




**Online  
Child Sexual Abuse:  
The Law Enforcement  
Response**



A contribution of ECPAT  
International to the World  
Congress III against the Sexual  
Exploitation of Children and  
Adolescents

*Rio de Janeiro, Brazil  
25–28 November 2008*



This thematic paper was written by Victoria Baines, CEOP Principal Analyst, on behalf of ECPAT International as a contribution to the World Congress III against Sexual Exploitation of Children and Adolescents.

Series Editor: Professor Jaap Doek

The views expressed are those of the author and do not necessarily reflect those of ECPAT International, Government of Brazil, NGO Group for the Convention on the Rights of the Child, or UNICEF nor endorsement by the Central Organizing Committee of the Congress.

The writing and research of this thematic paper have been made possible through the generous grants from the Swedish International Development Cooperation Agency (SIDA), the Ministry of Foreign Affairs of the Grand Duchy of Luxembourg, the Ministry of Foreign Affairs of France, Groupe Développement, ECPAT Luxembourg, Irish Aid, OAK Foundation, International Child Support (ICS), UBS Optimus Foundation, Church of Sweden, Bread for the World and AusAID.







**Online Child Sexual Abuse:  
The Law Enforcement Response**  
Dr Victoria Baines, CEOP Principal Analyst,  
on behalf of the Virtual Global Taskforce

Submitted by ECPAT International

# Table of Contents

<b>Acknowledgments</b>	<b>I</b>
<b>List of Acronyms</b>	<b>II</b>
<b>Executive Summary and Introduction</b>	<b>1</b>
The Virtual Global Taskforce	3
The Scale of the Problem	4
The Changing Online Environment	5
<b>1 Developments since World Congress II</b>	<b>7</b>
1.1 The Legal Framework	7
1.1.1 Virtual Child Abuse Material	9
1.1.2 Online Solicitation	10
1.2 Law Enforcement Resources and Expertise	11
1.3 International Collaboration	15
1.3.1 Harm Reduction and Capacity Building	16
1.3.2 Technical Tools and Victim Identification	18
1.4 Collaboration with Partner Agencies/Inter-Sectoral Working	21
1.4.1 The CEOP Model	22
<b>2 The Current Nature of Online Child Sexual Abuse</b>	<b>27</b>
2.1 Key Trends	28
2.2 Child Abuse Image Distribution	33
2.3 Volume of Images and Data Storage	34
2.4 Encryption	37
2.5 Wireless Technology	37
2.6 Mobile Technology	38
<b>3 Research and Development</b>	<b>39</b>
3.1 Commercial Exploitation	39
3.2 International Collaboration	40
3.3 Child Abuse Material	41
3.4 Young People who Display Sexually Harmful Behaviour	41
3.5 Offender Profiles	42
3.6 Further Ongoing Research and Related Developments	43
3.7 Technical Tools	43
<b>4 Concluding Remarks</b>	<b>45</b>
<b>Endnotes</b>	<b>47</b>
<b>Bibliography</b>	<b>50</b>

# Acknowledgments

This paper has been produced in consultation with experts in member agencies of the Virtual Global Taskforce (VGT): the UK Child Exploitation and Online Protection (CEOP) Centre; Interpol; the Australian Federal Police High Tech Crime Centre (AHTCC); the Royal Canadian Mounted Police National Child Exploitation Coordination Centre (NCECC); the US Department for Homeland Security Immigration and Customs Enforcement (ICE), and the Italian Postal and Communications Police. Special thanks go to them and to staff from the FBI and the National Center for Missing and Exploited Children (NCMEC) for contributing data and analysis.

# List of Acronyms

<b>AFP</b>	Australian Federal Police
<b>AHTCC</b>	Australian Federal Police High Tech Crime Centre
<b>BAU</b>	Behavioural Analysis Unit
<b>CEOP</b>	Child Exploitation and Online Protection Centre
<b>CETS</b>	Child Exploitation Tracking System
<b>CSP</b>	Communications Service Provider
<b>EU</b>	European Union
<b>FBI</b>	Federal Bureau of Investigation
<b>ICAID</b>	Interpol Child Abuse Image Database
<b>ICE</b>	Immigration and Customs Enforcement (US Department for Homeland Security)
<b>ICMEC</b>	International Centre for Missing and Exploited Children
<b>ICSE</b>	International Child Sexual Exploitation Database
<b>ICT</b>	Information and Communication Technology
<b>IM</b>	Instant Messaging
<b>IP</b>	Internet Protocol
<b>ISP</b>	Internet Service Provider
<b>IWF</b>	Internet Watch Foundation
<b>IYAC</b>	International Youth Advisory Congress
<b>MoU</b>	Memorandum of Understanding
<b>NCECC</b>	National Child Exploitation Coordination Centre (Royal Canadian Mounted Police)
<b>NGO</b>	Non-Governmental Organisations
<b>NSPCC</b>	National Society for the Prevention of Cruelty to Children
<b>OCG</b>	Organised Crime Group
<b>P2P</b>	Peer-to-Peer
<b>RBNet</b>	Russian Business Network
<b>UK</b>	United Kingdom
<b>URL</b>	Unique Resource Locator
<b>US</b>	United States
<b>VCoIP</b>	Video Chat over the Internet Protocol
<b>VGT</b>	Virtual Global Taskforce
<b>VoIP</b>	Voice Over the Internet Protocol

# Executive Summary and Introduction

This paper presents the law enforcement response since 2001 to the activity commonly referred to as online child sexual abuse, as experienced by member agencies of the Virtual Global Taskforce (VGT). The paper comprises i) a discussion of progress made since the Second World Congress regarding legal, resourcing, collaborative and partnership issues, ii) an assessment of the current and emerging threats to the protection of children and young people from sexual abuse online and to law enforcement investigation of such activity, and iii) a brief outline of future research and development with the potential to contribute positively to our understanding and to improve our investigation of online child sexual abuse.

Key findings are as follows:

- There is still some way to go to achieve equivalent legislation in all jurisdictions against the online sexual abuse of children. Discrepancies can cause difficulties for investigations both at home and abroad and, whilst criminalisation of these activities is essential, adequate provision must be made in those countries with new legislation to ensure successful investigative outcomes. Legislative provision must also continue to be responsive to changes in abusive behaviours and the environments for abuse.
- Law enforcement agencies, including members of the VGT, have made substantial headway in facilitating cross-jurisdictional investigations and information sharing. This has been achieved at practitioner level, rather than as a result of multilateral agreements or cooperation between nations at government level.
- There is also compelling evidence of increased inter-sectoral working, most notably in the UK Child Exploitation and Online Protection (CEOP) Centre and the National Child Exploitation Coordination Centre (NCECC) in Canada, in full recognition that the online sexual abuse of children cannot successfully be combated by any one of the child protection stakeholders in isolation. Rather, successful investigation and crime prevention are achieved through integrated partnership with the private sector, non-governmental organisations (NGOs), education specialists and other stakeholders.
- More can be done in this regard, however, particularly in relation to Internet and Online Service Providers. These should produce transparent child protection strategies and be accountable for providing a mechanism for reporting directly to law enforcement from the online environment in which the sexual abuse of children is experienced or detected.

- There is a requirement for all governments to include the sexual abuse of children amongst their national policing priorities, thereby facilitating the provision of adequate investigative and child protection resources at national and local levels. As access to the Internet continues to proliferate, accompanied by the mainstream introduction of mobile and wireless Internet technologies and an explosion in child abuse image distribution via peer-to-peer (P2P) file-sharing networks, the number offences to be investigated by law enforcement is increasing dramatically, and is likely to continue to do so.

### *A note on definitions*

For the purposes of this paper the term ‘online child sexual abuse’ comprises the following activities:

- The production, distribution, downloading and viewing of child abuse material (both still and video images), also known as child pornography.<sup>1</sup>
- The online solicitation of children and young people to produce self-generated child abuse material, to engage them in sexual chat or other online sexual activity, or to arrange an offline meeting for the purposes of sexual activity, also known as grooming or luring.
- The facilitation of any of the above.

The author of this document is aware that not all of the above are deemed to be illegal/criminal acts in all countries of the world – indeed, as will be discussed below, legislation can differ even amongst the nations in which VGT member agencies operate. Since, however, it is in the interests of child protection worldwide for these activities to be viewed as equally serious by law enforcement agencies regardless of jurisdiction, they will be discussed on the basis that they are universally recognised as harmful and reprehensible and are established as criminal offences in the forthcoming Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*.

Changes in the nature of sexual offending against children and young people, facilitated by technological developments such as the availability of digital cameras, web cameras (webcams) and peer-to-peer (P2P) file-sharing technologies, have served to blur the traditional distinction between ‘child sexual abuse’ and ‘child sexual exploitation’ adhered to in some legal instruments. The production of child abuse material, for example, is undoubtedly exploitative, in that it violates the rights of a child or young person for gain, be this commercial or in terms of sexual gratification or enhanced status in a paedophile network. At the same time, however, child abuse images are just that – images of the sexual abuse of children, not solely of their exploitation.

Equally, children and young people are sexually exploited in a number of ways which are not primarily commercial. One example is the online solicitation of children and young people to obtain self-generated webcam-enabled child abuse material for sexual gratification and for non-commercial distribution to other like-minded individuals: no money changes hands, but the scenario is clearly as exploitative as it is abusive. To this end, national specialist units such as the UK CEOP Centre and the NCECC in Canada do not confine themselves to cases of, for example, commercial sexual exploitation, but investigate all incidents in which a child or young person is alleged to have experienced sexual abuse online. Changes in the nature of offending facilitated by technological developments have engendered this overlap between what is 'abusive' and what is 'exploitative': as a result, this VGT assessment does not seek to distinguish between these two terms, and uses them interchangeably.

## The Virtual Global Taskforce

The VGT is composed of specialist law enforcement agencies from around the world working together to fight child abuse online, and was established in 2003. Its current membership comprises:

- UK Child Exploitation and Online Protection (CEOP) Centre
- Interpol
- Australian Federal Police High Tech Crime Centre (AHTCC)
- Royal Canadian Mounted Police National Child Exploitation Coordination Centre (NCECC)
- US Department for Homeland Security Immigration and Customs Enforcement (ICE)
- Italian Postal and Communications Police

The aim of the VGT is to build an effective, low cost, high impact, international partnership of law enforcement agencies that helps to protect children from online child abuse, and its specific objectives are:

- To make the Internet a safer place for children and young people;
- To identify, locate and help children and young people at risk; and
- To hold perpetrators appropriately to account.

Throughout this paper, case studies detailing operational and harm-reduction initiatives will illustrate the meeting of these objectives and any obstacles which may impact upon the effectiveness of current law enforcement intervention.

Since this paper draws for the most part on information and analysis supplied by those law enforcement agencies that are members of the VGT, it cannot be said to be representative of all law enforcement experiences worldwide, e.g. those of developing countries. It is, however, an accurate assessment of the nature of and scope for online child sexual abuse in a number of countries with specialist centres for its investigation, based on the information available to them.<sup>2</sup>

## The Scale of the Problem

Law enforcement agencies are often asked to determine the extent and scale of sexual offending against children and young people on the Internet, e.g. the number of child abuse images in circulation, or the number of people prosecuted. In the context of the boundless and constantly expanding online world, numbers are unhelpful. We can say, for instance, that fewer than 3,000 web domains were reported to the Internet Watch Foundation (IWF) for child abuse content in the 2007 calendar year.<sup>3</sup> This does not, however, provide an accurate assessment of the scale of image distribution because i) each domain can contain any number of individual pages (and therefore the number of pages is likely to be much higher than the number of domains) and ii) as will be discussed in the threat assessment in Chapter 3, distribution via pay-per-view websites is now just one means by which child abuse material is accessed. With regard to prosecutions, only those countries which legislate against the possession and distribution of child abuse material will necessarily be able to provide conviction rates and, indeed, have the resources to investigate these activities.<sup>4</sup> By the same token, in those countries where conviction rates are available, levels may be subject to considerable fluctuation due to investigative activity, and may therefore not accurately reflect the scale of offending per se. This is the case with regard to proceedings for Possession of Indecent Images of Children in the United Kingdom (UK), which increased by 143 per cent in 12 months (from 738 in 2002 to 1,790 in 2003), largely as a result of Operation Ore, the UK branch of the investigation into pay-per-view access to child abuse images by subscribers to the Landslide database.

What is clear is that the amount of identified traffic in child abuse material is greater than the law enforcement resources dedicated to investigate it.<sup>5</sup> Moreover, technological

developments since 2001 have ensured that individual collections of images have continued to increase in size and, whilst technological advances have also improved law enforcement techniques, this has had inevitable consequences for law enforcement resources and investigative capacity.

## The Changing Online Environment

Since 2001, the number of Internet users worldwide has increased by 205 per cent, from 479 million in June 2001 to 1463 million in June 2008: this same period has seen an increase in global coverage from 7.9 per cent of the world's population to 21.9 per cent.<sup>6</sup> The number of web pages has likewise increased by 403 per cent, from c.35 million in October 2001 to c.176 million in July 2008, and this number continues to grow by 3.14 million sites per month.<sup>7</sup> Increasing bandwidth and storage capacity have been accompanied by the mainstream availability of wireless and Internet-enabled mobile phone technology, whilst social and P2P functionalities have revolutionised the way Internet users communicate, network and share files.

