

**Parliamentary Joint Committee on the
Australian Crime Commission**

Inquiry Into Cybercrime

Submission No:2

Received 13 May 2003

Mr Darren Brookes

#656 South East Jamar Street

Pullman

WASHINGTON 99163 USA

☎ (509) 335 2264 

E-mail: dbrookes@wsu.edu

SUBMISSION TO AUSTRALIAN SENATE COMMITTEE ENQUIRY

CYBERCRIME: Child Pornography & Paedophile Activity.



**Darren George BROOKES
Fulbright Scholar
C/o Washington State University
Pullman
Washington**

CONTENTS

FOREWORD	page 3
1. INTRODUCTION	page 4
2. BACKGROUND	page 4
3. EVALUATION OF PROBLEMS	page 5
4. CONCEPTS – ANALYSIS	page 6
Profile	page 7
Risk	page 7
Textual Analysis	page 8
5. CRITICAL RISK ASSESSMENT	page 9
6. EDUCATION & TRAINING	page 10
Education	page 10
Training	page 11
7. PREVENTION	page 11
8. DETECTION	page 12
9. FRUSTRATION	page 12
10. LEGAL IMPLICATIONS	page 13
11. PERSONNEL / TRAINING IMPLICATIONS	page 14
12. COSTS	page 14
13. RECOMMENDATION	page 14
14. CONCLUSION	page 14
APPENDIX A: Newsgroups Chat rooms Communities Peer to peer Live Abuse	page 16
APPENDIX B: Definitions	page 18
APPENDIX C: References	page 20

Foreword

I am an Australian Resident, currently working on the Criminal Justice Program at Washington State University. I am a Fulbright Scholar and have been awarded a Bramshill Fellowship to pursue a PhD for research into characteristics of Internet paedophile.

I am a founder / member of the UK Experts Group that Combats Child Abuse on the Internet. (CCAI).

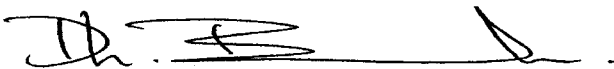
Prior to taking up my present position I was the Head of the Paedophile Unit (Interactive) in the United Kingdom. Here I was responsible for the pro-active investigation of all aspects of paedophilia, including the use of computers by paedophiles to facilitate crimes against children.

I have written extensively about paedophile behaviour and I was responsible for the first computer 'sting' operation of its kind using covert officers on-line. This type of online investigation has been copied on an international basis and I am presently working with the United States law enforcement to establish 'Best Practice'.

I am also responsible for the development of 'covert' sites to prevent / detect paedophile activity, and my current project is with the BBC in developing Virtual Reality as an investigative tool.

Prior to this I worked at the New South Wales Police Academy, Goulburn where I lectured on Investigations and computer crime.

NOTE: The views in this paper are those of the author and not necessarily those of Washington State University, West Midlands Police, the UK Experts Group or the Fulbright Commission.



D. G. BROOKES

Contact Address: #656 South East Jamar Street,
Pullman,
Washington,
99163
USA

Telephone: (509) 335 2264

E-Mail: dbrookes@wsu.edu
dgbrookes@yahoo.com

Introduction

- 1.1. The purpose of this paper is to provide an overview of current trends of on-line paedophile behaviour and any restrictions that legislation may place on this type of investigation.
- 1.2. This paper details possible responses and makes suggestions that could be implemented to contain, eradicate or reduce this type of offending behaviour.
- 1.3. My research is primarily centred on those persons who have used computers to commit offences against children. This can be from those who have used the Internet to obtain and 'possess' Indecent Images of Children to those who have shown 'adult' pornography to children as part of a 'grooming' process. The research also includes the use of peer to peer and 'chat rooms' by such offenders.
- 1.4. I have already identified that there is a necessity, to a certain degree, to profile those types of offenders who use the Internet. Doing this and conducting a dynamic Risk Assessment can plot the potential threat posed by individuals.
- 1.5. This document sets out the present research and its potential for use within law enforcement. Due to the nature of the Internet many of the issues impact globally but I have endeavoured to tailor this submission from an Australian perspective, and where appropriate I have referred to existing Australian legislation.

