SITUATIONAL PREVENTION OF CHILD ABUSE IN THE NEW TECHNOLOGIES

Richard Wortley

Jill Dando Institute of Security and Crime Science

University College London

Wortley, R. (2012). Situational prevention of child abuse in the new technologies. In K. Ribisl & E. Quayle, *Preventing Online Exploitation of Children*. London: Routledge.

r.wortley@ucl.ac.uk

Overview

Situational prevention shifts attention from the psychological characteristics of the individual performing behaviour to the facilitating role played by the immediate environment in which the behaviour occurs. Applied to the problem of Internet child pornography, the situational approach emphasises the role of opportunity in driving consumption. It is argued that under the right environmental conditions the potential to view children as sexual objects is more widespread than sexual deviance models suggest. The Internet allows individuals to satisfy their secret desires conveniently, cheaply and relatively risk-free. Situational prevention of Internet child pornography requires strategies that reduce the opportunities for accessing child abuse images by making the activity less rewarding, more difficult, and riskier.

In April 1982, the US General Accounting Office reported to the Sub Committee on Juvenile Justice of the House Committee on Education and Labor that:

> ... discussions with Federal, State and local officials indicated that commercially produced (child) pornography has declined. The factors responsible for this decline were (1) the Protection of Children Against Sexual Exploitation Act of 1977, (2) tougher State laws covering child pornography, (3) stricter enforcement of obscenity laws involving child pornography, (4) media attention, (5) the tendency of juries to convict child pornographers more readily than adult pornographers, and (6) the banning in 1979 of child pornography in Sweden and Denmark, which had been the major overseas supplier of child pornography. As a result of the decline in commercial child pornography, the principal Federal agencies responsible for enforcing laws covering the distribution of child pornography – the U.S. Customs Service and the U.S. Postal Service – do not consider child pornography a high priority. (Ahart, 1982, p. 7)

On January 1, 1983 the first standardised protocols for the Internet were implemented and everything changed. While it is impossible to accurately estimate the amount of child pornography currently available via the Internet, or the number of individuals who now access child exploitation images, all commentators agree that the problem has increased exponentially since the 1980s (Carr, 2004; Ferraro & Casey, 2003; Jenkins, 2001). Prior to the Internet, images were scarce, locally produced, of poor quality, expensive and difficult to obtain, traded furtively in hard-copy form among small, closely-knit networks of dedicated consumers. The Internet has dramatically escalated the child pornography problem by increasing the amount of material that is available, the efficiency of its distribution, and the ease by which it

can be accessed. It has made vast quantities of technically high-quality images instantly available, at any time, and with (apparent) anonymity. Alone and in the comfort of their own home, individuals are able to satisfy their secret curiosities and desires conveniently, cheaply and relatively risk-free (Calder, 2004; Wortley & Smallbone, 2006a).

The argument to be made in this chapter is that the growth of the child pornography problem in the Internet age is a classic example of supply-led demand. The treatment of children as sexual objects is as old as humanity, and there is a long history of erotic literature, drawings, and (since the mid-nineteenth century) photographs involving children (Bullough, 2004; Linz & Imrich, 2001; O'Donnell & Milner, 2007). However, the extent to which child pornography has been a social problem has been limited by the supply of pornographic material. What has changed since 1982 is the easy availability of images with which latent sexual interest in children can be satisfied. The prevention of Internet child pornography cannot be approached simply as a problem of individual sexual deviancy. The recent surge in child pornography usage is a product of the Internet, and any attempts to reduce levels of child pornography use that do not include reducing the opportunities provided by the Internet to access images are bound to be inadequate.

Theoretical orientation – the person-situational interaction

The role that opportunity has played in increasing the problem of child sexual exploitation derives from the principle that all behaviour is the product of a person-situation interaction (e.g., Mischel, 1968). The immediate environment is more than an incidental backdrop to behaviour; it plays a fundamental role in initiating behaviour and shaping its course. While this principle is fundamental in psychology, its full significance is widely overlooked by psychologists in their theorising and

practice. The causes of behaviour – particularly in the clinical field – are typically construed in person-centred terms. Explanatory models of aberrant behaviour focus on the historical processes by which an individual is assumed to have become deviant or disordered. Once a particular behavioural propensity has been acquired, then the behaviour is assumed inevitably to follow and the job of explaining it is complete. A person behaves in deviant ways because he/she has a deviant disposition. Accordingly, the way of preventing unwanted behaviour is seen to be through treatments that are designed to alter these underlying aberrant propensities.

Psychologists have recognised the tendency for human beings to construe causation in person-centred terms and to ignore or downplay the role of situational factors. This cognitive bias is referred to as fundamental attribution error (Jones, 1979; Ross, 1977). Even when someone's actions are unambiguously forced upon them by circumstances beyond their control, observers typically underestimate the role of these outside pressures and construct causal explanations that assume personal agency on the part of the actor. Fundamental attribution error is accompanied by an exaggerated belief in the stability of the personal characteristics of others and overconfidence that their behaviour is therefore constant from one situation to the next. It is thought that the tendency to categorise others in terms of predictable dispositions has evolved as an efficient information processing strategy that helps people deal with the complexity of the world around them. However, this ingrained faith in personal control makes it difficult for people to accept that situational factors play anything other than a trivial role in behaviour. There is perhaps some irony in the fact that, by focussing on the intrapsychic causes of deviant behaviour, many psychologists seem as prone to fundamental attribution error as is the general population.

