NETCLEAN REPORT 2018

A REPORT ABOUT
CHILD SEXUAL ABUSE CRIME

INTRODUCTION

RESULTS

SUMMARY

FOREWORD

THE MORE WE LEARN ABOUT THIS CRIME, THE MORE POWERFUL OUR RESPONSE CAN BE

The results in this year's NetClean report are not as clear-cut as in previous reports, where we considered big prevailing trends that showed a marked increase in child sexual abuse material, the level of violence directed at children and challenges derived from technological developments.

In this year's report we look in more detail at particular topics such as: self-produced material; developments in technologies; how such developments affect the way offenders operate; and the impact that this has on law enforcement investigations. This more detailed look has to a certain extent produced the contradictory result that we see in this report.

My analysis of these results is that we may be looking at two different groups of offenders who consume child sexual abuse material, and the gap between them.

The first group contains the majority of offenders. They are averagely technically astute and mainly consume child sexual abuse material that is readily available on the internet. Even though they might hoard material and exhibit compulsive behaviour around child sexual abuse material, they do not show any significant sophistication when they operate on the internet.

The second, smaller group, consists of offenders that are more sophisticated and very technologically astute. They are probably organised into groups and can use encryption and other technologies to avoid detection. Some might use crypto currencies to buy and sell child sexual abuse material.

The results might indicate that the gap between these two groups is widening. The more advanced offenders are becoming more advanced, organised and sophisticated in their use of technology. This group is probably not growing quickly in size. The other group, represents the big increase in people who consume child sexual abuse material. Their methods, however, remain the same.

This bigger group, consists of people who can be found by involvement from civil society and key figures such as employers. In last year's report we revealed that there is no such thing as a stereotypical offender who consumes

child sexual abuse material, however the data revealed that most are in employment. This makes the workplace a prominent place to identify this type of offender.

To build on this, we broadened this year's report by surveying employers to learn from their insight and experience of finding child sexual abuse in their IT environments. The data shows insight into how child sexual abuse crime is handled in the workplace, and revelations about how offenders react when they are confronted by their employers.

I am convinced that building and sharing knowledge about all aspects of this crime is the key to preventing it. In a world where technology is constantly developing, we need to ensure that we keep up with those developments and share what we know. Technology in itself is not the problem, we just have to use it to our best advantage to prevent crime, safeguard children and stop offenders.

We also need to ensure that there is better general understanding of offenders who abuse, document and consume child sexual abuse material. If we understand what drives them, we can find a way to stop their impulse to offend. More knowledge about the dissemination of material on the internet will aid work to remove images and films, and stop the abuse that generates this material.

I am pleased to introduce the fourth NetClean Report. It adds to the growing knowledge bank worldwide about child sexual abuse, and it brings a unique insight into what law enforcement and employers do to stop this crime.

Anna Borgström,
CEO, NetClean

INTRODUCTION BY DR VICTORIA BAINES

TECHNOLOGICAL DEVELOPMENTS HAVE FAR OUTSTRIPPED OUR EXPECTATIONS

We have entered the third decade of the global fight against child sexual abuse material (CSAM). In this time, law enforcement, policy makers, industry, civil society organisations, academic researchers and others have come together to develop truly innovative solutions.

Technological developments have far outstripped our expectations, changing beyond recognition how we all interact. They have had a hugely beneficial impact on children and young people, but also exposed them to the risk of sexual exploitation and abuse. And they have presented ever-evolving challenges to those whose job it is to protect children and combat offending.

From images to virtual reality

When I started my career in law enforcement, we were preoccupied with offenders who used their credit cards to buy photographs from websites. We were able to identify them by tracking payments and resolving their IP addresses. Then came the advent of chat rooms and social media, and for the first time adults and young people had the opportunity to interact in large numbers online. Grooming via social sites emerged, with the aim of meeting children offline for sexual activity. As digital camera and photo sharing capabilities rapidly improved, we witnessed an increase in the solicitation of CSAM directly from children and young people.

We are now in a new era, where self-generated CSAM is live-streamed, and where we are all having to think about how best to deploy emergency support to children and young people who may be experiencing crises in real time. Offenders, meanwhile, have taken full advantage of the technology at their disposal, making use of end-to-end encryption, darknet tools and cryptocurrencies to obscure their activities. Looking ahead, we are preparing ourselves for what child sexual exploitation and abuse (CSEA) may look like in emerging environments such as virtual and augmented reality, and what artificial intelligence may mean for efforts to combat CSAM.

Technologies to prevent abuse

At the same time, we have come to realise that technology is as fundamental to combating online child sexual exploitation as it is to its commission. As a global community of partners, we

started by focusing our efforts on identifying the victims – through the International Child Sexual Exploitation (ICSE) database – and, with Microsoft's PhotoDNA, removing the material. NetClean has played and continues to play an important role in the deployment of technological solutions in the community, especially in workplaces. Most recently, Canada's Project Arachnid has shown how machine learning can assist in the proactive identification and removal of CSAM.

More knowledge produces better results

This fight is everyone's responsibility. It requires you, me, and everyone on the planet – regardless of their role or affiliation – to make our best effort to prevent, combat and report the sexual abuse of children. Technology promises to assist not only in removing illegal material and bringing offenders to justice, but also in supporting children and young people who are victims or at risk of abuse, adults with potential to offend against children, and all those who work with them.

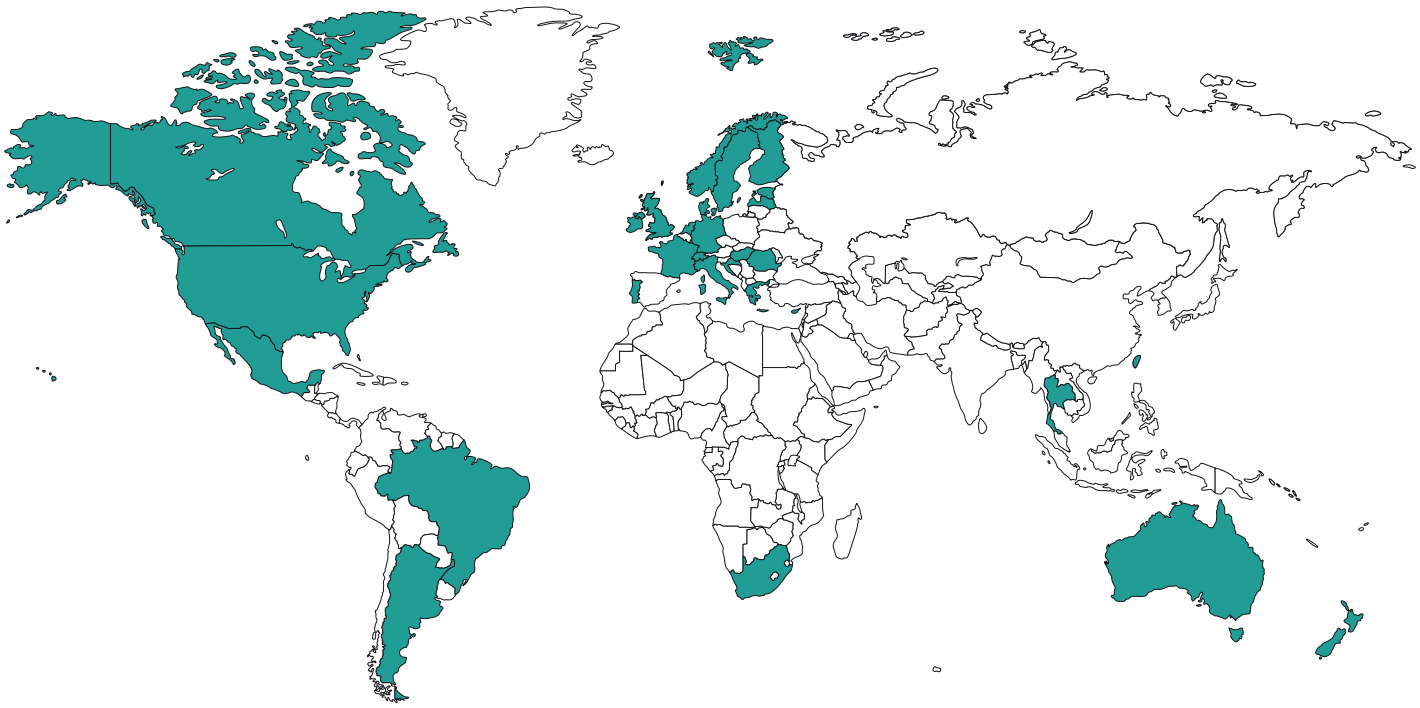
The more data we have on a problem, the better our decision-making and response measures will be. As a threat analyst by training, I constantly ask myself and others to challenge our assumptions on CSEA, and to base counter-measures on evidence. Technology now enables us to better understand CSEA online, to track changes in offending in live time, and to share this knowledge with partners in the global child protection community. The analysis presented in this report is a clear step forward, an evidence base that we can use to protect more children from sexual abuse. It is an honour for me to introduce it to you.

ABOUT THE AUTHOR

Dr Victoria Baines is a leading authority on online safety. Her most recent research examines international responses to online child sexual exploitation. Until 2017, Victoria was Facebook's Trust & Safety Manager.

Prior to this she spent a decade in law enforcement, as Principal Analyst at the UK CEOP Centre, and lead for Strategy & Prevention at the European Cybercrime Centre (EC3).

