
Draft pre-submission version (with author's formatting)

This version is available at: http://eprints.mdx.ac.uk/18271/

Copyright:

Middlesex University Research Repository makes the University's research available electronically. Copyright and moral rights to this work are retained by the author and/or other copyright owners unless otherwise stated. The work is supplied on the understanding that any use for commercial gain is strictly forbidden. A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge.

Works, including theses and research projects, may not be reproduced in any format or medium, or extensive quotations taken from them, or their content changed in any way, without first obtaining permission in writing from the copyright holder(s). They may not be sold or exploited commercially in any format or medium without the prior written permission of the copyright holder(s).

Full bibliographic details must be given when referring to, or quoting from full items including the author's name, the title of the work, publication details where relevant (place, publisher, date), pagination, and for theses or dissertations the awarding institution, the degree type awarded, and the date of the award.

If you believe that any material held in the repository infringes copyright law, please contact the Repository Team at Middlesex University via the following email address:

eprints@mdx.ac.uk

The item will be removed from the repository while any claim is being investigated.

See also repository copyright: re-use policy: http://eprints.mdx.ac.uk/policies.html#copy
Incidents of child sexual abuse (CSA) are frequently documented and have recently attracted intense police, public scrutiny and efforts of social control across the Western world. This paper aims to explore the very concerning issue of online CSA and the way in which the police is responding to this growing problem. It will present some of the challenges the police in the United Kingdom face daily in dealing with the threats to children’s online safety. It argues that although proactive undercover policing has helped police forces to unmask sex offenders who predate innocent victims online, the advancement of technology is making the work of police officers more and more challenging. The findings presented have been collected over the last decade (2003-2013) during two exploratory, grounded theory studies, which involved the interviews with 21 police officers and forensic examiners and the observation and analysis of three police operations at the London Metropolitan Police Paedophile Unit in London.

Keywords: online child sexual abuse, online safety, technology, undercover policing, police challenges

1. Introduction

The Internet provides immediate access to a vast array of materials as well as anonymity at an affordable price (Cooper, McLaughlin & Campwell, 2000 b; Robbins & Darlington, 2003). However, the Internet should not be viewed simply as a library or an exceptionally advanced encyclopaedia. It would be more appropriate to perceive the Internet as a mirror image of our society in all its diversity and human expression, including deviance.

One of the common discussions that frequently takes place in academic forums, police investigative units and policy-making environments is whether the Internet can be deemed responsible for the creation of the problem of online child sexual abuse. It is still not clear whether the unique characteristics of the Internet has encouraged offenders to commit offences or the use of technology has made it easier for law enforcement agencies to detect who is the deviant (Jung, Ennis & Malesky, 2012). However, we do know that the Internet has increased opportunities for grooming behaviour and sex offences. Seto and Hanson (2011) addressed the key question of whether Internet sex offenders were somehow different from sex offenders operating offline. They suggest there are two prevailing views: One view

---

1 Dr Elena Martellozzo is a Criminologist at Middlesex University in London and specialises in sex offenders’ use of the internet and online child safety. She offers regular expert advice to the London Metropolitan Police and Italian Police Force (Polizia di Stato and Carabinieri). Her work includes the analysis of online grooming, distribution of indecent images and police practice in this area. She can be contacted at E.Martellozzo@mdx.ac.uk

2 The terms ‘child sexual offender’ and ‘paedophile’ are often taken to be synonymous. However, there are important classificatory and behavioural distinctions which need to be clarified: Not all child sex offenders are paedophiles - paedophiles are sub-set of child sex offenders (Miller, 1997). Some may have fantasies about sex with children, but they do not act them out with a child. Others may abuse children in different ways, including non-physical sexual abuse and exploitation (www.ecpat.net/temp). This article has sought to avoid the term ‘paedophile’ and used instead the term (child) ‘sex offender’, ‘abuser’ or, ‘suspect’ as working labels.
considers Internet-facilitated sex offending to be an extension of conventional offending. The other view is that some individuals become involved in offending because of the unique properties of the Internet; without the Internet as a facilitator, they would not commit sexual offences (Seto & Hanson, 2011: 4).