In 2001, an individual engaging in the online sexual abuse of children and young people typically accessed the Internet using a dial-up connection, networked and shared child abuse images with each other using Internet Relay Chat (IRC) and Direct Client-to-Client (DCC) protocol, also perhaps purchasing images from pay-per-view websites, and was commonly limited to a maximum of 40 GB of data storage and opportunities to meet young people online in chatrooms. Whilst these avenues continue to be utilised in 2008, such an individual may prefer to or additionally use a high-speed broadband connection simultaneously to exchange hundreds of print-quality child abuse images and video files instantaneously and network with like-minded individuals via publicly available peer-to-peer file-sharing and instant messaging software, whilst using social, gaming and instant messaging functionalities to gain access to children and young people susceptible to online solicitation – be this to obtain self-generated abuse material produced on a child's webcam, to engage in other forms of online sexual activity or to effect an offline meeting. There is little doubt that the explosion in Internet accessibility and usability in recent years has made child abuse material more available to more people,<sup>8</sup> has given offenders more opportunity to share more images, and has enabled these and other individuals to contact children previously unknown to them as never before, to the extent that 15 per cent of 10-15 year olds surveyed in the United States (US) have been subject to sexual solicitation online in the last year.<sup>9</sup>

At the same time, it is evident that the thematic paper on *Child Pornography*<sup>10</sup> presented to the Second World Congress in Yokohama in 2001 highlighted key issues and made several recommendations which remain pertinent to tackling online child sexual abuse in 2008. The following section discusses Law Enforcement's response to these from the perspective of VGT. As will become evident, these key considerations are interconnected, to the extent that developments in one area have the potential to impact significantly on capacity in another.

# 1. Developments since World Congress II

## 1.1 The Legal Framework

The thematic paper for the Second World Congress recommended that a determined effort be made to harmonise national and international laws and definitions of ‘child pornography’;<sup>11</sup> accordingly, this was one of the aims of the 2001 Council of Europe *Convention on Cybercrime* (CETS No.185, Article 9). Whilst there is little doubt that equivalence in legislation across jurisdictions would improve the effectiveness of multi-jurisdictional investigations, there is yet to be significant progress in this regard. Indeed, as Moore and Clayton observe, optional aspects in the *Convention on Cybercrime* render it liable itself to abuse:<sup>12</sup> whilst a ‘minor’ is defined as “all persons under 18 years of age”, the addendum that “a party may, however, require a lower age-limit, which shall not be lower than 16 years” (Article 9.3), means that equivalence even of the age of majority as regards child pornography is not achieved, resulting in an age of majority of 16 for the subjects of such material in certain jurisdictions.<sup>13</sup>

This is not simply a question of legislative idiosyncrasy: the investigative reality is that an individual producing material in which a 17-year-old is sexually abused will not be prosecuted in such circumstances, nor will there be a guarantee of related victim identification or contribution to international databases of child abuse material in these cases. VGT therefore welcomes the definition without opt-out of a child as “any person under the age of 18 years” in the 2007 Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (yet to come into force at the time of writing),<sup>14</sup> but recognises that the clear definition of the age of a child needs to be extended to nations outside the European Union (EU), and notes that the fact that the *Convention* leaves the age of consent to sexual activity for states to determine is likely to be problematic for those investigating forms of online sexual abuse such as solicitation which do not constitute ‘child pornography’ according to the definitions stated.<sup>15</sup>

By the same token, the final clause of the 2001 *Convention on Cybercrime*, which states that “each party may reserve the right not to apply, in whole or in part” the procurement or possession of child pornography, perpetuates discrepancies in outcomes for investigations which cross jurisdictions. It remains the case that many nations do not legislate against the possession of images of child sexual abuse: a study conducted by the International Centre for Missing and Exploited Children (ICMEC) in 2006 identified that of the then 184 Interpol member countries, over half (95) had no laws whatsoever addressing

indecent images of children, and of those that did 41 did not criminalise their possession.<sup>16</sup> Again, there is no guarantee that law enforcement agencies that lack legislation against the possession of child abuse images will seize such material, work to identify previously unseen young subjects or indeed expedite the investigations of other nations into online child sexual abuse. And whilst the 2007 *Convention on Child Protection* urges nations to criminalise possession, criminalisation of access to child abuse material – viewing without downloading – remains optional.<sup>17</sup>

A number of VGT member agencies are able to prosecute their own nationals who commit such offences overseas. It is evident, however, that in addition to the potential for the indigenous online exploitation of children to go unchecked, a comparative lack of focus on online sexual offences against children in some countries has the potential to hinder successful investigation and prosecution of nationals from VGT countries who have committed offences overseas: as Jewkes and Andrews note,<sup>18</sup> due to the global character of the Internet international discrepancies in legislation can prevent a successful outcome even of investigations conducted in those countries with comparatively robust legislation against online child sexual abuse. Accordingly, where cooperation is secured it is often as a result of Memoranda of Understanding (MoU) between individual countries, rather than a multilateral understanding of the seriousness of these crimes amongst law enforcement agencies worldwide. Whilst VGT member agencies already undertake awareness raising work with foreign law enforcement representatives in this regard in VGT home nations, further awareness raising and capacity building in, for example, destination countries for travelling sexual offenders is urgently needed.

Equivalent legislation in all jurisdictions would undoubtedly offer enhanced protection to children and young people worldwide: any projected changes in legislation must, however, also be accompanied by the provision of adequate additional investigative capacity. And whilst this might most obviously apply to developing nations with very limited resources, equally it has the potential to have a detrimental impact on the efforts of specialist units such as VGT member agencies. For example, the UK *Criminal Justice and Immigration Act* 2008 (given royal assent on 9 May 2008) has dispensed with the previous requirement for ‘dual criminality’ for offences committed by UK subjects overseas, i.e. that there be a like offence in the country in which the subject has been operating in order to secure prosecution in the UK.<sup>19</sup> This is very welcome in that i) it may safeguard individual children in destination countries from further abuse and ii) it closes a loophole which travelling sexual offenders from the UK are known to have exploited, having chosen overseas destinations precisely because of, for example, a lower age of consent or an absence of legislation against child abuse images. In the long-term it may therefore act as a deterrent measure, since UK subjects who sexually abuse children and young people can now no

longer evade prosecution. However, it also is likely in the short and mid terms to have an impact on the workloads of UK police forces, especially in light of the aforementioned lack of equivalence in legislation and, by extension, prioritisation.

### 1.1.1 Virtual Child Abuse Material

The *Convention on Cybercrime's* definition of 'child pornography' includes "realistic images representing a minor engaged in sexually explicit conduct" (9.2.c), and under 9.4 each party may reserve the right to opt out of applying this definition. Such imprecision is perhaps symptomatic of the current confusion and lack of consensus concerning computer-generated child abuse imagery. In the first place, the mainstream availability of photo-editing software has led to the emergence of pseudo-photographic images which place children in abusive scenarios or otherwise sexualise them: to this end, VGT member agencies have received reports of instances in which individuals have hijacked legitimate images of young people from social networking profiles and have made them "look naked", subsequently using these images to coerce the same young people into engaging in sexual acts on webcam. Such pseudo-photographs are illegal in the UK and Canada: in the US, however, the Supreme Court held in *Ashcroft v. Free Speech Coalition* 2002 that since no real children were involved in creating this type of material, its ban under the *Child Pornography Prevention Act* of 1996 (CPPA) was unconstitutional and therefore invalid.<sup>20</sup>

Research to date has focussed largely on the issue of pseudo-photographic material. The emerging issue for law enforcement, however, in terms of offending behaviour, is that of non-photographic material, eg the use of *lolicon* or *shotacon hentai* (Japanese cartoons or animation depicting the sexual abuse of young girls and young boys respectively),<sup>21</sup> or the much-publicised 'age play' in virtual worlds such as Second Life. Advances in computer graphics and modelling in recent years have given rise to the development of complex online environments which are misused by some for the creation and distribution of realistic virtual images of child sexual abuse, thereby potentially fuelling the demand for such material and the depiction of sexualised virtual interactions.

Non-photographic representations present legislative discrepancies, even amongst the member nations of the VGT. They are, for instance, covered by the Canadian *Criminal Code*, in which the definition of child pornography includes any visual representation, photographic or otherwise (163.1.a), and the UN *Optional Protocol to the Convention on the Rights of the Child* (2002) defines 'child pornography' as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child primarily for sexual purposes". But this material is not as yet illegal in the UK: a Home Office consultation has recommended that distribution, making

(downloading) and possession of non-photographic child abuse images be a ‘stand alone’ offence, carrying more lenient penalties than those for possession of photographs or pseudo-photographs. Furthermore, in the most up-to-date piece of international legislation, the 2007 Council of Europe *Convention on the Protection of Children*, the criminalisation of “simulated representations or realistic images of a non-existent child” is optional.<sup>22</sup>

The production of non-photographic child abuse images may not be a contemporaneous record of an abuse scenario, but it may just as easily be a recollection of a real event with an identifiable child. And even in those cases where the abuse scenario is purely fictitious – the product of an individual’s fantasy, say – exposure of a child or a young person to such material may cause her/him significant harm, and in some cases features in the grooming process, factors which surely must be taken into consideration when deciding whether such activity should be criminalised. Ultimately, differences in legislation which result in a variety of outcomes and sentence lengths for offences which are essentially the same can be exploited by offenders, even to the extent of choosing to reside in countries where there is a smaller of risk of prosecution and lower penalties and shorter sentences than in a subject’s country of origin.

### **1.1.2 Online Solicitation**

There is also a requirement to recognise that advances in Internet-based technologies have given rise to proliferations in forms of child sexual abuse which cannot strictly be defined as relating to the production and distribution of child abuse images, e.g. solicitation or grooming, and that many nations do not legislate against these activities. Absence of legislation inevitably results in a lack of law enforcement focus on any such activity; conversely, in those countries where it is in force, legislation against online solicitation often serves to prevent the contact sexual abuse of children and young people, in so far as it disrupts inappropriate online relationships before they have the opportunity to escalate and move offline: with this in mind, 40 per cent of investigations conducted by the UK CEOP Centre concern alleged grooming activity. Simply put, the Internet has changed almost beyond recognition since 2001, and legislation needs to evolve in order to keep pace. At the very least, law enforcement agencies around the world must be enabled to gather and analyse intelligence concerning the online solicitation behaviours of their citizens in order to identify i) the environments in which children and young people are most at risk, ii) the methods by which adults engage them in inappropriate relationships, and iii) suspect persons who may be deemed worthy of further investigation. At present, legislative differences not only hinder efforts to hold perpetrators to account, but also efforts to regulate the Internet at both national and international levels, and to access data for investigative purposes. In addition to proactive work, law enforcement looks to members of the public and online service providers to report incidents of alleged

solicitation to the appropriate authorities. In most countries it is not, however, mandatory for Internet service providers (ISPs) to monitor online chat, nor is there an international standard for the retention of online data: there remain countries in which there is no legal obligation for ISPs to store data; as for the rest, data retention periods vary from a few hours to a maximum of five years. VGT therefore welcomes the 2007 Council of Europe *Convention on the Protection of Children's* criminalisation of the solicitation of children through sexual purposes through information and communication technologies (ICTs), again recognising the need for this to be extended to jurisdictions beyond the EU.

## 1.2 Law Enforcement Resources and Expertise

The thematic paper for World Congress II deemed it “vital to develop expertise and resources within national law enforcement agencies to ensure they have the right personnel and technology to allow them to act against child pornographers in their own countries, but also to participate in international actions against them”.<sup>23</sup> Since Yokohama a number of nations have established specialist centres for the investigation of online child sexual abuse, and member agencies of VGT are just some of them. Given the unprecedented expansion of publicly available Internet technologies, however, the opportunities for offending continue to outstrip the capacity of even the best resourced of these centres. At a grass-roots level, it remains the case even amongst some VGT nations that whilst awareness of the seriousness of online child sexual abuse is improving failure at government level to designate the investigation of such criminal activity as a policing priority results in the under-resourcing of local investigative capability.<sup>24</sup> Klain, Davies and Hicks’s observation in 2001 that “child sexual exploitation is not a priority in many jurisdictions especially when competing for attention with street violence, gang activity, and drug trafficking”<sup>25</sup> holds true seven years later, despite significant public interest in child protection and media attention afforded to this type of criminality: failure to include online child sexual abuse in government policing plans necessarily results in a lack of prioritisation and resourcing at both national and local levels.

Whilst specialist centres provide national coordination of intelligence, and are the focal points for international collaboration and technical resources such as forensic analysis and covert Internet investigation, the majority of investigations and arrests still fall to local territorial police forces, since the national centres are not sufficiently resourced to assume responsibility for all such crimes committed within a jurisdiction: this is consistent with Wolak, Mitchell and Finkelhor’s findings that two-thirds (66 per cent) of US investigations into Internet sex crimes against minors in 2000–2001 originated in non-specialised agencies.<sup>26</sup>

As Wortley and Smallbone note, the role of these local forces is vital,<sup>27</sup> however, the sheer size of the Internet, and the potential implications of investigating crimes committed in such a global arena, can put local resources under considerable strain. One commonly observed phenomenon concerns the investigation of subscribers to pay-per-view child abuse image websites. This type of investigation tends to involve very large numbers of suspects and different lines of enquiry, which themselves may create logistical difficulties for policing units.<sup>28</sup>

Typically, a local police force will receive details only of those suspects residing in their geographical area. Often, forensic analysis of the suspect's computer(s) will reveal that s/he has also been exchanging child abuse material non-commercially using P2P file-sharing software: a further investigation will then ensue which, given the Internet's lack of respect for county, state and national borders, will often identify further suspects outside the local or even the national jurisdiction with whom the original suspect has exchanged child abuse material, and intelligence on whom will then routinely be relayed to agencies in the relevant jurisdiction, regardless of whether a receiving agency is a member of VGT.