Victoria is a Visiting Associate of the Oxford Internet Institute and a Visiting Fellow at Bournemouth University. She serves on the Advisory Board of the International Association of Internet Hotlines (INHOPE).



ABOUT THE NETCLEAN REPORT 2018

The NetClean Report 2018 is the fourth report in this series. The aim of the Report is: to ensure greater awareness of and more insight into child sexual abuse crime; to contribute to effective ways of stopping the dissemination of child sexual abuse material; and, ultimately, to reduce the sexual abuse of children. The data in this report has been collected through two different enquiries that are set out below.

Part one: The experience and perspective of the police

Part one of this report is based on data collected from police officers across the globe who work on cases pertaining to child sexual abuse crime.

The respondents have contributed by filling out a survey anonymously. They are all users of Griffeye Analyze DI Pro and Griffeye Analyze DI Core, both investigative tools used by the police across the world to analyse images and video. Griffeye is NetClean's sister company.

The enquiry, an online survey, was undertaken between 2 May and 13 August 2018 and administered through Griffeye's user portal. 272 police officers from 30 countries participated in this year's survey. 54.4 percent of the respondents are from the US, and 34.7 come from Europe.

In this year's report we have chosen six areas at which to look more closely. They are:

1. Self-produced material.
2. Additional issues relating to grooming, sexual extortion and trafficking.
3. The level of organisation amongst offenders in forums and groups.
4. The use of cryptocurrencies to pay for child sexual abuse material.
5. Challenges that police officers face as a result of the manipulation of images and obfuscation techniques.
6. Whether new technology such as deepfakes are already present in child sexual abuse investigations.

These issues were selected based on intelligence gathered in the previous NetClean Reports, and from conversations with police officers about what they believe is relevant at this time.

272 respondents from 30 countries:

Argentina; Australia; Brazil; Canada; Croatia; Cyprus; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Ireland; Italy; Latvia; Mexico; Netherlands; New Zealand; Norway; Portugal; Romania; Switzerland; South Africa; Sweden; Taiwan; Thailand; United Kingdom; Unites States of America; and "other", which signified that the respondent work for an international organisation like Europol or INTERPOL.

Geographic distribution of respondents:

USA 54.4 %
United Kingdom 12.1 %
Sweden 6.6 %
Norway 3.7 %
Canada 2.9 %
Others 20.3 %

Interviews in the report:

To contextualise the results of the study, we have conducted interviews with a number of distinguished experts in this field, listed here in the order in which they appear in this report:

Dr Victoria Baines
Leading authority on online safety. Visiting Associate of the Oxford Internet Institute. Visiting Fellow at Bournemouth University. Member of the INHOPE Advisory Board

John Shehan
Vice President, Exploited Children Division (ECD), National Center for Missing & Exploited Children (NCMEC)

Cathal Delaney
Head of team, Analysis Project Twins, EC3, Europol

Thomas Andersson
Senior Advisor, ECPAT Sweden

Christian Berg
Founder, NetClean

Anna Borgström
CEO, NetClean

Björn Sellström
Team Leader, Crimes Against Children Unit, Vulnerable Communities Team, INTERPOL

Patrick Cordner
Head of Swedish Cybercrime Center (SC3), National Operative Department, Swedish Police

Michael Sheath
Manager & Principal Practitioner, Lucy Faithfull Foundation

With regards to deepfakes we wanted to know if this new technology is being used to produce child sexual abuse material, as it is a good indicator as to how quickly new technology is appearing in these types of investigations.

There are fewer respondents to this year's survey compared with previous years. However, in addition to the respondents, 250 people logged on to the survey without answering the questions. We attribute the reduced number of respondents to the fact that this year's questions were more complex than previous years, and required that the respondent work on advanced and in-depth investigations.

The experience and perspective of business

Part two of the report contains in-depths interviews with businesses and organisations from both the private and public sector that use NetClean ProActive to detect child sexual abuse material in their IT environments.

The businesses and organisations that were interviewed have in total 269,370 clients (software) installed on their computers. The installation period of NetClean ProActive in their IT environments ranges from two to eleven years. The responses were given anonymously and as one shared experience.

In the interviews we asked the businesses and organisations to share the data that they have collected about the person or persons who have consumed child sexual abuse material using a workplace computer and therefore triggered NetClean ProActive. We asked about: gender; age; profession; relationship status; and whether they have children. We also asked about the time of day (or night) that the alarm was triggered; how the offender consumed the material; how they reacted when they were challenged about it; and whether more child sexual abuse material had been discovered or other types of material considered a security issue or a breach of company policy had been found.

The companies that responded to these questions have found online child sexual abuse material in their IT systems in Europe, North America, Asia and South America.

The results generated from this survey is presented anonymously and as one shared experience.

EIGHT INSIGHTS INTO CHILD SEXUAL ABUSE CRIME

01

Self-produced material
Voluntarily self-produced material is most common

02

Grooming, sexual extortion and trafficking
Children of all ages are groomed and extorted

03

Organised offenders
Groups consist of thousands of individuals

04

Cryptocurrencies
Often connected to other types of crime

05

Manipulated and hidden images
A challenge for investigators

06

Technical development
One in five police officers has found deepfakes

07

Child sexual abuse crime in the workplace
One in 500 employees

08

Work computers used for child sexual abuse crime
Most common outside office hours

THE POLICE'S EXPERIENCE AND PERSPECTIVE OF INVESTIGATIONS INTO CHILD SEXUAL ABUSE CRIME

Topics covered in this year's report

We have in our previous reports seen recurring themes in the respondents' answers. One of these themes concerns self-produced material and another the challenges that arise from developments in technology.

In addition to looking at these themes we also asked police officers what else they would like to see included in this year's report.

As a result, the focus of this year's NetClean Report is as follows:

1. A general view of self-produced material.
2. A more detailed look at grooming, sexual extortion and trafficking.
3. The level of organisation amongst offenders in forums and groups.
4. Cryptocurrencies and their use in paying for child sexual abuse material.
5. Challenges faced by police officers because of the manipulation of images and obfuscation techniques.
6. If and how new technology, such as deepfakes, is already present in child sexual abuse investigations.

01 Self-produced material – Voluntary self-produced material is most common

Self-produced material is highlighted as an important issue in all three previous NetClean reports. In this year's report we therefore look closer at how big a problem police officers believe self-produced material to be, what types are most common, and what future trends are likely to be.

SELF-PRODUCED MATERIAL

Self-produced material can be found within a broad spectrum of images produced with different intended uses. We have chosen to divide the images into five different categories. We talk about images here, but this material can also include moving content.

1. "Innocent Images"
These are every day pictures, e.g. holiday snaps from the beach or home, that end up in a collection of child sexual abuse images. These images are often taken by the child's parents or relatives, but can also be taken by the child themselves.

2. Voluntarily self-produced material
These are undressed images where children or teenagers have taken pictures of themselves. They have subsequently found their way into collections of child sexual abuse images. These images may have been produced with the intent of sending them to a boyfriend or girlfriend.

3. Images produced as a result of grooming
These images have been produced and sent to the offender as a result of grooming. Grooming is a process whereby the offender slowly builds up a relationship with a child to win their trust and confidence.

4. Images produced as a result of sexual extortion
These images have been produced as the result of threats and extortion, often referred to as "sextortion". Grooming can develop into sextortion, or the offender might threaten the child from the start.

5. Images produced as a result of trafficking
This is where children have been forced to pose for or produce images in the context of trafficking; where they are sold and bought for sexual abuse.

SELF-PRODUCED MATERIAL IS COMMON

The result of the survey shows that all categories of self-produced material, apart from material taken in trafficking situations, are common or very common in police investigations.

Voluntary self-produced material is most common and on the rise

More than 90 percent of the surveyed police officers report that it is common or very common to see voluntarily self-produced material in investigations. Almost 60 percent of the police officers report that the most common category is voluntarily self-produced images, and close to 90 percent of the police officers report that this type of material is on the increase.

Grooming and sexual extortion

Images that are a result of grooming and sexual extortion were also described as commonly featuring in investigations.

Three quarters of the surveyed police officers report that it is common or very common to see images that are a result of grooming in their investigations. Just over one fifth report that this category is the most common in their investigations. The results indicate that this type of material is not increasing as quickly as voluntarily self-produced material. Although more than half of the police officers report that images as a result of grooming are on the rise, slightly more than 40 percent report that they are neither increasing nor decreasing.

Almost two thirds of the surveyed police officers report that is common or very common to see images that are a result of sexual extortion in their investigations. The trend around these images follows that of images produced as a result of grooming. Almost 60 percent of the police officers report that images as a result of sexual extortion are on the rise, while just over 40 percent report that they are neither increasing nor decreasing.

A reflection, or reservation, about the numbers above is that some of the police officers report that it can be difficult to determine if an image has been produced voluntarily or if it is as a result of grooming or sexual extortion.

> " It is very difficult to assess the 'genesis' of an image...an image that appears to be voluntarily self-produced can easily be that of sextortion."

> " Can't be sure which self-produced images are voluntary or the result of grooming/coercion."

Innocent Images

Along with the material discussed above, innocent images are also present in the surveyed police officers' investigations. Close to 60 percent of the police officers report that it is common or very common to see these types of images. More police officers, just over three quarters, report that this

category of material is neither increasing nor decreasing. Only one quarter report that the prevalence of innocent images is increasing.