The role played by situational factors in behaviour is consistent with the so-called control perspective on criminal behaviour (Gottfredson & Hirshi, 1990). The usual question in criminology and forensic psychology is to ask: how do individuals come to behave in antisocial ways? Most theories of crime are theories of the acquisition of behaviour. They begin with the assumption that individuals are born in a criminally neutral state, and that antisocial behaviours are learned via cultural and developmental experiences. Control theories turn this question around and ask: how do individuals come to behave in pro-social ways? Control theories begin with the assumption that the tendency to act impulsively and selfishly is the natural human condition and does not need to be explained. What needs to be explained is the process by which these natural impulses are brought under control. Control theorists ask you to imagine the case of a child raised without any constraints being placed on his/her behaviour. The result would be an individual who satisfies his/her urges indiscriminately. Socialisation involves learning to curb these self-satisfying urges. 'Deviant' and 'non-deviant' individuals differ not so much in the nature of their self-serving motivations but in their capacity to control those motivations. However, even individuals with high levels of self-control are not always successful in controlling self-gratifying impulses and may from time to time succumb to temptation.

The desire for sexual gratification is a powerful and universal motivator. Consider the inventive study carried out by Demetriou and Silke (2003). They established a website that contained links to legal sites, offering shareware and soft-pornography, as well purported links (that did not work) to illegal or obscene sites, offering commercial games, commercial software, hardcore pornography, and stolen passwords. People were directed to the website if they searched for 'shareware', 'freeware', 'free', 'free games' and 'free software', although some search engines

accessed other terms contained on the site itself. Tracking the key words used to arrive at the site, Demetriou and Silke found that of 803 visitors, only 26 were specifically looking for pornography. Nevertheless, the hard-core pornography link was by far the most popular of all the links, clicked by 483 visitors, while the soft-core pornography link, with 358 clicks, was the second most popular. Legal shareware, the reason most people visited the site in the first place, was the least popular link with only 268 clicks. Demetriou and Silke interpreted their findings in terms of the psychological construct of deindividuation. Deindividuation is the reduced capacity of individuals to self-regulate their behaviour under conditions of anonymity. Disinhibition is produced not just by a perceived freedom from the censure of others, but more fundamentally by freedom from self-censure. Freed from the personal and social controls that might otherwise have inhibited them from viewing hard-core pornography, the majority of visitors to the site chose to satisfy their sexual curiosities.

Viewing hard-core pornography is one thing, but what about clearly deviant inclinations such as sexual attraction to children? The problem with the sexual deviancy model is that no-one has adequately defined sexual normalcy against which deviancy can be measured. The human sexual response is extraordinarily versatile. The control approach suggests that the potential to view children as sexual objects is common (perhaps universal) in humans. Human males in particular – and the overwhelming majority of child sexual offenders are male – are evolutionarily designed for a sexual preference for youthful partners (Thornhill & Thornhill, 1987; 1992). In Victorian Britain it was legal to have sex with a girl as young ten years of age (raised to twelve by the Offences Against the Person Act, 1861), while there are still countries in the world in which the age of consent for girls is as low as twelve

years (Avert, nd). In fact, all of us have probably experienced being sexually attracted to a child when we ourselves were children. Thankfully, for most of us our sexual preferences have remained age-appropriate as we have aged. Any latent sexual attraction to children is controlled by our personal values and inhibitions, social pressures and expectations, cultural taboos and legal sanctions, and physical deterrents and barriers. However, where these controls break down, many men may take advantage of available opportunities for sexual gratification involving children. While clearly ethically problematic, it is intriguing to ponder what Demetriou and Silke (2003) might have found if they had included a purported link to a child pornography site in their Internet study.

There is an understandable reluctance about openly discussing the widespread potential for sexual attraction to children. Few people are comfortable admitting that they may have dark thoughts buried deep in the private recesses of their minds. Moreover, it may be feared that talking about sexual attraction to youthful partners as an evolutionary-endowed component of human nature is tantamount to excusing the sexual exploitation of children. Let me make it clear that whether or not men are designed to prefer youthful partners has no bearing on the moral or legal status of the sexual exploitation of children. If one accepted the logic of a link, then it could be equally argued that assault and murder ought to be legalised because human beings are naturally aggressive. There are very good reasons for making the sexual exploitation of children illegal. Indeed, it can be argued that treating the sexual exploitation of children as a legal rather than psychological issue makes the moral culpability of the offender clearer, not less clear. Sexual exploitation of children is illegal because we have chosen to make it illegal; as a society we have declared that we find such behaviour unacceptable and we want to stamp it out. Pretending that the

world is neatly dived into paedophiles and non-paedophiles may be comforting but it is unhelpful when formulating strategies to control the sexual exploitation of children.