Any still images or video files found on the suspect's computer hard drives or portable devices should be analysed to determine whether they contain previously unidentified victims who need to be safeguarded from further abuse: whilst the suspect may be in one local jurisdiction, the victim portrayed in the images and the agent of their distribution may be anywhere in the world, and further liaison at national and international levels will normally be required. The images may likewise reveal that the suspect has him/herself been producing abusive images of children to which s/he has had offline access: an investigation into contact sexual abuse will then ensue, with potential for locating and safeguarding further young victims. In addition, it may transpire that a suspect has been soliciting children and young people online, either to obtain self-generated child abuse images via webcam or to effect an offline meeting with the intent of engaging in sexual activity: depending on the nature of this activity, further victims may be identified and, once again, these could be anywhere in the world. When local police forces receive details of subscribers from other law enforcement agencies they quite understandably prepare themselves for the worst as best they can.<sup>29</sup> It is worth emphasising at this juncture that this process presumes the availability of appropriate investigative services: whilst common in VGT and other developed nations, it is unlikely to be an experience shared by those in, for example, developing countries, by virtue of even lower levels of resourcing.

### *Example 1*

Operation Sirdar was the name given to the investigation of over 1,600 UK citizens who came to notice in 2004 during the course of Operation Falcon, a combined operation by US law enforcement agencies into the supply of images of child sexual abuse on a total of 21 individually named websites.

Of these 1,600 suspects a single line of data pertaining to a 30-day subscription to one of the sites indicated the involvement of Alan Webster, a 40-year-old man residing in Hertfordshire, UK. Examination of Webster's hard drive uncovered images taken on his mobile phone which depicted Webster and his 19-year-old girlfriend raping and indecently assaulting a 12-week-old baby girl whom they had been babysitting. The baby's mother had been unaware of the abuse. Both Webster and his girlfriend pleaded guilty to the charges and received sentences of life imprisonment and five years' imprisonment (plus an extended licence period of 5 years) respectively. The case serves as an illustration not only of the involvement of some offenders in both online and offline offending, but also of the severity and complexity of many investigations and the level of resources required to sustain them. In theory, an offender like Webster can lie behind every line of data.

To meet the demands of such investigations, local law enforcement agencies must be enabled to provide dedicated child abuse investigation units, staffed by officers with child protection and other specialist training, and sufficiently resourced to investigate online child sexual abuse, be this the production and distribution of child abuse material, online solicitation of children and young people for sexual purposes, resulting offline contact sexual abuse, or other related forms of exploitation. National centres must then be afforded sufficient capacity to provide specialist support (e.g. covert online investigators) to these local units when required.

In practice, however, responsibility for investigations into online child sexual abuse remains fragmented.<sup>30</sup> By way of illustration, analysis of the UK law enforcement contacts database for the CEOP Centre reveals that a small but increasing number of the forces receiving intelligence and crime reports from the Centre have specialist Paedophile Online Investigation Teams (POLITs): for the rest, investigations may be passed variously to Central Referral Units, Force Intelligence Bureaux, Child Protection Teams, Public Protection Teams, High Tech Crime Units, Sexual Offences Units, Specialist Investigations Departments, or local Crime Investigation Departments, members of which will inevitably display different skill sets and expertise.<sup>31</sup> In the words of Jewkes and Andrews, "it is still somewhat surprising that such a "micro" approach prevails in the boundless and borderless sphere of cyberspace".<sup>32</sup> Intelligence indicates that as the online and offline worlds converge, so too does the online and offline

offending of child sexual abusers. For example, CEOP has seen instances of UK citizens engaging in the online grooming of children overseas in preparation for the commission of contact sexual offences outside the UK – thereby indicating that, in some cases at least, suspect activities which would often be investigated separately by law enforcement High Tech Crime and Public Protection Units respectively are in fact part of a single offending process. As offending approaches become more sophisticated, so too are there requirements for international, national and local intelligence gathering and investigative as well as preventative responses to develop accordingly. And whilst the multiplicity of responsible investigative units need not always be problematic per se, it can present additional challenges to the successful coordination of investigations and strategies, and the development of skills and expertise.

The costs attached to the investigation of online child sexual abuse should not be underestimated. In addition to staffing and infrastructure, law enforcement agencies in many jurisdictions must pay to acquire essential data from some ISPs and Communications Service Providers (CSPs).<sup>33</sup> In the UK, for example, an initial subscriber check to identify the suspect or victim behind a username or Internet Protocol (IP) address can cost GB£40–65 (US\$80–130). This has significant cost implications for law enforcement agencies, regardless of their investigative capacity: such checks cost CEOP GB£100,000 (US\$200,000) per year – the equivalent of three additional investigators for the same time period, or one investigator for three years. Consideration must therefore be given to regulating and standardising at an international level the supply of Internet and communications data by service providers – for example, by compensating ISPs and CSPs from central government, rather than law enforcement, funds.

National and international units have a role to play in galvanising and motivating investigators at a local level: to this end, VGT member agencies provide inputs to senior police officers, raising awareness of the importance of providing adequate resources for the investigation of online child sexual abuse, and practical training for investigators on the ground, including:

- Covert Internet Investigation techniques
- Victim Identification
- Research and Intelligence Analysis
- Behavioural Analysis
- Interviewing Techniques
- Sexual Offences Legislation

Since the online sexual exploitation of children and young people is a borderless crime,<sup>34</sup> a number of these inputs are offered internationally. To this end, the issue of resourcing and expertise is inextricably linked with that of international collaboration. Recent research in Canada, for example, has shown that 80 per cent of cases opened by the national specialist unit, the Royal Canadian Mounted Police NCECC, were multi-jurisdictional and trans-border investigation.<sup>35</sup>

### 1.3 International Collaboration

Law enforcement more often collaborates internationally despite an absence of equivalent legislation against the online sexual exploitation of children across all jurisdictions, a lack of government designation of these crimes as policing priorities, and insufficient resources at national and local levels to combat them successfully.

More specifically, international collaboration is most often achieved at practitioner level: accordingly, VGT is composed not of member states but of individual agencies that work together in the course of their day-to-day investigations. VGT was established in response to practical requirements rather than as a result of multilateral agreements or protocols. Secondment of staff from member agencies, e.g. from the Australian Federal Police (AFP) and US Department for Homeland Security Immigration and Customs Enforcement (ICE) to CEOP, facilitates joined-up working practices. The following case study serves as an example of the way in which this is achieved.

#### *Example 2 – Operations Chandler and Hella*

In 2006–2007 VGT partners conducted an investigation into a UK-based non-commercial online trading ground for indecent images of children and live exchanges of abuse. This 10-month investigation involved the co-ordination of law enforcement agencies from 35 different countries and their subsequent, ongoing investigations – intelligence from which indicated that there were more than 700 suspects worldwide. The UK branch of the investigation centred on 200 suspects, the majority of whom have subsequently been subjected to active police enquiries.

*Kids the Light of Our Lives* was an Internet chatroom dedicated to the sexual exploitation of children. Hundreds of members worldwide used it to trade a range of material, including photographs and videos of children being subjected to sexual abuse and serious sexual assault. A 27-year-old man, Timothy David Martyn Cox, hosted the website from his home address in the UK, masquerading behind the online identity *Son\_of\_god*. When trading, he used the name *I\_do\_it*.

Cox was identified after intelligence linking the chatroom to the UK was passed to the CEOP Centre by Canadian partners within the VGT in August 2006. On receiving this information, specialist officers immediately began enquiries to trace the host, using a range of techniques and undercover online activity. Cox was located and subsequently arrested by officers from Suffolk Constabulary on 28 September 2006. This allowed undercover officers from the CEOP Centre to infiltrate the chatroom and gather valuable evidence.

Over a period of 10 days, officers from the CEOP Centre and Toronto Police conducted online surveillance. They were able to identify further suspects and secure vital information regarding potential victims before closing down the site. When UK forensic teams examined Cox's computer they found 75,960 indecent and explicit images in addition to evidence that he had supplied 11,491 images to other site users. Cox was subsequently charged with nine offences relating to the *Possession and Distribution of Indecent Images of Children*, and received an indeterminate custodial sentence.<sup>36</sup>

In September 2006, Gordon McIntosh from Hertfordshire also became a key subject in the UK inquiry. The 33-year-old man attempted to resurrect *Kids the Light of our Lives* following Cox's disappearance as Host. Officers from the CEOP Centre carried out extensive work to identify and locate the individual behind the usernames *silentblackheart* and *Iust4skoolgurls*. With the assistance of Hertfordshire Police, the CEOP officers arrested Mackintosh on 9 January 2007.

CEOP officers, in collaboration with VGT partners from AFP, ICE and Toronto Police, undertook 24-hour online surveillance to infiltrate the chatroom for a second time and collate details of all the offenders attempting to trade material.

McIntosh's computer was found to contain 5,167 indecent and explicit images of children, in addition to 392 indecent movie files. He pleaded guilty to 27 charges of making, possessing and distributing indecent images and movies, and received an indeterminate sentence.

### **1.3.1 Harm Reduction and Capacity Building**

Launched in January 2005, the VGT website provides information and support to adults and children on how to stay safe online. VGT member agencies have been able to pool their resources to provide a round-the-clock response to fast-time reports of abuse via the Report Abuse function at [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com): reports are automatically forwarded to the appropriate country of jurisdiction, e.g. to [www.ceop.gov.uk](http://www.ceop.gov.uk) in the UK, and [www.cybertip.ca](http://www.cybertip.ca) in Canada.

In addition to enhancing the investigative strength of individual operations, collaboration through the VGT facilitates the implementation of innovative preventative initiatives. One such initiative is Operation Pin, a deterrent operation targeting casual or opportunist offenders seeking to access child abuse image websites.<sup>37</sup>

Operation Pin involves the creation of a website that purports to contain images of child abuse but which, in fact, is a law enforcement site. Anyone who enters the site and who attempts to download material is confronted with an online law enforcement presence. The individual is informed that he has entered a law enforcement website, has committed an offence and that his details may have been captured and forwarded to the relevant national authorities.

Since its launch in December 2003, Operation Pin has captured the details of individuals from a number of different countries who were actively looking for child abuse material. However, this is not the primary aim of this initiative. Operation Pin is designed as a crime reduction measure, and its real success has been in undermining the confidence of those who think that the Internet is an anonymous place where paedophiles and other criminals can operate without fear of being held to account. The VGT has an ongoing commitment to Operation Pin, and continues to work with industry and others to refine aspects of the operation.

VGT member agencies also share their resources and expertise with law enforcement agencies in developing countries – particularly those in which there are links between child prostitution and the production of images of child sexual abuse – not only to expedite VGT investigations of crimes committed overseas but also to enable developing nations to optimise their investigations of indigenous crimes.

Project Childhood, for example, is a joint initiative of Interpol and the United Nations Office on Drugs and Crime (UNODC) that will support local law enforcement and criminal justice authorities in Thailand, Cambodia and Vietnam, to increase the number of successful investigations, apprehensions and prosecutions of child sexual offenders and traffickers by:

- Strengthening national human capacity to prevent and suppress trafficking in children for sexual exploitation and child-sex tourism by providing technical and operational assistance to local law enforcement; and
- Strengthening national institutional capacity to ensure that authorities are properly equipped to carry out action related to investigations and criminal procedures.

Through Project Childhood it is hoped that visible intolerance of child sexual offenders and traffickers will engender a decline in demand for children to be sexually exploited and, ultimately, contribute to the reduction of trafficking in children for sexual exploitation in Southeast Asia.

In terms of awareness raising, VGT partners have contributed financial assistance and content for the development of a television commercial which is now shown in member countries. The commercial highlights the fact that law enforcement agencies are active on the Internet and are committed to locating offenders.

### **1.3.2 Technical Tools and Victim Identification**

Because the Internet has no borders, uploading an illegal image essentially constitutes an international crime. The thematic paper presented to the Yokohama Congress highlighted the need for the establishment of common databases for the investigation of child abuse images. Interpol has since developed the Interpol Child Abuse Image Database (ICAID), to which a total of 35 Interpol member countries – including VGT agencies – have contributed to varying degrees. This database contains hundreds of thousands of images of child sexual abuse, and uses image recognition software to compare details of where the abuse took place and connect images from the same series of abuse or images taken in the same location with different victims, thereby enabling investigators to determine whether images seized belong to known series with already identified victims or represent new sexual abuse crimes requiring the identification and safeguarding of previously unknown victims. This has the potential not only to save investigators valuable time and unnecessary exposure to images in assessing individual collections, which often run into the hundreds of thousands, but also to link and coordinate image-related investigations across a number of jurisdictions. The identification of victims is a global issue, not least because a previously unseen image may add vital information to investigations of known series.<sup>38</sup> The following case studies serve to illustrate this:

#### *Example 3*

Two young girls, aged 9 and 11, were being sexually abused and filmed. A video of the abuse was found in Australia, where authorities requested the assistance of the Interpol General Secretariat to identify the language spoken and hence possibly the location of the victims. The involvement of various authorities led to the identification of the location and safeguarding of the victims, arrest of the abuser, the girls' father, in Belgium, and arrest in Italy of the man who filmed the abuse.

#### *Example 4*

Two men were arrested in early 2005 for their involvement in the sexual abuse of children as young as 18 months. Close cooperation between the Interpol General Secretariat and the police and National Central Bureaux in Spain and Canada uncovered a network of child sexual abusers operating throughout Spain.

The case started in February 2005, when a Canadian police officer discovered images of child abuse and liaised with Interpol for further analysis. A Spanish officer working at the Interpol General Secretariat was able to confirm the location of the crime as Spain, based on the computer keyboard visible in the video. Analysis of the images yielded other clues, resulting in the arrest of the abusers and the identification of seven victims aged 2–4 years. The chief abuser worked as a babysitter, which provided him with easy access to children.