2. Background

- 2.1 My research has been funded by the Fulbright Commission and supported by West Midlands Police (WMP) via a Bramshill Fellowship for my doctorate. WMP has an international reputation in respect of its innovative work in the child protection arena, in particular in respect of paedophile investigation. Several recent operations Operation MONTOVANI and ORE have served to further enhance this reputation.
- 2.2 Therefore the goal of this research is to continue this impetus towards investigating those paedophiles that use technology to thwart the activities of Law Enforcement.
 - 2.2.1 The objective is to conduct research into a specific group of paedophiles that use computers to facilitate crimes against children. The research conducted and the methods used will be formulated to make recommendations on how to best contain, eradicate or reduce offending against children.
- 2.3 There are a number of Law Enforcement Agencies both Nationally and Internationally looking into Internet use by paedophiles. However, this research is

unique as I am trying to understand the motivation or 'trigger' for using computers in this manner. By further understanding how this paedophile 'community' engages in this type of behaviour then we may be able to police this community in a more productive fashion. Therefore it may be possible at an early stage to identify those most likely to engage in 'real time' abuse.

- 2.4 The acts of paedophilia have been shown to form a circular pattern of offending behaviour. It is by recognising these patterns of behaviour, the motivators and the areas that are exploited by paedophiles that we can put measures in place, which will significantly impact on their offending behaviour.
- 2.5 Some of these measures fall outside of the scope of policing but do fall within the wider definition of law enforcement via work with other agencies. Examples of areas where this research will impact upon are:

- ❑ Education
- ❑ Crime Prevention
- ❑ Treatment Programs
- ❑ Victim Pool Identification
- ❑ Monitoring
- ❑ Risk Assessment

3. **Evaluation of Problems**

- 3.1.1. The problems associated with this research have increased considerably since I embarked on this project. There has been a proliferation of this type of crime that has received a high level of media and public interest.¹
- 3.1.2. Equally of those engaged in the making and distributing child pornography, have significantly changed their methods of operation. The use of the Internet has assisted in providing the ideal medium to quickly produce such material at relatively little cost or fear of detection.
- 3.1.3. The ability to web cam² with other like-minded individuals and children enforces this environment. The web cam is being increasingly used by Paedophiles to entice or groom children 'on-line' usually in IRC³ or 'chat room'⁴ environments. Many 'chat rooms' also allow for 'live' web-caming and for the exchange of images or files.

¹ See DAVID, F, GRABOSKY, P & GRANT, A. – 1999.

² Web cam – short for Web Camera. This is a camera, connected to a computer that can take or send a single or continuous image(s) over the Internet.

³ Internet Relay Chat - computer conferencing on the internet.

⁴ Chat room – an interactive discussion 'chat' about any topic.

3.1.4. Many Paedophiles operate in specific areas on the Internet⁵. The main areas are:

- Newsgroups;
- Chat rooms;
- Communities;
- P2P (peer to peer);
- Live abuse.

3.1.5. The research is not intended to justify the involvement of the police in this sensitive area. However, it is intended to provide a guide to the appropriate area of criminality that finite resources should be focused. The overall intention is to be able to assess work that is presented to investigators, in such a way that resources can be channelled to the most appropriate cases, those where there is a substantial belief that a child or children are at risk of abuse.

3.1.6. This can only be achieved by carrying out a risk assessment of the offence / offender in question. This a relatively simple task when faced with a known offender and victim or potential victim. Unfortunately the nature of paedophile offending behaviour on the Internet is such that it is increasingly difficult to establish, who they are, where they are and importantly their ability to carry out their offending.

3.1.7. The ability to remain anonymous, enter 'private' Internet chat rooms and 'groom' children on-line all fuels the fire of concern. It also makes it increasingly difficult for those tasked with policing this type of offending behaviour.

