WePROTECT GLOBAL ALLIANCE

Global Threat Assessment 2018

Working together to end the sexual exploitation of children online

WARNING:
This document contains case studies some readers may find distressing.
It is not suitable for young children. Reader discretion is advised.

PA

Acknowledgements

The WePROTECT Global Alliance wishes to thank **INTERPOL**, the **US Department of Justice**, the **UK's National Crime Agency** and **NetClean** for providing specialist advice; and **PA Consulting Group** for assisting with the compilation of this report.

Contents

01 Foreword
by Ernie Allen, Chair of WePROTECT Global Alliance

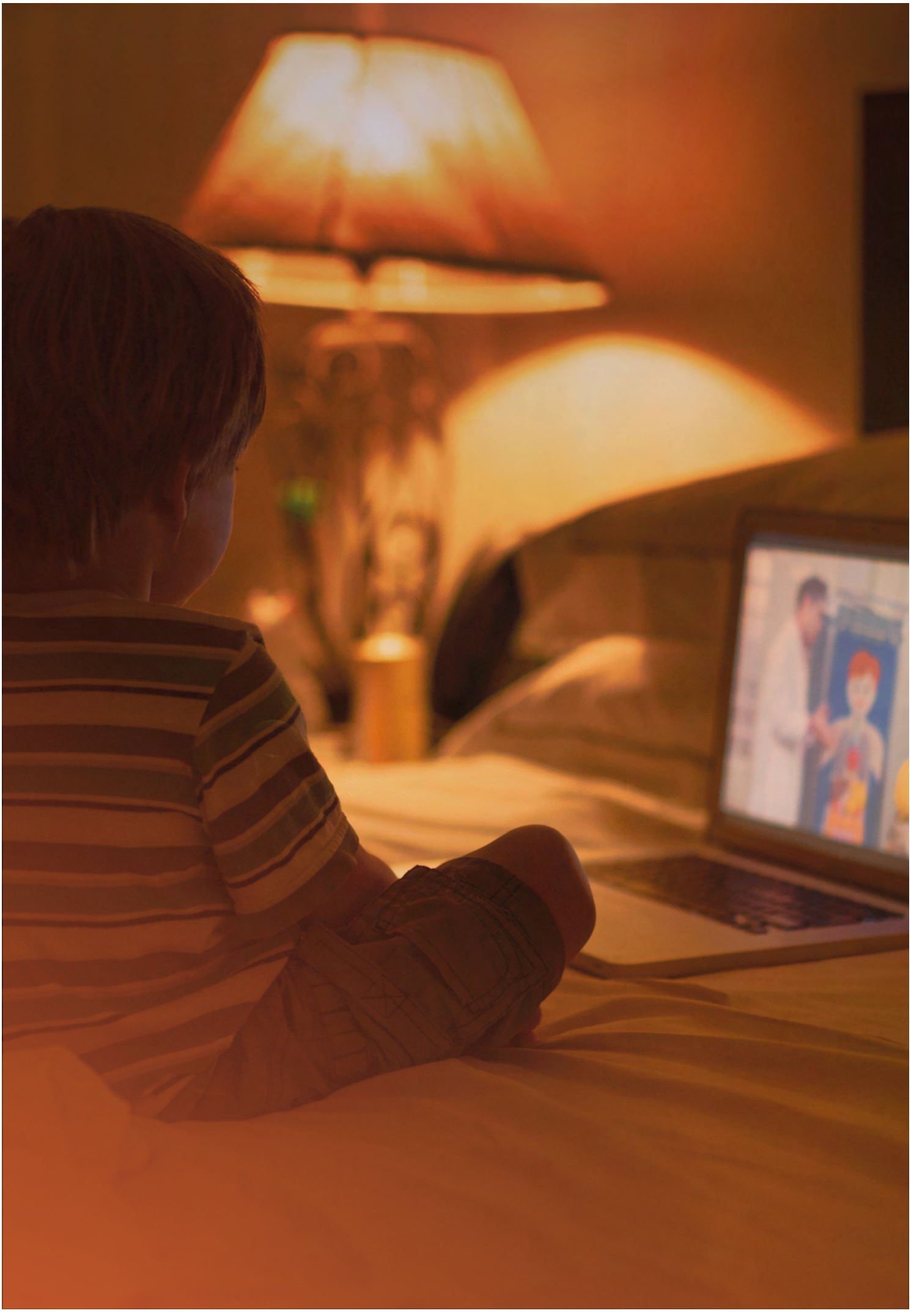
Since the merger of the WePROTECT and Global Alliance initiatives in 2016 we have seen the continued growth of a single global movement against the sexual exploitation of children online. Membership of WePROTECT Global Alliance now stands at 82 governments, 20 global technology companies and 24 leading international and non-governmental organisations. I am honoured to serve as Chair of the WePROTECT Global Alliance Board and am particularly grateful to the UK, US and EU Commission for their leadership.

In 2014, our top priority was the record number of child sexual exploitation and abuse (CSEA) images being shared and distributed online. The more we looked, the more we found. Since then, our partner governments and organisations have exploited digital photo 'DNA' technology, built databases and established hotlines to move towards proactive identification and removal of this material. We are now taking steps to increase the speed and efficiency of takedown through automated solutions.

We cannot be complacent. CSEA imagery is a continuing concern, but we are now facing new challenges as the pace of technological change continues unabated. The WePROTECT Global Alliance Threat Assessment 2018, which has been developed with the assistance and expertise of our Board members, aims to demonstrate how technology has been exploited by offenders and increased the risks to children. It uncovers disturbing new trends such as growth of offender communities protected by unprecedented levels of security; 'on-demand' and crowd-sourced production of CSEA material; as well as live-streaming, grooming and sextortion. The explosion of smartphone technology around the world has acted as a catalyst to intensify the threat.

Time and time again I have stated that this is not a problem that any single country or institution can handle alone. Now that we understand more about the global reach and impact of this heinous crime, we need to come together to provide global solutions.

Ernie Allen
Chair, WePROTECT Global Alliance Board



02 Aims of the Global Threat Assessment

The Global Threat Assessment is the first of its type, both in terms of the broad stakeholder community that it draws from but also in its global vision to strengthen and further develop the international response to this growing and persistent threat.

The report has been commissioned with the following aims:

- raising international awareness of online child sexual exploitation (OCSE);
- greater understanding of the threat and how it is evolving;
- greater understanding of both the impact to victims and the wider societal impact of OCSE;
- creating a baseline which can be used to monitor both the level of the threat and the positive impact that interventions are having on the offender population;
- to provide evidence based examples to support members in making domestic and international decisions or investments.

82 countries already members of WePROTECT or the Global Alliance

20 of the biggest names in the global technology industry

24 leading international and non-governmental organisations

The WePROTECT Global Alliance to End Child Sexual Exploitation Online combines two major initiatives: the Global Alliance against Child Sexual Abuse Online, led by the US Department of Justice and the EU Commission, and WePROTECT, convened by the UK. This new, merged initiative has unprecedented reach, with 82 government members of the WePROTECT Global Alliance, along with major international organisations, 20 of the biggest names in the global technology industry, and 24 leading international and non-governmental organisations.

Global Threat Assessment

The Global Threat Assessment is a call to arms against OCSE, with a focus on the changing nature of the threat, the impact on victims and the wider societal harm caused by these crimes. The purpose is to demonstrate the nature, scale and complexity of the threat in order to support broad mobilisation – compelling nation states, the global technology industry and the third sector to find new ways of working together to combat a new and evolving range of crimes. The next step will be the design and activation of a Global Strategic Response, based on the findings from the Global Threat Assessment.

03 Summary Conclusions:

Technology is enabling offender communities to attain unprecedented levels of organisation, creating new and persistent threats

The sexual exploitation and abuse of children online is the most insidious form of modern cybercrime. Technology is enabling offenders and offender communities, providing them with unprecedented levels of access, new capabilities and increasing confidence to abuse children on a mass scale.

The current scale of offending has been further facilitated through the ubiquity of mobile devices, anonymous access and encryption, which has enabled child sexual abuse material (CSAM) at a previously inconceivable scale. There are hidden services sites with over one million persistent profiles, where victims are re-victimised many hundreds of times a day.

For the past decade, the global law enforcement community has been working to counter the threat posed by offenders who engage in child sexual abuse online, and where it crosses over to contact offending.

The rapid expansion of high speed internet connectivity, compounded by the growing ownership of mobile devices by young people, has permitted offenders, almost anywhere in the world, to interact with children from any connected location through anonymous, rich media connections.