Older accounts prove that, unfortunately, CSA goes far back to the Byzantine period, where technology and the Internet were not even imaginable. John Lascaratos and Effie Poulakou-Rebelakou (2000) in their analysis of historical cases of CSA in Byzantine Society (324–1453 A.D.) found that children were abused under cover of premature marriages, child prostitution, pederasty and incest. They also found that mothers did not want their children to be far from home because they ‘run the risk of sexual attack by paedophiles offering sweets and nuts’ (ibid., 2000:1088). CSA is indeed an ancient phenomenon with severe physical and psychological repercussions on the victims. However, despite being present in our society for centuries it has been recognised as a serious social problem only in the past two decades (Wells, Finkelhor, Wolak & Kimberly, 2007).

Online CSA is becoming increasingly more difficult to police as the Internet, technologies and social networks develop apace (Martellozzo, 2012). Sociologist Manuel Castells claims that ‘networks became the most efficient organizational form as a result of three major features of networks that benefited from the new technological environment: flexibility, scalability, and survivability’ (Ibid. 2004: 5). These three characteristics may be applied to sex offenders’ online communities. In can be argued that sex offenders are not lonely figures in cyberspace but have created online communities or ‘networks’ that are able to change their components if necessary, while keeping their main goal: their interest in children (flexibility). Furthermore, because they are able to operate in a wide range of configurations, they can expand or shrink in size with little disruption (scalability) and resist any police threat by recreating other communities elsewhere in cyberspace (survivability). Digital networks are also global because, as Castell (2004) argues, they are able to reconfigure themselves. However, the people that police these communities are local, both in territorial and cultural terms and are unable to respond rapidly to the changes in the architecture of the network deviant society.

According to the British National Crime Agency, sex offenders are now turning to anonymous sites and encryption technologies so they can trade indecent images of children freely (BBC News, 2014). There are sites in the so called dark-web that receive as many as 500 page views per second (ibid., 2014). These sites are currently unpolicied (Police Oracle, 2015) and have become unspoiled habitats for sex offenders to create online communities.

In this article I argue that online social interaction may pose specific risks that do not exist in unmediated interaction for children. For example, it allows potential offenders to adopt a strategic presentation of self that would be unworkable in real life. This is a major risk as sex offenders can disguise themselves and their intentions to an extent that is impossible in direct interaction in the real world. However, the possibilities for a strategic presentation of self that exist in cyberspace are also presented to undercover police officers. They can in fact portray themselves as children or as sex offenders in a way that would hardly be credible in a real-life surveillance operation.

The article begins with the definition of online grooming and presents the ways in which sex offenders use the medium to abuse children. It will then move on to explore the way in which the British police has responded to this serious problem. Throughout the article, practitioners’ views on policing online child sexual abuse are
presented to offer a deeper understanding of how the policing of online abuse occurs and the challenges faced by the police to tackle this serious phenomenon on a daily basis.

Research on policing online child sexual abuse is still in its infancy. This article seeks to make a contribution to knowledge and understanding in this area and, through the British experience, contribute to the development of police practice around the world.

2. Methodology

2.1 The studies

This article draws on a range of data from two empirical studies I conducted over the last decade (2003-2013) at the London Metropolitan Police High Technological Crime Unit and Paedophile Unit (Martellozzo, 2010; Martellozzo, 2012; Martellozzo & Taylor, 2008). The two studies explored the complex and multi-faceted relationships between online grooming behaviours, risk assessment, police practices, children’s vulnerabilities and reporting for the Metropolitan Police Paedophile and High Technology Crime Units.

The first study sought to understand and explain the problem of online child sexual abuse and the way in which investigative tactics and operational procedures were employed by the London Metropolitan Police High Technological Crime Unit (HTCU) and Paedophile Unit (2003-2008). The follow up study aimed at enhancing police practices to counter the growing threat of online predation of children and increasing child safety and security in the digital world.