I should also emphasise that I am not arguing that all men are equally vulnerable to performing sexually exploitive behaviour towards children and that dispositions do not matter. Most men reading this chapter will (quite rightly) deny any adult experiences of sexual attraction children. The concept of a person-situation interaction, in fact, depends upon this being the case. By definition, a person-situation interaction occurs when different individuals react differently to the same situation, with some people more dispositionally susceptible to respond to particular situational cues than others (see Wortley, in press). Thus, the effect of the situation on behaviour depends upon (interacts with) the characteristics of the person; the stronger the individual's propensity to perform a given behaviour the weaker the situational pressures required for that behaviour to occur, and vice versa. Undoubtedly, there is a relatively small core of men who are strongly predisposed to sexually exploit children. They need little in the way of situational encouragement and will actively and determinedly seek out opportunities to satisfy their sexual urges. Most men are not preferentially attracted to children. However, to varying degrees according to their dispositional characteristics, they may be tempted or induced to engage in sexually exploitative behaviour given the 'right' situational conditions (Smallbone, Marshall & Wortley, 2008; Wortley & Smallbone, 2006b). Of course, for most these 'right' circumstances will never eventuate.

The person-situation interaction provides an explanation for why the introduction of the Internet has resulted in such a dramatic escalation of the child pornography problem. The Internet has exacerbated the child pornography problem in two ways, by increasing both the amount of available pornography and the number of

individuals accessing that pornography. First, for those individuals with an active interest in child pornography the Internet has greatly facilitated their access to the images that they crave. Had these individuals lived in the pre-Internet era, many may have sought out hard-copy child pornography images. However, the task would have been much more difficult, the choice much more restricted, and the collection of images that they would have managed to accumulate much smaller. It is not uncommon for offenders to be arrested with child pornography collections exceeding half-a-million images (Carr, 2004).

Second, while no-one has accurate figures comparing the number of people using child pornography pre- and post-Internet, there seems little doubt that the Internet has allowed many individuals who otherwise would not have used child pornography to now do so. Jenkins (2001) reported that a single child pornography site received over one million hits in a one-month period. In the pre-Internet era, many of these new users would have lacked the know-how and/or dedicated sexual interest in children that was required to hunt down hard-copy images. By making it easier for people to view child pornography, the Internet has provided individuals with the opportunity to explore their perhaps casual and vaguely formed sexual attraction to children. Conventionally, we tend to think of deviant sexual behaviour as resulting from deviant sexual motivations. However, it is possible that for many users of child pornography the order of causation is reversed; the act of viewing child pornography ignites and strengthens their sexual interest in children. Initially curious, over time the individual may become increasingly interested in child pornography, become attracted to images of increasing severity, and become desensitised to the harms that victims experience. It is noteworthy that attempts to profile Internet child pornography offenders have identified few distinguishing psychological and socio-

demographic characteristics, and share few features with contact child sex offenders (Elliott, Beech, Manderville-Norden & Hayes, 2009; Sheldon & Howitt, 2007; Webb, Craissati & Keen, 2007). Most Internet pornography offenders are likely to be male, to be between the ages 26 and 39 years, to be white, to be in a relationship, to be employed, to have above average IQ, to be college educated, and not to have a criminal record (Blundell, Sherry, Burke & Sowerbutts, 2002; Schwartz & Southern, 2000; Wolak, Finkelhor & Mitchell, 2005; Wolak, Mitchell & Finkelhor, 2003). Those arrested for online pornography crimes have come from all walks of life, and include judges, soldiers, dentists, teachers, academics, and police officers (Calder, 2004). It is the ordinariness, not the deviance, of many online child pornography users that is striking.

Situational Prevention

Just as psychologists typically think about the causes of behaviour in person-centred terms, so too they tend to think about prevention of behaviour in person-centred terms. Prevention of criminal behaviour is seen to require fundamental changes to the individual's disposition. This might be achieved via developmental interventions aimed at altering the early risk factors for criminality, or more commonly through the treatment of individuals once they have exhibited unwanted behaviours. However, if behaviour is the product of a person-situation interaction, then attempting to change behaviour by addressing the situational side of the equation is at least as valid as is the traditional focus on attempting to change the individual's dispositions.

Clinicians will be familiar with environmental interventions in the form of behaviour therapies such as relapse prevention and stimulus control. In these treatments, clients are instructed to identify and avoid situations that might trigger unwanted behavioural patterns. For example, a person on a diet might ensure that

food is put away in cupboards, and a convicted child sex offender might avoid walking past schools. However, developed originally in criminology (Clarke, 1997; 2008; Cornish & Clarke, 2003), situational prevention has more in common with the public health primary and secondary prevention models than with the clinical treatment model. Situational interventions are designed to prevent behaviour before it occurs. Moreover, they are not formulated for a single client in the manner of behaviour therapy, but are directed at specific environments that might facilitate the unwanted behaviour of many individuals. It is the crime event rather than the individual that is the object of analysis. By carefully analysing the situational characteristics of crime events, the prevention practitioner is in a position to develop environmental counter-strategies. The object of situation interventions is to inhibit unwanted behaviour in specific contexts, not to cure individuals.