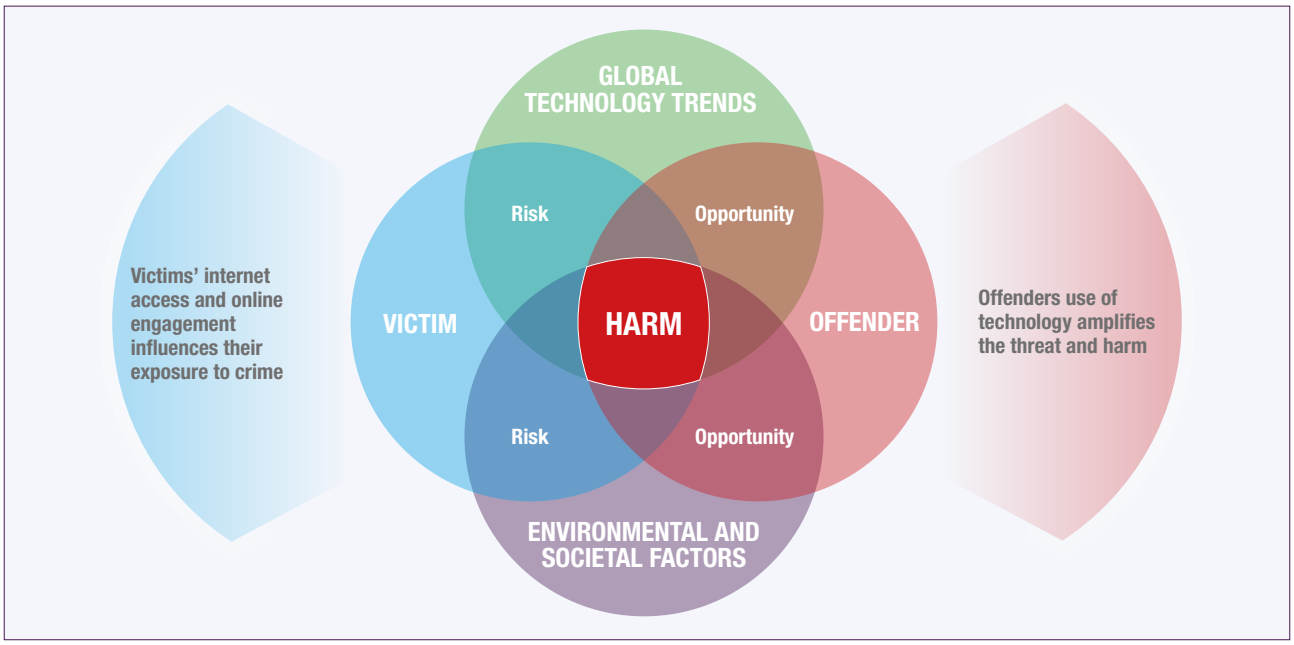
Increasingly, offending is taking place online and includes coercing or extorting children into producing indecent images of themselves or engaging in sexual activity via webcams, which can be captured and distributed by offenders. The nature and scale of these crimes continues to evolve rapidly inline with technology.

> “Technology is permitting offender communities to attain unprecedented levels of organisation, which in turn creates new and persistent threats as these individuals and groups exploit online ‘safe havens’ and ‘on-demand’ access to victims.”

Harm may arise where vulnerable children are brought into contact with offenders via social media and other online services where they are exposed to that risk by a caregiver, as well as where the internet is used as the means of sharing CSAM or as a secure virtual meeting place for offenders to share information.

In the past three years the level of active offender organisation, facilitated by technology, has created new, safe havens online for offenders to share, discuss and plan coordinated OCSE offences. The scale, complexity and danger of the threat has escalated. This must not be allowed to continue.

The Global Threat Assessment examines the impact through five lenses



Section 4: Global technology trends that increase victims' online exposure and offenders' ability to share child sexual abuse and exploitation (CSEA) imagery securely and interact anonymously with children online.

Section 5: Local environmental and societal factors exacerbate the global issue. Variations make it difficult to establish common ground internationally over what constitutes abuse, which is increasing the challenge of any international response to child safeguarding, offender identification and apprehension.

Section 6: The victim, offender and technology intersection. Technology permits offender communities to attain unprecedented levels of organisation, which in turn creates new and persistent threats as these individuals and groups exploit online 'safe havens' and 'on-demand' access to victims.

- Victim preconceptions may prevent children at risk from being identified. There is a need to improve our understanding of victim vulnerability and how children's interactions with both technology and offenders affect their vulnerability.
- Understanding the scale of threat and offender methods and motivations is critical to forming targeted interventions to remove threats and improve victim protection.
- Technology enables 'safe havens' for offenders to gain access to content, victims, offending peers and educational material.

Section 7: Assessing the total cost incurred through OSCE to societies delivering an effective, balanced and proportionate global response, the global community needs to quantify the **impact of societal harm** by improving our assessment of the cost of OSCE on individuals and societies.

Section 8: International law, policy and enforcement frameworks surrounding OCSE should be focused on a consistent approach to addressing the international nature of the threat – underpinned by the Model National Response.

04 Global technology trends

Technology has generated a paradigm shift in both the victims' online exposure and the offenders' ability to share CSAM securely and interact anonymously with children and other offenders online.

Global society continues to be increasingly connected via the internet and the communication services that it supports. This enables people to interact in new and continuously evolving ways. The use of the internet and 'smart' mobile devices has become standard in all aspects of our modern connected lives, with increasingly younger users spending more and more time online.[1]

While not inherently insecure or unsafe, many popular websites and social media services present a target for offenders who actively seek out environments where young people regularly congregate online to meet new people, or join new communities.

The threat persists even for those who have yet to venture online, as the internet facilitates their abuse by creating safe havens for baby and toddler CSAM to be shared.

The international community must continue to monitor global technology trends and to understand how structured interventions can ensure safer experiences for young people, while enabling them to enjoy the intended benefits of new devices and services.

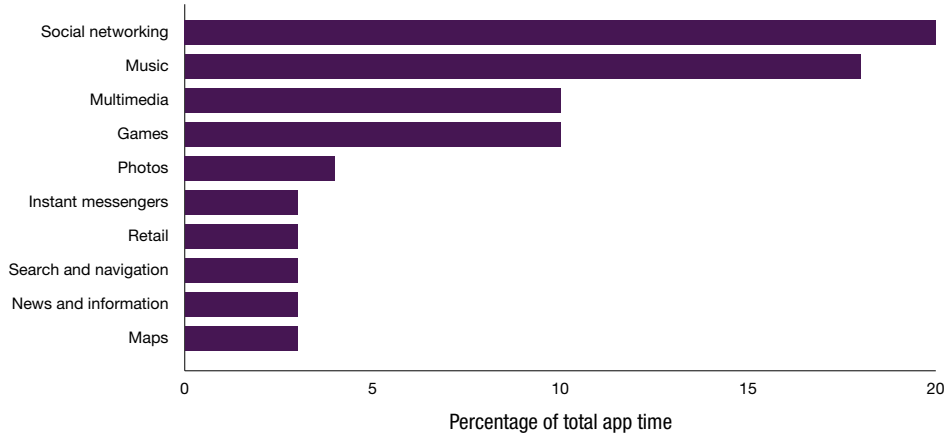
The challenge faced by law enforcement agencies (LEAs) lies in finding a balance that allows young and vulnerable users to maximise the immense benefits of the internet in a way that is as safe as possible, while countering the CSEA threat. Among the trends that factor in that challenge are:

- increasing global access to the internet, with increasing speeds for richer services;
- reducing the complexity of creating secure eco-systems;
- reducing production and consumption costs for rich media.

Increasing global access to the internet, with increasing speeds for richer services

- Social media is the dominant means by which unrelated people meet and interact on the internet. In 2016, social media platforms connected more than 2.8 billion people – one third of the world's population.[2]

Graph showing percentage of time spent on app type



- In developed countries, internet access has for the most part stabilised in terms of subscribers and user base. It has however, increased in terms of time spent on online services, again increasing the threat.
- Over the next 3–5 years we will continue to see an increase in users from developing regions such as Central Africa, South East Asia and Latin America.[3]
- Internet access and traffic will grow the fastest in the Middle East and Africa, followed by Asia Pacific. Traffic in the Middle East and Africa will grow at a compound annual growth rate of 42% between 2016 and 2021.[4]
- In many newly connecting areas, the opportunity to skip a technological generation and surpass typical internet speeds by installing 5G/LTE mobile networks will allow emerging nations to avoid the significant cost of installing and operating fixed line infrastructure.
- Live internet video will grow 15 times from 2016 to 2021 and account for 13% of internet video traffic by 2021.[5]
- The proliferation and penetration of internet connectivity in previously unconnected regions could also partly explain reports stressing an increase in non-Caucasian victims featured in CSAM.[6]

Reducing the complexity of creating secure eco-systems

- In the last 5 years there have been a number of high-profile news stories covering government surveillance; the challenges from anti-piracy initiatives and copyright infringement orders; and a range of cyber breaches involving personal data or banking details. These have accelerated the development of secure and anonymous services.