#### *Example 5*

In October 2003, Interpol's Trafficking in Human Beings unit received 50 images of child abuse from the Swedish police; the pictures were called the *Green Leaves* series. In August 2005, the Interpol General Secretariat received an additional 20 videos from the Canadian authorities featuring the same victim. With assistance from officers at the General Secretariat, the language spoken in the videos was identified as Polish.

In the spring of 2006, a Polish police officer participating in a training programme with the Trafficking in Human Beings Sub-Directorate at the General Secretariat further analysed the film. A section of a children's playground area could be seen outside the room where the footage was shot, and the officer identified the area as being in a specific neighbourhood of Warsaw. With this information, police were able to pinpoint the location where the film had been made. In August 2006, the abuser was arrested and his victim, who had suffered many years of abuse, was located.

These cases demonstrate the effectiveness of an international point of contact and coordination. At the same time, shared image systems assist investigators by reducing the amount of time they are exposed to child abuse images.<sup>39</sup> In recent years, assistance with image cases has also been sought from members of the public, most notably for Operations Vico and Ident, the Interpol-led searches for Canadian and US males wanted for sexual contact and image offences in Southeast Asia.

Since 2001 there has been a sea change in the focus of investigations in VGT member agencies and elsewhere. As will be discussed below in relation to the CEOP Centre, closer liaison with child protection specialists has resulted in a stronger emphasis on victim identification, location and safeguarding, whilst the requirement to hold perpetrators to

account has not been neglected. No longer can it be said that law enforcement devotes resources towards securing convictions in preference to safeguarding children – at least as far as the member agencies of the VGT are concerned: rather, calls for the investigation of images to have a child protection and more victim-centred focus have been heeded.<sup>40</sup>

With regard to information management, international collaboration is facilitated by the deployment of the Child Exploitation Tracking System (CETS), a case management system developed for law enforcement by Microsoft and used by agencies inside and outside VGT. Because the scope of the Internet is global, there is potential for the same suspect to be investigated by a number of different law enforcement agencies. Cross-jurisdictional coordination is required, therefore, in order to avoid duplication of effort and resources.<sup>41</sup> CETS allows investigators to check whether a particular suspect, username, IP address or online resource is already under investigation, and automatically links information on known entities, enabling investigators to have all the relevant intelligence at their disposal.

Investigators in one part of the world may unwittingly hold a piece of information which is key to an investigation in another: CETS has the power to enable them to dispense with the time-consuming and labour-intensive business of contacting all relevant national units to determine whether each piece of information is relevant to them. At present, use of CETS is a prerequisite of VGT membership: all investigators of online child sexual abuse in Canada now have access to the system, and in other VGT jurisdictions use of CETS by national specialist centres is increasingly complemented by use in local investigative units (these national systems are yet to be linked). In 2005, CETS was awarded a gold medal at the Canadian Government Technology Awards, and in 2006 received the Imagine Canada Business and Community Partnership Award.

VGT also uses off-the-shelf products such as Groove to share information. Groove is collaboration software, which allows users to work together in a more efficient manner, sharing files and messages in real time without a centralised system. Its role in facilitating the timely referral of data for the purposes of locating and safeguarding child victims is illustrated by the following case study:

#### *Example 6*

Child abuse images found on a suspect's computer in the US showed the abuse of a very young child by an adult thought to be in the UK. These images were passed by the Federal Bureau of Investigation (FBI) in the US to the CEOP Centre, where investigative work by staff identified the suspects and their location. Within 6 hours, Social Services and the local police were brought in and a search warrant executed on a specific address. Two adults were found guilty of a series of child abuse offences, and a number of children have been safeguarded from abuse.

The usefulness of these shared systems is necessarily constrained by the extent to which national agencies use them: as Holland has observed, Interpol does not as yet receive notification of all victim identifications, nor of all images seized.<sup>42</sup> At the same time, there are occasions when it is not possible to identify the country of origin. In this event images should be sent to Interpol for further investigation and circulated amongst its Victim ID working group: however, given the aforementioned legislative discrepancies between different nations and lack of prioritisation and resourcing in some jurisdictions, it cannot be guaranteed that this will always be the case.<sup>43</sup> By this same token, the larger the number of countries contributing to ICAID and using CETS, the more comprehensive and effective will the international law enforcement response to online child sexual abuse be.

## 1.4 Collaboration with Partner Agencies/Inter-Sectoral Working

The online sexual abuse of children cannot successfully be combated by law enforcement alone. Engagement with child protection specialists is essential in the first instance to assess the level of immediate risk of harm to a child on initial receipt of a report of abuse, and to safeguard children in the longer term. At the same time, the amount of harm to which children and young people are exposed on the Internet may be reduced by the development of resources which empower children and young people to stay in control of their online interactions, raise awareness amongst the adults who care for them, including parents and teachers, and enable all of these groups to report directly to the authorities should a child find her/himself in a situation which makes her/him feel uncomfortable. Such measures will be discussed in greater detail below, with reference to the current UK model.

Online service providers (not only ISPs but administrators of social networking sites, file-sharing services and the like) are likewise key to ensuring the effective provision of actionable intelligence and data concerning suspected criminal activity online, to making technologies popular with children and/or liable to exploitation by offenders safer by design, and to providing prominent and easily accessible mechanisms for reporting alleged abuse, e.g. Microsoft's embedding of a Report Abuse button in Windows Live Messenger, which enables members of the public to report directly to law enforcement via [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com).

An increasing number of service providers are showing a commitment to combating the online sexual abuse of children. Whilst this is to be applauded, the level of commitment has been left to the discretion of the service providers, perhaps because their legal obligations

with regard to these offences are often themselves unclear and because the emphasis to date has been on self-regulation. Clarity of message is now required, along with provision of a visible and accessible means to report abuse to the authorities.

Law enforcement must now engage with service providers to provide active and meaningful deterrents and lines of communication. Industry awareness of an ability to report to specialist national units is not enough: these mechanisms must be readily accessible and clearly signposted in the very environments in which a child or young person may be subject to unwanted contact, or in which child abuse imagery may be discovered. When highly visible, such mechanisms may also have a deterrent effect, warning potential offenders that law enforcement is present within a specific environment, and at the very least just one click away. They can also provide much needed reassurance to parents and carers that – despite the moral panic that sometimes abounds concerning the sexual solicitation of children and young people – online environments are in fact being policed.

For now, it remains the case that requests to remove websites containing child abuse images are actioned much more slowly by ISPs than are, for example, requests to remove phishing websites and online fraud concerns – thereby suggesting that loss of revenue is still more important to industry than child protection.<sup>44</sup> Consequently, law enforcement, NGOs and others must continue to engage with ISPs to emphasise the reputational benefits of having a sound child protection strategy which has been developed as a result of direct consultation with these stakeholders. At the same time, law enforcement agencies need to be more creative in their engagements with ISPs by seeking as much to make online environments safer by design during development as to enforce the law in environments already popular with potential offenders. Creative engagement by VGT member agencies has already resulted in the modification of online functionalities which have been misused by individuals with a sexual interest in children and those who seek to profit from such a proclivity: adoption of the VGT Report Abuse button by Microsoft is just one such example, and it has even proved possible to persuade an online provider of peer-to-peer file-sharing software to remove a service misused for the distribution of child abuse images. It should not, therefore, be assumed by law enforcement professionals that industry developments will continue apace in spite of the concerns of, and without consultation with, child protection specialists.

### **1.4.1 The CEOP Model**

The CEOP Centre is an example of a law enforcement agency which employs a holistic approach based on an integrated partnership model. Established in April 2006, CEOP

brings together specialists from law enforcement, child protection, central government and industry, in full recognition of the fact that, in isolation, the police – however well resourced and trained – cannot successfully combat the online sexual of abuse of children and young people. Along with other VGT member agencies, and in accordance with the 2007 Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*,<sup>45</sup> it seeks to move towards a continuum of services related to crimes against children, coordinating online police resources, working constructively with the online industry, informing government-inspired reviews and acting as the primary focus of outreach activity, targeting every family with vital ‘safety first’ messages about the online environment.

CEOP’s partnership with the UK National Society for the Prevention of Cruelty to Children (NSPCC) has enabled the integration of specialist child protection officers into each of the Centre’s key business areas<sup>46</sup>. These individuals bring their unique expertise in working with and supporting child victims, whatever level of abuse they have experienced. A senior child protection social worker provides a child-focussed risk assessment of all reports of abuse made to the Centre, prioritising cases on the basis of risk of harm to each child. A further NSPCC specialist sits with the Victim Identification Team, to ensure that every investigation remains victim-centred and that there is proper provision at a local level for the young subjects of previously unseen abusive images. NSPCC staff are also seconded to advise on Offender Management and operational considerations. In addition, the NSPCC ensures, via audit, that all of CEOP’s policies reflect best practice in safeguarding children and are in accordance with the relevant child protection guidance and legislation.

In line with its more victim-centred approach, CEOP has also established a Survivor’s Advisory Panel. This panel, comprised of adults who experienced sexual abuse as children, advises the Centre and contributes to its knowledge of the long-term consequences of these crimes. It is anticipated that this resource will be vital not only for CEOP but also for policing in general, providing an insight which will inform all areas of investigation.

The importance of including children and young people in developing preventative measures is widely recognised, with child and youth participation one of the key recommendations of the declaration resulting from World Congress II and of the 2007 Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*.<sup>47</sup> Children and young people not only have a right to contribute, but very often also have the in-depth knowledge to advise on how to make the Internet safer for all. To this end, CEOP’s 60-strong Youth Advisory Panel of 11-16 year olds actively participates in the

work of the Centre, reviewing new preventative initiatives, providing context for observed trends in offending and victim behaviours, and contributing to training inputs for law enforcement and education specialists.

July 2008 saw more than 140 young people aged between 14 and 17 years, from countries as diverse as the USA, Australia, Egypt, Argentina, India, Poland and Namibia, convene for the first International Youth Advisory Congress. This CEOP-led initiative, supported by the VGT and partnered by leading corporations such as Microsoft, Virgin Media and Visa Europe, enabled young people to come face-to-face and work with those responsible for Internet safety and security – representatives from government, industry, law enforcement and the media – giving them the opportunity to shape the Internet and online environments for children and young people across the world. The outcomes of the Congress, including recommendations for the media, industry, law enforcement, governments and amendments to the United Nations *Convention on the Rights of the Child* (UNCRC), will be taken forward to World Congress III.

The *Thinkuknow* education programme sits at the heart of the CEOP Centre's drive to advise children and young people of ways in which they can continue to have fun online while staying in control and remaining safe from sexual predators. Since CEOP's inauguration, 2.25 million children between the ages of 8 and 16 years have seen specialist *Thinkuknow* sessions delivered by around 11,000 education and child protection professionals across the UK.

In the last 12 months, CEOP has expanded this work into the primary sector with Cybercafé, for 8-10 year olds and *Hector's World*, for 5-7 year olds, enabling children and parents to safely explore the online world together. Talking to children and young people is one thing, but the gulf between what children are doing and what their parents, teachers and carers think they are doing is a concern. Hence CEOP has created the *Purely for Parents* resource – breaking down the terminology, exploring the technology and demystifying the threat.<sup>48</sup> In addition, the Centre makes its annual threat assessment of online child sexual abuse, the *Strategic Overview*, available to as wide an audience as possible and operates a registration programme that enables parents, carers and those with an active interest in child protection to receive regular email updates.

CEOP's partnership approach is a departure from conventional practice in law enforcement. Partnerships enhance all areas of the Centre's work and provide a continuous flow of expertise, experience and resources into the organisation. The Centre defines a partnership as an agreement or Memorandum of Understanding (MOU) with a company or an organisation that commits to provide pro bono expertise, experience or resources to

the Centre. Partnerships are considered on the basis that they will meet CEOP objectives, be proactive rather than reactive, build knowledge and share expertise, encourage higher levels of commitment and engagement, and be ethically sound, transparent and compliant with best practice in the public sector.

Examples of successful CEOP partnerships in addition to that with the NSPCC:

- VISA Europe has provided financial support to CEOP's Financial Investigation Team, facilitating investigations into the commercial distribution of child abuse images. In addition, it contributes expert understanding of the ever-changing 'payment' market. VISA Europe is also a founder member of the incipient European Union Financial Coalition, and supported and actively participated in the International Youth Advisory Congress (IYAC).
- Microsoft not only delivers a contemporary understanding of how technology is developing but also, in the UK, must be applauded as the first to adopt and deliver the Report Abuse mechanism into the online environment, empowering countless children and young people to protect themselves and their peers. Microsoft also supported IYAC and continues to develop the CETS in consultation with law enforcement practitioners.

Genuine collaboration with industry partners can make the Internet a safer place for children and young people. To that end, CEOP works with a large number of organisations to learn about the user experience, create opportunities for online providers to identify concerns and develop joint harm-reduction solutions. More specifically, work continues in order to improve the quality of reporting from online service providers, designing training for online moderators; to raise awareness of child protection issues; and to optimise prevention, intelligence gathering and investigation in online environments favoured by children and, by extension, those with a sexual interest in them.

The sexual abuse of children and young people continues to present challenges, with complex tactics adopted by offenders in order to victimise young people. In the last 12 months, CEOP has trained 2,600 UK and international law enforcement officers in specialist techniques to enable them to better meet these challenges. With the support of the University of Central Lancashire, CEOP provides an academically accredited course of study for child protection specialists across the UK through the CEOP Academy. Additionally, CEOP's international outreach programme has undertaken regional training and capacity building programmes to law enforcement agencies in Romania, Vietnam and Cambodia.