3.1.8. Over the last 6 months there has been an increase in the number of potential offenders, who have been identified via 'sting' operation, intelligence and police work carried out on the Internet. With this increase there is a necessity to be able to adequately analyse the potential risk that these individuals pose to children.

4. **Concepts - Analysis**

4.1.1. The identified problems require further evaluation but I have been able to categorise the main issues for further research as:

- PROFILE – the characteristics, both sociological and psychological, of those offenders who commit this type of crime.
- RISK – the potential risk that those profiled pose to society.

⁵ See Appendix A for a more detailed explanation of how each area is exploited.

- **TEXTUAL ANALYSIS** – the ability to analyse text of chat logs, e-mails and SMS to establish the intentions of the author

4.1.2. The concept of **Profile, Risk and Textual Analysis** when taken together with traditional policing methods provides a detailed pattern of offending behaviour. This potential for offending forms part of a **Critical Risk Assessment (CRA)**. The CRA allows the user to examine each case and to establish the *risk* that this individual poses to society.

4.1.3. By creating a CRA one is able to identify patterns and trends in offending behaviour but all assists those tasked with such investigations to allocate resources.

4.2. Profile

4.2.1. To establish a profile research was conducted with those paedophiles that have used computers to facilitate crimes against children.

4.2.2. The meaning of ‘facilitate’ is to use the computer in any way, so as to enable the offender, to fulfil his / her ultimate goal. This can be by directly committing crimes against children, by grooming children in chat rooms and arranging meetings, or by showing sexually explicit images via a computer in the offender / victims home. The use of a computer indirectly would be by collecting indecent images of children (Child Pornography⁶) from Websites or via FTP sites that allow file transfer.

4.2.3. The profiling of such offenders is achieved by interviewing those convicted Sex Offenders who have used a computer in this way. These offenders have been identified via State / Federal Penitentiaries, Probation Service, Law Enforcement and Sex Offender Treatment Programs.

4.2.4. The culmination of the interviews is to establish a behavioural pattern that can be interpreted by law enforcement so as to identify a type of offending behaviour, often referred to as a ‘profile’.

4.3. Risk

4.3.1. There are already well established Risk Assessments that are in use in respect of Sexual Offending behaviour.⁷ Commonly the risk assessment used in Australia is the one recommended in the Australia / New Zealand Standard 4360: 1999.

⁶ Child Pornography - this term indicates or implies financial agreement between the performer(s) and the pornographer. The reality is that there is little financial gain and all the images show a crime scene. Therefore it has been agreed, in the U.K, that this type of material will be referred to as ‘Child Abuse or Indecent Images of Children’

⁷ See - CONNOLLY, M and WOLF, S (1995).

- 4.3.2. The assessment commonly used by the UK Probation Service was the Thornton Scale, which has since been updated to produce the Matrix 2000 Risk Assessment.⁸ This assessment is meant to be dynamic and to take account of a number of variables when making a clinical risk assessment of a sex offender.
- 4.3.3. The assessment commonly used in Canada and parts of the United States is the Static-99: Sex Offender Need Assessment Rating (SONAR).⁹
- 4.3.4. The majority of those engaged in child protection within Australia are familiar with AS/NZ Standard and this greatly assists in the management of Sex or Dangerous Offenders. The value of using such an approach in the management of such offenders is that it gives indications on the potential for an individual to re-offend or to require further monitoring. Conversely it also allows for a reduction in levels in policing, if the subject responds to the management.
- 4.3.5. To this end any risk assessment that is to be used in conjunction with the profiling of Internet Paedophiles should adhere to the principles of AS/NZ 4360. It is my view that any results will only be enhanced by its use and increases the credibility of any assessment.
- 4.3.6. This assessment can be further enhanced by the judicious use of traditional law enforcement methods. Some of these methods are not relevant to each and every enquiry or are practical. For example surveillance is a well-established practice for law enforcement but difficult to instigate when the subject / location is not known.
- 4.3.7. Therefore to further improve our ability to obtain an accurate assessment I have looked at the practicalities of the use of 'textual analysis, in appropriate cases.