The most common model of situational prevention is opportunity reduction (Clarke, 2008; Cornish & Clarke, 2003; 2008). In line with the control perspective on behaviour, individuals are assumed to act in ways that will deliver them benefits. Opportunity reduction involves manipulating the immediate environmental contingencies so as to increase the perceived costs of offending. Reducing the opportunities for crime can significantly slow down prolific offenders, and may deter completely those less determined offenders. In this section, three opportunity-reduction strategies are examined and applied to the problem of Internet child pornography – reducing perceived rewards, increasing the perceived effort, and increasing the perceived risks.[1]

Reducing perceived rewards

[1] Clarke's (2008; Cornish & Clarke, 2003) latest model of situational prevention involves five general strategies. Two are not discussed here – reducing provocations and removing excuses – since they are not strictly methods of opportunity reduction. They target the offender's motivation to offend.

According to the opportunity thesis, offenders commit crimes because they are seeking to benefit in some way from the outcome of the crime. In the case of Internet child pornography, the primary benefit is the acquisition of images from which the offender derives sexual gratification. Reducing the rewards of Internet child pornography essentially involves removing or denying access to the child pornography images that are targeted by offenders.

ISPs have a central role to play in reducing the number of child pornography images available on the Internet. The legal obligations of ISPs vary among jurisdictions. By-and-large they are not required to actively seek out and remove illegal sites (Klain, Davies & Hicks, 2001; Stanley, 2001) although they may be required to report sites of which they become aware (McCabe, 2008). The policing of child pornography on servers therefore usually depends upon industry self-regulation. A number of ISP associations have drafted formal codes of practice that explicitly bind members to not knowingly accept illegal content on their sites and to removing such sites when they become aware of their existence. Service agreement contracts with clients will often set out expected standards that apply to site content, including explicit proscription of the uploading of child-pornography. Large ISPs may have active cyber patrols that search for illegal sites. In addition, some ISP associations have set up Internet sites or hotlines that allow users to report illegal practices (Stewart, 1997). ISPs may also be notified by police Internet child exploitations (ICE) investigators about illegal child pornography hosted on their servers.

ISPs can also apply filters to the browsers and search engines their customers use to locate websites (Carr, 2004; Jenkins, 2001; Linz & Imrich, 2001). There are numerous filtering methods. For example, filters can effectively treat certain key words as if they do not exist, so that using these words in a search will be fruitless

(Thornburgh & Lin, 2002; Lee, Hui & Fong, 2003). Additionally, some search engines display a warning message advising the searcher when he/she may be about to enter and illegal site. Software that can identify pornographic images is also being developed (Thompson, 2009).

There are two competing commercial forces acting on ISPs with respect to self-regulation. On the one hand, if an ISP restricts access to child pornography on its server, it may lose out financially to other ISPs who do not. Therefore, it will always be possible for offenders to find ISPs who will store or provide access to child pornography sites. On the other hand, ISPs also have their commercial reputation to protect, and it is often in their best interests to cooperate with law enforcement agencies. Most major ISPs have shown a commitment to tackling the problem of child pornography, partly motivated by the desire to protect the reputation of their brand name. In some cases direct economic pressure may be applied to service providers to encourage them to monitor illegal content. In one example of this, major brands have withdrawn advertising from networks that carry child pornography (Adegoke, 2003).

The success of reducing rewards as a prevention strategy has had mixed results. Calder (2004) estimated that ISPs have removed over 20,000 pornographic images of children from the Internet over the previous eight years. However, removing all child pornography from the Internet is an enormous, and frankly impossible, task. Arguably there has been considerable success in reducing the volume of child pornography in open areas of the Internet such as the World Wide Web (www)[2]. Many researchers believe that because of the vigilance of ISPs and the

[2] While the terms Internet and the World Wide Web (www) are often used interchangeably, the web specifically refers to the world-wide collection of electronic documents and other files stored as web-pages and web sites throughout the Internet. In addition to the www, the Internet enables a number of other forms of communication. These services include e-mail, newsgroups, bulletin boards, chat

police in tracking down and closing child pornography websites, it is unlikely that a normal web search using key words such as 'childporn' would reveal much on the way of genuine child pornography (Forde & Patterson, 1998; Jenkins, 2001; Lesce, 1999). Instead, at most, searchers are likely to find legal pornography websites with adults purporting to be minors, and they may encounter police sting operations or vigilante sites[3]. One consequence has been to drive dedicated offenders to deeper levels of the Internet where they trade images in specific child pornography chat rooms and newsgroups. While most commercial servers block access to such sites they are much more difficult to regulate. Equally, they are also more difficult for offenders to access. Offenders require the knowledge of where to locate child pornography sites and the technical skill to access them. Many child pornography chat rooms and newsgroups are secured sites, that is, a password is required in order to gain access to them. Passwords, in turn, can be difficult to obtain. Because of the risk that these sites will be infiltrated by undercover police, potential users are carefully vetted before being allowed to join. Thus, the movement of child pornography activity to these hidden areas of the Internet has at least increased the effort that offenders must expend in order to locate child pornography images, and as described in the following section, effort is a deterrent.

Increasing the perceived effort

All things being equal, offenders will select crimes that are easy to commit, and they may impulsively commit crimes just because they require so little effort. Even where increased effort does not prevent crime it may reduce the number of offences that can

---

rooms and instant messaging. They permit a user to have direct contact with other individuals, as well as to share electronic files.