2.2. The role of the researcher and the research process

Taking into account the epistemological position which suggests that knowledge or evidence of the social world can be generated by observing or participating in interactive situations (Hobbs, 2000; Silverman, 2004), overt participant observations took place throughout the years spent on site with the officers ‘doing their job’ (Hobbs, 2000). The choice of this specific field role was strictly linked to access. I secured unprecedented access to these sites, officers, documents and data. Furthermore, one of the unique characteristics of both studies was the role I was able to take: that of the overt observer and be in the participants’ natural environment (McNeill, 1990). The findings were obtained through the analysis and development of case studies across three major police operations (two in the first project and one in the second project). Undercover officers acted as children or as sex offenders seeking to share information with other members of the offending community. In both studies, data were also collected through observational notes and recorded live-online communications between offenders and undercover police officers. Furthermore, in the first study, 21 one-to-one semi-structured interviews were conducted with officers and forensic examiners who play a significant role in the policing of cyberspace:

3 This was a six-month project focusing on ‘Understanding Sex Offenders’ Online Activities: Developing Research and Training for Covert Internet Investigators’ funded by the Metropolitan Police Service. A two-day training was developed on the basis of a number of key results and was delivered to 30 officers working for the Child Exploitation Online Protection Centre and the Metropolitan Police Service.
• Six interviews were conducted with all the members of the HTCU
• Six with the officers of the paedophile unit working in the operation chosen for observation
• Six with the forensic examiners working for the paedophile Unit who analyse the electronic equipment confiscated from sex offenders
• Three with senior management.

All interviews were recorded, transcribed verbatim and analysed using Nvivo.

2.3. Data analysis

One of the main challenges in qualitative data analysis is to ensure that ‘the voice of the other is heard and allowed to enter into dialogue with pre-existing understandings’ (Ezzy, 2002: xiii). These two pieces of research actively engaged these preexisting understandings and assumptions, allowing them to be transformed and be modified to accommodate new theories. It is with these recommendations in mind that qualitative interviews were carried out throughout this research. A grounded theory approach to coding was chosen (Charmaz, 2006; Jupp, 2006; Robson, 2002) as others have done when dealing with this line of enquiry (Webster et al, 2015; Quayle et al, 2014; Bourke, Ward & Rose, 2012; Burrows & Day, 2011). The author participated in the development of the emerging themes and interpretation of the findings. Data analysis was inductive and it was carried out with the aid of NVivo. The first study focused on police officers posing as children; the second study on officers posing as adults and entering sex offenders’ online communities. These areas informed initial broad codes and a book on online grooming (Martellozzo, 2012).

2.4. Ethical considerations

Ethical approval was obtained through the University of Westminster Research Ethics Committee for study one, and from the Middlesex University Research Ethics committee for study two. Anonymity and confidentiality were the two main concerns for both studies. Anonymity was, of course, guaranteed to all those who participated in this study. It was agreed that all transcripts would be made anonymous and that individuals who participated in the study would not be identifiable from the way in which the findings are presented. Furthermore, assurance was provided that documents containing extremely sensitive data were collected only for research purposes and kept in the Metropolitan Police Force’s offices to which the researcher had full access for analysis. That sensitive data comprised:

• Chat logs
• Police interviews
• Names, addresses and online profiles of convicted offenders
• Sentences
• Indecent images of children and adult pornography.

3. Setting the scene: Understanding sexual grooming

This section provides the definition of ‘sexual grooming’ and an overview of the grooming process. Section 15 of the Sexual Offences Act (SOA) 2003 makes ‘meeting a child following sexual grooming’ a serious offence. This applies to
Internet-enabled technologies (smart phones, mobile phones, game consoles and tablets) and the ‘real world’ where a person arranges to meet a child who is under 18, having communicated with them on at least one previous occasion (in person, via the Internet or via other technologies), with the intention of performing sexual activity on the child (Davidson & Martellozzo, 2008). However, as it was recognised by Whittle et al. (2013), the SOA fails to include in the definition the act of grooming a child for another person to abuse. Therefore, this definition is adopted here:

‘A process by which a person prepared a child, significant adults and the environment for the abuse of this child. Specific goals include gaining access to the child, gaining the child’s compliance and maintaining the child’s secrecy to avoid disclosure. This process serves to strengthen the offender’s abusive pattern, as it may be used as a means of justifying or denying their actions’ (Craven et al., 2006: 297).