Images from the trafficking category are reported on differently to the other categories of self-produced material. Only one quarter of the surveyed police officers report that it is common or very common to see images that are a result of trafficking. A third report that it is uncommon or very uncommon to see these types of images. Three quarters say that they do not believe that this category is increasing or decreasing.

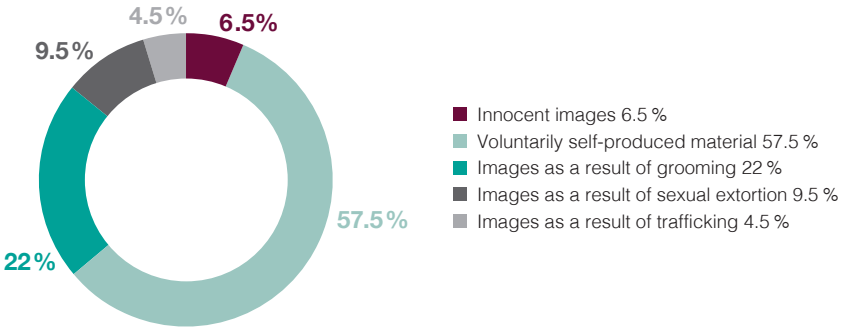
The respondents pointed out that it can be difficult to determine exactly under which circumstances the images has been produced; especially where there is no additional information about the child in the image.

" Last question is difficult. How do you know if the child was trafficked?"

HOW COMMON DIFFERENT TYPES OF SELF-PRODUCED MATERIAL ARE.

	Very uncommon	Uncommon	Neither common nor uncommon	Common	Very common
Innocent images	6.1%	12.8%	22.4%	36.7%	21.9%
Voluntarily self-produced material	3%	2%	3.5%	38.9%	52.5%
Images as a result of grooming	3.6%	4.1%	16.3%	49.5%	26.5%
Images as a result of sexual extortion	3.1%	11.2%	20.4%	47.4%	17.9%
Images as a result of trafficking	13%	22.3%	39.9%	17.6%	7.3%

THE MOST COMMON TYPE OF SELF-PRODUCED MATERIAL.



WHETHER DIFFERENT TYPES OF SELF-PRODUCED MATERIAL ARE INCREASING OR DECREASING.

	Decreased	Neither increased nor decreased	Increased
Innocent images	8.8%	66%	25.3%
Voluntarily self-produced material	0.5%	10.2%	89.3%
Images as a result of grooming	2.1%	43.0%	54.9%
Images as a result of sexual extortion	1.6%	42.2%	56.3%
Images as a result of trafficking	3.2%	75.3%	21.6%

02 Grooming, sexual extortion and trafficking – Children of all ages are coerced and threatened

To further contextualise the issue of self-produced material we asked additional questions about the material generated as a result of grooming, sexual extortion and trafficking.

GROOMING AND SEXUAL EXTORTION – CHILDREN IN ALL AGE-BRACKETS

In the survey we asked police officers to state the ages of the children that they see in images that have been produced as a result of grooming and sexual extortion.

The results show that children of all ages are prevalent in investigations; both in images produced as a result of grooming and through sexual extortion. The range of the ages runs from children that are younger than five years old up to eighteen. When the surveyed police officers were asked to point to the most common age, all age brackets were included in the answers. However the more detailed questions show that some age brackets feature more heavily than others.

Most common: 8–16 years

In cases concerning grooming most children fall into the bracket of eight to sixteen years of age, with the majority being between the ages of eleven to thirteen years old. In cases concerning sexual extortion, ages are slightly higher with most children being between the ages of eleven to sixteen years old.

Younger children can also feature

According to the police officers, younger children also feature in the investigations. Roughly 16 percent report that children younger than five years old have featured in grooming investigations, and close to a third report that they have seen children between the ages of five to seven years old.

INFORMATION ABOUT AGE BRACKETS PERTAINING TO SELF-PRODUCED MATERIAL.

	Grooming		Sexual Extortion	
	Age brackets encountered	Most common age bracket	Age brackets encountered	Most common age bracket
< 5 years	16.4%	7.4%	7%	4.2%
5–7 years	26.9%	13.2%	11.1%	7.9%
8–10 years	58.2%	34.9%	26.5%	11.6%
11–13 years	70.4%	55.6%	66.7%	47.6%
14–16 years	47.1%	32.3%	60.3%	51.9%
17–18 years	19.6%	6.9%	28%	11.1%

This table shows the extent to which the respondents have seen the respective age categories in their investigations, and which age category is most prevalent. The respondents were able to tick several answers.

Seven percent of police officers report that they have seen images of children younger than five years old in cases pertaining to sexual extortion, and one in ten report that they have seen children between the ages of five to seven years old.

GROOMING AND SEXUAL EXTORTION – NO MAJOR CHANGE

Almost a third of the surveyed police officers report that they have not seen a marked difference in grooming and sexual extortion cases over the past three years.

The quarter who have seen a difference report that the number of cases concerning sexual extortion is increasing; that they see more instances of grooming that progress to sexual extortion; that there has been an increase in the use of apps for messaging in these types of cases; and that the children they see in their investigations are becoming younger.

“ Sexual extortion cases are now 20–30% of our squads case load and has increased over the last five years. […]”

“ It tends to start out as grooming, but gets nasty when the child tries to stop the communication. This is where the extortion starts.”

“ Most of the grooming and extortion is now coming from social media apps; unlike a few years ago where most of it occurred by someone that had access to the child.”

“ Younger (prepubescent) children are being extorted.”

SEXUAL EXTORTION – THREATS TO OBTAIN MORE IMAGES

In sexual extortion cases it is almost always the case that children are forced to send more undressed images or films to the offender. Some of the surveyed police officers report that the children have been extorted for money. Some also report that children can be extorted into live-streamed abuse or be made to meet the offender in person to suffer physical sexual abuse.

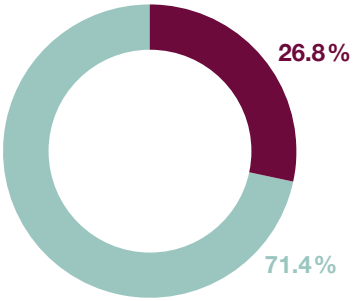
Threats that the images will be shared

The main threat made towards children is that undressed images of the child will be circulated either online or to people the child knows. Just under a third of the police officers also report that it is common to see threats of physical harm against the child's family. Other threats mentioned are: threats of violence towards the children themselves; threats to divulge information that the child has given in confidence; and threats that the offender will tell the police about the child.

> " The threats vary widely, but generally they're either direct threats against the children themselves, more often their family (especially if the children are young) or threats of spreading the images (usually common among 14-18 year old children)."

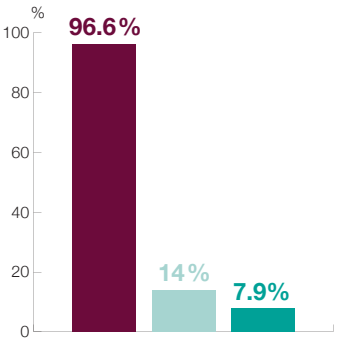
> " For older children, threats to expose to people they know. for younger children, threats to expose to family/ parents."

WHETHER GROOMING OR SEXUAL EXTORTION CASES HAVE CHANGED IN THE PAST THREE YEARS.



- Yes 28.6%
- No 71.4%

WHAT THE CHILDREN ARE EXTORTED FOR.

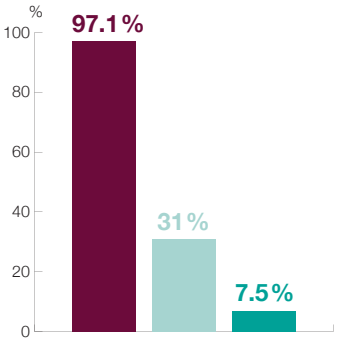


- More images 96.6%
- Money 14%
- Other extortion purposes* 7.9%

* Mainly live-streamed abuse or physical meetings with the offender.

The respondents were able to tick several answers.

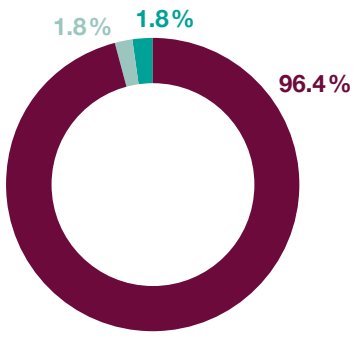
TYPES OF THREATS IN CASES OF SEXUAL EXTORTION.



- That images of the child will be posted on the internet or to people that the child knows 97.1%
- Threats against the child's family 31%
- Other threats: Mainly threats towards the child; threats that information that they have given in confidence will be shared; or threats about reporting the child to the police 7.5%

The respondents were able to tick several answers.

THE **MOST COMMON** TYPE OF THREAT IN CASES OF SEXUAL EXTORTION.



- That images of the child will be posted on the internet or to people that the child knows 96.4%
- Threats against the child's family 1.8%
- Other threats: Mainly threats towards the child; threats that information that they have given in confidence will be shared; or threats about reporting the child to the police 1.8%

02 Grooming, sexual extortion and trafficking – Children of all ages are coerced and threatened, cont.

NO CLEAR CONNECTION TO TRAFFICKING

More than 80 percent of the surveyed police officers report that they do not see a connection between child sexual abuse images and trafficking in their investigations. .

" I haven't had a case yet where the two could be proven that they were connected."

" Haven't had any cases that have this connection this year."