4.4. **Textual Analysis**

- 4.4.1. Textual analysis is used by many disciplines to analyse the meaning from a body or part of a text. The majority of such analysis is concentrating on the meaning of the particular paper, book or subject matter. However, it is possible to achieve this through the examination of smaller text, such as letters, speeches and lengthy correspondence.
- 4.4.2. The greater the length that a body of text is, the more accurate the analysis would be. As most Computer Mediated Communication (CMC) is short or uses acronyms as in Short Messaging Services (SMS), commonly referred to as 'texting' the opportunities to obtain accurate results are limited.
- 4.4.3. However, research to date has shown that those paedophiles intent on meeting with a child, will engage in a form of 'grooming' online. This is often a pattern

⁸ See - Hanson, R.K. and Thornton, D. (2000)

⁹ See - Hanson, R. K., and Harris, A. J. R. (2000)

of e-mails, chat logs or instant messages. It would be difficult to analyse one simple text message but several could supply the observer with sufficient detail to carry out such an examination.

- 4.4.4. This research is in its infancy but if appropriate it may have implications in other fields of investigation, for example terrorism and / or organised crime. This is part of my ongoing research and will not be discussed further in this paper

5. **Critical Risk Assessment (CRA)**

- 5.1. A CRA is intended to provide the user with the ability to look at a case objectively and taking account of all the variables, produce a valid risk assessment.
- 5.2. Once the CRA is complete the Police or other agencies would then monitor the subject to varying degrees. This can be from as low as “Intelligence – only” or “Operation” status. The information obtained is, where appropriate, then shared and if required a periodic review is imposed.
- 5.3. By ensuring that this assessment is ‘dynamic’ it follows that the process is continually updated. This allows the user to establish at varying stages, what risk, if any the subject is to society.
- 5.4. The risk factors will be High, Medium or Low and the subject may move either up or down dependant on the available factors.
- 5.5. This will ultimately allow those tasked with overseeing sex offender behaviour, to be able to make informed decisions as to what appropriate action to take. The obvious use for this would be in identifying those that pose the greatest of risks out of a large number of subjects. As law enforcement develops its ability to tackle this type of crime there will be a requirement to ensure that all is done to direct finite resources at the most relevant investigations.
- 5.6. Equally when conducting any on-line operations, it is necessary to be able to identify the collateral effect that these types of operations have within ‘virtual’ communities. For example when engaged in Interactive investigations operatives will be approached, ‘online’ by paedophiles other than the target. Presently these offenders are dismissed but what of the collateral effect? I believe that the use of a CRA will to some extent alleviate or reduce this issue.
- 5.7. Once this is accomplished then law enforcement has an infrastructure whereby it can begin to tackle the issues surrounding paedophile activity and the manufacture and distribution of Indecent Images.
- 5.8. Once an infrastructure is in place then resources should be channelled into the following areas:

EDUCATION & TRAINING

PREVENTION

DETECTION

FRUSTRATION

6. EDUCATION & TRAINING

6.1.1. Education

6.1.2. In relation to education this should include all members of society and not those just tasked with a duty to investigate.

6.1.3. Educating and the training should be an on going process, it is a sad fact that no matter what government implements crimes will still be committed. Therefore education programs should cover before, during and after a crime is committed.

6.1.4. Education before the fact should be aimed at:

- Children – all ages, and should include older children who can identify issues with younger siblings.
- Parents / Carers – there is a need to ensure that these adults are provided with simple information to be able to understand the risks their children may be exposed to.

6.1.5. Education to deal with the aspects of the crime should be aimed at:

- Police – (i/c those tasked with this type of investigation) need to understand the issues surrounding this type of offending behaviour. Officers need to understand the concepts of computer use, so they can respond effectively and ensure all evidence is preserved.
- Support Agencies – need to receive training into how a paedophile initiates contact with children and how children are manipulated. In this way they can ensure all is done to support a victim but more importantly be able to identify the potential scenario where the child may fall victim again.