[3] As a researcher in this field, I regularly conduct online searches using search terms such as 'child pornography' and have only ever been directed to websites and scholarly articles concerned with the control of child pornography.

be committed by a given offender. At a trivial level, we can observe the effect of effort on our own behaviour when we decide that we cannot be bothered to get up from the couch to make ourselves a cup of coffee. However, effort plays a significant role in even deeply motivated behaviour. Consider the classic study by Clarke and Mayhew (1988) on suicide patterns in the UK. Traditionally, up to 40% of suicide cases involved the use of domestic coal gas, which is toxic. However, from 1958 to 1977 the UK progressively switched from coal gas to non-toxic natural gas. As the changeover occurred, suicide rates fell from 5,298 to 3,944, a reduction that was almost entirely accounted for by the drop in suicide by gassing, which fell from 2,637 to 2. Gassing is a relatively convenient and easy method of suicide, requiring little in the way of little skill or planning. Many potential suicide victims who might have selected gassing as their method of choice, abandoned their suicide attempt when that option was denied rather than seek out other less convenient methods.

In the context of Internet child pornography, increasing the perceived effort involves making it more difficult for offenders to access child pornography images. As noted in the previous section, removing easily accessed child pornography from the Internet has the effect of forcing offenders to expend greater effort in order to obtain images, an effort that many cannot or will not make. Other suggestions to increase effort include making it more difficult to get Internet access, to send and receive child pornography, and to pay for child pornography.

One way to increase the effort required to gain Internet access is for ISPs to verify the identities of people who open Internet accounts. Currently in most jurisdictions accounts may be opened using false names and addresses, and this makes it difficult to trace individuals who engage in illegal Internet activity. In addition, without verifying users' ages, there is no way of knowing if children are operating

Internet accounts without adult supervision. This problem of Internet anonymity has increased as accessing the Internet via mobile phones has become commonplace, and both ISPs and mobile phone networks need to strengthen procedures for user verification (Carr, 2004).

Internet child pornography images must be traded electronically. At present there are a number of relatively simple strategies that offenders can employ to send and receive images safely. One technique is to trade via peer-to-peer (P2P) networks, in which computers connect directly to one-another's hard drive without the need for a central server. There have been repeated calls for tighter regulation of P2P networks, and police agencies are increasingly targeting P2P networks in crackdowns on child pornography (GAO, 2004; Lemos, 2008; Lyman, 2004). Another strategy is to send files via anonymous remailers. Remailers are servers that forward emails after stripping them of sender identification. It has been argued that much tighter regulation of remailers is necessary. Some have advocated making remailer administrators legally responsible for knowingly forwarding illegal material, while others have called for a complete ban on remailers (Mostyn, 2000). In the language of situational crime prevention, targeting the use by offenders of P2P networks and remailers is an example of controlling the tools that aid the commission of crime (Cornish & Clarke, 2003).

Finally, in many cases child pornography often has to be paid for, and this is most easily done via credit card transactions. It has been argued that credit card companies have a duty to not knowingly contribute to illegal acts (Taylor & Quayle, 2006). A number of credit card companies now block payments for child pornography (Sutton & Jones, 2004). A similar strategy has been applied to block the illegal sale of cigarettes over the Internet. Ribisl et al (2011) showed that banning credit card

payments for illegal cigarette sales resulted in a 3.5 fold decline in traffic to the most popular Internet Cigarette Vendor sites.

Increasing the perceived risks

Most major police jurisdictions have dedicated units devoted to scanning the Internet for ICE images and infiltrating ICE newsgroups. However, law enforcement personnel are under no illusions that they will be able to make a serious dent in the number of illegal sites or to arrest significant numbers of offenders. This is not because it is too difficult to find offenders but because it is too easy. The sheer volume of traffic in child pornography makes the task of prosecuting all offenders impossible and in truth the chances of an Internet child pornography offender being arrested are very small (Jewkes & Andrews, 2005). In the US, for example, around 1,000 people per year are arrested for possessing Internet child pornography (Wolak et al, 2003), while a major sting operation can result in fewer than 100 arrests world-wide (Federal Bureau of Investigation, 2002). While no-one knows exactly how many offenders there are accessing child pornography, these figures most certainly represents a drop in the ocean.

However, risk and perceived risk are two different things. As the previously cited study by Demetriou and Silke (2003) suggests, a crucial factor that governs Internet behaviour is the perception of anonymity. People can behave very differently on the Internet than they do in other areas of their life and interacting anonymously with a computer in the safety of one's own home is a disinhibiting experience and encourages people to express hidden thoughts and desires (Quayle & Taylor, 2001). One of the chief purposes of policing the Internet is not so much to catch offenders as it is to create the impression that the Internet is an unsafe environment in which to access child pornography images.