Live-streaming or "marketing"

The police officers who report that they have seen a connection mainly point to cases of live-streaming where offenders pay for streamed material featuring children; most commonly in Asia. Some point to images that have been produced to "market" children who are sold for sexual abuse purposes, or that the images are a result of documenting physical abuse, and that the images themselves were therefore a bi-product of the abuse.

" Live-streaming is becoming a big problem. Children in Thailand or the Philippines and parts of Eastern Europe and Africa are being trafficked for child sexual abuse material."

" Images and videos are taken to advertise the child. The material is then shared on a closed group setting, dark web or if the child is older, on Craigslist."

" In the images that I have seen of trafficking it is clear that the child has been bought for sex and the images that are produced are for "capturing the moment", rather than the child being bought specifically for taking images of them to share."

The main aim is to make money

The surveyed police officers who do not see a connection between child sexual abuse material and trafficking express that view because trafficking is closely connected to organised crime and money. According to them images are not produced as an end in themselves, but rather constitute a risk for the offender.

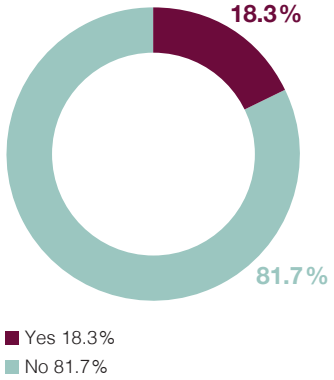
" The merging of commercial sex trafficking with child abuse images is not correct. Can the production of child abuse material result in commercial sex trafficking of children? Yes, but the vast majority of commercial sex trafficking is done for money not the production of child abuse material."

" I have never seen a link. I am surprised as I would have thought there would be adverts. However, in the cases of abusers of trafficking being arrested, NO images have ever been found on their devices. This is more organised crime fuelled by money so they know that taking images is highly risky which differs to abusers who do this for sexual thrills."

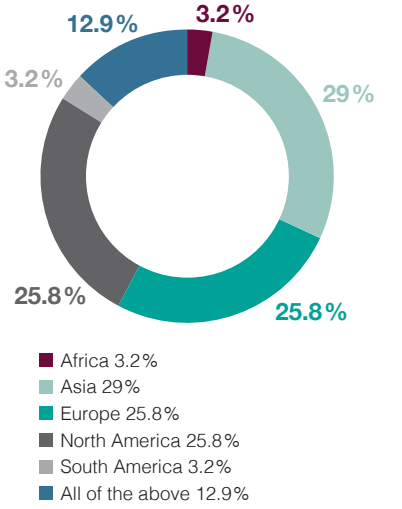
Most common in Asia, Europe and North America

The surveyed police officers report that the connection that exists between trafficking and child sexual abuse material is not dependent on where it happens in the world. This connection is strongest in Asia, Europe and North America. In the NetClean Report 2016, we asked where the children in the sexual abuse material came from and the answer was that the images derived mainly from North America, Europe and Asia. According to the 2016 research it was less common to see children from Asia. However this year's research showed that child sexual abuse material linked to trafficking was seen to be just as common in all three continents.

POLICE OFFICERS' INSIGHT INTO WHETHER THERE IS A CONNECTION BETWEEN THE PRODUCTION OF CHILD SEXUAL ABUSE MATERIAL AND TRAFFICKING.



POLICE OFFICERS' INSIGHT INTO WHERE IN THE WORLD THERE IS A CONNECTION BETWEEN CHILD SEXUAL ABUSE MATERIAL AND TRAFFICKING.



COMMENT ON INSIGHT 1 AND 2

John Shehan, Vice President, Exploited Children Division (ECD),
National Center for Missing & Exploited Children (NCMEC)

There has been a significant increase in self-produced material

This NetClean Report data about self-produced material matches the data patterns that we see at NCMEC. We have seen a significant rise in this type of material over the past ten years. It is, however, important to highlight that the majority of child sexual abuse material is still produced by people in close proximity to children, e.g. a parent, grandparent, more distant relative, coach or similar.

Increase in grooming and sexual extortion

When looking at grooming and extortion, our data points to a greater increase in grooming and sexual extortion than the NetClean Report does. We have been tracking child grooming and sexual extortion crimes since 2013 and have seen an increase in cases (2015-2016) of 150 percent; a number that is continuing to rise.

There are also a large number of hidden cases. Behind every discovered case there are often tens or hundreds of other victims that the offender has groomed and extorted. The majority of those victims do not come forward and continue to comply with the offender because of threats of material being posted on social media and sent to the victim's parents.

Similar to the NetClean Report, our data suggests that children are extorted primarily for more images. We have also seen a development in how offenders operate. They are now moving children increasingly quickly off gaming platforms, onto social media and then onto video platforms that are not as closely monitored. Likewise, the conversation is now moving quicker from innocent messages to explicit demands and threats. With the increased use of the video format the demands have become increasingly graphic. This is because the offender is able to ask for material with motion and sound, rather than just an image.

The children range from 8 to 17 in age

Examining the extortion material in our database, we see that the age range of the children is between 8 and 17 years old, with an average age of 15 years. 78 percent of the children are girls. We have not come across children younger than 6 or 7 years old, and I would say that when that happens, those cases are anomalies, and the result of older siblings having been groomed or extorted into involving them.

Trafficking is a complicated issue

A less clear-cut area concerns images connected to trafficked children. It can often be difficult to determine how old these children are, because of the make-up and attire that they are made to wear. These images are often not as sexually explicit or undressed as other types of child sexual abuse material. We are currently working with a number of large technology companies to help them develop indicators for the trafficking of children.

An important component in our work to stop the dissemination of child sexual abuse material is our hash list which we share with our partners. We are continuously developing this list and we are working to add a hash list of self-produced material. The aim is to help those children get the images and videos removed from the Internet.

NCMEC

NCMEC (National Center for Missing and Exploited Children) is the US' national clearing house for reports on child sexual abuse material for US based IT companies. NCMEC also operates a hotline where the public can report suspected child sexual abuse material.

03 Organised offenders – Groups consisting of thousands of people

In the NetClean 2017 Report, we looked at: whether there is such a thing as a typical consumer of child sexual abuse material; the correlation between consuming child sexual abuse material and physically abusing children; and how offenders come into contact with children. In this year's report, we focus on: how offenders organise themselves in internet forums and groups; and whether the level of organisation has changed over time.

A MAJORITY OF POLICE OFFICERS HAVE ENCOUNTERED ORGANISED GROUPS

The majority of surveyed police officers (85%) report that they have encountered organised forums and groups of offenders in their investigations. Amongst those who have not come across this sort of activity, they refer to the fact that they do not work on cases that lead them to investigate this type of online criminal activity.

" In my specifics there is no monitoring of forums and groups."

A large majority of police officers report that they have worked on investigations where they have seen one to ten organised forums over a period of three years. However, a larger majority report that they mainly come across individual offenders in their cases.

" We've mostly encountered single offenders who have had contact with individual, single offenders rather than organizing themselves in any kind of forums."

A fifth of the surveyed police officers report that they have worked on investigations where they have encountered up to fifty organised groups over the past three years. A small segment have seen 100–500 organised groups. A handful have seen more than one thousand, or several thousand, forums. They explain (analogously to the police officers above who do not work in this area), that they have seen so many forums and organised groups because they work specifically on these types of cases.

" We have identified hundreds of forums and groups connected to different organizations, however we find the same individuals in different forums with the same alias."

" Impossible to estimate. I mostly only investigate organized forums or groups of offenders, it's always networks."

INDICATIONS THAT THE NUMBER OF GROUPS IS INCREASING

Just under half of the surveyed police officers report that the number of organisations has increased. A third of the police officers report that they have neither increased nor decreased. There has been no clear trend concerning the increase of forums and groups used by offenders over the past three years.

GROUPS OPERATE ON DARKNET AND THE OPEN INTERNET

According to the surveyed police officers, the forums exist in equal numbers on the open internet and the darknet/TOR. The police officers report that offenders use social media apps, or messaging apps, to communicate via direct message. The applications most commonly mentioned by the police officers are KIK, WhatsApp, Telegram, Facebook and Skype, and in addition links are shared through tools such as Dropbox*.

" Put it this way, the vast majority of material is on the open web. They make contact with people of similar interest and trade indecent images of children."

" Telegram groups disseminating images/videos and links to cloud storage."

" Any platform that facilitates group communication e.g. Facebook, Messenger Apps, certainly darknet groups."

" The dark web still plays a very significant part in organised crime groups involving child sexual exploitation and indecent images of children offenders."

VARIED SIZE OF GROUPS

When answering a question about the size of the groups of offenders, the surveyed police officers' answers vary from 2 people to 5,000–6,000 individuals. According to the report the biggest forums consist of 100 000–200 000 individuals, and one police officer reported that they worked with a forum that consisted of one million individuals.

** You can find more information and analysis about the social media platforms and applications that are most prevalent in police investigations in the NetClean Report 2016.*

OFFENDERS ARE GETTING MORE ORGANISED

More than half of the surveyed police officers report that how offenders organise themselves and the level of organisation within the forums is changing. According to almost half the surveyed police officers, groups are becoming increasingly organised, while one in ten reports that the offenders are becoming more careful. Only five percent report that the groups have become less organised.

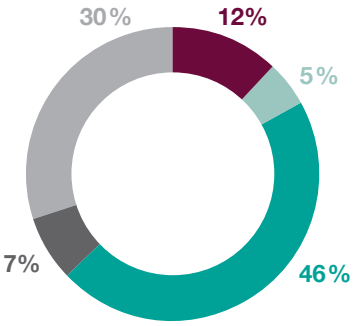
" They are becoming more organized and creative in ways to hide their activity and identities."