6.1.6. Education after the fact should be aimed at:

- Judiciary / Prosecutors – The concept of cyber-crime needs to be understood by those tasked with administering the law. By educating the judiciary there is an increased likelihood that the concepts of this type of crime will be better understood.
- Probation Service – the Probation Service is often neglected when it comes to education. However, they play a pivotal role in ‘controlling’ offenders when they are returned to the community. Therefore it follows that they must understand the criminals offending behaviour so as to ensure all is done to reduce the levels of recidivist behaviour.

6.2. Training

- 6.2.1. The need for relevant training cannot be under estimated. Those specifically designated for this type of work i.e. the ACC should, in my opinion, have dedicated teams that specialise in this type of computer investigation but are NOT carrying out a Hi-Tech role.
- 6.2.2. To become more effective they should be supported by National and International Hi-Tech Crime Units. Traditionally it is these units that have instigated the investigations, but due to the volume of work they have been relegated to a mainly a reactive role.
- 6.2.3. In this way the dedicated teams do not get ‘bogged down’ with the technical aspects of the investigation. To use the analogy, drugs squad detectives are not required to analyse their seizures. This is left to Forensic Services, and allows the drugs squad to be more flexible in its approach. Cyber crime can and should be tackled in the same manner.
- 6.2.4. By releasing the investigators from the ‘burden’ of computer examination, frees them up to concentrate on a traditional law enforcement role. Training then can be diverted to other aspects of specialisation i.e. Undercover working, surveillance, intelligence gathering.
- 6.2.5. The final point under training that should not be ignored is that of Research and Development. The use of technology by criminals is subject of rapid change, therefore so as not to limit the ability of the ACC to tackle cyber-crime, there is a need to research offending trends. By doing so allows for protocols to be put into place to adequately respond to change.

7. **PREVENTION**

- 7.1. Prevention is by far the most cost effective way of dealing with any type of crime be it in the real or virtual world. Suggested preventive measure to consider should be:

- Early identification of both victim and offender pools
- Use of existing technology to thwart offender behaviour – i.e. Blocking, Filtering or Monitoring Software.
- Use of covert and overt web sites.
- Premier Bob CARR has muted preventative legislation – the introduction of Sex Offender Orders similar to Apprehended Violence Orders (NSW). This is an effective piece of legislation but to be more effective it should look at the offender's pattern of behaviour **before** an offence is committed. If sufficient evidence is presented before a court an order could be made prior to an offence-taking place against a child.
- Any enacted legislation should be simple to apply and carry sufficient sanctions to act as a deterrent.

8. DETECTION

- 8.1. When faced with a 'new' problem often the reaction is to try and introduce legislation. In many cases the 'new' problem is often an old one in disguise. In many cases current legislation exists that can adequately be used to impact upon this type of offending behaviour. For example offences under the Crimes Act of Child Abduction and Sexual Offences against children, adequately deal with issues in the 'real' world.
- 8.2. The use of inchoate offences i.e. incitement, conspiracy, procurement or attempts to commit such crimes, carry the same penalty had the substantive offence been committed. These offences transfer adequately to deal with so called 'cyber crime'. In some cases they are easier to prove as the computer provides 'documentary' evidence of crimes such as procurement or incitement, which in the past have been notoriously difficult to prove.
- 8.3. Again, the use of technology cannot be ignored and legislation should support the use of 'capture' software, to legally obtain evidence against suspects.
- 8.4. Legislation exists to allow investigators access to information held by Internet Service Providers (ISP). However, it is my view that this legislation should be revisited to ensure that with the required authority, information should be swiftly provided.
- 8.5. In the investigative process the use of 'on-line' informants cannot be ignored. Protocols should be in place to adequately tap into this resource and, where appropriate, protection given to those who provide such information.