Wortley and Smallbone, amongst others, have stressed the importance of effective media coverage of law enforcement activities in deterring the online sexual abuse of children, in so far as it goes some way to diminishing the perception amongst potential offenders of the Internet as a risk-free and anonymous environment in which to operate.<sup>49</sup> Such publicity has also been observed to have the effect of increasing direct public engagement with law enforcement: analysis of reports made to CEOP reveals that reports made by members of the public rise and fall in line with the amount of media coverage afforded to the Centre in any given month. The value of the media as a conduit for raising awareness should therefore not be underestimated. As Jewkes and Andrews observe, police “must present an image of a technologically literate force of cybercops”.<sup>50</sup> An effective media strategy has the potential to prevent offences and to reassure members of the public, including children and young people themselves.

The decision to publicise a particular investigation must be taken responsibly, particularly for those investigations with an international element, as a lack of national and international coordination in media strategies can result in offenders being forewarned and the loss of valuable evidence. Lessons have been learned since Operation Ore, the UK investigation into the subscribers to the Landslide portal: media coverage of the first wave of arrests alerted other offenders who were yet to be arrested, and this delay in turn enabled some to destroy their hard drives and other material.<sup>51</sup> In light of recognised discrepancies in resources afforded to the investigation of such offences in different jurisdictions, those agencies reaching more speedy outcomes must therefore be aware that they may jeopardise operations in other countries by engaging the media without prior consultation. To this end, VGT agencies include best practice press strategy guidance when disseminating intelligence relating to large-scale international operations.

## 2. The Current Nature of Online Child Sexual Abuse

VGT agencies use strategic intelligence analysis to identify trends and patterns in offending and victim behaviours, and technological, legal and other developments liable to exploitation by individuals with a sexual interest in children and young people. Effective strategic analysis of online child sexual abuse informs education campaigns, investigators at local, national and international levels, and partnership activity, identifying opportunities for law enforcement activity and key harm-reduction messages.

This section of the paper draws on assessments by VGT member agencies of online child sexual abuse in response to operational law enforcement requirements, most notably the CEOP *Strategic Overview 2007–8*.<sup>52</sup> The following is not intended as a substitute for more comprehensive academic research, but rather to complement it.

Crime and intelligence analysts use defined analytical techniques to identify and explain patterns of crime and incidents, and infer who or what may be responsible. They draw conclusions and inferences from a range of information sources; support strategic decision making and the tactical deployment of resources to prevent crime, and detect and disrupt criminal activity; and proactively solve problems. More specifically, strategic threat assessments evaluate the current, emerging and long-term issues affecting a police force or region and make key judgements and recommendations concerning the direction of future policing strategy and tactics.

The VGT acknowledges that its understanding of the scale and nature of online sexual offending against children can only be partial for the following reasons:

- Whilst strategic intelligence and crime analysis naturally draw on information from NGOs, industry and other partners, they are inevitably based on information, which for the most part consists only of those crimes reported to police and intelligence regarding suspected criminal activity, held by law enforcement agencies. Continued engagement with partners external to law enforcement is therefore required to complete the picture.
- Even within the VGT, not all agencies synthesise and systematically analyse this information in order to identify trends in offending and behaviours or technological developments liable to exploitation.

- Since the VGT currently consists of a small number of agencies in developed countries, its assessment of online child sexual abuse may not be representative of non-VGT nations, e.g. developing countries.

In order to make VGT's analysis more comprehensive and representative, analysts in VGT member agencies therefore supplement their own analyses of law enforcement crime data and intelligence with open source research, horizon scanning, and consultation with colleagues in NGOs and the private sector.

## 2.1 Key Trends

One of the most significant trends for law enforcement in recent years is that of convergence, both in terms of technology and behaviour. Now more than ever there is a requirement for all agencies involved in child protection to dispense with the distinction between 'online' and 'offline', 'real' and 'virtual'.<sup>53</sup> Children and young people do not perceive this distinction so clearly, nor do those with a sexual interest in them. To this end, CEOP has seen instances in which children and young people have been groomed to produce indecent images of themselves which have subsequently been subject to non-commercial distribution. Offence data from UK police forces likewise details combination offending behaviours including the distribution of indecent images of children taken during the commission of contact sexual offences, and contact sexual abuse subsequent to online grooming. The Internet allows offenders simultaneously to scan globally for images and solicit locally for potential offline victims.

Research indicates that in 2000–2001 40 per cent of those arrested for possessing child abuse images were dual offenders who had also sexually victimised children, with both crimes discovered in the same investigation, and that a further 15 per cent had attempted to sexually victimise.<sup>54</sup> Whilst data for more recent child abuse image offenders has yet to be analysed, law enforcement continues to see a considerable amount of dual offending, with image offenders also engaged in grooming or solicitation and contact sexual abuse, both online and offline. Equally, intelligence indicates that children overseas have been groomed online by UK individuals as a prelude to the commission of contact sexual offences in destination countries, and that the Internet is being used to exchange information for travelling sex offenders on sympathetic travel agents and hotels, tips for overseas offending, etc.<sup>55</sup>

Meanwhile, the Internet has changed immeasurably, even in the last 12 months, and continues to evolve. The traditional types of online environments are now merging. Image and video-

sharing sites allow users to make contact with others by posting feedback on content shared. In this regard they are arguably just as 'social' as networking sites such as Bebo, MySpace and Facebook, and accordingly VGT has received reports of grooming and precursor behaviours in these environments. By the same token, social networking sites now provide picture, video and music sharing, blogging, email and instant messaging functionalities in a single account. For this reason, industry has coined the wider term 'social sites' for all those online environments which facilitate interaction between users. As more and more social sites incorporate instant messaging – a medium which facilitates the establishment of private relationships – an increase in reports of grooming in these environments is anticipated.

At the same time, online culture is increasingly participatory, with the advent of Web 2.0 significantly increasing Internet users' ability to create online content for others to view.<sup>56</sup> As it does so, children and young people are not only spending an increasing amount of time online but are also using online media to share an ever-widening range of image-based and text-based content pertaining to their offline lives, effectively constructing their social identities in these environments. This proliferation in participation arguably brings new kinds of risk. In the first place, the expression of opinions and preferences is now an integral part of life online for children and young people. Preventative messages and media attention focus with good reason on the need to protect personal information which may be used to locate a child or young person offline. Equal attention, however, must be paid to the speed with which suspects are able to build online relationships with children and young people on the basis of positive feedback and the pretence of common interests or points of view – an observed offline grooming technique with a much wider application in those online environments where young people feel free to express themselves.<sup>57</sup>

With regard to specific risk-taking behaviours, a number of reports to CEOP in the UK and the NCECC in Canada indicate a concerning trend for cyber-bullying in which, for example, young people create a bogus social networking profile using the details of a school friend or acquaintance or post their contact details on adult dating sites, thereby exposing them to risk by inviting contact from unknown persons, in some cases specifically adult males. Similarly, feedback from schools would suggest that some young people are wilfully directing suspect online contacts to another young person, providing an online introduction or contact details without the consent of the child or young person concerned. Whilst the online confidence of these young people is in one sense encouraging, the above behaviours would indicate that some young people do not fully comprehend the implications of putting another young person in a compromising situation over which they may have limited control.

In addition, parents have posted images of their young children modelling or bathing on social sites, only to find that they have been appropriated or that persons unknown have

added comments to them of a sexual nature. Such reports not only highlight a requirement for informing parents and carers of the consequences of sharing images of children on the Internet, but also demonstrate the degree to which some individuals with a sexual interest in children are prepared to express themselves in public environments.

The range of reported online locations for grooming and solicitation continues to increase in line with the rapidly developing trend for use of multi-function social software that encourages content creation, enhanced participation and social interaction. Amongst these developing functionalities, online role-playing gaming enjoys ever-increasing popularity. By default, this has led to increased risk to children of inappropriate contact from adults in these environments. In addition, the convergence of online gaming with other technologies, for example instant messaging and Voice Over the Internet Protocol (VoIP) – used to transmit phone calls over the Internet – further facilitates the establishment of close relationships between children and persons previously unknown to them, whilst the ongoing integration of VoIP, Video Chat over the Internet Protocol (VCoIP) and instant messaging technology into handheld games consoles has the potential to expose children and young people to unsolicited contact of a sexual nature away from parental supervision. Such developments, and early indications of their misuse by offenders, serve as an illustration of the potential volume and gravity of offending to be combated in the near future.

Accordingly, online gaming is increasingly cited in reports to law enforcement as a location for grooming and solicitation of children. Observed offending behaviours in these environments are similar to those in other online environments popular with children, e.g. requests for children and young people to perform sexual acts on webcam, requests for personal details and requests to meet offline. More specifically, intelligence indicates that some suspect online gamers issue requests for sexual chat and sexual acts on webcam in return for virtual money and virtual items craved by children and young people.

As the popularity of online gaming sites increases amongst children and young people, so too will it increase with those who have a sexual interest in children. Of note, the development of gaming environments for a younger demographic of 6-10 year olds has identified a requirement for awareness raising amongst younger children, prompting the development by VGT agencies of education resources for younger children.

There has been a notable increase in reports of abuse using VoIP in recent months, including grooming behaviours akin to those observed in instant messaging (IM) environments and the establishment of P2P chatrooms for individuals with a sexual interest in children and young people. Whilst the popularity of these services has thus far been limited largely to

the more technologically savvy sectors of society, it is predicted that both VoIP and VCoIP will be part of the Internet mainstream within the next two years.

As for the methods of those who solicit children and young people online, it would appear from analysis of reports made to CEOP by members of the UK public that threatening behaviour is increasingly being used as part of online grooming techniques. It is likely that as a result of improved public awareness, education and parental supervision children and young people are increasingly aware of the risks online, and are therefore better equipped to combat those more traditional grooming techniques observed both online and offline, e.g. claiming to be known directly or as a friend of a friend. As a result, offenders have to resort to threats and blackmail in order to place children in a situation over which they may feel they have little or no control. One example of this is where a child has provided self-generated images to an offender, which can then be used to blackmail the child to take part in further sexual abuse. Another common tactic is the hacking, or threat of hacking, of a young user's instant messaging or social networking account. Whilst this displacement demonstrates that children and young people are better able to protect themselves against more traditional grooming techniques, it is also a worrying development that requires further exploration and understanding.

Other observed behaviours include:

- Taking over a young person's online account, posing as the account holder in order to groom her/his contacts;
- Hacking a young person's online account and verbally abusing her/his contacts (this in itself sometimes serving as a prelude to a more aggressive style of grooming, including threats of violence); and
- Sending – or threatening to send – a Trojan file to a child's computer in order to gain remote access to files and devices such as webcams.

Blackmail is facilitated not only by technical means (hacking, etc) but by playing on the fears of the children and young people targeted. The creation of Internet content is increasingly important to children and young people and is a significant contributing factor to their sense of identity. In observed cases where suspects have assumed control of this content it would appear that this has been done expressly to exert power over its creator. Accordingly, CEOP in the UK continues to receive a number of reports from children and young people who have been victims of hacking without sexual abuse and it is clear from these that hacking is perceived not so much as an administrative issue but as a violation or breach of trust. In a similar vein, suspects have been observed to use basic and publicly available photo-editing programmes to sexualise legitimate images posted by children and young

people, subsequently threatening to post these ‘faked’ images on the Internet unless their subjects engage on webcam.

Instant messaging (IM) is the most cited environment for online child sexual abuse in the UK, a finding which correlates with recent US research.<sup>58</sup> This functionality is now more popular with children and young people than that offered by chatrooms, and this is one of the key developments of the last few years.<sup>59</sup> While IM’s prominence in reports of abuse may to some extent be explained by increased accessibility of reporting via the VGT Report Abuse tab in the most popular instant messaging programme, Windows Live (formerly MSN) Messenger,<sup>60</sup> it is evident that the comparative privacy of these environments and the use of P2P technology makes them attractive to individuals with a sexual interest in children and young people. To this end, having made initial contact in social networking, online gaming and other public social sites, suspect persons often encourage children and young people to transfer their interactions to instant messaging programmes.

Until very recently, IM has also been the preferred environment for those wishing to interact via webcam. Given that exposure and participation in sexual acts on webcam is the predominant feature of a significant proportion of public reports of online sexual abuse (25 per cent over the course of all UK reports from under 18s), it follows that IM would see an elevated number of reports of abuse for this very reason. This distribution is likely to be subject to change as more social sites acquire IM and webcam functionalities:<sup>61</sup> consequently, there is an urgent requirement to embed mechanisms which enable direct reporting to law enforcement – such as VGT Report Abuse button – in these social environments.

In addition to those grooming scenarios in which social networking sites are used to gain an initial introduction to a child or young person, with a subsequent switch to IM for further contact, it is apparent that some individuals with a sexual interest in children are using social networking sites to ‘collect’ and manage young contacts – potentially hundreds at a time – and may, by the very fact of having a large number of young contacts, give the appearance of being a ‘safe’ person to know. Whilst recent US research confirms law enforcement findings that the majority of young people who are sexually solicited online do not report this as occurring on a social networking site, the proportion of those who do (25 per cent) is large enough to suggest that safety measures in these environments – such as a mechanism for reporting directly to law enforcement – could reduce the frequency of such unwanted contact.<sup>62</sup> To a lesser extent, suspect individuals are using social networking sites to post child abuse images and pro-paedophile sentiments.

The number of children who report being asked to strip on webcam is on the increase, as is the amount of self-generated child abuse images. According to reports received

from members of the UK public, children and young people are encouraged to switch on their webcams as a prelude to being asked to perform sexual acts, and/or to witness an adult exposing themselves or masturbating. For some offenders, exposing themselves to a child or gaining child abuse images generated by children themselves would appear to be an end in itself. For others, the ability to generate images of children, without even having to meet a child, is a useful tool for offenders who can then go on to use that image either to increase their status in paedophile networks or in the grooming process, seeking to ensure continued compliance to obtain further images or arrange an offline meeting by threatening to publish images already obtained from children and young people.