" The organized are more organized, and focus on crypto and anonymity, groups on Skype, for example, are more open, using their own IP addresses."

" It is remaining constant ... organised groups, with hierarchies and security etc, have existed for a long time."

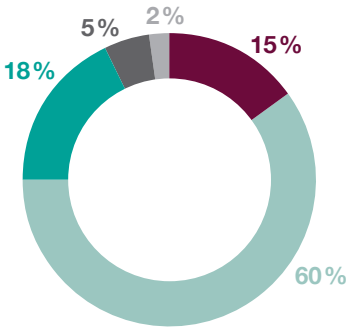
" Less organized as they frequently create new groups."

WHETHER THE DEGREE OF ORGANISATION WITHIN FORUMS AND GROUPS OF OFFENDERS HAS CHANGED AND IF SO, HOW.



- No change 12%
- Decreasingly organised 5%
- Increasingly organised 46%
- More careful 7%
- Don't know/N/A 30%

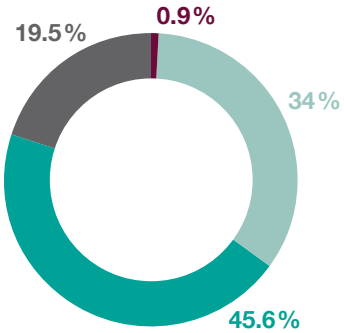
ESTIMATED NUMBER OF FORUMS ENCOUNTERED BY POLICE OFFICERS OVER THE PAST THREE YEARS.



- 0 not N/A*: 15%
- 1–10: 60%
- 11–50: 18%
- 100–500: 5%
- More than 1000: 2%

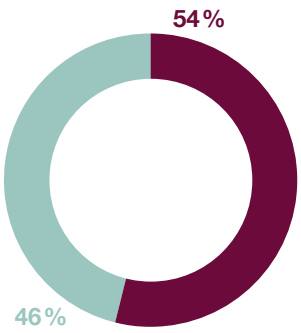
* N/A: The respondents reported that they work on cases where these types of forums are not part of the investigation.

WHETHER THE NUMBER OF ORGANISED FORUMS AND GROUPS OF OFFENDERS HAS INCREASED OR DECREASED OVER THE PAST THREE YEARS.



- Decreased 0,9%
- Neither increased or decreased 34%
- Increased 45.6%
- Don't know/do not wish to comment 19.5%

THE LOCATIONS OF ONLINE ORGANISED FORUMS AND GROUPS OF OFFENDERS.



- The open internet*: 54%
- Darknet/TOR 46%

* This includes social media applications, chat apps and similar ways to communicate through direct messaging.

Cathal Delaney, Head of Team, Analysis Project Twins, EC3, Europol

Offender groups are becoming more organised and businesslike in their set-up

In Europol's recent report Internet Organised Crime Threat Assessment (IOCTA) 2018, we looked, amongst other things, at the level of organisation among online offender forums and groups. We have growing intelligence pointing to increased organisation among particular users, especially on the darknet. The information to support these conclusions is contributed by Europol member states, which affords us a good overview of the situation and allows us to draw conclusions with a reasonable degree of accuracy.

Detailed and consistent advice

The conversations in different forums highlight that key individuals are increasingly sharing advice on things like anonymisation techniques and encryption on a more detailed, widespread and consistent level than before. This sort of advice on how to take precautions to hide online activity is not new, but there is now more structure around these conversations. It is the extent of advice and consistency in the messages that is new.

The forums themselves are also becoming more organised and businesslike in structure. In many cases individuals perform specific roles to ensure the efficiency of the forum. This points to the fact that the forums are developing.

A change in how individuals communicate

We have also seen a development in how people who belong to these online groups communicate. To start with groups who used different direct messaging services were formed through invitations on the darknet. Now they do not necessarily coexist in the same space, and do not move from one technology to the next as frequently as before. The individual choice of technology is most frequently based on what they are most comfortable using, and which technology they perceive to be the most secure; i.e. while one person chooses an app for direct messaging because it is perceived as the most secure technology, somebody else might be using the darknet for the same reason.

Groups and sub-groups

We don't know the exact number of online offender groups or forums. Larger forums typically consist of many smaller sub groups, and it is a pointless exercise to count them all. The groups may be divided on the basis of: shared language; shared country of origin; a proclivity for the same type of child sexual abuse material; or the same age range of children featured in the material. The variations of these groups are endless. Hence, we do not need to know exactly how many groups there are; it is enough for us to know that they pose a risk to children.

Europol and European Cybercrime Centre (EC3)

Europol assists the 28 EU Member States in their fight against serious international crime and terrorism. Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and help protect European citizens, businesses and governments from online crime.

“IT IS THE EXTENT OF ADVICE AND CONSISTENCY IN THE MESSAGES THAT IS NEW.”

04 Cryptocurrencies – Often connected to other types of crime

According to finance coalitions across the world, cryptocurrencies pose a current and future threat to victim identification efforts and investigations into child sexual abuse crime. With this in mind we focused some of our research into how police officers view the phenomenon of cryptocurrencies in their investigations today.

RELATIVELY RARE TO SEE CRYPTOCURRENCIES

Slightly more than two thirds of the surveyed police officers report that they have not worked on investigations where cryptocurrencies have been a factor. Some report however that the use of cryptocurrencies can be very hard to detect.

" We have not seen this in a case in our lab, though we have been made aware of the potential for the use of cryptocurrencies in obtaining contraband images."

" It's extremely hard to track or even discover in the first place."

Others report that cryptocurrencies are not used frequently because offenders tend to pay each other by swapping child sexual abuse material.

" Most child sexual offenders in my sphere of work go by the mantra that "don't pay for child sexual abuse material."

" […] Crypto's are too valuable to trade for media files. User's prefer to trade indecent images of children in return for indecent images of children."

Where police officers have worked on investigations where they encountered cryptocurrencies, more than half report that it is uncommon or very uncommon for cryptocurrencies to be used. Only one fifth report that it is common or very common.

OFTEN CONNECTED TO OTHER TYPES OF CRIMES

The same cohort report that the use of cryptocurrencies is most prevalent in live-streaming investigations, while others report that they mainly see the use of cryptocurrencies in other types of crimes.

" Seen in "live-streaming" cases."

" The typical consumer of child sexual abuse material […] has neither the knowledge or resources to dabble in cryptocurrencies. Some do, though, and the child sexual abuse cases that I have seen involving this almost always started as drug cases."

" Our cryptocurrencies cases are generally related to other crime areas, predominantly fraud and extortion."

BITCOIN MOST COMMON

According to the surveyed police officers, Bitcoin is the most commonly used cryptocurrency. However Etherium, Monero, Dash Litecoin, Electroneum and Ripple are also mentioned.

A CHALLENGE TO TRACE

According to those police officers who have come across cryptocurrencies, more than 60 percent report that the biggest challenge is to trace both the cryptocurrency and the offender. In addition, some police officers report that the investigations are more difficult because of their "international' reach. Some also report that there is a need for more training on this issue.

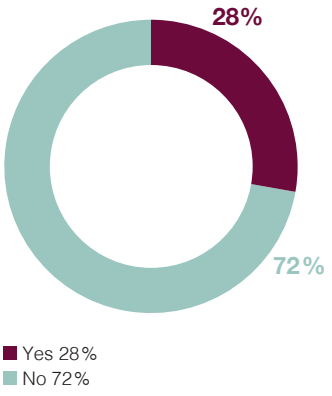
" Being able to follow up on the exchange and identify the people behind the trades, especially in dealing with other countries and the lack of support when serving legal paperwork."

" Difficulty tracking and difficulty with internal education to make investigators more aware of what to look for. Most digital forensics experts have a good knowledge of the subject but the main investigator might not know what to ask for or what possibilities there are."

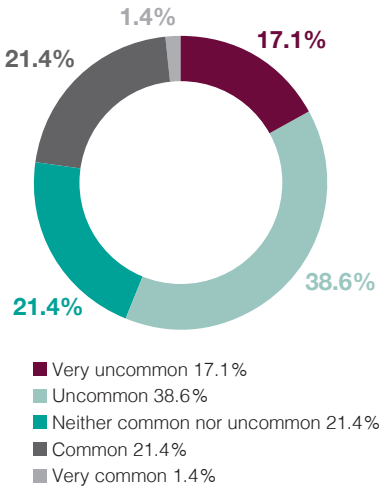
A few of the surveyed police officers also report that even if crypto-currencies are prevalent, they are in themselves not a major challenge to the investigative work.

" The issue still comes down to whether the images exist and are in the possession of the suspect, the use of such currencies is potentially an aggravating factor but not necessary to prove the offence. Clearly the biggest problem is identifying the internet account used in the first place."

PERCENTAGE OF INVESTIGATIONS WHERE CRYPTOCURRENCIES FEATURE.



PREVALENCE OF CRYPTOCURRENCIES IN INVESTIGATIONS (RESPONSE BY POLICE OFFICERS WHO HAVE ENCOUNTERED CRYPTOCURRENCIES).