9. FRUSTRATION

- 9.1. An often-neglected issue is the ability that the government and law enforcement has to 'frustrate' the activity of criminals who use technology to commit their crimes.
- 9.2. Simple techniques can be adopted at no additional cost that can 'frustrate' this criminal activity.
- 9.3. Examples of such techniques that work effectively are:
 - Imposed bail conditions that restrict access to children. This can and should include restricting access to particular mediums and to premises such as Cyber-cafes, or libraries.
 - Adequate management of known or suspected sex offenders. Part of any pre-trial bail should include regular, logged visits to offender's homes.
 - Legislation that allows for periodic access to offender's computers to examine for recidivist behaviour.
 - DNA 'flagging' against unsolved sex crimes or where recidivist behaviour is likely.
 - It is of benefit prior to the commencement of the operation to have a media strategy. This can often apply to very sensitive cases, where it may be necessary to compromise the operation, as a child may be at risk. In some cases no charges may follow and this maybe capitalized upon by some offenders. A good media strategy can offset or even prevent this.
 - A media strategy can be offered to those effected by the activities of the accused. For example, an offender who works for a Child Charity or a school may bring about media interest. This can in many cases be harmful to such organizations that are genuinely there to support and assist children. Offering a media strategy such as a joint police school operation will prevent negative media coverage.

10. LEGAL IMPLICATIONS

- 10.1. There are a number of legal implications in respect of implementing new legislation of any kind, the majority of which revolves around issues of privacy and civil rights. However, there is sufficient legal precedent in place to

introduce legal change.

11. **PERSONNEL / TRAINING IMPLICATIONS**

- 11.1. As outlined in Section 5 education and training is an essential part of the process. Therefore there are a number of personnel and training implications.
- 11.2. Firstly, the right personnel need to be selected for this type of work. Those who work within this environment need to be offered the necessary support. In particular the exposure to child images can be both harrowing and distressing. Therefore there are some financial implications in respect of ensuring there is enhanced support within the relevant HR departments.
- 11.3. Secondly, technology changes so rapidly that it is soon out of date. Therefore it is necessary to ensure that staff receives regular, updated training in the use of such technology and how it is being misused.

12. **COSTS**

- 12.1. Dependent on what issues are implemented dictates the cost involved. However, many of the infrastructures are in place and therefore the costs are, in some cases, purely administrative.

13. **RECOMMENDATION**

- 13.1. Within this paper I have tried to take a holistic approach to this type of investigation and attempted to make suggestions to improving our ability to deal with this type of crime.
- 13.2. The impact of 'cyber crime' remains a global issue. Therefore I recommend that it should be tackled as one, and that a simple and uniformed approach be taken to the below issues:

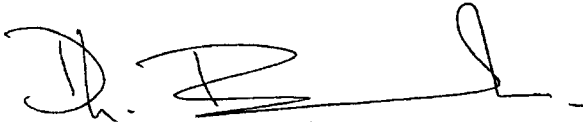
- EDUCATION & TRAINING
- PREVENTION
- DETECTION
- FRUSTRATION

14. **CONCLUSION**

- 14.1. It must be remembered paedophilia is about corruption, therefore once a pattern is established then there is a serious risk of offending. Also, we must keep in mind there are no 'cyber' courts, so any enacted legislation must reflect the

global impact that this type of crime causes.

- 14.2. It is my opinion that the 'virtual' World can be policed in very much the same way as the 'real' World. However, we must not lose focus on the fact that in respect of paedophile activity, somewhere a child is being exploited, and the computer is a secondary issue.

A handwritten signature in black ink, appearing to be 'D. G. Brookes', written in a cursive style.

APPENDIX A:

Newsgroups - (also known as Internet Discussion Groups)¹⁰

This usually starts by someone posting a question or comment and others reply. This in turn causes others to reply and so on. The result is a chain of comments known as a 'message thread'.

These were popular amongst Paedophiles on the Internet prior to the creation of the World Wide Web (www).¹¹ Few newsgroups are moderated and no single server or online service hosts them. Newsgroups tend to be organized into a topical hierarchy, which include *alt* (alternative), *misc* (miscellaneous) *rec* (recreational) and others. For example *alt.sexpics* or *alt.preteen*. These give the receiver an idea of what may be seen but is also a good source of information for law enforcement.