Analysis of reports from the UK public reveals that the vast majority of reporters in the UK aged under 18 (73 per cent) are targeted by individuals located, or at least claiming to be located, in the UK. This may be indicative of the importance of i) commonality of language in establishing an intimate relationship and ii) geographical proximity in effecting an offline meeting. At the same time, a comparatively high proportion (35 per cent) of UK reports from under 18s which cite abuse on webcam report that suspect persons were – or claimed to be – outside the UK, thereby suggesting that individuals whose primary aim is to obtain self-produced indecent images of children and young people, or who derive gratification from exposing themselves to children and young people, are not necessarily bound by geography.

VGT member agencies are currently investigating scenarios in which consenting young people create and send to each other images of a sexual nature. In the eyes of the law, at least in the UK, these young people are producing and distributing child abuse images: there is therefore a requirement to make children and young people aware of the permanency and implications of sharing such images, be this by mobile phone, Internet or, indeed, mobile Internet – a facet of, amongst others, CEOP's *'ThinkuKnow'* education programme.

## 2.2 Child Abuse Image Distribution

Whilst it is difficult to quantify in terms of exact numbers, it would appear that the non-commercial distribution of child abuse images via publicly available P2P file-sharing programmes is outstripping distribution via pay-per-view sites. The distribution of child abuse images is no longer a 'cottage industry', nor can it currently be said that "much of the child pornography today can only be accessed via credit cards".<sup>63</sup> Rather, in a recent poll of investigators responsible for the forensic analysis of suspect hard drives, P2P networks

were believed to be the predominant means of image distribution, and the source of a quarter (24.6 per cent) of indecent images found, with just 7.5 per cent of the total sourced from pay-per-view websites.<sup>64</sup> Clearly much has changed since 2001, when US data for those arrested for possession of child abuse images showed that less than 1 per cent were using P2P networks.<sup>65</sup>

P2P technology functions on a computer-to-computer (C2C) basis, facilitating the exchange of large numbers of image files. In contrast to other web-based applications, content shared in this way is in most cases stored on a client's hard drive and not on an external server. Forensic analysis reveals that some image distributors run multiple clients in order to optimise their distribution and access to new images. In contrast to pay-per-view websites hosting child abuse images, where the motivation is largely financial, non-commercial distribution is motivated rather by the kudos of possession of sought-after images or the provision of previously unseen material. Analysis of chat logs from seized hard drives would indicate a preference amongst offenders for programmes which allow them to network and share thousands of high quality images simultaneously, thereby facilitating joint fantasy over these images and putative contact sexual offences. Accordingly, the number of investigations into image distribution facilitated by P2P has increased dramatically in recent years.

In addition, there is already some evidence that non-commercial child abuse image distributors on publicly available P2P image-sharing programmes also engage in voice chat using VoIP technology, thereby highlighting the potential use of these applications by individuals who wish to engage in or view real-time direct contact sexual abuse.<sup>66</sup> The appearance of a large amount of previously unseen child abuse images circulating in these environments would indicate that it is a preferred outlet for distributors who are themselves contact sexual abusers. It is therefore anticipated that as mainstream usage of VoIP and VCoIP increases, so too will its use by child sexual offenders.

## 2.3 Volume of Images and Data Storage

As the quality of and access to still and video images improves, so too does the amount of data to be analysed and stored by law enforcement. In the UK, for example, the last 12 months have seen the seizure of multi-terabyte external hard drives and internal storage of 200–400 GB, along with other media such as USB thumb drives and memory sticks.

In 2003, research suggested that there were 140,000 unique still child abuse images in circulation online at that time, and that the volume was increasing:<sup>67</sup> in 2008, law enforcement investigators routinely seize child abuse image collections of this size or larger. Increasingly

large amounts of video material are being seized, both in terms of numbers and duration:<sup>68</sup> so, whilst CEOP's largest seizure of 182,000 still child abuse images does not exceed the UK record of 450,000,<sup>69</sup> this same collection came with c.400 hours of video, all of which was required to be subject to review. Tools such as C4P (Categorising For Pictures) – a software tool written in Canada which facilitates the categorising of images – can save time by helping to eliminate duplicate images. However, it is clear that the current investigative capacity and technical solutions are insufficient to provide in every case an analysis which is both thorough and timely. Specialist units worldwide rightly guard against prioritising cases on the basis of the number of child abuse images in any individual collection: in terms of the relation between the size of a collection of child abuse images and the risk posed to children by its owner, the general consensus amongst law enforcement in the UK is that the number of images is an unreliable indicator.<sup>70</sup> Current research includes practitioner scoping of the potential for selective acquisition of data from suspects (which may be necessary despite obvious concerns about the potential for previously unseen images to remain unidentified), and the development of software tools facilitating the timely analysis of video content.

Additionally, the number of previously unseen images is on the increase, suggesting an increasing amount of contact abuse that is being recorded and subsequently distributed,<sup>71</sup> in turn requiring the identification and location of an increasing number of victims, and entailing an increasing number of investigative hours in specialist units across the globe. In light of this upward trend, victim identification will be at even more of a premium than in recent years.

In terms of content, the number of non-commercial images showing babies or toddlers is on the increase: victims in commercial images also are increasingly young, with 80 per cent estimated to be less than 10 years old.<sup>72</sup> Moreover, a number of investigations by UK and overseas law enforcement agencies have highlighted the fact that there are many series of images in which the victims appear to have been abused a number of years earlier but where the images have only just come to light. This is particularly true for images of boys and where the material has been seized from a contact sexual abuser – in turn suggesting that offenders who have previously been content to keep a record of the abuse for their own personal gratification may have been detected after succumbing to the urge to share this material on the Internet. In recent years law enforcement has also seen the emergence of images – albeit so far a relatively small number – containing victims of non-white origin, including those of South American and Southeast Asian origin. This proliferation of images from a variety of source countries points to the role of the Internet in facilitating truly global communications and networking across obvious language and cultural barriers. At the same time, it raises the possibility that an

increasing number of travelling offenders are taking still and video footage of contact sexual abuse committed overseas.

In addition, interviews conducted by the CEOP Centre's Behavioural Analysis Unit (BAU) with those convicted of possessing child abuse images suggest that the proportions who are interested in sadistic sexual acts are greater than previously recognised. This demand for materials depicting violent and sadistic sexual acts against children is likely to be met by increased supply from commercial and non-commercial distributors alike.

There are approximately 2,000–3,000 established domains recorded each year worldwide that offer access to child abuse images by payment of subscription.<sup>73</sup> Of that total there are approximately 250–300 offering access at any one time: sites may remain online in one place for relatively short periods of time in order to frustrate tracing and detection or because their unique resource locators (URLs) have been blocked in jurisdictions that operate hotline enforcement. In general, blocking is effective in preventing subscribers from accessing the site content and cuts the flow of money to the criminal, but is only a temporary preventative measure and an inconvenience that is likely to be factored into criminal business planning. Criminals overcome this action by changing URLs and using a different host server on the same block of servers or, if necessary, in another jurisdiction.

The US continues to provide a significant proportion (49 per cent for the 2007 calendar year) of host servers carrying child abuse images and has a greater number of active sites, due for the most part to the large number of server companies in operation there. In recent years there have been a similar proportion of sites (40 per cent) hosted in Russia, mainly on one particular group of servers controlled by a single entity known as the Russian Business Network (RBNNet).<sup>74</sup> After considerable publicity, commercial and political pressure, RBNNet's access to the Internet was disconnected in September 2007, and the sites hosted on their servers disappeared temporarily. The offending sites have reappeared on different servers in jurisdictions not previously associated with this type of material.

The widespread use of Internet payment systems has been the most notable laundering development of recent years, with both legitimate accounts exploited (e.g. the recruitment of unsuspecting 'money mules') and fraudulent accounts registered for the purpose of transferring the proceeds of crime, ultimately to organised crime groups.

Meanwhile, it is clear that the nature of organised crime, at least as regards the commercial distribution of child abuse images, is changing. Whilst networks may be constrained by commonality of language and culture, the traditional concept of organised criminal groups

as hierarchical no longer applies. Rather, networking is often motivated by immediate and temporary requirements for specialist services and advice supported by IT infrastructure, while for some networks the distribution of child abuse images may be just one of a number of illegitimate businesses generating income.

## 2.4 Encryption

In 2001, concerns were rightly raised about the use of encryption by online child sexual offenders, as evidenced by the online network known as the Wonderland Club.<sup>75</sup> Encryption continues to be used by some of the more security-conscious offenders. Thus far, however, its use has not been as widespread as predicted: rather, the vast majority of individuals under investigation by law enforcement lack either the understanding or the patience required to protect their files.<sup>76</sup> That is not to say that encryption is no longer a threat to the successful investigation of sexual offences against children: if the usability of encryption software improves, e.g. through its incorporation into standard operating systems, the threat is likely to increase significantly. Continued law enforcement engagement with software developers is therefore required, not only to obtain advance information on industry developments but also to raise awareness amongst industry representatives of the impact of such developments on child protection. Meanwhile, legislation permitting investigators to request passwords for encrypted files is already in force in the UK and serves as a deterrent to offenders seeking to evade detection by these means: extension of such legislation to other jurisdictions therefore has the potential to prevent image offending in certain cases.

## 2.5 Wireless Technology

Wireless technology (Wi-Fi) enables offenders to have more flexible access to the Internet, which in turn may engender increased offending and, by extension, the number of offences to be investigated by law enforcement agencies.

The opportunities that wireless access presents to offenders are increasing as more and more companies and services are providing wireless access nodes and hotspots, and unsecured wireless broadband connections are liable to unauthorised use (piggybacking). Downloaders, distributors and groomers may choose to take advantage of local unsecured connections rather than engaging in illegal activity via services registered in their own names.

Account holders could be held liable for the actions of those gaining unauthorised access to an unsecured connection, since in these cases it will be their IP address – and not that of the offender – which will be linked to any child abuse images or other activity. Awareness

raising campaigns alerting wireless broadband subscribers to the dangers of leaving their connections unsecured could therefore go some way to preventing this manner of offending.

For the same reasons, wireless hotspots and ‘Pay and Go’ wireless services also are perceived as facilitating more anonymous access to the Internet, which may be exploited by those committing both image and grooming offences in order to evade detection. It is therefore vital that ISPs continue to work with law enforcement to provide all the information at their disposal which may identify and therefore locate the offenders and victims behind online identities.

## 2.6 Mobile Technology

The integration of Internet functionalities, e.g. instant messaging, social networking and online gaming, into mobile phones means that children and young people are now more available more of the time. This is further impacted by the convergence of mobile services and location-based services, whereby GPS technology is integrated into mobile phones. Constant online access via mobile phones and the ability to locate a child via developing Internet functionalities create a heightened risk to children from sexual offenders and, indeed, of ‘self-harming’ by means of engagement in sexual acts via mobile Internet. As previously noted,<sup>77</sup> parents are less and less able to supervise children’s access to the Internet, a development which diminishes the impact of preventative strategies involving parental control, and by the same token highlights the importance of empowering children and young people to stay in control of their online interactions, and equipping them to manage situations about which they feel uncomfortable.

With regard specifically to the distribution of child abuse images, mobile Internet technology not only facilitates the speedy uploading of real time’ images and their distribution using mobile versions of P2P networks, but also adds to the number of storage devices requiring seizure and forensic analysis by investigators of child sexual abuse. It must also be borne in mind that mobile Internet technology is likely to open up the Internet to regions, including developing countries, which have previously seen comparatively limited uptake – something which may in turn uncover hitherto untapped markets for online child sexual abuse in all its manifestations.<sup>78</sup> It therefore follows that the provision of adequate legislation and investigative capacity and expertise will be essential in these regions.

## 3. Research and Development

Strategic analysis identifies intelligence requirements, which in turn prompt research and development. The following overview of research and development is not exhaustive, but serves rather as an indication of the level of commitment shown by VGT agencies and their partners to meet the current and future challenges to combating the online sexual abuse of children and young people.

The need for collaborative research which draws on the full gamut of data, information sources and experiences of law enforcement, NGOs, academics and ISPs has been raised in a number of arenas.<sup>79</sup> Such research is urgently required at an international level in order to gain a more comprehensive and accurate assessment of the scale and nature of online offences against children.

### 3.1 Commercial Exploitation

CEOP is currently leading on the development of a European Financial Coalition of stakeholders against child exploitation and abuse images in the EU. The Coalition aims to address the commercial sexual exploitation and abuse of children online by:

- Implementing a monitoring system with the support of parties involved in Internet payment systems and hampering the merchant side of this growing business. This would incorporate existing mechanisms such as the IBOT Project (led by the Italian Police), which looks at education, intelligence gathering and investigation of all aspects of on-line child exploitation matters;
- Assisting financial service providers (more specifically credit card companies, banks and other payment providers) and ISPs to combat the abuse of their systems for the purchase of child exploitation or abuse images by instigating governance procedures and appropriate amendments to terms and conditions that will enable the isolation of offenders and frustrate the consumer side of the problem;
- Involving economic stakeholders (financial service providers, banks and ISPs) in the development of coordinated strategies, ultimately allowing law enforcement to trace and arrest offenders who profit from the commercial distribution;

- Developing intelligence to direct law enforcement activity against offenders via a law enforcement-led tasking and coordination group; and
- Ensuring that victim identification processes are prioritised, developed and defined in each area of the Coalition's activity.

Ultimately, the coalition aims to address the problem of commercial exploitation from both the supply and demand sides, hampering the commercial viability of the sale of child abuse images on the Internet. The project therefore proposes in its development phase to scope the nature and scale of online commercial exploitation through the production of strategic threat assessments and other research, to both improve understanding at an international level and determine the best focus for operational interventions in the European context. It will work in partnership with the US Financial Coalition, sharing analytical findings and best practice.