Thomas Andersson, Senior Advisor, ECPAT Sweden

We see limited use of cryptocurrencies as payment for child sexual abuse material

In our experience it is extremely rare that child sexual abuse material is sold on the internet. Offenders either search for the readily available free material, or they trade images and films with each other. This is facilitated by big or small international online networks where offenders can discuss child sexual abuse and share material that they have produced. These spaces are also used to exchange tips, experiences and information about security issues.

Fake pages are common

With that said, we sometimes encounter what looks like ecommerce pages, or pages that seem to be commercial pages, but they are almost always a scam. Anyone who hands over their name and credit card details in order to buy child sexual abuse would be the perfect victim of a crime.

We have also seen pages on TOR that seem to be selling child sexual abuse material. The prices are given in Bitcoin, but as a rule there is no payment button. In order to pay, the offender has to email a ProtonMail address to get instructions for payment.

Payments using Bitcoin

One example is a page on TOR that purports to sell access to live-streamed child sexual abuse. The page used to advertise recurring events where they charged one Bitcoin to view and ten Bitcoin to direct the abuse. The value of one Bitcoin at that time was the equivalent of 7,000–8,000 SEK (ca. €650–770 or $US770–880 today, which is hugely more expensive than the couple of hundred kronor that Swedish offenders have been known to pay for live-streamed abuse from the Philippines).

It is possible that this site, along with other similar pages on TOR is fake and that those who pay don't get anything in return. These types of pages do however contain some of the most brutal child sexual abuse material that we have seen, posted with the purpose to "advertise" the content and to convince visitors that the site is real.

We have not seen cryptocurrencies in live-streaming cases

We have seen the use of internet based payment services connected to websites that sell web-cam shows as a means to pay for live-streamed child sexual abuse. However we have not seen request for cryptocurrencies there. I believe we have a problem on our hands if crypto-currencies are being used, as reported by some of the police officers in this report. Crime that has been facilitated by cryptocurrencies is very difficult to investigate and these crimes cause a great deal of suffering to child victims.

If we look to the future, new cryptocurrencies that come with increased security features could pose big challenges. However, there are so few users of this type of currency that the risks are relatively low. Producers of child sexual abuse material would find that their customer base would be too small if they insisted on using a niche cryptocurrency.

ECPAT Sweden

ECPAT Sweden is an NGO that works to combat all forms of child sexual exploitation. ECPAT Sweden is part of an international network of organisations based in more than 90 countries.

“NEW CRYPTOCURRENCIES THAT COME WITH INCREASED SECURITY FEATURES COULD POSE BIG CHALLENGES.”

05 Manipulated images and hidden images – A challenge for investigators

In our previous reports we asked police officers about the main challenges they face in their investigations of child sexual abuse material. In the NetClean 2016 Report, we identified that the major challenges were: encryption; anonymisation technologies; live-streaming; and deleters (people who consume material and then delete it). In the NetClean 2017 Report, we saw encryption and anonymisation technologies as the main challenges, but also cloud based services and use of chatrooms.

In this year's report, we have chosen to look more closely at the challenges police officers face when offenders hide or manipulate images in different ways. We asked questions relating to two different areas: how common is it that the content of an image is manipulated to make it difficult to identify people and/or places? And how common is it that offenders use obfuscation techniques to hide images or files on their computers or on the internet?

NO CLEAR-CUT ANSWER

The response to the question about hidden images does not present a clear picture. More than 45 percent of the surveyed police officers report that it is common or very common that offenders try to hide the files. However almost as many, nearly 40 percent, report that it is uncommon or very uncommon.

The statistics are similar in relation to the question about the manipulation of image content. Just over 40 percent of the surveyed police officers report that it was common or very common for offenders to manipulate images, and almost as many responded that it is uncommon or very uncommon for this to happen. In response to whether these techniques are becoming more common, almost half report that they are becoming more common, whereas the rest respond that they have not seen any changes to the trend. The following quotes illustrate the varied thoughts on this issue:

" Although we talk about this it rarely happens. Remember a suspect lives in his own bubble. They are lazy and need access to their material quickly. They are not necessarily techy […]"

" In about 10% of my cases they try to hide the material."

" Increased slightly but not insurmountable."

" Greatly increased – there are so many new and secure applications that provide encrypted storage. Also the web related applications which do not store any data."

THREE CATEGORIES OF CHALLENGES

The challenges that the surveyed police officers face from manipulation and obfuscation techniques can be divided into three categories. The first relates to the visual content in the pictures, the second to offenders trying to hide files, and the third relates to encryption.

Manipulation of images

The result of the survey shows that police officers encounter different types of manipulation of image content, often in an attempt to hide the background and identity of people depicted in the images. The most specific answer, from nearly a quarter (23 percent) of the surveyed police officers, was that the techniques are used to hide the victim's and/or offender's face. What they see most frequently is an attempt to erase the face, or the placement a black square or other type of image onto the face. Images can also be cropped to remove faces. The surveyed police officers also see images where a child's face has been edited into adult pornography, or where the face of a different child to the victim has been edited into the child sexual abuse material. In contrast to these methods, (and as a plausible explanation for the variation in responses as to how common it is to see the manipulation of images) Taskforce Argos highlighted in the NetClean Report 2017*, that images with hidden identities have a 'lower value' than those rich in detail within forums where child sexual abuse material is swapped.

Obfuscation techniques

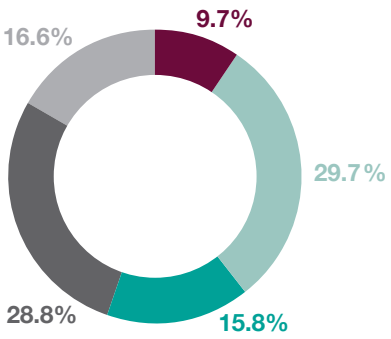
Another challenge is the work offenders put into hiding files. There are different methods such as filters in cloud-based services, hidden apps for images, using darknet/TOR, virtual machines or different anti-forensic approaches. Close to one fifth (18 percent) of police officers surveyed report that they often see attempts to hide that an image file is an image file. Roughly one out of ten police officers (13 percent) also mention attempts to hide material in complex file structures, and one out of ten (10 percent) report that they often see image files that have been placed in different types of files, such as a Word document or PDF.

Encryption

The most common challenge, which nearly a third (32 percent) of the police officers mention, is encryption. Where previous NetClean Reports have considered the challenges faced by the police officers in their investigations encryption has consistently featured).

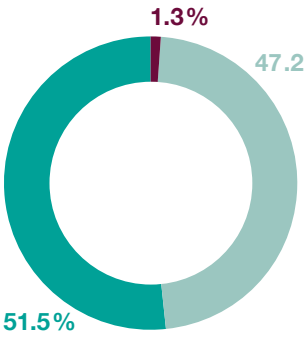
** The NetClean Report 2017. Comment on Insight 7: "We need to teach kids safe Internet behaviour"*

HOW COMMON IT IS TO FIND THAT OFFENDERS HAVE TRIED TO HIDE CHILD SEXUAL ABUSE MATERIAL.



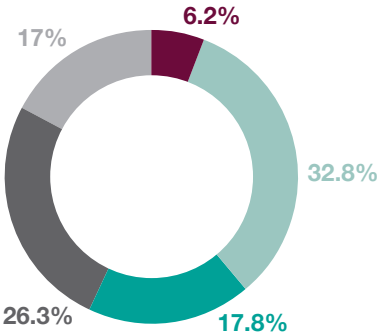
- Very uncommon 9.7%
- Uncommon 29.7%
- Neither common nor uncommon 15.8%
- Common 28.2%
- Very common 16.6%

WHETHER IT HAS BECOME MORE OR LESS COMMON FOR OFFENDERS TO TRY TO HIDE CHILD SEXUAL ABUSE MATERIAL.



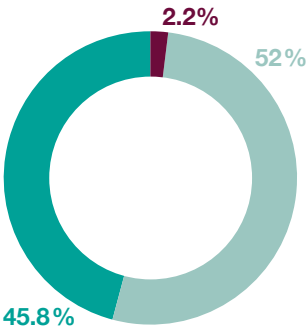
- Decreased 1.3%
- Neither increased nor decreased 47.2%
- Increased 51.5%

HOW COMMON IT IS THAT OFFENDERS MANIPULATE THE CONTENT OF IMAGES OR FILMS TO MAKE IT DIFFICULT TO IDENTIFY PEOPLE OR PLACES.



- Very uncommon 6.2%
- Uncommon 32.8%
- Neither common nor uncommon 17.8%
- Common 26.3%
- Very common 17%

WHETHER IT HAS BECOME MORE OR LESS COMMON FOR OFFENDERS TO MANIPULATE THE CONTENT OF IMAGES OR FILMS.



- Decreased 2.2%
- Neither increased nor decreased 52%
- Increased 45.8%

Cathal Delaney, Head of Team, Analysis Project Twins, EC3, Europol

Project "Trace an Object" – details help the police identify children

Encryption is becoming more widely used by the public at large, and this echoes the trend that we see in child sexual abuse investigations. It is more difficult to say something certain about the manipulation of images or obfuscation techniques. While these techniques are currently not used in the majority of investigations that we work on, this does not necessarily mean that the use of them is not increasing. What we can say is that the more technologically sophisticated offenders, who are also taking other security measures to hide their identity, are the ones that also use these technologies.

Images of specific objects

There is always a question as to how much information we should share about these techniques, as it highlights the importance of details in images in victim identification work. However, in the project "Trace an Object" we have opted to ask the public for help to identify objects or locations in images where we have exhausted all other ways of investigation, to help us find the children depicted in the images. At www.europol.europa.eu/stopchildabuse we share images of specific objects and specify what information we are seeking for that particular object or location.