Police can create uncertainty about the safety of the Internet in a number of ways. Law enforcement agents may enter pedophile newsgroups, chat rooms, or P2P networks posing as pedophiles and request emailed child pornography images from others in the group (US Department of Justice, 2004). Alternatively, they may enter child or teen groups posing as children and engage predatory pedophiles lurking in the group who may send pornography or suggest a meeting. Wolak, Finkelhor and Mitchell (2009) report increasing use of this strategy by law enforcement personnel, with 3,100 US arrests in 2006 for solicitation of undercover investigators posing as minors, a 381% increase over the previous six years. A variation of the sting operation is to place ads on the Internet offering child pornography for sale and wait for replies (Lesce, 1999). Police may also set up 'honey trap' sites. These sites purport to contain child pornography but in fact are designed to capture the IP or credit card details of visitors trying to download images. Rather than keep these operations secret in order to maximize the number of arrests, police may do just the opposite and widely publicise crackdowns on Internet child pornography. This is a case where general deterrence takes precedence over specific deterrence. Coverage of crackdowns in the mass media increases the perception among potential offenders that the Internet is an unsafe environment; they can never be entirely sure that site they have accessed is real or bogus.

A classic example of the use of a honey pot trap to increase the perception of risk is Operation Pin (BBC News, 2003). The operation was started in 2003 by West Midlands (U.K.) police and was expanded to include the FBI, the Australian Federal Police, the Royal Canadian Mounties, and Interpol. Far from being a covert operation, it was officially launched with media releases by the relevant police forces. A website purporting to contain child pornography was set up. Visitors to the site were required

to go through a series of web pages, which appeared to be identical to real web porn sites, searching for the image they wanted. At each point it was reinforced that they were in a child pornography site, and they were given the option to exit. When they did try to access an image they were told they had committed a crime. They were tracked down via their credit card details, which they were required to provide to login. The operation resulted in numerous arrests, although the precise numbers are not available. However, its main purpose of the operation was to make searchers of child pornography on the Internet uncertain that they can do so anonymously.

Increasing the perceived risk of searching for child pornography online can be achieved without the setting up of elaborate stings. Police and other law enforcement personnel routinely scan the Internet monitoring the traffic to servers known to contain child pornography. Theoretically, many of the individuals attempting to access these sites could be traced and, if they are operating in a region that falls within the jurisdiction of the ICE unit, they could be arrested. However, the cost and effort that would be required to trace each individual and to mount a conviction is far too great to make that course of action feasible. However, in addition to blocking access to the offending site, ICE personnel could send a message to the potential users warning them that their attempt to access the site has been intercepted by law enforcement officials and that their online activity is now being monitored (see Williams, 2005).

Conclusion

The scale of the child pornography problem has increased dramatically with the introduction and rapid growth of the Internet. While statistics about Internet use are notoriously unreliable and often little more than guesses, there are undoubtedly many more child pornography images available now, and many more individuals accessing

those images, than would have been the case had the Internet not existed. The Internet is not just an alternative platform that dedicated paedophiles happen to use to view child pornography; the Internet is a *cause* of child pornography. Relying solely on traditional models of individually-focussed tertiary prevention – arrest and rehabilitation – is not a viable solution to the problem of Internet child pornography. Certainly, offenders – especially those at the more serious end of the spectrum involved in producing and distributing child pornography – ought to be targeted by law enforcement personnel and arrested where possible. But there are many more people accessing child pornography via the Internet than can ever be arrested, and the impact of treating those few who are arrested – even with very good rehabilitation programmes – is negligible in the overall scheme of things. If, as I have argued, the proliferation of child pornography is a function of increased opportunity, then tackling the child pornography problem must by centred on reducing that opportunity.

Admittedly, the task is not a simple one. The structure of the Internet makes the control of child pornography very difficult (Wortley & Smallbone, 2006a). The Internet is an international communication tool that crosses jurisdictional boundaries. Offenders may access child pornography images that were produced and/or are stored on another continent. This raises jurisdictional problems for law enforcement officers and makes necessary international cooperation. Moreover, the Internet is a decentralized system with no single controlling agency or storage facility, making it difficult to enforce legislation or to electronically screen content even when there is agreement between jurisdictions. Because it is a network of networks, even if one pathway is blocked there are many alternative pathways that can be taken to reach the same destination. Technological developments such as P2P networks, remailers and file encryption only exacerbate the control problem (Burke, Sowerbutts, Blundell &

Sherry, 2002; Ferraro & Casey, 2003; Jewkes & Andrews, 2005).

Because of the difficulties policing the Internet, it is easy to be pessimistic about the prospects of controlling Internet child pornography. There is especially the danger of interpreting partial success as complete failure. Undoubtedly none of the situational strategies that have been discussed in this chapter work perfectly. Offenders vary considerably in the strength of their attraction to child pornography and the technological sophistication they are able to employ to access images and to avoid detection. Whatever we do, there will a core of dedicated offenders who possess both the determination and technical skills to thwart prevention attempts (Jewkes & Andrews, 2005). But to get the issue into perspective, let us turn the question around. Imagine that we did nothing to inhibit access to child pornography on the Internet; that there were no efforts to take down child pornography sites, no search filters, no police stings, and so on. Would there be more child pornography on the Internet, and more offenders accessing that pornography? Of course it is impossible to know the answer for certain but common sense suggests that if child pornography was freely available on the Internet then the problem would be significantly greater than is currently the case. The battle to prevent Internet child pornography is not one that can ever be won once and for all. Rather it is an ongoing arms race characterised by a cycle involving the deployment of prevention strategies, the adaptation of offenders to those strategies, and the deployment of new prevention strategies to counter offender adaptation.