Secure messaging and rich media exchange continue to grow at an exceptional rate

- A single secure messaging platform achieved over 100 million monthly active users, with 350,000 new users each day and the exchange of 15 billion messages per day.[7]
- Providers of new messaging applications often base their infrastructure and offices in jurisdictions with less robust legislation, creating barriers to international cooperation. As a result, investigators rely on limited structures to support cooperation.
- Virtual Private Network (VPN) usage has continued to grow, especially in technologically advanced countries. By the end of 2017 VPN services were in the top five communications apps by revenue in the Google Play store across Scandinavia. The VPN app was in eighth position worldwide.[8]
- Darknet/TOR usage continues to grow, from an initial user base of just under one million directly connecting users in 2013, to over four million users by the start of 2018.[9]

Reducing production and consumption costs for rich media

- A major factor in the growth of OCSE crimes is the ability to create and distribute content at very low cost.
- Historically, production required expensive hardware and broadband internet connectivity for distribution. The advent of smartphones has meant that high-resolution cameras have arrived in a single, internet enabled device suitable for both photograph and video capture.
- The average cost of smartphones dropped from $440 USD in 2010 to $283 USD in 2016[10] Trends indicate that mass produced phones for as little as $30-40 USD will become increasingly popular in Asian and African markets over coming years.[11]

- New generations of mobile devices continue to have better camera resolutions, connection speeds and more powerful processors to deal with increasingly complex operations, such as encryption.
- The growing availability of more powerful devices, combined with increasingly cost effective prices means it is projected that smart phone users will break 5 billion by 2019, with 1.7 billion devices expected to be shipped in 2021 alone.[12]
- A significant number of 'new' and recycled devices are entering the consumer market each year, creating a growing volume of smartphone hardware that permits encryption, rich media creation and live streaming for remote viewing.

Use of darknet forums for exploitation of pre-verbal children

In recent operations, LEAs have noted an increased interest in pre-verbal children, who offenders prefer specifically because they are unable to self-report their abuse.

In 2016 a British citizen was sentenced to 85 years imprisonment in the United States for conspiracy to traffic CSAM. The offender created and administered a website that contained imagery involving infants and toddlers, allowing him and his co-conspirators to advertise and distribute CSAM and to aide each other in upskilling their offending.

Today, hidden services on the darknet have largely replaced such groups. One such service has over 18,000 registered members and is described as 'dedicated to infant/toddler abuse, incentivising abuse and production'.[13] Another site, used as a forum for discussing abuse, has a hit counter standing in excess of 23 million.[14]

Darknet sites exist across the full spectrum of CSAM and are dedicated to various aspects of offending. Many have registered members in the tens or hundreds of thousands. The US Department of Justice reports that an aggregate 1.9 million users are registered across nine sites dedicated to this material.[15]

> "Technology is allowing offenders to develop networks with likeminded people that are more complex and on a larger scale than ever before. As a network, as opposed to an isolated individual, they are more innovative, collectively intelligent, pervasive and robust and therefore ultimately more dangerous to children."
>
> **INTERPOL**

The darknet is an overlay network accessed only with specific software, configurations or authorisation, often using non-standard communications protocols and protective measures.

Darknet sites are appealing to OCSE offenders because they are now relatively easy to operate and access, while being difficult for law enforcement to remove. They allow the offender community to become more stable, as sites can exist in plain sight of LEAs over long periods of time, accumulating more content, more information and more users.

05 Environmental factors

Local environmental factors can compound vulnerability. The existence of these factors makes it difficult to establish common ground internationally over what constitutes abuse, as well as increasing the challenge of any international response to child safeguarding, offender identification and apprehension.

The sexual abuse and exploitation of children is an international issue. Children around the world share many of the same vulnerabilities, local social and environmental variations, detrimentally or preventively, contribute in different ways to this vulnerability.

The internet has blurred traditional notions of jurisdiction and sovereignty, making this issue global in scope and requiring a coordinated national and international response.

Despite the internet intersecting and transcending geographical barriers, users engage with it in countless different ways influenced by their geography and the society they inhabit. Local attitudes to children, gender equality, extended family units, sexual orientation, religious practices and levels of education vary greatly. These variations make it challenging to identify and safeguard victims, apprehend offenders and prevent offences from taking place.

Different socio-cultural conditions and attitudes at a local level are contributing to the vulnerability of children and likelihood of offending.

Apart from the inherent personal characteristics that each child possesses which create the risk of vulnerability, there are also external factors, relating to a child's family and social environment, as well as local variations in attitudes and tolerances which either compound vulnerability or act as protective factors.

These variations differ in numerous ways and on a global scale. The risk factors do not correspond to certainties, and are derived retrospectively from observed associations between these factors and victimisation.[16]

Poverty, inequality, social exclusion, discrimination based on ethnicity or gender, lack of access to education and protection from family and institutional environments are all common factors framing vulnerability.

Other root causes, such as lack of employment opportunities, forced migration and repression exacerbate the potential for CSEA.[17] For example, in areas with strong prejudices against homosexuality, the victimisation of boys tends to be clandestine and social attitudes make victims and their families less likely to report any abuse.

Similarly, regions displaying a general taboo against the open discussion of sexual topics, and an even more specific taboo when children and abuse are involved, share common challenges to combating and assessing CSEA. For instance, children will rely on less secure channels to inform themselves about sex and will find it difficult to differentiate between what is and is not acceptable without proper guidance.[18]

While countries should strive to meet international standards they must become, and remain, informed of the risks their own cultural and societal norms exacerbate.

Vulnerabilities enhanced by social norms or taboos increase the likelihood of abuse and exploitation within a community and also act as pull factors for online and offline offenders globally.

Globalisation has given rise to an increasingly interconnected world where people travel for leisure and business on an unprecedented scale. Offenders are known to travel to seek out environments where they can exploit the vulnerabilities of other societies and also avoid the barriers to offending in their home country, such as sex offender registration and effective law enforcement. These factors create a 'pull' to a foreign environment, making it more attractive to offenders.[19]

It is known that offenders looking to abuse and exploit children share knowledge of these factors online in offender forums and communities. Traditional offender travel trends have diversified and it has become increasingly difficult to categorise countries as countries of origin, countries of destination, countries of transit, or countries of victimisation, as 'countries can be any – or all – of these'.[20]

It must be noted that there is now increasingly less need to travel to exploit a child. The internet has facilitated a number of new ways to exploit or abuse children.

Furthermore, many traditional factors of vulnerability have also been subverted. For example, a child in a relatively wealthy nation is not made vulnerable by their poverty but by the privilege of their access to the internet, the possession of an often private device to do so, and the confidence or curiosity to engage with others online.[21]

It is for this very reason that children with no apparent traditional vulnerabilities can still be targeted online by those looking to extort or exploit.

Globalisation and hyper-connected communities, combined with the existence of factors that are deemed to create a permissive offending environment, will drive the demand for CSAM globally.

In some regions, understandably, legislation, education, law enforcement and parents have not been able to keep up with the disproportionately negative impacts of rapid technical development[22,23] In many places, the threat has not been prioritised or there is a lack of ability to invest in infrastructure or safeguards to protect children. The nature of the internet means that a growth in the number of vulnerable, naive or dangerous online users is not an isolated problem for that nation or region alone, but a problem for the international community.

On demand child sexual abuse (cybersex trafficking)

Cybersex trafficking has emerged as a new and brutal form of modern-day slavery. Offenders search online and pay to sexually abuse children of any age from anywhere in the world via webcam. In the Philippines alone, authorities receive thousands of cybersex trafficking referrals each month.[24]

In some instances, this crime is a precursor to travel for contact offending. In 2017, a US citizen was sentenced to 14 years in prison for attempting to arrange to rape an 8 year-old child overseas. The offender participated in live-streamed webcam sessions depicting minors engaged in sexually explicit conduct, while also instant messaging with adults in the Philippines and elsewhere.

During some of these online conversations the offender discussed plans to rape a woman's 8 year-old daughter during an upcoming trip to the Philippines, as well as engaging directly with the child. After the mother's agreement, he sent her $200 USD and offered to pay an additional $300 USD after raping the child.

The offender subsequently travelled to the Philippines in order to abuse the 8 year-old and other children. During this trip he also paid to sexually abuse a 16 year-old girl. In total, he sent wire transfers of more than $33,000 USD overseas, the majority of which was used to pay for live webcam shows depicting minors engaged in sexually explicit conduct. The court found that this offender routinely sought to persuade parents in the Philippines to allow him to abuse their children.[25]

> “Cybersex trafficking is on the rise as internet access increases everywhere. Now, paedophiles anywhere in the world can direct live sexual abuse of boys and girls hidden in private homes or internet cafes.”
>
> **International Justice Mission**

Live-streamed abuse is not only increasingly common, but also increasingly affordable. Five or six years ago, access to live-streamed abuse cost in the region of $50 USD. Today, it is available for $15–20 USD. LEAs predict costs will continue to decrease.[26]

06 The victim, offender and technology intersection

A victim's internet access and online engagement influences their exposure to crime, while an offender's use of technology increases their capability and makes them more dangerous.