Here the viewer can see how the thoughts of individuals are expressed and how they often justify their offending behaviour. Alfred Grossbrenner¹² called this the 'collective consciousness' this is also referred to by many psychologists as 'cognitive distortion'.¹³ The ability to be able to reinforce their own 'norms' and 'values' in this way is in my view, one of the most significant reasons for Paedophile Internet usage.

Chat rooms

These are the areas that in recent months have courted the most media interest. These are a favourite amongst adolescent children and many have instant Internet messaging. This means that the child knows when 'friends' are 'on-line' and can access this simply at the click of a mouse. Many chat rooms offer 'mobile' Internet messaging so contact can be made via 'cell' telephones.

The popularity of such 'rooms' has been exploited by Paedophiles, here they can often 'lurk' in rooms in 'invisible' mode and target a specific child. This is where the majority of 'grooming' takes place, as the child can be asked to enter a 'private' room, which cannot be monitored.

Many rooms have enhanced features allowing for image transfer of files or via web cam. This is often where Paedophiles will engage in 'chat', grooming the child and sending indecent or pornographic images. In many cases the Paedophile will wish to establish contact and physically meet with the child.

¹⁰ Newsgroup – a message board on the Internet i.e. Usenet.

¹¹ World Wide Web – for further reading on the creation and use of the 'web' see "Weaving the Web" – Tim Berners-Lee (1999) Harper, San Francisco ISBN 0062515861

¹² The Information Brokers Handbook – Ruggie, S and Glossbrenner, A – (1994) McGraw/Hill 2nd Edition.

¹³ See – Services for Juvenile Sex Offender Issues in establishing programs. Connolly, M & Wolf, S- (1995)

This is one of the most feared scenarios for parents, but an area that can be investigated by law enforcement officers. With the right techniques and established working practices officers can assume the role of a child or many children, and in some cases other Paedophiles.¹⁴

Communities

These are often an extension of chat rooms allowing for a wider discussion of a particular subject. Many communities branch off and have sub communities as in normal everyday society. The creation of a Paedophile community is somewhere between the real and the virtual worlds. This is something that still has not been fully explored but by better understanding this community enables us to police it more effectively.

Peer to Peer

This is a User to User¹⁵ facility where users can share files or access resources on each other's computers. This allows for the distribution of indecent images without them being actually 'hosted' on a server. This was initially created for music file sharing i.e. *Napster*¹⁶ but has been exploited by *Kazaa*,¹⁷ where the distribution of both adult and child images is commonplace.

The use of peer to peer can allow for more serious offences of distribution or possession with intent to distribute 'indecent images of children', being levered against the suspect.

Live Abuse

This is by far the most serious aspect of the Internet that has been utilised by Paedophiles. The ability to show web cam images at 'real time' has in effect enhanced the capabilities of those who wish to engage in live sex acts. Those with access to the known sites will engage in 'real time' abuse. Some are simple voyeurs who indicate to the person with the child, what actions should take place. Conversely the person who is taking part in the abuse gets satisfaction by being involved in making of such images.

¹⁴ For further reference on dealing with 'on-line' abduction see R v A (CLR) and R v LEATHER (CrimLR 516, 1993).

¹⁵ User(s) – denotes those persons who have access to the Internet via a computer.

¹⁶ Napster - A digital music delivery service, allowing for the sharing of MPS files.

¹⁷ Kazaa – A file sharing system allowing for fast uploading and downloading of images or files.

APPENDIX B: Definitions

Blocking software:

A computer program that allows parents, teachers, or guardians to "block" access to certain Web sites and other information available over the Internet. All blocking software has filtered the information before blocking access to it. (See also "**filtering software.**")

Chat rooms:

An interactive discussion (by keyboard) about a specific topic that is hosted on the Internet or on a Bulletin Board Service (BBS). On the Internet, chat rooms are available from major services such as America On Line (AOL), individual Web sites and the Internet Relay Chat (IRC) system, the Net's traditional computer conferencing.