References

Adegoke, Y. (2003). Top brands start to pull ads from P2P networks. *New Media Age*, April 24, p. 1.

Ahart, G.J. (1982). Sexual exploitation of children – a problem of unknown magnitude. *Report to the Chairman, Subcommittee on Select Education, House Committee on Education and Labor*. Gaithersburg, MD: U.S. General Accounting Office.

Avert. (nd). World wide ages of consent. http://www.avert.org/age-of-consent.htm

BBC News (December 18, 2003). Police trap online paedophiles." news.bbc.co.uk/1/hi/uk/3329567.stm.

Blundell, B., M. Sherry, A. Burke, and S. Sowerbutts (2002). Child pornography and the Internet: Accessibility and policing. *Australian Police Journal 56(1)*: 59–65.

Bullough, V.L. (2004). Children and adolescents as sexual beings: A historical overview. *Child and Adolescent Psychiatric Clinics of North America, 13*, 447-459.

Burke, A., S. Sowerbutts, B. Blundell, and M. Sherry (2002). Child pornography and the Internet: Policing and treatment issues. *Psychiatry, Psychology and Law* 9(1): 79–4.

Calder, M.C. (2004). The Internet: Potential, problems and pathways to hands-on sexual offending. In M.C. Calder (Ed). *Child sexual abuse and the Internet: Tackling the new frontier.* Lyme Regis UK: Russell House Publishing

Carr, J. (2004). *Child abuse, child pornography and the Internet*. London: NCH.

Clarke, R.V. 1997, Introduction, in R.V. Clarke (ed.), *Situational crime prevention: Successful case studies* (2nd ed.), Albany NY, Harrow and Heston, pp.2-43.

Clarke, R.V. (2008). Situational crime prevention. In R.Wortley & L. Mazerolle (eds.) *Environmental criminology and crime analysis*, Cullumpton, Devon: Willan.

Clarke, R.V. Mayhew, P. (1988) The British gas suicide story and its criminological implications, in M. Tonry and N. Morris (eds) *Crime and Justice, vol 10.* Chicago, Il: University of Chicago Press.

Cornish, D.B., & Clarke, R.V. (2003). Opportunities, precipitators and criminal dispositions: A reply to Wortley's critique of situational crime prevention', in M.J. Smith & D.B. Cornish (Eds.), *Theory for practice in situational crime prevention. Crime prevention studies*, Volume 16. Monsey, NJ: Criminal Justice Press.

Cornish, D.B. & Clarke, R.V. (2008). Rational choice perspective. In R. Wortley & L. Mazerolle (eds.) *Environmental criminology and crime analysis*, Cullumpton, Devon: Willan.

Demetriou, C., & Silke, A. (2003). A criminological Internet 'sting': Experimental evidence of illegal and deviant visits to a website trap. *British Journal of Criminology, 43*, 213-22.

Elliott, I.A., Beech, A.R., Manderville-Norden, R., & Hayes, E. (2009). Psychological profiles of Internet sexual offenders: Comparison with contact sexual offenders. *Sexual Abuse: A Journal of Research and Treatment, 21*, 76-92.

Federal Bureau of Investigation (2002). "Operation Candyman." www.fbi.gov/pressrel/pressrel02/cm031802.htm.

Ferraro, M.M., & Casey, E. (2005). *Investigating child exploitation and pornography: The Internet, the law and forensic science*. San Diego: Elsevier.

Forde, P., and A. Patterson (1998). Paedophile Internet activity. *Trends & Issues in Crime and Criminal Justice, No. 97*. Canberra: Australian Institute of

Criminology. www.aic.gov. au/publications/tandi/ti97.pdf.

GAO (2004). File sharing programs: Users of peer-to-peer networks can readily access child pornography. *Testimony Before the Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce, House of Representatives.* Washington, DC: United States General Accounting Office.

Gottfredson, M.R., & Hirschi, T. (1990). *A general theory of crime*, Stanford, CA: Stanford University Press.

Jenkins, P. (2001). *Beyond tolerance: Child pornography on the Internet*. NY: New York University Press.

Jewkes, Y., and C. Andrews (2005). Policing the filth: The problems of investigating online child pornography in England and Wales. *Policing and Society, 15*: 42–62.

Jones, E.E. (1979). The rocky road from acts to dispositions, *American Psychologist, 34*: 107-117

Klain, E., H. Davies and M. Hicks (2001). *Child pornography: The criminal justice system response*. Washington, D.C.: National Center for Missing & Exploited Children. www.missingkids.com/en_US/publications/NC81.pdf.

Lee, P., S. Hui, and A. Fong (2003). A structural and content-based analysis for web filtering. *Internet Research: Electronic Networking Applications and Policy* 13(1): 27–37.

Lemos, R (2008). P2P investigation leads to child-porn busts. *Security Focus*. http://www.securityfocus.com/brief/801

Lesce, T. (1999). Pedophiles on the Internet: Law enforcement investigates abuse. *Law and Order* 47(5): 74–78.