Victims

Reports of OCSE have risen significantly, commensurate with global trends of increasing internet use, the uptake of social networking, and the ubiquity of mobile internet-enabled devices with media capture distribution quality.

Preconceptions about victims are fundamentally unhelpful. OCSE is a transnational crime and there is no age at which children are immune to its threat. Abuse can play out in diverse ways and it is usually the victim's age and capacity to interact with both technology and offenders that affects how it is manifested.

In order to better protect children from abuse, there is a need to focus on what we do know about victims and what makes some children more vulnerable.

Age – from birth to adulthood, children can be victims of OCSE

As a child progresses through childhood they may become susceptible to a range of different and variant threats. These are in many ways compounded by the socio-economic environment they find themselves in, but also by the addition of internet technologies and by how and with whom they interact.

Trends have revealed an increase in CSAM showing younger victims and as such, there is a perception that victims are 'getting younger'. The reality is that throughout childhood, there is a risk of exposure to abuse.[27] Previously niche areas of OCSE, such as the abuse of infants or 'pre-verbal' children, have become increasingly prevalent.

A child's age and interaction with technology impacts how they might be harmed. Though there are regional variations and differences in parenting style, children may become users of tablet or smart phone games when they are less than a year old. Their ability to communicate, the extent to which their usage is supervised and the frequency of their access are factors that all increase with age and which change the type of abuse to which they are vulnerable.

Use of technology – older children access the internet with reducing levels of supervision

Though it differs between families and across cultures, there is a turning point in children's lives where the frequency of their access to the internet, their engagement with social networks and the lack of supervision they experience all increase to create the perfect storm of opportunity for offenders.

The proliferation of mobile, camera-enabled devices and the ease with which it is possible to self-generate explicit images or videos and share them makes any child with access to a device a potential victim. The privacy that comes with use of mobile devices makes it difficult for parents to monitor their children's internet use in an unobtrusive way. Ownership of personal devices, used in privacy, enables children to easily hide their online activity from their parents and diversifies the risk they face online.

Once children begin to manage their own internet use, the ways in which they can be exploited increase. While children may self-generate imagery to be shared within the confines of an age-appropriate relationship, they can also be groomed to share images with adult strangers online, or have images that they've shared used to manipulate them through sextortion. The potential impacts can be severe; from the psychological effects of regret, fear and embarrassment, to instances of self-harm when the images are widely shared and an increase in the volume of CSAM online.

Relationship to offender – engagement with technology impacts the offender-victim relationship

Where infants and young children appear in CSAM or are exploited in other ways, someone they know has been active in their abuse. For older children and teenagers, it is more likely that they have been engaged or exploited via their use of social media, or via apps, video games or messaging environments.

Social networks are so commonly used that a teenager's social circle today is vastly broader than it would have been fifteen years ago. Teenagers are much more accustomed to communicating with friends of friends or strangers online. As such, there is a much higher chance that they can be groomed into self-generating imagery that can be shared, or that they may be sextorted online.

Location – a global threat has global victims

Common wisdom might dictate that the victims of OCSE are largely based in developing countries with existing travelling child sex offender (TCSO) problems. However reports from law enforcement indicate that these are by no means the only places victims are found. LEAs tell us that there are just as many victims in North America and Europe, while numbers in emerging technology markets such as Latin America, Africa and the Middle East are rising quickly.

The capacity and capability of Western companies in reporting may skew the perception of where these crimes are most prevalent. It is increasingly evident that the threat exists everywhere and that as offenders become more sophisticated, their understanding of where and how to access their preferred types of victim grows.

In many countries, particularly in parts of Asia, the Middle East, and Africa, less is known about how children access the internet, let alone what the consequences might be. Some of these countries are both home to the majority of the world's children and the regions where internet access is now growing most rapidly.[28] It has already been recognised that the spread of mobile devices and internet access in South East Asia is facilitating the exposure of child offensive material with the aim of making children accustomed to sexual violence and generating a sense of normalisation.[29]

Just as children may be at risk when exploring their sexuality, there is also a high probability that those from orthodox or particularly conservative religious backgrounds are less likely to share their experiences of abuse, from fear that they will be seen as complicit or that they could be ostracised by their communities.

There is a particular risk associated with parts of the developing world where widespread use of the English language intersects with relative poverty. This is considered a contributing factor to the trend of live-streamed abuse in the Philippines, as it makes communication between offenders and victims – or offenders and other offenders – significantly easier in an environment where the dollar is strong and there is little understanding of the long term detrimental effects of sexual abuse on children.[30]

Social and socioeconomic factors – vulnerability factors that increase risk

Children who are inherently vulnerable to abusive relationships – because they are in foster care or through poverty, disability or poor mental health – are also vulnerable to abusive relationships online.

Children who are exploring their sexuality, particularly when they come from traditionally conservative countries or strictly religious families, are also more likely to seek out intimate relationships online and may do so through accessing sites designed for

adults, or through communicating in forums that make their vulnerability apparent. They are also less likely to share their experiences of abuse from fear that they will be seen as complicit, or that they could be ostracised by their communities, which in turn makes them more at risk to offender interaction.

Among the trends emerging from the rapid global rise in child and teenage internet use is the desensitisation of young people to sexual and violent content.[31] Ease of access has enabled children to more easily look at age inappropriate content online and share it with their friends, including content which is graphic, violent and abusive.

Numerous studies of teenagers in western countries show that viewing such content online is prevalent, has a negative impact on the way that teenagers interact, what they expect, and what they deem age appropriate sexual behaviour.[32]

Using a children's website to find and exploit victims

The UK National Crime Agency – Child Exploitation Online Protection (NCA:CEOP) investigated an offender who was using a children's website to meet and groom children, with the view to moving them on to video chat platforms where he could engage in more serious offending.

The offender first approached victims on a popular children's website, attempting to engage them in sexualised conversations. He would then invite victims to leave the site and join him on messaging platforms which had a video chat function. If successful, the offender would perform sexual acts on webcam, while the victim watched, or incite the victims to engage in sexual activity on their own webcams.

The offender used easy to use, freely available anonymising services when accessing the children's website in an attempt to evade identification by law enforcement. This also made it difficult for site moderators to immediately identify and block accounts created by the offender as he was constantly using different IP addresses through secure network services.

Over a two year period he was linked to 407 accounts on the site, which he used to facilitate his offending. These accounts would ultimately be blocked by moderators, but not before he was able to engage with victims and move them to video chat platforms. Analysis indicated that around 9,000 children were approached directly by the offender. The offender pleaded guilty to 14 offences including:

- inciting children under 13 to engage in sexual activity on at least 50 occasions;
- engaging in sexual activity in the presence of under 13s on at least 205 occasions;
- attempting to engage in sexual activity in the presence of under 13s on at least 500 occasions.

The offender was sentenced to 10 years imprisonment and an extended 5 year licence period.[33]

Secure network services reroute the user's online traffic through a different, or multiple different, IP addresses, giving them a secure or encrypted connection. They may be used to avoid country-specific blocking or to anonymise or 'hide' online activity. These services are usually legal, however they can be purposed to facilitate anonymous access to sites hosting illegal content, such as CSAM, or for hiding the location of an offender using legal sites to access victims.

Offenders

Literature in this area often divides CSEA offenders into a number of categories, based on a variety of factors including technical sophistication, online or offline offending or modus operandi.[34] While these categories are necessary and useful for describing the many facets of how and why people offend against children they detract from the very clear issue that offenders often do not fall neatly into different exclusive typologies.[35]

There is no typical offender

Effort has traditionally been dedicated to identifying demographic characteristics to define 'typical' offenders; however this is becoming progressively redundant, particularly in the face of globalisation and growing global connectivity.

It is becoming increasingly evident that offenders who engage in every or any type of child abuse and exploitation may represent any age, race, sex, occupation, socio-economic status or geographical area.[36] Understanding offenders' methods and motivations is still critical for combating the threat they pose.

The number of offenders and offences appears to be growing globally. Increasingly, the detection and apprehension of offenders will require the collaboration of international partners. While this can be partially explained by a risen increase in reporting and more proactive policing in some regions, it is thought that the growth in reported numbers is somewhat substantiated by an increase in actual offences. In a global survey, 26 of 32 responding countries indicated that they perceived the number of offenders to have increased, while 28 of 30 responding countries indicated that the number of images in circulation has risen.[37] Even where reporting of offences does not increase, this does not mean that offending is not happening.

