pornography Offenders* SAGE Publications.

Wee,T *Online child abuse images – urgent call to identify and protect child abuse victims in online images* Canadian Red Cross, 2006.

Wolak J, Finkelhor D, Mitchell K, Ybarra M *Online 'Predators' and Their Victims - Myths, Realities and Implications for Prevention and Treatment*, American Psychologist, March 2008.

Appendix A

Practitioner interviews/questionnaire conducted

Dr. Joe Sullivan, Principal Forensic Behaviour Analyst, CEOP

John Hodge, Victim Identification Team, CEOP

Kate Richardson, Child Protection Team, NSPCC

Martin Joss, Group Leader Operations, CEOP

Melissa Ryan, Australian Federal Police and VGT

Dr Zoe Hilton, Head of Safeguarding and Child Protection CEOP

Anders Ahlqvist, National Criminal Police, Sweden

Antonio Parilla, Criminal Analysis Division, Guardia Civil, Spain

Dave Jansen, Dutch Police, the Netherlands

Erik Planken, Dutch Ministry of Justice, the Netherlands

Frédéric Malon, Ministere de L'Interieur, France

Giuseppe Giliberti, Italian Postal and Communication Police, Italy

Matthew Dunn, Immigration and Customs Enforcement, USA

Steve Selves, Internet Watch Foundation, UK

Valerio Papajorgji, Europol

Cathy Cummings USFCACP

Other papers

ACPO National Strategic Assessment 2008.

European Council Framework Decision on combating the sexual exploitation of children and child pornography repealing Framework Decision 2004/68/JHA.

Operation Koala briefing paper – Europol.

IWF 2009 annual report.

Problem profile on pre-paid cards – EFC Law Enforcement Working Group.

Strategic concept on commercial websites containing child abuse images – Ministerie van Justitie/Dutch Police.

Strategic Threat Assessment – Child Trafficking in the UK April 2009, CEOP.

USFCACP Backgrounder Document August 2010.

Strategic Review and Forward Vision for Combating Technically Sophisticated Commercial Child Pornographers. December 18, 2006, Produced by The Detection and Action Working Group of the US Financial Coalition Against Child Pornography.

Other sources used are not listed as investigations are on-going and cannot be compromised or the source requested anonymity.

Appendix B

Payment methods from FACS

Payment method	*Accepted to gain access to website*	*%*
Credit card (type not specified)	234	69%
Western Union	80	24%
Visa	37	11%
Mastercard	37	11%
Delta	8	2%
Egold	16	5%
PayPal	12	4%
JCB	9	3%
Wire transfer	8	2%
Cash	7	2%
Maestro	8	2%
Discover	8	2%
Money order	8	2%
Bank transfer	8	2%
Cheque	4	1%
Webmoney	3	1%
Phone	4	1%
Fax	4	1%
SMS	2	0.5%
Electron	1	0.5%
Amex	2	0.5%
Eurocard	2	0.5%
Liberty Reserve	2	0.5%
Membership only	1	0.5%
Yandex	2	0.5%

Appendix C

EFC members

Allen & Overy (advisory members)
AOL (advisory members)
American Express
Child Exploitation and Online Protection Centre
Crown Prosecution Service UK
Dutch Police
e-money association
eNACSO
Eurojust
Europol
French Gendarmerie
French National Police
Guardia Civil Spain
International Center for Missing and Exploited Children (advisory members)
Internet Watch Foundation
Italian Postal and Communication Police
Jugendschutz.net
MasterCard
Microsoft
Ministry of Justice – the Netherlands
Missing Children Europe
Newcastle Building Society
PayPal
Save the Children
South Eastern European Coalition, Smile of the Child
Swedish Police
Swiss Police
Team Cymru
Visa
Western Union

Appendix D

INHOPE hotlines

As well as including 25 Hotlines across Europe, it also includes 11 Hotlines outside the EU. There are three hotlines in Germany and two in the Czech Republic.

European

Austria
Belgium
Bulgaria
Cyprus
Czech Republic (2)
Denmark
Finland
France
Germany (3)
Greece
Hungary
Ireland
Luxembourg
Netherlands
Poland
Portugal
Romania
Slovak Rep
Slovenia
Spain
United Kingdom

International

Australia
Canada
Iceland
Japan
Latvia
Lithuania
Russia
South Africa
South Korea
Taiwan
United States

Appendix E

Glossary of terms

3D	3 Dimensional
ACPO	Association of Chief Police Officers (UK)
ARWG	Awareness Raising Working Group
ASACP	Association of Sites Advocating Child Protection
CAI	Child Abuse Images
CEOP	Child Exploitation and Online Protection Centre
CIRCAMP	COSPOL Internet Related Child Abuse Material Project
COSPOL	Comprehensive Operational Strategic Planning for the Police (European Police Chiefs Task Force)
CALF	Child Abuse Link Farm
EC	European Commission
EFC	European Financial Coalition
FACS	Flagging and Co-ordination System
FCACP	Financial Coalition Against Child Pornography (US)
I&TWG	Internet & Technology Working Group
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
IWF	Internet Watch Foundation
LEA	Law Enforcement Agency
LECWG	Law Enforcement Co-operation Working Group
LeWG	Legal Working Group
MLF	Model Link Farms
NCMEC	National Center for Missing and Exploited Children (US)
NGO	Non-Government Organisation
PIWG	Payments Industry Working Group
UK	United Kingdom
URLs	Universal Resource Locator
US	United States


ALLEN & OVERY
CEOP
EUROPOL
EUROJUST
International Centre
FOR MISSING & EXPLOITED CHILDREN
MasterCard
Microsoft
Missing Children Europe
PayPal
VISA