Sexual Grooming has also recently been added to the Crimes Amendment Act 2005 in New Zealand. In the United States it is an offence to electronically transmit information about a child aged 16 or under for the purpose of committing a sexual offence (US Code Title 18, Part 1, Chapter 117, AS 2425). The Australian Criminal Code (s218A) makes similar restrictions, as does the Canadian Criminal Code (s172.1). The legislation in the UK differs in that the sexual grooming offence applies both to the Internet and the ‘real world’ whereas legislation in other countries addresses only electronic grooming via the Internet and mobile phones.

John McCarthy and Nathan Gaunt define the phenomenon of online sexual grooming ‘as a type of online behaviour designed to ‘seduce’ or lure children into sexual behaviour or conversations with or without children’s knowledge’ (2005). However, a particular problem that occurs when we attempt to define the grooming process is that it is not possible to establish when it starts or stops (Gillespie, 2004). In his latest pioneering work, Michael Seto (2013) explains that there are three main variables that contribute to the commission of sexual abuse against children. These are: an antisocial trait in the offender, a sexual interest in children, and situational factors such as access to children. He argues that the presence of antisocial behavior and opportunity factors can be the distinguishing factors that may trigger contact abuse. His ‘Motivation-Facilitation Model of Sexual Offending against Children’, is supported by the findings from the most recent meta-analysis on Internet sex offenders (Babchishin et al., 2014), which recognises that the main predictors of recidivistic contact sex offending amongst offenders who use indecent images of children are being antisocial, having access to children and the lack of barriers to acting on one’s deviant impulses.

Grooming is a crucial part of the so-called ‘cycle of abuse’ (Wolf, 1985; Finkelhor, 1986; Eldrige, 1990; Sullivan & Beech, 2004) and it does not only take place online, although this is a recent and major concern. The grooming process consists of sex offenders socialising and grooming children over prolonged periods of time to gain their trust and preparing them for sexual abuse (Webster et al, 2015) and will ensure that abuse will take place without being disclosed (Sullivan, 2002). Grooming can be differentiated in stages and usually begins with befriending a child (termed by Calder (2004) as ‘hands off offending’) and moves on to relatively inappropriate touching4 by a familiar adult in whom the child trusts. Calder (2004) terms this as ‘hands on’ sexual offending. In this manner, the child does not become

---

4 Susan P Phillips et al (1993) define inappropriate touching as touching parts of the body, such as fondling.
distressed and is unaware of the importance of what is happening. This behavior gradually continues and becomes more and more sexual in nature, so the child becomes accustomed to what is happening. Gallagher (2000) defines this behaviour as ‘entrapment’; that is the process in which ‘perpetrators draw children into abusive situations and make it difficult for them to disclose’ (Gallagher, 2000: 810). He argues that this method consists of a number of techniques, but ‘chief among these is the involvement of children in increasingly intimate physical contact, and the provision of a variety of inducements, whether these are material, illicit or emotional in nature’ (Gallagher, 2000: 810). Recent studies on sex offenders’ grooming behaviour supports the idea that the Internet does not create new stages in the cycle of abuse, but allows the cycle of abuse to be quickened (Gillespie, 2004).