## 3.2 International Collaboration

In a similar vein, CEOP and the ICE are now working with the VGT on an initiative to improve law enforcement ability to investigate across different jurisdictions. The working group has already met on two occasions, developing several strategies to help ensure a successful product. Assistance is currently being sought from national hotlines such as the IWF in the UK and the NCMEC in the US to pool and analyse the data they collate, to direct investigations towards the right targets and ensure a coordinated and focussed approach against organised international distributors.

Cybertip.ca in Canada and NCMEC in the US have a close working relationship and have begun to identify common data points that should be collected for each commercial distribution report. The goal is to expand this working relationship to the other VGT countries and eventually to other hotlines outside the VGT countries. Additionally, the working group intends to establish a system for centralising the reports related to commercial distribution. This would enable the working group to:

- Compare the reports from each VGT country to determine the scale of the problem;
- Assess the extent of involvement of international organised crime groups (OCGs);
- Assess the methods used by international OCGs for targeting potential customers;
- Identify and prioritise investigative targets; and
- Assess the impact of law enforcement action.

### 3.3 Child Abuse Material

Research to date has found that the victims depicted in child abuse material are predominantly of white European or – to a lesser extent – Asian appearance.<sup>80</sup> CEOP and researchers from the academic community have therefore initiated a research project into the ethnicity of victims in still images of child sexual abuse. Involving the examination and classification of up to 1 million recently seized images from a range of offenders (possessors, distributors and some contact abusers), analysis will be conducted on the basis of victim ethnicity, gender, apparent age group (i.e. pre-ambulatory, pre-pubescent or pubescent), level of indecency (0–5 according to UK sentencing guidelines) and the presence and ethnic appearance of an offender.

Data will be analysed through descriptive statistics, with initial analysis taking place after data entry for each cohort of 1,000 images, complemented by a more purposive sampling of collections seized from 10 known offenders. It is anticipated that this analysis will contribute to a more differentiated approach to understanding risk in offenders, and that it will be regularly updated with smaller samples to determine any changes in the demographics of the images from the original baseline sample; in addition, a practitioner survey of Interpol member states will be initiated to identify any similarities to or differences from the UK sample.

### 3.4 Young People Who Display Sexually Harmful Behaviour

Young people are increasingly exploring and developing their sexuality online. The false sense of security and anonymity provided by the Internet encourages them to push the boundaries of sexual development, e.g. by exposing themselves on webcam or encouraging others to do so.<sup>81</sup> A proportion of young people engaging in these behaviours – and effectively grooming, inciting, even possessing or distributing child abuse material – will not even realise that they are committing offences, thereby reinforcing the need for continued education and awareness raising amongst young people regarding the implications of certain online activities.

Equally, there are a number of young people who, for a number of complex reasons, may develop a sexual interest in children, offending as adolescents and continuing to offend as adults. Amongst specific intelligence gaps is how adolescent offenders use the Internet in their offending behaviour, i.e. whether this use may fuel their fantasy and assist in them committing other offences. Initial indications are that this group is accessing adult

pornography or computer generated images (CGIs) of abuse, including representations of cybersex in online gaming environments.

According to data on online child sexual abuse supplied to CEOP by UK police forces, 3 per cent of suspects (where known) were under 18 at the time of the offence – a proportion that correlates with findings from the US.<sup>82</sup> The challenge currently faced by law enforcement and partners is how to differentiate between those young people engaging in sexual activity on the Internet as part of their normal development and those with sexual behaviour problems.<sup>83</sup> At the same time, concern has been expressed over whether looking at online deviant sexual material may act as a catalyst to engage in sexually problematic behaviour with another child or children.<sup>84</sup>

In light of this, CEOP's BAU has initiated a research project which seeks to gain a greater understanding of sexually problematic behaviour displayed online by under 18s and, in time, the impact on children and young people of the viewing of child abuse material. It is anticipated that these findings will contribute to the development of a risk-assessment process, which will afford consistency in dealing with young people who commit online offences, and will enable CEOP to advise law enforcement Public Protection Units accordingly.

### 3.5 Offender Profiles

Research suggests that the vast majority of suspects for image offences – between 85 per cent and 100 per cent – are males of white European appearance.<sup>85</sup> Taking its lead from Carr's analysis of New Zealand offenders,<sup>86</sup> the Australian Federal Police's Child Protection Operations (CPO) has instigated a project which enables data collection, statistical analysis and reporting on Australian online child sex offenders. The data pertaining to 172 Australian online child sex offenders subject to search warrant execution for the period 1 January to 31 October 2007 is currently being collected and analysed. Whilst it is not within the purview of this project to provide a psychological insight into offending, the data obtained may provide scope for further research in this area. Findings relating to demographics, detection, offence-related behaviour, judicial processing and the content of image collections will be used by law enforcement to improve the identification, processing and treatment of offenders, and to proactively respond to the issues surrounding the prevention of offences of this nature. This information will be compared with the existing findings from earlier statistical analyses of online child sex offenders,<sup>87</sup> which will then be integrated with the present data set to increase the representative quality of future research.

## 3.6 Further Ongoing Research and Related Developments

- The Australian Federal Police and the NCECC in Canada are conducting research into the effects on law enforcement personnel of viewing child sexual exploitation material.
- The NCECC Research and Development section in Canada has helped establish a network of international researchers. Since Internet-facilitated child sexual exploitation offences cross all boundaries, this network draws on the experience of researchers globally.<sup>88</sup>
- A gap in front-line medical professionals' awareness of the links between sexual assaults on children and the Internet has been identified in Canada. The NCECC is working on a joint research project with the Child and Youth Protection Program at the Children's Hospital of Eastern Ontario, the Suspected Child Abuse and Neglect Program at the Hospital for Sick Children and the Ontario Network of Sexual Assault/Domestic Violence Centers. The project is the first of many that will gather information from health-care clinicians as well as sexually assaulted children and youth with respect to Internet-facilitated child sexual exploitation. Themes to be explored include prevention, awareness and education as well as management and response strategies. A comprehensive survey of health-care professionals has been distributed and results are being assessed.

## 3.7 Technical Tools

- VGT agencies are currently developing various software tools for searching P2P file-sharing networks for child abuse material, and for locating and identifying those involved in its non-commercial distribution. Given, however, that engagement in such proactive work is likely to identify many hundreds of new suspects around the globe, these technical solutions must also be complemented by provision of additional investigative resources in terms of staffing in both national and local units.
- Interpol is currently developing a new version of its Child Abuse Image Database (ICAID). The International Child Sexual Exploitation database (ICSE), funded by the G8, will address some of the weaknesses of the original and will allow remote access for approved personnel by means of Interpol's i24/7 virtual private network.

- The NCECC in Canada identified the need for an image analysis tool that provides a centralised data repository to identify victims and offenders depicted in images, videos and text documents. This tool/database is in the beta stages of development with an RFP (request for proposal) prepared to identify vendors to provide specific enhancements. The tool will be made available nationally, and there are plans to share information with international partners who have image databases (e.g. Interpol, UK). To strengthen the capacity of police partners, multiple agency access to the database is under development.<sup>89</sup>

## 4. Concluding Remarks

Law enforcement agencies in some nations have made significant progress in investigating the online sexual abuse of children and young people, most notably adopting a more victim-centred and collaborative approach. It must be acknowledged, however, that even those national specialist centres established since World Congress II are still insufficiently resourced to meet the challenges of investigating the sexual abuse of children and young people in an environment which is constantly expanding and evolving, thereby providing unprecedented opportunities for sexual exploitation. It is therefore not merely the case that successful international collaboration models (such as the VGT) and inter-sectoral models (such as that employed by CEOP in the UK) need to be extended to other jurisdictions and regions – although this is clearly a priority. On the basis of emerging trends in offending and victim behaviours, and technological developments liable to misuse, we need to be looking ahead *now* to offending in the online environment *tomorrow*. This is no mean feat, as comparisons of online child sexual abuse in 2001 and 2008 have illustrated; but it is essential to ensuring adequate investigative provisions and child protection resources to meet these increasing challenges in the years to come. Amongst specific requirements are the following:

- Equivalent legislation in all jurisdictions, criminalising all aspects of online child sexual abuse, including
  - o The production, distribution, possession and access to/ viewing of child abuse material;
  - o The online solicitation of children and young people under 18 years of age for sexual purposes; and
  - o The facilitation of any of the above.
- The said legislative provision to be accompanied by the necessary investigative and judicial procedures, capacity and resources for its successful implementation.
- The criminalisation of “simulated representations or realistic images of a non-existent child” should not be optional, but internationally binding – again with accompanying provision of increased investigative capacity for the prosecution of such activity.
- The investigation and prosecution of online child sexual abuse offences to be a policing priority at international, national and local levels, with governments required to

provide adequate specialist resources and expertise, in the form of national specialist centres (where these do not already exist) and specialist training and resources for local territorial units, to successfully bring offenders to justice.

- The international collaboration model of the VGT to be replicated across all jurisdictions on the basis of an identified commonality in offending behaviours, resourcing levels etc or geographical location – e.g. Association of Southeast Asian Nations (ASEAN), Central and South America, African Nations – as appropriate. If geographically aligned, member nations with better developed child protection arrangements and investigative resources to provide support to those nations in which they are less developed.
- All Interpol member states to contribute to the Interpol Child Abuse Image Database (ICAID) and its successive versions.
- The monitoring of online interactions by service providers to be mandatory, with immediate referral to law enforcement of alleged incidents of online child sexual abuse.
- Service providers to be required to collaborate with law enforcement to make new and existing online environments safer by design; with regard specifically to online solicitation, service providers to provide mechanisms for Internet users to report directly to law enforcement from the online environments in which the sexual abuse of children is experienced or detected; governments to ensure that there are adequate resources for responding to reports received.
- Online access and communications data to be retained for investigative purposes for a standardised period and supplied free of charge in all jurisdictions, as evidence of service providers' corporate social responsibility.
- All jurisdictions to develop and deliver awareness raising programmes which empower children and young people to stay in control of their online interactions, inform the adults responsible for them, and enable both to report abuse directly to the relevant authorities.

# Endnotes

- 1 VGT member agencies do not use the term ‘child pornography’, as this i) indicates legitimacy, compliance on the part of the victim, and therefore legality on the part of the abuser and ii) conjures images of children posing in ‘provocative’ positions, rather than being subjected to sexual abuse.
- 2 It should be noted, however, that this is a UK-authored document which does not attempt to give an exhaustive account of activities by VGT agencies, but focuses rather on VGT-wide initiatives and takes the Child Exploitation and Online Protection (CEOP) Centre as a case study of inter-sectoral working.
- 3 Moore & Clayton (2008) p.6; IWF (2008) p.6
- 4 Quayle (2008) p.442
- 5 Cf Wortley & Smallbone (2006) pp.25-27
- 6 Internet World Stats. Accessed on 1 September 2008 from: <http://www.Internetworldstats.com/emarketing.htm>
- 7 Netcraft. *July 2008 Web Server Survey*. Accessed on 1 September 2008 from: [http://news.netcraft.com/archives/2008/07/07/july\\_2008\\_web\\_server\\_survey.html](http://news.netcraft.com/archives/2008/07/07/july_2008_web_server_survey.html)
- 8 Cf Quayle & Taylor (2006) p.117: “Until the advent of the Internet, material that would have been considered illegal was difficult to access”.
- 9 Ybarra & Mitchell (2008) p.354, from a national cross-sectional online survey of 1588 youth.
- 10 See note 1 above for the VGT’s objections to the use of this term.
- 11 Carr (2001) p.6
- 12 Moore & Clayton (2008) p.5
- 13 For which see Wortley & Smallbone (2006) p.25-7
- 14 Council of Europe Treaty Series (CETS) 201 3.a
- 15 CETS 201.18.1
- 16 ICMEC (2006)
- 17 CETS 201.20.4
- 18 Jewkes & Andrews (2005) p.44
- 19 *Criminal Justice and Immigration Act 2008* s.72
- 20 As noted by Moore & Clayton (2008) p.5; cf Oswell (2006) p.249; Wolak, Finkelhor & Mitchell (2005) p.21.
- 21 Use of which was correctly predicted to rise by ECPAT International (2005) p.32.
- 22 CETS 201.20.4
- 23 Carr (2001) p.6
- 24 Cf Jewkes & Andrews (2005) p.42
- 25 Klain, Davies & Hicks (2001) p.54; cf Jewkes & Andrews (2005) p.50, Sheldon & Howitt (2007) p.251: “... police priorities are assessed by reference to government key performance indicators, which fail to include the effectiveness of policing child pornography”.
- 26 Wolak, Mitchell & Finkelhor (2003) p.12
- 27 Wortley & Smallbone (2006) p.2. They also cite findings that 56 per cent of arrests for Internet child pornography crimes [in the US] originated from non-specialised law enforcement agencies.
- 28 As recognised by Krone (2005) p.5
- 29 Cf Krone (2005) pp.2 and 5 for the potential ‘mushroom’ effect of routine investigations into online child sexual abuse.
- 30 As identified in 2001 by Klain, Davies & Hicks (2001) p.54
- 31 As observed also by Jewkes & Andrews (2005) p.46f
- 32 Jewkes & Andrews (2005) p.47
- 33 Microsoft, AOL and Yahoo are notable amongst ISPs and CSPs in the UK that supply data at no cost. Charges in other countries vary, and include: up to €60 for a single request in Germany; up to €90 for an IP address in France; up to A\$15 for a single request in Australia; up to €60 per hour in Norway; and as much as €167 for an IP address in Switzerland.
- 34 For which, see Renold, Creighton, Atkinson & Carr (2003)