The trends in recorded offences will vary across nations for reasons beyond the true volume of offending.

A number of organisations in western countries can offer figures and data to inform estimations of the number of offenders and scale of CSAM online.[38] Investigations, arrests and reporting are likely to only represent a fraction of offenders. More work is required to understand how the estimations of offender volume, that we have, can be applied on a global scale.

Offender method and motivation

Those who offend against children vary greatly in their level of IT literacy, though some possess advanced and sophisticated technical skills and are adept at shielding their online behaviour from law enforcement. The offender population in CSEA has been quick to make use of both common and emergent technologies to enable their offending. As we become more connected, with greater access to the internet, law enforcement is seeing a more permissive environment online for international offender behaviour, grooming and sextortion.

Modern, accessible and cost effective technologies are permitting the most extreme offenders to connect and form persistent, highly-skilled communities, which in turn are compounding and ratifying their offending behaviour.

A factor that has recently emerged in online offender patterns is a pre-existing familiarity with advanced technologies among younger – 'millennial' – offenders.[39] It is important to recognise that technical sophistication does not equate to greater risk of contact abuse to a child, but does decrease their chance of detection and apprehension. It is evident that offenders target and exploit vulnerabilities that emerge through the full spectrum of childhood, often facilitated by both offender and victim access to technology.

The commercialisation of child sexual abuse material

In 2015, an Australian national was arrested in the Philippines, where he is alleged to have produced a series of exceptionally extreme videos involving the torture and sexual abuse of a toddler by himself and a female accomplice, and the sexual abuse and torture of prepubescent girls.

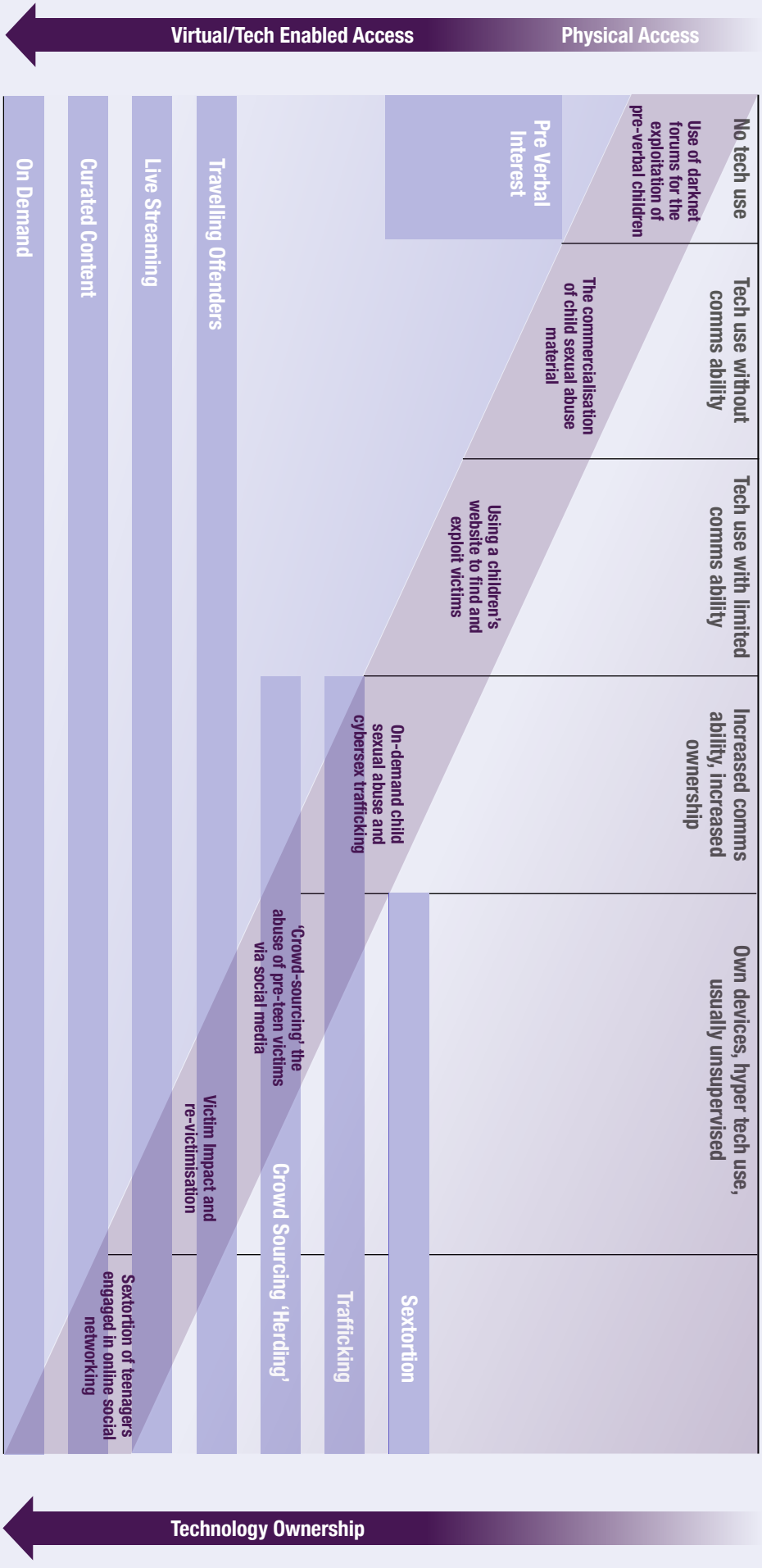
The videos were hosted on a darknet site specialising in torture and sexual abuse. The suspect acted out and live-streamed these videos at the request of an online community of offenders. He was able to charge up to $10,000 AUD for one video depicting the torture of an 18-month-old girl, which has been discussed by offender communities as the model of abuse material they specifically seek.

The suspect has also been charged with the murder of one of his alleged victims and awaits trial in the Philippines.[40]

The victim, offender and technology intersection

Victims

As a child progresses through childhood they may become susceptible to a range of different and variant threats. These are in many ways compounded by the socioeconomic environment they find themselves in, but also by the addition of internet technologies and by how and with whom they interact.



Offenders

The offender population in CSEA has been quick to make use of both common and emergent technologies to enable their offending. As we become more connected, with greater access to the internet, law enforcement is seeing a more permissive environment online for international offender behaviour, grooming and sextortion. Modern, accessible and cost effective technologies are permitting the most extreme offenders to connect and form persistent, highly-skilled communities, which in turn are compounding and ratifying their offending behaviour.

‘Crowd-sourcing’ the abuse of pre-teen victims via social media

In 2017, members of an international child exploitation network pleaded guilty to their roles in operating two websites for the purpose of coercing minors as young as 8 years old to engage in sexually explicit conduct on webcams.

The conspirators created false social networking profiles posing as teenagers. Some members of the conspiracy would identify and lure children to the websites and show them pre-recorded videos of prior minor victims, often engaging in sexually explicit conduct.

As a result, the new victims thought they were chatting with age-appropriate peers. Using these videos, the conspirators groomed children to engage in sexually explicit conduct on their own webcams, which could be viewed live by multiple adult offenders without the victim’s knowledge.

Videos were automatically recorded and made available for later download. The websites ranked the efforts of members to successfully lure children to the site and to coerce and entice them to engage in sexually explicit conduct on live web camera.

Agents have worked tirelessly to identify the children lured to and exploited on these websites and have so far identified over 350 child victims in the United States alone. [41]

> “Believing they were cloaked in the anonymity of the Internet, the members of the group sexually exploited hundreds of children around the nation and globe through deceit and trickery. This case exemplifies the threat of online predators to the world’s most unsuspecting and vulnerable victims.”
>
> **US Department of Justice**

Crowd sourcing is a means of creating a ‘supply’ of victims by luring children at scale to engage with offenders online. Popular social media sites are among the most commonly used tools, where fake profiles may target hundreds of children at once. In some cases, victims may then be enlisted to engage other children.

Technology

Technology has greatly enriched the lives of a huge proportion of the global population, offering increasingly faster access to new services and improved security, which has for the most part been incredibly beneficial to society. It has allowed people to access content, new communities, like-minded peers and new knowledge and advice.

Technology is, however, also unintentionally creating safe havens for offenders to gain access to content, victims, offending peers and educational material. The same positive aspects of the internet and our smart, connected, global population means that offenders are actively benefiting from the same technologies and approaches that have otherwise enriched people's lives. The use of anonymous or secure services is allowing offenders to gain confidence and the offender community to mature, as the threat of identification and arrest is believed to be reduced.