Generally speaking, when people set up the profiles on social networking sites, they do so through the requirements (name, sex and age) of standardized electronic membership forms of social networking and similar websites and the verification processes of service providers. The data they insert are checked electronically but not physically by a person. Therefore, offenders can make any desired claim about their identity, including the use of any profile picture. These profiles and the messages posted are designed to attract either children or likeminded people. In many cases, it seems to work. Research conducted with victims of online abuse has shown that in a small number of cases, young people thought they met someone special whom they could implicitly trust. However, in reality, they had been talking to an adult who had a sexual interest (O’Connell, Price & Barrow, 2004). These adults target young people with the ultimate objective to abuse them. They achieve their aims by gaining the child’s trust, by making the child feel special, loved and comfortable. Some of the techniques used are so well planned that children may not understand, at least initially, that they have being groomed (Berliner & Conte, 1990). The victim then realises that they have engaged willingly in the previous behaviour and feel that it is too late to stop it. Owing to the gradual nature of abuse, some children cannot define such behavior as wrong until a later stage.

However, finding potential child victims may not happen as quickly, as not all children are at risk of online abuse. As argued by Sonia Livingstone (2010) ‘the identification of online risk does not imply that harm will follow, nor that all users are equally effected; rather, it is a probabilistic judgment regarding an outcome that depends on the particular and contingent interaction between user and environment’ (ibid., 2010: 3). Online risks in some cases may lead to harm but in others, they may facilitate resilience (ibid., 2010: 13). However, it appears to be the case that offline vulnerability extends its consequences online, as risk migrates from traditional to new sites. Therefore, children who are ‘vulnerable’ offline are more likely to be susceptible to online abuse.

4. Analysis and discussion

4.1. Principle of agent provocateurs

The way in which grooming takes place over the Internet appears to be different from the real world, although the ultimate aims are the same. Study 1 helped to understand and explore the anonymous nature of the Internet, which allows offenders to hide behind a computer screen and use a false identity. Suler (2004) defines this feature as dissociative anonymity which enables people to dissociate their actions from their real world identity, making them feel more open and less vulnerable. Therefore,
individuals are able to separate the reality of who they are, often by creating a fake identity, from their online behaviour. Invisibility is also a distinctive feature of online grooming, although interrelated with anonymity. It refers to individuals not being physically seen or heard which may disinhibit them to visit sites and behave in ways they would not do in the physical world (Suler, 2004). Suler (2004) argues that even if the identity is visible, the opportunity to be physically invisible amplifies disinhibition in the sense that allows people to say what they wish to say openly without being concerned of embarrassing themselves or of being rejected. To deal with issues of invisibility and dissociate anonymity, police forces and some organisations around the word have been challenged to develop innovative and explorative techniques, such as that of going undercover. For example, the charity, Terre des Hommes, carried out a 10-week sting operation in Holland, posing on video chat rooms as ‘Sweetie’, a 10 year-old Filipina girl. Thousands of men across the globe befriended her and some offered her money. The names of these men were passed to their countries’ respective police forces (BBC News 5 November 2013). It was found that in the UK, for the police to be able to intervene effectively, obtain evidence for their investigations, and to reduce threats to children’s online safety, they employ a variety of reactive and proactive tactics. The fact that the police are covertly accessing the Internet in their efforts to capture those engaging in sexual offences against children is widely known. The practice is recognised as a legitimate tool. As argued by Noorlander (1999), ‘modern policing no longer relies solely on detection, confession and the hope that witnesses will come forward. Increasingly, law enforcement agencies in the United Kingdom and in other countries are turning to pro-active, intelligence-led methods such as the use of surveillance devices, informants and undercover officers’ (Noorlander, 1999: 49). However, while these are regarded as effective policing methods, there are a number of fundamental principles of covert investigation that the Police need to respect in order not to interfere with the human rights of those ‘under surveillance’. According to Harfield and Harfield (2005) one of the most fundamental principles of covert investigation is that all covert human intelligence sources (CHIS)\(^5\) (whether they are participating informants or undercover investigators) should never incite the commission of a crime. So for example, if they are acting as a child and speaking to a potential sex offender, they are not allowed to suggest a meeting, offer sex to the offender or share indecent images. If this principle is not respected and police officers or informants have incited the commission of an offence that would not otherwise been committed, then the court would hold that the investigators have been acting as agent provocateurs. The principle of an agent provocateur is extremely important in undercover policing. It is applied heavily to policing child sexual abuse, and particularly to grooming online, where officers need to play different roles depending on the operation. When operating undercover, Covert Internet Investigators (CIIs) need to be fully immersed in the identity of the person they choose to be. For example, if they are assuming the identity of a child, officers need to create a profile of a child, need to interact like a child and speak like a child and if necessarily need to share some of the weaknesses of that child. They also need to know the differences in