- <sup>35</sup> Sinclair & McColl (2007) p.9; for a similar proportion of US investigations (79 per cent) cf Wolak, Mitchell & Finkelhor (2003) p.viii
- <sup>36</sup> Under the terms of this sentence, an offender must satisfy the authorities that s/he is fit for release and does not pose a risk to the community before s/he can ever be considered for release.
- <sup>37</sup> Cf Wortley & Smallbone (2006) p.55 for discussion.
- <sup>38</sup> Cf Loof (2005) p.154
- <sup>39</sup> For which see Sheldon & Howitt (2007) p.252.
- <sup>40</sup> For instance, those made by Holland ((2005) p.76; and Svedin & Back (1996) p.65f
- <sup>41</sup> Cf Wortley & Smallbone (2006) p.25f.; Krone (2005) p.2
- <sup>42</sup> Holland (2005) p.77
- <sup>43</sup> Cf Sheldon & Howitt (2007) p.251
- <sup>44</sup> Moore & Clayton (2008) p.20: “The long lifetimes of websites hosting child sexual abuse images is particularly striking. In spite of a robust legal framework and a global consensus on the content’s repulsion, these websites are removed much slower than any other type of content being actively taken down for which we have gathered data. An average lifetime of 719 hours is over 150 times slower than phishing websites hosted on free web-hosting and compromised machines.”
- <sup>45</sup> CETS 201.10
- <sup>46</sup> Cf Holland (2005) p.88 for the need for multi-disciplinary teams to investigate cases.
- <sup>47</sup> See, for instance, ECPAT International (2005) p.6; CETS 201.9
- <sup>48</sup> The need to educate parents has already been recognised by ECPAT International (2005) p.10: “As they are on the frontline, parents and carers will be a primary target of awareness-raising and education initiatives about how to be safe in cyberspace.”
- <sup>49</sup> Wortley & Smallbone (2006) p.44
- <sup>50</sup> Jewkes & Andrews (2005) p.55
- <sup>51</sup> For which see Jewkes & Andrews (2005) p.58
- <sup>52</sup> CEOP (2008)
- <sup>53</sup> Cf – amongst many others – Crowe & Bradford (2006) p.331 on the ‘porous boundaries’ between the material and virtual aspects of young people’s leisure.
- <sup>54</sup> Wolak, Finkelhor & Mitchell (2005) p.viii
- <sup>55</sup> Cf NCECC (2005) p.2
- <sup>56</sup> Whilst Web 2.0 has been notoriously difficult to define, it is perhaps most helpfully described as the “ongoing transition of the World Wide Web from a collection of websites to a fully fledged computing platform serving web applications to end users. It refers to a supposed second generation of Internet based services – such as social networking sites, wikis, communication tools, and folksonomies – that emphasize online collaboration and sharing among users” (accessed on 14 March 2008 from: <http://www.2020systems.com/Internet-ad-glossary-r-z.html>).
- <sup>57</sup> Research recently published in the US (Wolak, Finkelhor, Mitchell & Ybarra (2008)) posits that young people who send personal information to unknown people are more likely to encounter individuals who make online sexual advances, but also stresses that “interactive behaviours, such as conversing online with unknown people about sex...more clearly create risk” (p.117).
- <sup>58</sup> Ybarra & Mitchell (2008) p.350
- <sup>59</sup> Predicted by ECPAT International (2005) p.49
- <sup>60</sup> Accordingly, 30 per cent of reports submitted to CEOP online were referred by the Windows Live Messenger ‘Report Abuse’ tab.
- <sup>61</sup> Accordingly, the US has already seen a drop in teen IM usage – cf Lenhart, Madden, Macgill & Smith (2007) p.27.
- <sup>62</sup> Ybarra & Mitchell (2008) p.356
- <sup>63</sup> Renold, Creighton, Atkinson & Carr (2003)
- <sup>64</sup> Digital Detective Forensic Forum Poll based on 158 votes – closed 10 August 2008, with data available on request. Cf Baartz (2008) p.4
- <sup>65</sup> Wolak, Finkelhor & Mitchell (2005) p.9

- <sup>66</sup> Cf ECPAT International (2005) p.4 for an earlier expression of concern regarding “advances in technology that enable sexual violence against a child to be organised to occur live online, in real-time, whereby multiple abusers may participate from different physical locations across the world”.
- <sup>67</sup> Renold, Creighton, Atkinson & Carr (2003)
- <sup>68</sup> Cf Jewkes & Andrews (2005) p.51 for the “ever-ascending uphill struggle” faced by investigators in this field.
- <sup>69</sup> As cited by Wortley & Smallbone (2006) p.12f
- <sup>70</sup> According to a Digital Detective Forensic Forum poll, conducted 22 November 2007 – 10 April 2008.
- <sup>71</sup> Jewkes & Andrews (2005) p.58
- <sup>72</sup> IWF (2008) p.7
- <sup>73</sup> It should be borne in mind that each domain may have many URLs, and as a result URL numbers are not a reliable indicator of how many sites actually operate.
- <sup>74</sup> Source: Internet Watch Foundation
- <sup>75</sup> Carr (2001) pp.5 and 33
- <sup>76</sup> Cf Wolak, Finkelhor & Mitchell (2005) p.9, where just 6 per cent of image possession offenders in the US used encryption.
- <sup>77</sup> Cf ECPAT International (2005) p.10f; Quayle and Taylor (2006) p.124f
- <sup>78</sup> Cf Quayle and Taylor (2006) p.124
- <sup>79</sup> Most recently, the European Regional Preparatory Meeting for World Congress III.
- <sup>80</sup> Eg Carr (2004); Quayle (2008) p.446
- <sup>81</sup> For which see Quayle and Taylor (2006) p.117
- <sup>82</sup> Wolak, Mitchell & Finkelhor (2003) p.7; Wolak, Finkelhor & Mitchell (2005) p.vii
- <sup>83</sup> Cf Longo (2004); Quayle & Taylor (2006) p.121
- <sup>84</sup> Quayle & Taylor (2006) p.117
- <sup>85</sup> Eg Carr (2004) p.135; Baartz (2008) p.3; Wolak, Mitchell & Finkelhor (2003) p.viii; Wolak, Finkelhor & Mitchell (2005) p.vii; Quayle (2008) p.446
- <sup>86</sup> Carr (2004); cf Sullivan (2005).
- <sup>87</sup> Eg Baartz (2008)
- <sup>88</sup> Sinclair & McColl (2007) p.13
- <sup>89</sup> Ibid. p.8

# Bibliography

Baartz, D. *Australians, the internet and technology-enabled child sex abuse: a statistical profile*. Australian Federal Police. 2008.

Carr, A. *Internet Traders of Child Pornography and other censorship offenders in New Zealand*. New Zealand Department of Internal Affairs. 2004.

Carr, J. *Child Pornography*. London. 2001. Accessed on 3 October 2008 from: [http://www.ecpat.net/eng/Ecpat\\_inter/projects/monitoring/wc2/yokohama\\_theme\\_child\\_pornography.pdf](http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf)

CEOP. *Strategic Overview 2007-8*. London. 2008. Accessed on 3 October 2008 from: <http://www.ceop.gov.uk/downloads/documents/CEOPStrategicOverview2008.pdf>

Crowe, N. & Bradford, S. Hanging out in RuneScape: identity, work and play in the virtual playground. *Children's Geographies*, 4 (3), 2006, 331-346.

ECPAT International. *Violence Against Children in Cyberspace*, ECPAT International. Bangkok. 2005.

Holland, G. Identifying Victims of Child Abuse Images: An Analysis of Successful Identifications. In E. Quayle & M. Taylor (Eds.), *Viewing Child Pornography on the Internet*. Lyme Regis. 2005. pp. 75-89.

ICMEC. *Child Pornography: Model Legislation and Global Review 2006*. International Centre for Missing and Exploited Children. Brussels. 2006.

IWF. *Internet Watch Foundation 2007 Annual and Charity Report*. 2008. Accessed on 15 May 2008 from: [http://www.iwf.org.uk/documents/20080417\\_iwf\\_annual\\_report\\_2007\\_\(web\).pdf](http://www.iwf.org.uk/documents/20080417_iwf_annual_report_2007_(web).pdf)

Jewkes, Y. & Andrews, C. Policing the Filth: The Problems of Investigating Online Child Pornography in England and Wales. *Policing and Society* 15 (1), 2005, 42-62.

Klain, E., Davies, H. & Hicks, M. *Child Pornography: The Criminal-Justice-System Response*. American Bar Association Center on Children and the Law for the National Center for Missing & Exploited Children. 2001.

Krone, T. *International Police Operations against Online Child Pornography*. Australian Institute of Criminology, Canberra. 2005. Accessed on 25 August 2008 from: <http://www.aic.gov.au/publications/tandi2/tandi296.pdf>

Lenhart, A., Madden, M., Macgill, A.R. & Smith, A. *Teens and Social Media*. Pew Internet and American Life Project. 2007. Accessed on 23 March 2008 from: [http://www.pewinternet.org/pdfs/PIP\\_Teens\\_Social\\_Media\\_Final.pdf](http://www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf)

Longo, R.E. Young people with sexual behaviour problems and the Internet. In M. Calder (Ed.), *Child Sexual Abuse and the Internet: Tackling the New Frontier*. Russell House. Lyme Regis. 2004.

Loof, L. Global Issues and Regional Co-operation Fighting Child Exploitation. In E. Quayle & M. Taylor (Eds.), *Viewing Child Pornography on the Internet*. Russell House. Lyme Regis, 2005. pp. 151-160.

Moore, T. & Clayton, R. *The Impact of Incentives on Notice and Take-down*. Seventh Workshop on the Economics of Information Security (WEIS 2008). 25–28 June 2008.

NCECC. *Internet Based Sexual Exploitation of Children and Youth: Environmental Scan*, National Child Exploitation Coordination Centre Strategic and Operations Support Services. Ottawa. 2005.

Oswell, D. When Images Matter: Internet Child Pornography, Forms of Observation and an Ethics of the Virtual. *Information Communication and Society* 9 (2), 2006, 244-265.

Quayle, E. & Taylor, M. Young People who sexually abuse: the role of the new technologies. In M. Erooga & H. Masson (Eds.), *Children and Young People who Sexually Abuse Others: current developments and practice responses*. Routledge. London. 2006. pp. 115-127.

Quayle, E. Online Sex Offending: Psychopathology and Theory. In D. Laws & W. O'Donohue (Eds.), *Sexual Deviance: Theory, Assessment and Treatment*, 2<sup>nd</sup> ed. Guilford. New York. 2008. pp. 439-458.

Renold, E., Creighton, S., Atkinson, C. & Carr, J. *Images of Abuse: A review of the evidence on child pornography*. National Society for the Prevention of Cruelty to Children, UK. 2003.

Sheldon, K. & Howitt, D. *Sex Offenders and the Internet*. John Wiley & Sons. New York. 2007.

Sinclair, R. & McColl, E. *The National Child Exploitation Coordination Centre Interim Progress Report #1, April 2004 – June 2007*. The National Child Exploitation Coordination Centre, Ottawa. 2007.

Sullivan, C. *Internet Traders of Child Pornography: Profiling Research*. New Zealand Department of Internal Affairs. 2005.

Svedin, C.G. and Back, K. *About Children who don't speak out: about children being used in child pornography*. Rädda Barnen (Save the Children Sweden). Stockholm. 1996.

Wolak, J. Mitchell, K.J. & Finkelhor, D. *Internet Sex Crimes Against Minors: The Response of Law Enforcement*. National Center for Missing and Exploited Children. Alexandria, VA. 2003.

Wolak, J., Finkelhor, D. & Mitchell, K.J. *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study*. National Center for Missing and Exploited Children. Alexandria, VA. 2005.

Wolak, J., Finkelhor, D., Mitchell, K.J. & Ybarra, M.L. Online Predators and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. *American Psychologist*, 63 (2), 2008, 111-128.

Wortley, R. & Smallbone, S. *Child Pornography on the Internet: Problem-Oriented Guides for Police*. (Problem-Specific Guides Series No. 41). 2006. Accessed on 25 August 2008 from: <http://www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf>

Ybarra, M. & Mitchell, K. How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs. *Paediatrics* 121 (2), 2008, 350-357.



The World Congress III against Sexual Exploitation of Children and Adolescents aims to mobilise all countries to guarantee the rights of children and adolescents to be protected against sexual exploitation by taking action to:

- Build on current achievements, examine new challenges and dimensions of sexual exploitation and set more targeted strategies and measures to address them.
- Examine initiatives that have been effective in different regions and identify channels to facilitate better exchange of experience, skills and knowledge.
- Open new channels and secure greater international cooperation on key issues (including cross-border and inter-regional cooperation) to facilitate collaborations for counteraction.
- Catalyse a systemic and inter-sectoral approach to guarantee children and adolescents' right to be protected from sexual exploitation.
- Establish time-bound goals to promote and monitor progress on action plans made by the Congress.

Commercial sexual exploitation of children occurs in many different ways and in a wide variety of settings. The underlying causes are numerous, complex and closely interrelated and must be analysed, understood and confronted accordingly. In order to facilitate the implementation of the objectives of the World Congress III, the Central Organizing Committee (Government of Brazil, UNICEF, ECPAT and the NGO Group for the Convention on the Rights of the Child) has commissioned thematic papers on five major areas of this complex phenomenon and violation of child rights.

The World Congress III themes are on:

- Theme 1: Dimensions of Commercial Sexual Exploitation: prostitution of children, child trafficking for sexual purposes, child abuse images and sexual exploitation online, sexual exploitation of children in tourism
- Theme 2: Legal Frameworks and Law Enforcement
- Theme 3: Integrated Inter-Sectoral Policies
- Theme 4: Role of the Private Sector and Corporate Social Responsibility
- Theme 5: Strategies for International Cooperation