People can, anonymously if they wish, send in information about the objects to the site. The tips are then dealt with by Europol's victim identification team, who pass credible leads on to the country to which the object appears to refer to. There it becomes the responsibility of the police authorities to decide whether to develop an investigation or not.

Eight children have been identified

"Trace and Object" has been up for eighteen months now, and we have seen good results. We have asked for the public's assistance with 145 different objects, and as a result one offender has been arrested and eight children have been rescued. These are eight children that we would not have found without this project and the assistance of the public.

We invest a lot of time and effort to ensure that the project and site are working as intended. We only use this possibility when we have already followed all other possible leads to identify a child in an image. Before posting an image on the site, we follow a structured process with internal procedures as well as permissions from the police authority in the country that is in charge of the investigation. We also notify other police authorities to give them a chance to solve the case before we post the image.

The public input is much appreciated

The response to this project has been very positive, and we are grateful for the traction that "Trace and Object" has had, as it has generated many qualitative tips. We intend to build on this success and hope to see more identified children as a result.

Europol and European Cybercrime Centre (EC3)

Europol assists the 28 EU Member States in their fight against serious international crime and terrorism. Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and help protect European citizens, businesses and governments from online crime.

“ONE OFFENDER HAS BEEN ARRESTED AND EIGHT CHILDREN HAVE BEEN RESCUED.”

06 Technology development – One in five police officers have found deepfakes

In previous reports we have looked at new trends that police officers encounter in their investigations. In this year's report we have researched technology development, and how quickly it manifests in child sexual abuse investigations. We look more closely at a new technique called deepfakes. It was widely publicised in the media in Spring 2018. Deepfakes can with the help of machine-learning technology, or AI, swap a person's face for another in moving imagery. Here we have looked at whether this technology has reached the realm of child sexual abuse material.

One in five police officers have found deepfakes

The large majority (more than 80 percent) of the surveyed police officers, report that they have not encountered deepfakes in their investigations. Fewer than one fifth report that they have encountered deepfakes. Out of these respondents a quarter report that deepfakes are common or very common in their investigations. However, just over 40 percent of those who have encountered deepfakes report that they are uncommon or very uncommon.

" More so seeing cartoon child pornography."

" It is very common to see photo-shopped and deepfake videos and images on cases."

A belief that it will increase

Three quarters of the surveyed polices officers believe that the prevalence of deepfakes will increase in the future, there were however responses that contradicted this belief.

" As it becomes more known it will increase like everything else with technology."

" If there is an easy way to do it someone will use it to produce new material."

" Since most of our cases involve subjects that have average or less than average computer skills, I do not believe that this will become prevalent."

" Deep fakes are like the old pseudo images. Offenders sometimes take pics of family members placing them on porn images and reinforcing their cognitive distortions to reinforce their sexual attraction. This is the same here. There will be no doubt this will happen but in the paedophile world, REAL is key to success."

Identifying victims is a challenge

The surveyed police officers point to a number of challenges that can arise if deepfakes become more prevalent in the future. One problem could be that any child could feature in the sexual abuse material, as long as the offender has had access to enough of images of that child (to create a deepfake a large number of images of a person taken from many angles is needed).

" All and everyone are now possible victims, videos from social media enable children to be victimized without having been abused."

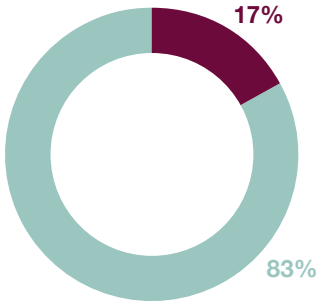
The current main challenge faced by police officers is, however, identifying victims. Secondly there is also a jurisdictional problem, as computer generated material is not illegal in all countries.

" Difficult to distinguish fake from true content. Is there a real victim/child or just manipulated content?"

" Victim identification will become harder since the body might not match the victim. Legal issues with what kind of damage has been done to the child."

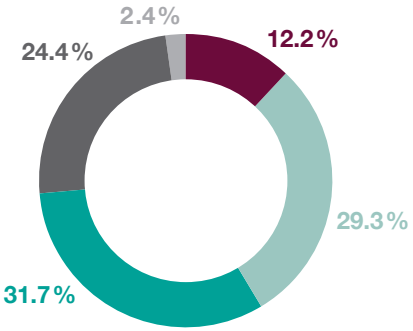
" The countries where the mandate requires a real child to have been abuse would not have an offence for this material."

PERCENTAGE OF POLICE OFFICERS WHO HAVE ENCOUNTERED DEEPFAKES.



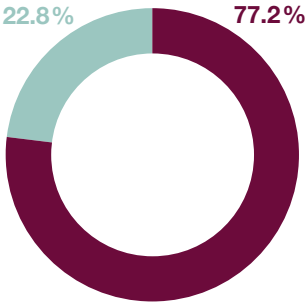
Yes 17%
No 83%

HOW COMMON DEEPFAKES ARE IN INVESTIGATIONS (RESPONSE BY POLICE OFFICERS WHO HAVE ENCOUNTERED DEEPFAKES).



Very uncommon 12.5%
Uncommon 29.3%
Neither common nor uncommon 31.7%
Common 24.4%
Very common 2.4%

PERCENTAGE WHO BELIEVE THAT DEEPFAKES WILL BECOME MORE COMMON IN THE FUTURE.



Yes 77.2%
No 22.8%

Christian Berg, Founder, NetClean

The main challenge is victim identification

Deepfakes is a technology that was more widely identified last Autumn, and discussed when media picked up on it in December 2017 and Spring this year. When I read that almost one out of five police officers have seen deepfakes in their investigations, I thought that was a proportionately large number, and that it looks as if the technology has become widely known quite fast.

Can be used to create material

This is not very surprising. We know that technologies are used to produce child sexual abuse material; a prime example is the role that the internet and darknet have played since their inception.

Deepfakes can be used to produce new online child sexual abuse material from already existing material. Using this technology, offenders can in addition produce material using images of children who have not been subjected to actual sexual assault, which means that in theory all children can become victims of this abuse.

Time-consuming to produce

However, the risks associated with the use of this technology is negated by the fact that it takes a lot of man-hours and commitment to produce this material. A large number of images of a person's face are required to produce a deepfake. In addition, a technical know-how to find out how deepfakes are produced is necessary (even if the technology in itself does not require advanced technical knowledge).

Something that also works against an even wider use of deepfakes is the fact that child sexual abuse material is readily available online, removing the need for more material to be created, especially as offenders have a predilection towards material that is genuine, above other forms of online child sexual abuse.

However, there is no doubt that investigators will need to handle deepfakes, if they are not already doing so.

Victim Identification is a challenge

The biggest challenge with deepfakes is that they make it difficult to identify children, especially as the deepfake obscures the physically abused child's real face. There is also a risk that investigators waste time looking for the wrong child, or for a child who in reality has not been sexually abused (even though one can argue that the film itself is sexual abuse).

In order to solve this problem investigators need ways to identify which films are deepfakes and the original film. In order to do so they need a good reference library of child sexual abuse films, which can be used to quickly determine if a film is "real" or not, if the material is already known and if the child in the film has been identified or not.

NetClean

NetClean is a world leading developer of technologies that protect IT environments from child sexual abuse material. Using hash technology child sexual abuse material is detected on work computers.

“THERE IS NO DOUBT THAT INVESTIGATORS WILL NEED TO HANDLE DEEPFAKES, IF THEY ARE NOT ALREADY DOING SO.”

WHEN BUSINESSES AND ORGANISATIONS DETECT CHILD SEXUAL ABUSE MATERIAL

Observations about individuals who view child sexual abuse material on their work computer, and insight into how they operate.

In last year's NetClean Report (2017), we asked police officers across the globe if there is such a thing as a typical offender. The data showed that apart from the fact that the offender is most often male, there are no other typical attributes such as age, profession, family situation or otherwise.

To follow up on last year's results, we have interviewed businesses and organisations that have NetClean ProActive installed on their computers and in their IT environments. NetClean ProActive is software that detects online child sexual abuse material. We asked the surveyed employers to tell us what happens when it is discovered that employees have used their work computer or company network to consume child sexual abuse material.

The findings from the interviews with the businesses and organisations are presented as a summary.

When we use the term "alert" in this report it is alerts from NetClean ProActive to which we refer.

NetClean ProActive

NetClean ProActive software detects known child sexual abuse material in organisations' IT environments. It works similar to an antivirus programme, however instead of detecting viruses, NetClean ProActive detects images and films that the police have classified as child sexual abuse material.

NetClean ProActive alerts

NetClean ProActive detects if an individual views child sexual abuse material, with the result that the software sends an alert, either as an email or SMS, to the individual whom the organisation has designated to handle these issues.

07 Child sexual abuse crime in the workplace – One in 500 employees

NUMBER OF ALERTS
513 alerts in total
Calculated on the installation base of 269 370 clients, and over time. Each client represents a work computer with a software installation to detect child sexual abuse material.

Number of alerts per thousand employees
1 (0.95) individuals per 500 employees.

SEX
Exclusively male
In all cases where an alert was triggered in the businesses or organisations interviewed, the individual responsible was male. In fewer than a handful of cases the computer that sent the alert belonged to a female employee, however further investigation showed that it was a man close to the woman who had used the computer and triggered the alert.