Accessing and producing content

- Offenders are now able to access CSAM from a range of sources on the open web and from across hidden services (darknet). This may be images or video, which can be streamed from cloud hosted services – similar to modern, commercial film and video subscription streaming services.
- Over a six week period in 2017 Project ARACHNID covered circa 230 million web pages on the open web, detecting 5.1 million pages hosting CSAM and identifying 40,000 unique images of child sexual abuse. Project ARACHNID is now identifying 80,000 unique images per month.[42]
- The number of Cyber Tipline reports received by the National Centre for Missing and Exploited Children (NCMEC) has increased year on year. In 2017 NCMEC received over 10.2 million reports, a marked increase from the 1.1 million it received in 2014.[43]
- The majority of these are made by internet companies reporting indecent images of children. The Internet Watch Foundation saw and increase in the number of countries linked to producing CSAM in 2016 than in 2015 and also identified the increased use of generic top level domains hosting material.[44]
- These content communities are maturing rapidly, with some providing organised libraries of content and the mechanisms to request custom made content. These sites and services have now reached a level of resilience and availability such that many offenders have no need to retain content on local devices, but rather can on-demand stream as required.
- The reduction in the cost of mobile devices and associated video production and storage has permitted offenders to produce first generation, high-quality material with nothing more than their latest mobile phone.
- This content can be uploaded securely, live streamed, or securely shared across a closed community through common applications, which are available on the majority of phones or are part of the handset when it ships.

Accessing potential victims

The internet has provided access to an infinite number of potential victims for offenders.

- Through social media and similar community sites, offenders are able to engage with young people. The ability to remotely access a community of 2.8 billion users, anonymously from a smart device, in a range of locations, means that the level of interaction that offenders are able to conduct is unparalleled in today's connected culture and is often 'unseen' by guardians.

- Anonymous services are allowing multiple personas or avatars, potentially from the same individual to conduct coordinated grooming activity against either a single victim or a particular target community or demographic.
- There is also evidence of children on adult dating and sex service sites, where they are not necessarily hiding their true age and users have failed to report their activity.
- Equally, there are reports of some offenders actively seeking these users via adult sites and this resulting in contact abuse. This is particularly likely when a child questioning their sexuality signs up to a service seeking friendship or support, making them inherently vulnerable.

Accessing significant numbers of peers

Technology has allowed offenders to interact with like-minded people, permitting the threat to evolve and escalate.

- Many of the offender sites on hidden services, such as the darknet have significant numbers of offenders. One CSEA site has as many as 432,235 registered members, with others ranging from a few thousand users.[45]
- Secure, anonymous sites have enabled child sex offenders to gather in communities and develop the worldwide demand for new child abuse material, providing their members with encouragement, validation, training and status and normalising offender behaviour.[46]
- The development of technologies has provided offenders with an unparalleled opportunity to not only access preferential content on-demand, but to network with other likeminded individuals resulting in an eroding of offenders' inhibitions.[47] Technology has facilitated the creation of accepting online communities of accepting like-minded individuals, which exist for all areas of abuse and exploitation.[48] Specific volumes or types of abuse must be owned and demonstrated by a user seeking to join closed communities, as a demonstration of their interest.
- One darknet site has permitted more than 18,000 users with an interest in newborn babies and toddlers to regularly meet and discuss their preference in detail.[49]
- Without new technologies it simply would not have been possible for this number of people with this interest to have gathered. Through modern, freely available technology they are able to confidently and regularly, meet, exchange content, and discuss their preferences in extreme detail, including on 'VIP Producer Areas' which give preferential access to those who frequently provide new content.
- These sites are encouraging and evolving the threat, not only through the normalisation of behaviour but also through the requirement to conduct escalating abuse in order to access more restricted aspects of the site – usually with 'new' content. These sites typically have specific and published access criteria relating to the site's offenders' preferences.

Accessing advice and tools

- The growth of these communities is of extreme concern not only because it fosters the normalisation of offending, but because tradecraft shared in these communities can upskill offenders in accessing victims.
- Secure operating procedures are developed, tested and shared across these communities. These focus on all aspects of offender behaviour, from creating new personas on sites, through to establishing secure or anonymous communication mechanisms to protect the identity and location of the offender and impacting law enforcement ability to disrupt the threat.
- LEAs are seeing the development of offender toolkits and peer to peer advice on techniques

and profile images, which will make the offender more successful in their specified preference. These are continually being updated and developed as part of the community.

- Offenders also share advice on law enforcement or legal approaches and methods, which are often focused on which global locations they should and could travel to for contact abuse, the local law enforcement position on CSEA and mechanisms to circumvent or evade detection.
- As a result of greater and more secure communication between offenders, there is evidence of groups working together to groom children and procure CSAM.
- The development of these communities and network represents a maturing of the threat and the growing diversification and confidence of offenders.

Victim impact and re-victimisation

Beyond the trauma of abuse when it first occurs is the lasting psychological impact that comes with knowing that images or videos depicting your abuse still exist and are unlikely to ever be entirely destroyed.

Even if the original offender has been brought to justice and the victim has been identified, made safe and received support in recovery, once CSAM has been shared the chances are that it will continue to appear on sites and be shared by offenders, in effect re-victimising the child in perpetuity and into adulthood.

In one case, a psychiatrist compared the victim's experience of knowing that her pictures were still being shared to a 'slow acid drip', particularly as they were known to be used as a means of grooming future victims.[50]

> "I live in constant fear that someone will see my pictures and recognise me and that I will be humiliated all over again…I am powerless to stop it…it's like I am being abused over and over and over again."
>
> **Paroline v. United States, Victim Impact Statement**

07 Assessing the total impact of OCSE to societies

The global community needs to quantify the impact of societal harm by improving our assessment of the impact of OCSE on individuals and societies.

The harm caused by OCSE takes an enormous and often life-long toll on the child victims, the families and societies at large.

Victims and families

Wellbeing: personal, financial and social

The impact of abuse and exploitation on the emotional and physical wellbeing of the victim and their family, as well as to the families of offenders, can be life-altering. Though OCSE is a relatively new crime, and the longevity of its effects are less well known, the harm is likely comparable to that of traditional forms of CSEA where victims are more likely to be socially isolated; to suffer from mental health problems; to attempt suicide; and to develop alcohol or illegal drug dependencies. It has also been found that adult survivors of child abuse are more likely than the general population to be re-victimised later in life – for example, through domestic violence.[51] Beyond treatment costs, the impact extends to education, employment, productivity and financial prospects, which diminish for those with poor mental health or addiction.

Society and Common psyche

Recent major enquiries on organised sexual exploitation of children have generated a significant public response. These incidents are likely to have increased awareness of the threat and could have a negative impact on our common psyche, through persistent fear and concern about offenders.

There are significant global environmental differences in how the threat is reported and discussed, from a conspicuous absence of reporting in some areas to sensationalist coverage in others. The effect of exploitative news coverage on our understanding and emotional response to a threat can be significant.

While the impact on each person may be small, the collective impact of our concern for child safety can make parents reluctant to talk to their children about safety online. They may feel that they have no way of protecting them, or feel inclined to shut their children off from the internet altogether.[52]

The rapid growth of OCSE has left a gap between the scale of the threat and our understanding of its impact. There is an urgent need to invest in academic, governmental and industry assessments to close this gap. Ensure that we are prepared both nationally and internationally to invest sufficient resources to prevention, to bring offenders to justice and to support survivors.

Starting to quantify the cost

At present there have only been limited efforts to cost the economic impact of the threat, and none have looked at the impact from a global perspective, due in part to the complexities of reaching an agreement on the best way to carry out such an assessment. While financial settlements for victims can serve as an indicator, and have been reached in some countries, it is harder to quantify the impact on societal 'wellbeing'. Among the available mechanisms to assess the cost of a physical or mental illness is Quality Adjusted Life Years (QALY), which measure a person's health by looking at the cost of treatment against the improvement it makes to quality of life, as a means of understanding the value of healthcare interventions.[53] This offers interesting insights into the costs of mental health conditions and of experiencing trauma, particularly where these costs can be compared over time to conditions such as cancer or physical injury.

In terms of the economic cost, assessments have so far been country specific and tend to take into consideration all forms of child sexual exploitation, though it is likely to be difficult to separate those costs fully. In 2012–13, a conservative estimate of the cost of CSEA to the UK alone reached £3.2 billion annually.[54] Estimates on this scale reinforce the need for a consistent global assessment of the threat's impact.

The investment we make to tackle OCSE should be proportionate in the context of comparable threats. Understanding the manner and extent of its impact is an essential first step.

Responsible news coverage and readily available information that evolves in parallel with the changing nature of the threat are key factors in ensuring child safety online, while the emotional impact of the stress related to addressing the threat cannot be underestimated.