Linz, D., & Imrich, D. (2001). Child pornography, in S. White (Ed.), *Handbook of youth justice.* NY: Kluwer Academic Press.

Lynam, J. (2004). Feds crack down on P2P child porn. *TechNewsWorld*. http://www.technewsworld.com/story/technology/33836.html

McCabe, K.A. (2008). The role of Internet service providers in cases of child pornography and child prostitution. *Social Science Computer Review, 26*: 247-251.

Mischel, W. (1968). *Personality and Assessment*. New York, NY: Wiley.

Mostyn, M. (2000). The need for regulating anonymous remailers. *International Review of Law, Computers & Technology* 14(1): 79–88.

O'Donnell, I., & Milner, C. (2007). *Child Pornography: Crime, Computers and Society*. Cullompton, UK: Willan.

Offences Against the Person Act (1861). http://www.legislation.gov.uk/ukpga/1861/100/pdfs/ukpga_18610100_en.pdf

Quayle, E., & Taylor, M. (2001). Child seduction and self-representation on the Internet: A case study. *Cyber Psychology and Behavior, 4*, 597-609.

Ross, L. (1977). The intuitive psychologist and his shortcomings: Distortions in the attribution process', in L. Berkowitz (ed.), *Advances in Experimental Psychology* (Vol.10), New York, Academic Press.

Schwartz, M.F., & S. Southern (2000). Compulsive cybersex, in A. Cooper, ed., Cybersex: The Dark Side of the Force. New York: Brunner/Mazel.

Sheldon, K., & Howitt, D. (2007). *Sex offenders and the Internet*. Chichester: John Wiley.

Smallbone, S., Marshall, W.L., & Wortley, R. (2008). *Preventing child sexual abuse: Evidence, policy and practice*. Cullompton, UK: Willan.

Stanley, J. (2001). *Child abuse and the Internet*. National Child Protection Clearinghouse, No. 15 Summer. Melbourne: Australian Institute of Family Studies. www.aifs.org.au/nch.

Stewart, J. (1997). If this is the global community, we must be on the bad side of town: International policing of child pornography on the Internet." *Houston Journal of International Law,* 20: 205–246.

Sutton, D., and V. Jones (2004). *Position paper on child pornography and Internet-related sexual exploitation of Children*. Save the Children.

Taylor, M., & Quayle, E. (2006). The Internet and abuse images of children: Search, precriminal situations and opportunity, in R. Wortley and S. Smallbone (eds.) *Situational Prevention of Child Sexual Abuse. Crime Prevention Studies, Vol. 19*. Monsey, NY: Criminal Justice Press.

Thompson, G. (2009) Automatic detection of child pornography. Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia, 3 December 2009.

Thornburgh, D., and H. Lin (2002). *Youth, pornography, and the Internet*. Washington, D.C.: National Academy Press.

Thornhill, R. and Thornhill, N. (1987) 'Human rape: the strengths of the evolutionary perspective', in C. Crawford, M. Smith and D. Krebbs (eds), *Sociobiology and Psychology: Ideas, Issues, and Applications.* Hillsdale, NJ: Lawrence Erlbaum.

Thornhill, R. and Thornhill, N. (1992) 'The evolutionary psychology of men's coercive sexuality', *Behavioral and Brain Sciences,* 15: 363-375.

U.S. Department of Justice (2004). *Department of Justice, Homeland Security announce child pornography file-sharing crackdown: Law enforcement initiative targets child pornography over peer-to-peer networks*.

www.fbi.gov/dojpressrel/pressrel04/p2p051404.htm.

Webb, L., Craissati, J., & Keen, S. (2007). Characteristics Internet child pornography offenders: A comparison with child molestors. *Sexual Abuse: A Journal of Research and Treatment, 19*, 449-465.

Williams, K.S. (2005). Facilitating safer choices: Use of warnings to dissuade viewing of pornography on the Internet, *Child Abuse Review, 14*: 415–429

Wolak, J., Finkelhor, D., & Mitchell, K.J. (2005). *Child pornography possessors arrested in Internet-related crimes.* US. Alexandria, VA: Department of Justice, National Center for Missing and Exploited Children.

Wolak, J., Finkelhor, D., & Mitchell, K.J. (2009). *Trends in Arrests of "On-line Predators"*. Durham, NH: Crime Against Children Research Center.

Wolak, J., Mitchell, K., & Finkelhor, D. (2003). *Internet sex crimes against minors: The response.* Alexandria, VA: Crime Against Children Research Center, University of New Hampshire.

Wortley, R. (in press) Exploring the person-situation interaction in situational crime prevention, in N. Tilley and G. Farrell (eds) *The Reasoning Criminologist: Essays in Honour of Ronald V. Clarke.* London: Routledge.

Wortley, R. & Smallbone, S. (2006a). *Child pornography on the Internet. Problem-oriented guides for police series.* Washington DC: U.S. Department of Justice

Wortley, R., & Smallbone, S. (2006b). Applying situational principles to sexual offending against children, in R. Wortley & S. Smallbone (eds.), *Situational prevention of child sexual abuse. Crime prevention studies,* Volume 19. Monsey, NY: Criminal Justice