---

\(^5\) Covert Human Intelligence Sources (CHIS) is defined under RIPA as: A person who establishes or maintains a personal or other relationship with a person for the purpose of facilitating the doing of anything that a) covertly uses such a relationship to obtain information or to provide access to information to another person; or b) covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship. Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.
tastes of music, language, school’s activities etc. that exist among girls under the age of 13, for example. It was found that one of the difficulties for undercover police officers was to respond to specific questions and demands of the online groomer. This is highlighted below by one of the officers interviewed in the context of the first study:

‘I was running a profile of a 12 year-old-girl. [Before starting the operation] I researched what year she was in at school and her interests, what her particular pop band was. But then I came up against a teacher who took an interest in the girl sexually. He took an interest in her education and in particular maths. So then he went on to try and help the girl with her maths homework. I was sitting there thinking: ‘I don’t know what you’re talking about’. So if something like this happens we have to research further. Well, someone else researched for me immediately whilst I was online, so I’d have an idea of what a 12 year old was learning in maths, and we got away with it.’ (Police Officer: ID6).

It is clear that undercover police officers cannot work in isolation. They are assisted by a team of researchers and forensic examiners who are involved in the operation and support the CIIIs in moments like the one described by the officer (ID: 6).

4.2 Officers posing as children

When officers are posing as children, they need to respond to the offender’s question passively and need to constantly ensure that the offender is fully aware of the age of the child. Table 1 below presents a conversation between an undercover officer pretending to be a 12 year old girl and an online groomer. It shows that the undercover investigator’s approach is mindful of not inciting the commission of an offence.

Table 1 Interaction between a Suspect (S) and a Covert Internet investigator (CII- where the CII is assuming the personality of a 12 year old girl):

<table>
<thead>
<tr>
<th>S:</th>
<th>CII:</th>
</tr>
</thead>
<tbody>
<tr>
<td>im not here to get pushy with you but i do want to get to know you</td>
<td>kwl</td>
</tr>
<tr>
<td>i also like the thought that you like older guys at least im in with a chance</td>
<td></td>
</tr>
<tr>
<td>we could have a lot of fun</td>
<td>[silence]</td>
</tr>
<tr>
<td>im a very gentle guy</td>
<td>kwl</td>
</tr>
<tr>
<td>sounds sooo nice</td>
<td></td>
</tr>
<tr>
<td>and thats what u need the first time</td>
<td>yehkw</td>
</tr>
<tr>
<td>xx</td>
<td></td>
</tr>
<tr>
<td>id give you lots of kisses in all the right places</td>
<td></td>
</tr>
<tr>
<td>this sounds reeel gd</td>
<td></td>
</tr>
<tr>
<td>i know you would love it</td>
<td></td>
</tr>
<tr>
<td>defin</td>
<td></td>
</tr>
<tr>
<td>would you like it if i kissed your tummy</td>
<td></td>
</tr>
<tr>
<td>kissed your boobs</td>
<td></td>
</tr>
<tr>
<td>yehtats reeel nice</td>
<td></td>
</tr>
</tbody>
</table>
This was the first conversation between the ‘girl’, Lucy, and the suspect where the suspect, a 34-year-old man with no previous convictions, approached Lucy and befriends her. The suspect approaches the girl on a social networking site, and then he invites her to move to MSN5, an instant messaging service. The suspect is a 42-year-old man with no previous convictions who approaches the girl to ‘get to know her’. However, within a minute he immediately moves on to what O’Connell (2003) defines as the ‘sexual phase’: ‘we could have a lot of fun’. He feels confident that the young girl would enjoy exploring sex with him ‘id give you lots of kisses in all the right places’. His confidence is clearly reinforced by the young girl’s response: ‘kwl (cool)’; ‘sounds sooo nice’; ‘xx (kiss, kiss)’ ‘defin (definitely)’. It can be argued that the key feature underpinning groomers’ behaviour is the assessment of how the young person responds to the sexual phase; the more positive the response the more disinhibited the groomer feels and as a result the more explicit, intense and faster the sexual interaction becomes. As this online interaction shows, the process of online grooming may take seconds but it may also take hours, days or months. As argued by Webster et al. 2012 ‘online groomers remained at different behavioural points for various lengths of time according to a dynamic inter-relationship between their goals and needs, and the style, needs or reactions of the young person’ (Webster et al., 2012: 6). Arguably, those offenders who spend more time grooming online might pose a more serious risk to children. As this CII states:

‘You tend to get the impression quite quickly of who is serious about meeting a child or not. Say he just wants to incite you to commit an offence or put the camera on and masturbate then that would happen in the first 10, 15 lines of a chat. It would be quite in your face: ‘Are you a virgin? Have you ever seen a cock before? Do you want to see one?’ And they’re off and running. To me that’s not grooming; that’s just someone who wants to commit that offence. Whereas someone who might talk to me, show an interest in me: ‘Oh do you like doing that? Oh wow! What sports do you like?’ And then they’ll interject with a little bit of flattery: ‘Oh you have a nice picture; you’re a really pretty girl.’ And they might pull it open a little bit. Next time they speak to you they would ask: ‘How’s school today? ’ Yeah fine. ‘It would be nice to take you for coffee one day.’ These may be the most dangerous. You tend to find it’s
the ones that don’t rush you are the ones who are probably going to want to meet. Not every occasion is the same however.’ (Police Officer ID: 14)

Table 2 presents the online conversation between the suspect (S) and a Metropolitan Police CII where the CII assumes the personality of a 12 year old girl. The conversation shows how invisibility and anonymity may assist the suspect to become disinhibited with the child, despite this being their first online interaction.

**Table 2: Interaction between a Suspect (S) and a Covert Internet investigator (CII- where the CII is assuming the personality of a 12 year old girl):**