Economic Costs

Healthcare, social services and the welfare state

The economic impact of OCSE is more easily measured, though a country's expenditure does not always reflect the scale of its problem. Healthcare and social services are obvious places where costs are incurred, although it is likely that the impact of OCSE may not be obviously identifiable, particularly when masked by other social or health problems. Equally, reduced productivity or problems that affect job retention are likely to impose a cost on the welfare state which may not be directly attributable to the effects of childhood sexual abuse.

Impacts on the third sector can include intervention work with survivors of abuse, financial or other support to those in need as a consequence of abuse, preventative work with sex offenders and the funding of academic or policy focused work on the subject.

Criminal justice, policing and historical inquests

Costs to criminal justice and policing systems often depend on both capacity and frequency of reporting, with LEAs reporting that they have significant volumes of material that they cannot process as quickly as it comes in. The cultural factors discussed in this paper mean that the scale at which OCSE is now reported is still unlikely to reflect its true scale.

Accordingly, the societal costs (such as wellbeing) may be increasing in the background, while it is likely that criminal justice and policing costs will continue to rise and require a growth in investigative resources. As governments increasingly recognise the scale of the issue, they are likely to also increase spending in safeguarding through preventative work with offenders.

The nature of child sex abuse is such that reporting can often happen years after the fact, as has been the case with the recent watershed of CSEA inquests in the UK. It is highly possible that similar cases relating to OCSE will emerge in future.

Workforce resilience
The retention of a healthy, operational workforce in child protection is difficult, as the nature of the work inevitably impacts on employees' emotional wellbeing. Costs may be incurred by more frequent employee rotations, more frequent recruitment processes, more hands on management needs and potentially for meeting the costs of mental health among child protection professionals.

There is an element of western bias in our current understanding of the economic costs of OCSE, as the factors considered here are mostly focused on the likely costs to developed economies. The economic impact of OCSE is unlikely to have peaked and will in future require greater investment to address it.

Similarly, growing connectivity and uptake of smart devices in developing countries means that state costs in these countries will inevitably increase in coming years.

Sextortion of teenagers engaged in online social networking

In 2017, a 38 year-old Dutch citizen was sentenced to over 10 years in prison for online fraud and cyber blackmail in relation to the exploitation of 39 victims, from countries including the Netherlands, Australia, Norway, the UK and the US.

The primary targets of this abuse were teenagers. The offender gained their trust by posing as someone of a similar age, chatting with them online and then persuading them to perform sexual acts in front of a webcam. He threatened to share images of them with people they knew or post them to pornography sites if they did not continue to comply with his demands.

He did not stop at threats. If the victim did not share more with him, he sent sexual images to the family and friends of the victims or posted the images on the internet, a crime which is now referred to as 'sextortion'.

The same offender is now facing extradition to Canada to face charges in relation to the cyber-bullying of Canadian teenager Amanda Todd. In October 2012, Todd, who was 15 at the time, committed suicide after posting a video online detailing the abuse to which she had been subject. After the initial incident, she had moved schools and home, but been traced by the offender and had her photographs repeatedly shared with classmates and friends. After her suicide, the offender used her images to threaten other victims, telling them they didn't want to end up like Amanda.[55]

> "If you think back to 5 or 6 years ago, unless you intentionally went out and bought a webcam you probably wouldn't have one; whereas today it's difficult to even find a laptop computer, a gaming device or even a cell phone that doesn't have a built in standard webcam that's internet capable, so this crime has become much easier to commit."
>
> **Canadian Police**

Sextortion entails blackmailing somebody online by convincing or intimidating them to share sexually explicit material, then threatening to share that material more widely as a means of coercing the victim to share more, increasingly explicit content. In some cases, offenders have followed a victim over months or years, using social media to stalk and control them.

08 International law, policy and enforcement

OCSE is a persistent and deeply rooted threat. The pace of change is rapid and at present, our response mechanisms are struggling to keep up. The global community needs a consistent approach to addressing the international nature of the threat, underpinned by the Model National Response.

A range of international frameworks, conventions and statutes on child sexual exploitation exist, however, few of them are explicit about online abuse and establish global response strategies.56 Reviewing national responses and legal frameworks around the issue, it is evident that discrepancies exist in both national responses and implementation.[57]

Significant challenges lie in the international nature of the threat, the constraints of relying on policy elsewhere, the lack of reciprocal agreements and the complexity of seeking justice where there is little coordination or regulation between countries.

International law, policy and enforcement frameworks surrounding OCSE should be focused on a consistent approach to addressing the threat, underpinned by consistent uptake of the Model National Response (MNR)58 and the need for the development of a Global Strategic Response.

Consistent global standards

Definitions, standards and terminology

There is currently no consistently used set of standards across governments, LEAs, industry and civil society for referring to and defining OCSE.

The Luxembourg Guidelines provide a mechanism for correct terminology, but are not consistently used.[59] Even law enforcement officials working in the same language do not always refer to types of abuse in the same way, making the processes for international cooperation to bring offenders to justice complex.

As such, definitions around what constitutes abuse and whether certain offender behaviours are criminalised, as well as how law enforcement in different regions categorise and understand victimhood, manifestations of abuse and offender behaviour.

Cultural differences

As discussed earlier in this report, cultural differences around the age of consent, marriage, children and sexual behaviour can all play a complicating role in the pursuit of a global response to OCSE. Setting consistent and agreed definitions of abuse is further complicated by cultural variations such as age of consent against marital norms.

The greater a country's engagement with international treaties, particularly where they have ratified the UN Convention on the Rights of the Child and its Additional Protocols, and the Council of Europe Convention on the Protection of Children from Sexual Exploitation and Abuse, the more consistent their national responses are with standards on age of consent and attitudes to children and sexual activity.

Education and understanding

For many, one of the greatest challenges of the Model National Response has been in their in-country understanding of what the threat is and where it lies.[60] Keeping up with the changing nature of such a diverse, complex and fast-moving threat is difficult when consistent information may be lacking and where perceptions imply that the scale of the threat is less than it is.

Underlining the scale of the threat and ensuring there are frequent assessments, using consistent language, will be key to enabling any effective global response.

Regulating online spaces, anonymity and industry input

Among the greatest challenges that governments face in fighting OCSE is that presented by the integral transnationalism of online spaces, the prevalent use of the darknet and encryption services and the onus on industry to self-regulate social networks, file-sharing sites and apps.

Anonymity

The growth of passively adopted encryption services – particularly in messaging apps – has nurtured an impenetrable space where grooming and exploiting children, and sharing CSAM has been able to flourish. The maturity of online spaces on the darknet, where offenders can engage with one another virtually unchecked, is another deeply concerning example of an area governments struggle to regulate.

Where there is no person, country or organisation obviously responsible for hosting content online, or where those responsible cannot be held to account by the government investigating the offence, LEAs find it incredibly difficult to bring offenders to justice or to have content permanently removed from the internet.

The heightened focus on the need for online privacy for individuals must be carefully balanced with the rights and protection of the vulnerable, and wider society. Offenders cannot be allowed to misuse privacy measures to exploit and abuse children. It is therefore essential that government authorities have access, under due process, to the necessary data and evidence to protect children, to ensure effective investigation and support prosecution of offenders.

Industry input

It must be specified that technology and social media companies face huge challenges in managing the use of their sites, apps and devices and preventing their use for grooming, sextortion, capability building or rich media distribution.

Responses to the MNR reporting survey indicate that governments feel they are lacking mechanisms to regulate industry.[61] Cooperation to regulate online spaces and swift collaboration with LEAs is essential, as is information sharing across industry and across borders to develop best practice.

To tackle the illegal use of everyday platforms and services effectively, there will be an increasing reliance on industry partners to act, by:

- creating products and services that are ‘safe by design’;
- stopping CSAM material being shared or generated via their platforms;
- proactively identifying and taking action to remove material;
- proactively identifying those who seek to use their platforms to groom and exploit vulnerable people;
- investing in global technology innovation and making it available across the wider, trusted, industry community;
- contributing to a comprehensive understanding of the threat through forums with government, international and non-governmental organisations and law enforcement partners.

Interoperability and collaborative justice

Amplifying the debate and recognising a global issue

The engagement of LEAs, government, industry and civil society through the growth of global advocacy networks focused on ending OCSE is promising, but advocates must ensure that debate is reflected in their national conversations.

The MNR has been adopted by a geographically diverse range of countries, however areas remain

where adoption rates have been low. Enlisting regional bodies to take responsibility for raising local engagement could help to bring more countries on board.

Amplifying the public conversation is essential to ensuring that governments are held accountable for working domestically and internationally to end all forms of violence against children. Ensuring the public is clearly and responsibly informed is essential to effective civil society engagement.

Building and implementing an international investigatory commitment

Child sexual abuse is not a new phenomenon, but the capabilities the internet has given to potential offenders has transformed the threat making it a global issue, which requires a global response.