AGE
Most frequently between 30–50 years of age
The individuals who were found to have viewed child sexual abuse material on their work computers range from somewhere in their 20s to pension-age. The interviews showed that there was a certain bias towards individuals between 30–50 years of age, and many stated that the individuals were in their 40s.

FAMILY SITUATION
Slightly more common that the individual is in a relationship and has children
To the extent that employers know about the employee's family situation, which is not a given, they stated that it is slightly more common that the individual was in a relationship. They stated however that this is also a reflection on how societies operate as whole.

The same line of reasoning is applied to whether the individual has children or not. The employers who have this information state that there is a bias towards individuals who have children.

PROFESSION
All professions
With regards to profession and level of responsibility, the response was that it can be anyone from ordinary employees to senior managers, people with a lot of client contact to people with very little contact outside the organisation. This list also includes people who work with children. The alerts were biased towards people with higher academic achievement, however this was believed to be because they more often have a work computer, in many cases a laptop. Many of the businesses and organisations also stated that there is a certain bias towards employees who have a background in technology.

08 Work computers used for child sexual abuse crime – Most common outside office hours

TIME OF DAY

Most common outside working hours

Most alerts are triggered away from the work place and outside of working hours, during evenings, holidays, leave and work trips, and it is not uncommon for the individual to turn off the internet and network connection in order to avoid detection.

Some alerts occur during down-time in the work place, e.g. during lunch hours or early in the morning. In some cases the same individual has caused the software to send several alerts. In these cases the alerts have occurred at different times of day and night, including during work hours. In these instances, where several alerts have been triggered, large amounts of images and films have often been found.

METHOD OF ACCESSING IMAGES

Most frequently by using a USB-stick

Although almost all of the interviewed businesses and organisations stated that they had received alerts caused by individuals searching the internet for illicit material, the overwhelming majority of alerts were triggered by USB-sticks, which were in the main privately owned. Instances where child sexual abuse material was saved together with sensitive business information on USB-sticks and / or external hard-drives was also reported.

NUMBER OF IMAGES THAT CAUSE ALERTS

A few images in most cases

In most cases the alerts referred to just a few images that had been recognised by the software; often no more than 2–5 images. However, in many of the businesses and organisations interviewed, they had also found alerts that involved 15–20 images. In a few cases the alert involved several thousand images, to up to twenty thousand images from a single individual.

NUMBER OF IMAGES ON THE COMPUTER

More material is frequently found on the computer

Businesses and organisations have different procedures when they find that an employee has consumed online child sexual abuse material. Some conduct a thorough forensic investigation of the individual's computer, others report the alert to the police without further investigating the computer. The businesses and organisations that have undertaken an investigation have in most cases found further material or catalogue structures that clearly contain online child sexual abuse material.

" It is important to give the police a chance to investigate, even in cases where only a few images have been found. A house search can reveal that the few images are just the tip of the iceberg, widening the case to one that involves a collection and distribution of hundreds of thousands of child sexual abuse images.

In addition, we have to consider the strong arguments that consumption of child sexual abuse material is linked to physical abuse of children. In a Swedish case, a discovery of three images led investigators to two children who had been subjected to brutal sexual abuse. Every found image is worth investigating, as it has the potential to save a child and give them the chance to grow up and meet their full potential."

Björn Sellström, Team leader, INTERPOL, Crimes Against Children Unit, Vulnerable Communities Team.

" It doesn't matter where the images are stored – be it USB memory sticks, external hard-drives, or different cloud based services – they must be handled somewhere. This is why the work computer is such an important focal point. If businesses protect their computers, they will be able to detect if child sexual abuse material is consumed."

Anna Borgström, CEO NetClean.

08 Work computers used for child sexual abuse crime – Most common outside office hours, cont.

OTHER SECURITY RISKS

Large amounts of pornography

In some cases the interviewed businesses and organisations also investigated whether there was other illicit material on the individual's computer that could pose as a security threat or breach of company policy. Roughly half of those businesses stated that they frequently also find large amounts of "adult pornography", whereas the rest stated that they do not find any such material. A few of the businesses and organisations also found torrent clients on the individual's computer, which can be seen as a security risk to the company.

According to the interviewed businesses and organisations there were instances of individuals who have a clear predilection for child sexual abuse. This was evident from the catalogue structure, or from the fact that all the material found on the computer contained child sexual abuse.

FURTHER MATERIAL IN THE HOME

House searches frequently unearth more material in the home

Businesses and organisations do not always have information about what happens after the police have taken over the investigation. The data that we have about this issue is therefore in comparison less comprehensive. The interviews showed however that in cases where there is knowledge about a house search and the outcome, more material has in the majority of cases been found at the home of the offender.

REACTIONS FROM THE INDIVIDUAL

Reactions differ when individuals are confronted

According to the businesses and organisations interviewed, reactions vary when individuals who have viewed child sexual abuse material on their work computers are confronted. Most individuals confess and it is not uncommon to hear confessions that they have a problem and need help. Many state that it is an illness and that they can't stop.

Some individuals do not react at all, and seem to be unfazed by the issue, denying all knowledge of the crime. Other individuals act surprised or uncomprehending. Some blame friends or even their children – stating that they have used their computers to view the material. Some get into a panic, some become aggressive and some react with shame and regret. Several employers say that the individuals who express regret mainly do so thinking about their own situation and what is at stake. Few show any insight into the plight of the children in the images or show any remorse on their behalf.

" It is important that businesses and organisations that use detection tools report alerts to the police. The found material can be an indication that the individual who has triggered the alert has further involvement with this crime.

It is also important that the police act on reported alerts quickly and assist businesses and organisations with gathering and securing evidence."

Patrick Cordner, Sektionschef Nationellt it-brottscentrum (SC3), Nationella Operativa Avdelningen, Svenska Polisen.

COMMENT ON INSIGHT **07** AND **08**

Michael Sheath, Manager & Principal Practitioner, Lucy Faithfull Foundation

Lack of insight and empathy part of the problem

The data in NetClean's survey echoes my experience of working with men who consume child sexual abuse material. They are "normal" men with an education, family, work and socially functional lives. They are not men who make other people uncomfortable or raise suspicion.

One of the problems that we see in tackling child sexual abuse crime is the demonisation of child sexual offenders. The image of the stereotypical offender focuses people's attention in the wrong direction; away from the fact that it can be the respectable man with the nice family, the big house and the expensive car who also consumes child sexual abuse material.

Compulsive behaviour

The risks associated with viewing this sort of material in the workplace or on a work computer is indicative of the compulsiveness in these individuals' behaviour. This is especially evident in cases where employees have viewed child sexual abuse material several times. Taking this risk signals the scale of the compulsion.

There are several additional factors that combined with compulsive behaviour can tip these individuals into viewing child sexual abuse material. One factor is stress, which can trigger the impulse. There is also a proven strong connection between sexual arousal and poor decision making, impulsivity, and a reduction in empathy.

Anonymity is a key driver

I am not surprised that these individuals primarily consume the material away from the workplace and outside of working hours. I am convinced that it has to do with a sense of anonymity. Anonymity is one of the biggest drivers in the consumption of child sexual abuse material. The "logic" behind it is that if one is not caught out, one has not performed the action is question.

Lack of insight and empathy

In my experience most men who view child sexual abuse material don't understand that they are a part of the problem. They don't realise that their consumption increases the demand and leads to the sexual abuse of children. Their reasoning is that the abuse has already occurred, it was not their fault that it happened, and they do not contribute to any further harm if they merely view the material.

This lack of insight is connected to the reactions of these individuals when it is discovered that they have viewed child sexual abuse material on their work computer. The strongest reaction is a sense of shame, and not guilt. Most worry solely about what other people will think, and do not consider the harm that their actions have brought to children.

Ultimately, this crime has a close connection to empathy or lack of empathy. Many men genuinely want help to stop viewing child sexual abuse material. The key to this is to get them to understand how much their actions hurt the children who are depicted in the material. It is possible to help some offenders stop if they are helped to understand the consequences of their actions.

The Lucy Faithfull Foundation

The Lucy Faithfull Foundation is a UK charity which runs the only helpline in the UK for people who have concerns about negative aspects of their sexuality.

ACKNOWLEDGEMENTS AND CONCLUSION

IT IS TIME TO TURN KNOWLEDGE INTO ACTION

I would like to extend my gratitude to the nearly 300 police officers who participated in our research. The work that they do is invaluable to children and to the communities they serve around the world, and we must always be grateful for the ambition, innovation and drive with which they approach their work.

I would also like to extend my gratitude to NetClean's customers who trusted us with information about their experiences of finding child sexual abuse material in their IT environments. I am grateful that they allowed us to share their data and insight into the circumstances surrounding incidents in their IT environment.

I also would also like to say a big thank you to our sister company Griffeye, who shared their customer database and knowledge with us on this issue. Without them this report would not exist.

Now is the time to turn our research, knowledge and ambition into action. It is the key to providing children with a happier childhood, free from sexual abuse. Looking at the work of dedicated police officers and employers who have taken concrete action, we know that there is a place for everyone and anyone to help. It is now time for leaders, governments, businesses, organisations and individuals to play their part.

With the right knowledge we can focus our resources where they are needed most. We have to act on every level in our communities as well as on the internet. We have to make the most out of technology and ensure that it is used in the right way. When we do, we can break the circle of abuse and give children across the world a brighter future.

Anna Borgström,
CEO NetClean

NetClean.

a Safer Society Group company