C.M.C:

Computer Mediated Communication. All types of communication that is carried out via a computer. This includes e-mail, SMS, Instant Messaging and other types of communication that involve the sending and receiving of messages.

Cyberspace:

A very general term used in a number of ways. "Cyberspace" can refer to the electronic areas and communities on the Internet and other computer networks; the culture developing on (or across) the global network of phone wires that make up the Internet; a new publishing or communications medium separate from conventional media; and a "place" separate from or in addition to physical space.

Discussion group:

An area online focused on a specific topic where users can read and add or "post" comments ("post" in the sense of posting something on a bulletin board). You can find discussion groups, also referred to as "discussion boards," for almost any topic. See also "Newsgroups."

FTP:

(File Transfer Protocol) a protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a Web site on a local machine, they are typically uploaded to the Web server-using FTP.

Unlike e-mail programs in which graphics and program files have to be "attached," FTP is designed to handle binary files directly and does not add the overhead of encoding and decoding the data.

Internet:

Referred to as "Net" for short, a collection of thousands of connected computers and computer networks.

I.R.C:

Computer conferencing on the Internet. There are hundreds of IRC channels on numerous subjects that are hosted on IRC servers around the world. After joining a channel, your messages are broadcast to everyone listening to that channel. IRC client programs, such as mIRC, provide a graphical interface for all functions, including logging onto popular servers and obtaining a list of their active channels.

ISP:

Internet Service Provider - A company that sells access to the Internet, most often through a local phone number. ISPs are usually distinguished from commercial services, which link to the Internet but also offer additional services, such as content and chat, only available to their subscribers.

Newsgroups:

Discussion groups on the Internet (not on the Web, which is only one area of the Internet) that are broken down and categorised by subjects. These discussion groups consist of messages sent by other Internet users and displayed publicly for everyone in the group (or under the topic area) to read. The word "news" in "newsgroups" does not mean news services or journalists run them.

S.M.S:

(Short Message Service) Also known as a text message service that enables short messages of generally no more than 140-160 characters in length to be sent and transmitted from a mobile phone.

Webcam:

(**WEB CAMera**) - A video camera that is used to send periodic images or continuous frames to a Web site for display. WebCam software typically captures the images as JPEG or MPEG files and uploads them to the Web server. There are countless WebCam sites throughout the Internet that have cameras pointed at virtually everything, including people just going about their daily work.

APPENDIX C:

References

Connolly, M and Wolf, S (1995) "*Services for Juvenile Sex Offenders Issues in establishing Programs*" – Australian Social Work, Vol 48, No. 3 September 1995

David, F, Grabosky, P and Grant, A (1999) "*The Commercial Exploitation of Children*" – Paper presented at the Children & Crime: Victims and Offenders Conference convened by the Australian Institute of Criminology, Brisbane, 17 – 18 June 1999.

Hanson, R. K., and Harris, A. J. R. (2000) "Where Should We Intervene? Dynamic Predictors of Sexual Offence Recidivism." *Criminal Justice and Behavior* 27 (1), 6 – 35

Hanson, R.K. and Thornton, D. (2000) "Improving risk assessments for sex offenders: A comparison of three actuarial scales." *Law and Human Behavior* 24(1), 119-136.

Risk Management Standard: Australia / New Zealand 4360: 1999

s87 Crimes Act, 1900 – *Child Abduction*.

SONAR: (Sex Offender Need Assessment Rating). *Developed from the Dynamic Prediction Project* by Hanson and Harris (2000)

Case Law

R v (CLR) R v LEATHER (CrimLR 516, [1993]) see also R v LEATHER [1997]1 FLR 392 – Criminal Law Review - United Kingdom.

Websites

www.smh.com.au/articles/2003/03/13/1047431150279.html - Sydney Morning Herald 2003 Elections.

www.jocsoft.com - Search and Capture Software

www.kazaa.com - Kazaa

www.napster.com - Napster