Solely focusing on a national level response will not meet the international challenges of this global threat. Recognition of this fact is the first step to developing more collaborative and therefore effective approaches to safeguarding and justice; especially in the face of a resilient, evolving offender community. Particularly in developing countries, law enforcement agencies face technology challenges in their ability to track and identify offenders.[62]

Where a victim is located in one location and an offender in an apparent other and the internet service being hosted elsewhere – LEAs are forced to rely on cooperation, hindered by the challenges presented by differing priorities, definitions of abuse and extradition policies.

LEAs have reported instances in which an offender has targeted victims overseas, the offender's country would not extradite its own citizens and the offender was essentially free to continue exploiting victims globally.

The collective global community is now more reliant than ever on one another's national legislation and engagement. Establishing reciprocal agreements – including on areas such as extradition and primacy – and common response frameworks is essential, but meaningless without implementation. Ensuring an international investigatory commitment to combating the threat, which extends to cover the effective implementation of existing laws and regulations needs to be a priority for national governments, LEAs and industry.

There is a view from some LEAs that greater international engagement on law enforcement has galvanised in-country responses to safeguarding, a trend that must be encouraged to continue.

Safeguarding as the priority

The work that LEAs around the world are doing to bring offenders to justice and ensure they cannot do further harm is invaluable. However, the importance of building an international investigatory commitment must be secondary to the need for a renewed emphasis on victim safeguarding and prevention.

Emphasis needs to be placed on reducing the risk to children through education, greater parental engagement with the issue and stronger safeguards online.

Effort should also be targeted towards encouraging potential offenders to come forward and seek preventative treatment in a safe and confidential space before they do harm, as well as on working to rehabilitate convicted offenders and prevent reoffending.

Where countries have strong track records and experience, they should be empowered to take a leading role in sharing best practice.

Putting these priorities front and centre will be crucial to any global effort to end OCSE.

09 Looking ahead

This Global Threat Assessment shows us in stark terms how criminals with a sexual interest in children continue to leverage technology to achieve their ends. We are now seeing the facilitation and growth of large offender communities, with safe havens in hidden corners of the web. This feeling of impunity has enabled diversification of their methods of operation, resulting in new and persistent threats.

We must act now. Technology will only become more advanced; access to the internet more easily available; and therefore, the threats to children more imminent and diverse. The consequences of online child sexual exploitation are devastating, and we are only beginning to quantify the impact and damage that it can have. All this means we must act now.

In response to this threat assessment, the WePROTECT Global Alliance will coordinate and target the global effort towards tackling the new challenges we face. We will:

- Continue to support national efforts to tackle online child sexual exploitation through our Model National Response.
- Work more closely with the technology sector, law enforcement and civil society to innovate against the threat.
- Drawing on our Threat Assessment, identify and promote action that needs to be taken on an international basis through a Global Strategic Response.

Today, through the WePROTECT Global Alliance, you can join this fight and become part of the global solution to this heinous crime.

10 Endnotes

1. www.comscore.com/Insights/Presentations-and-Whitepapers/2017/The-2017-US-Mobile-App-Report (accessed 30 January 2018)
2. Cisco Visual Networking Index: Forecast and Methodology, 2016–2021 (CISCO: pg. 17)
3. Cisco Visual Networking Index: Forecast and Methodology, 2016–2021 (CISCO: pg 6)
4. Cisco Visual Networking Index: Forecast and Methodology, 2016–2021 (CISCO: pg 3)
5. Statista Digital Economy Compass April 2017 (Statistica: pg 22)
6. 'Internet Organised Crime Threat Assessment' (Europol, 2016: pg. 26)
7. www.telegram.org/blog/100-million (accessed 30 January 2018)
8. www.statista.com/statistics/693959/leading-google-play-communication-apps-worldwide-by-revenue/ (accessed 30 January 2018)
9. TORproject.org (accessed 30 January 2018)
10. 'Average selling price of smartphones worldwide from 2010 to 2016 (in U.S. dollars)' (Statista, accessed 30 January 2018)
11. 'A startup is making a $30 dollar smartphone in Africa' (Business Insider, accessed 30 January 2018)
12. www.statista.com/statistics/263441/global-smartphone-shipments-forecast/ (accessed 30 January 2018)
13. US Department of Justice, January 2018
14. INTERPOL, January 2018
15. US Department of Justice, January 2018
16. 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.' (UNODC, 2015: pg. 23)
17. 'The commercial sexual exploitation of children in Latin America.' (ECPAT International, 2014: pg.8)
18. 'Victims are not virtual.' (UNICEF, 2016: pg. 16)
19. 'Global study on sexual exploitation of children in travel and tourism.' (ANPPCAN, 2015: pg. 16)
20. 'Offenders on the move: Global study on sexual exploitation of children in travel and tourism.' (ECPAT International, 2016: pg. 107)
21. 'Digital dangers: the impact of technology on the sexual abuse and exploitation of children and young people.' (Barnardo's 2015: pg. 27)
22. 'Emerging global threats related to the online sexual exploitation of children.' (ECPAT International Briefing Paper: pg. 1)
23. 'Victims are not virtual.' (UNICEF, 2016: pg. 15)
24. International Justice Mission: www.ijmuk.org/cyber-trafficking (accessed 30 January 2018)
25. US Department of Justice, January 2018
26. US Department of Justice, January 2018
27. 'NetClean: Eight Important Insights into Child Sexual Abuse Online.' (NetClean, 2017: pg. 17)
28. 'Information and communications technology and child sexual exploitation.' (UN Human Rights Council, 2015: pg. 14)
29. 'Sexual exploitation of children in travel and tourism in South East Asia.' (ECPAT International, 2015)
30. 'Online Child Sexual Exploitation: an analysis of emerging and selected issues.' (ECPAT International 2017: pg. 56)
31. 'A review of the research on children and young people who display harmful sexual behaviour online.' (NSPCC, 2016: pg. 18)

32. ‘Young people, sex and relationships: the new norms.’ (Institute for Public Policy Research, 2014: pg. 21)
33. CEOP, National Crime Agency (UK), January 2018
34. ‘A review of the research on children and young people who display harmful sexual behaviour online.’ (NSPCC, 2016: pg. 38)
35. ‘Behaviour and characteristics of perpetrators of online facilitated child sexual abuse and exploitation.’ (NatCen Social Research, 2017: pg. 34)
36. ‘The National Strategy for Child Exploitation Prevention and Interdiction.’ (US DoJ, 2016: pg. 71)
37. ‘Threat Assessment.’ (Global Alliance Against Child Sexual Abuse Online, 2016: pg. 4)
38. ‘Technology Briefing Series: Online Child Sexual Abuse Imagery.’ (Demos, 2018: pg. 7)
39. US Department of Justice, January 2018
40. Information provided by international law enforcement agencies, January 2018
41. US Department of Justice, January 2018
42. Project Arachnid: www.cybertip.ca/app/en/projects-arachnid (accessed 30 January 2018)
43. Annual Report (NCMEC, 2014); Annual Report (NCMEC, 2015); Annual Report (NCMEC, 2016); US Department of Justice Annual Report (NCMEC, 2014); Annual Report (NCMEC, 2015); Annual Report (NCMEC, 2016); US Department of Justice
44. Annual Report (Internet Watch Foundation, 2016: pg. 10)
45. US Department of Justice, January 2018
46. ‘The National Strategy for Child Exploitation Prevention and Interdiction.’ (US DoJ, 2016: pg. 73)
47. ‘Final Report.’ (EU Online Grooming Project, 2012: pg. 8)
48. ‘Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.’ (UNODC, 2015: pg. 34)
49. US Department of Justice, January 2018
50. US v. McDaniel, 631 F3rd 1204 (11th Circ 2011)
51. ‘Effects of child abuse and neglect for adult survivors.’ (Child Family Community Australia, 2014)
52. ‘What should I do? NSPCC helplines: responding to children’s and parents’ concerns about sexual content online.’ (NSPCC, 2014)
53. National Institute for Health and Care Excellence Glossary (accessed 30 January 2018)
54. ‘Estimating the costs of child sexual abuse in the UK.’ (NSPCC, 2014)
55. US Department of Justice, January 2018
56. ‘Victims are not virtual.’ (UNICEF, 2016: pg. 25)
57. ‘Framing Implementation: A Supplement to Child Pornography: Model Legislation & Global Review’ (ICMEC, 2017)
58. ‘Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response’ (WePROTECT Global Alliance, 2016)
59. ‘Terminology Guidelines for the Protection of Children from Sexual Exploitation and Abuse.’ (ECPAT International, 2016)
60. Home Office (UK) Responses to Model National Response Survey (2017)
61. Home Office (UK) Responses to Model National Response Survey (2017)
62. Home Office (UK) Responses to Model National Response Survey (2017)

Find out more

You can find more information on our website
www.weprotect.org

or follow us on Twitter @weprotect