<table>
<thead>
<tr>
<th>CII</th>
<th>Suspect</th>
<th>CII</th>
<th>Suspect</th>
<th>CII</th>
<th>Suspect</th>
<th>CII</th>
<th>Suspect</th>
<th>CII</th>
<th>Suspect</th>
<th>CII</th>
<th>Suspect</th>
<th>CII</th>
<th>Suspect</th>
<th>CII</th>
<th>Suspect</th>
</tr>
</thead>
<tbody>
<tr>
<td>hi lucy here</td>
<td>hi</td>
<td>kw1</td>
<td>I used to play hockey in my younger days by the way</td>
<td>how old r u now</td>
<td>yeh</td>
<td>lol. not too old I hope. good at sex anyway lol</td>
<td>i dont play now</td>
<td>discovered boys and sex huh</td>
<td>aint dun sex yet</td>
<td>interested though?</td>
<td>corse</td>
<td>I'd love to be your first</td>
<td>yeh rite</td>
<td>lol</td>
<td>im only 12</td>
</tr>
<tr>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
</tr>
<tr>
<td></td>
<td>hi how are you sweetie?</td>
<td>kw1</td>
<td>how old r u now</td>
<td>yeh</td>
<td>lol. not too old I hope. good at sex anyway lol</td>
<td>i dont play now</td>
<td>discovered boys and sex huh</td>
<td>aint dun sex yet</td>
<td>interested though?</td>
<td>corse</td>
<td>I'd love to be your first</td>
<td>yeh rite</td>
<td>lol</td>
<td>im only 12</td>
<td>I would though - I’m good at it. did you read my hi5 profile?</td>
</tr>
<tr>
<td></td>
<td>kw1</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
<td>CII</td>
<td>Suspect</td>
</tr>
<tr>
<td></td>
<td>kw1</td>
<td>kw1</td>
<td>I used to play hockey in my younger days by the way</td>
<td>how old r u now</td>
<td>yeh</td>
<td>lol. not too old I hope. good at sex anyway lol</td>
<td>i dont play now</td>
<td>discovered boys and sex huh</td>
<td>aint dun sex yet</td>
<td>interested though?</td>
<td>corse</td>
<td>I'd love to be your first</td>
<td>yeh rite</td>
<td>lol</td>
<td>im only 12</td>
</tr>
<tr>
<td></td>
<td>kw1</td>
<td>kw1</td>
<td>how old r u now</td>
<td>yeh</td>
<td>lol. not too old I hope. good at sex anyway lol</td>
<td>i dont play now</td>
<td>discovered boys and sex huh</td>
<td>aint dun sex yet</td>
<td>interested though?</td>
<td>corse</td>
<td>I'd love to be your first</td>
<td>yeh rite</td>
<td>lol</td>
<td>im only 12</td>
<td>I would though - I’m good at it. did you read my hi5 profile?</td>
</tr>
<tr>
<td></td>
<td>kw1</td>
<td>kw1</td>
<td>how old r u now</td>
<td>yeh</td>
<td>lol. not too old I hope. good at sex anyway lol</td>
<td>i dont play now</td>
<td>discovered boys and sex huh</td>
<td>aint dun sex yet</td>
<td>interested though?</td>
<td>corse</td>
<td>I'd love to be your first</td>
<td>yeh rite</td>
<td>lol</td>
<td>im only 12</td>
<td>I would though - I’m good at it. did you read my hi5 profile?</td>
</tr>
<tr>
<td></td>
<td>kw1</td>
<td>kw1</td>
<td>how old r u now</td>
<td>yeh</td>
<td>lol. not too old I hope. good at sex anyway lol</td>
<td>i dont play now</td>
<td>discovered boys and sex huh</td>
<td>aint dun sex yet</td>
<td>interested though?</td>
<td>corse</td>
<td>I'd love to be your first</td>
<td>yeh rite</td>
<td>lol</td>
<td>im only 12</td>
<td>I would though - I’m good at it. did you read my hi5 profile?</td>
</tr>
</tbody>
</table>

It appears that the suspect is aware of the girl’s (CII) age, but he does not seem to be concerned whether the girl is at home with somebody, and he does not question her identity. On the contrary, when the girl reveals her age (‘im only 12’) he promptly asks ‘I would (like to be your first) though – I’m good at it’. He then moves further and suggest they should meet ‘so maybe we can have some fun together sometime. if you wanted to hehe’. It is evident that the risk factor is completely overlooked.
Furthermore, in less than three minutes the suspect moves directly to the sexual phase and asks: ‘[have you] discovered boys and sex huh’ and ‘I’d love to be your first [lover]’. It appears that often, online groomers do not invest much time in forming a relationship with a child and do not assess risk. Clearly, cyberspace provides the offender with an inflated sense of security and the achievement of immediate personal rewards via exposure and the use of pornography, which may be used for personal gratification (e.g. masturbation).

4.3. Officers posing as adults

When officers are posing as adults with sexual interests in children, their response is different. They need to show enthusiasm and interest but at the same they cannot commit any offence (e.g. distribute indecent images of children). Furthermore, they need to establish a trustworthy online relationship with the suspect so to assess if the suspect is fantasising or posing any risk to children. Table 3 shows an example of an online interaction between a suspect (S) and a CII. The CII met the suspect in a ‘nudist forum’ where people interact with other people interested in nudity and share nude pictures.

Table 3: Online interaction between Suspect (S) and CII

| CII: You were telling me about your daughter | S: Yeah, we have just started going nude at home |
| CII: Oh Nice. How did you suggest it? | S: Well I am divorced and she comes to visit in hols and weekend, she found some nudist mags and we started talking about it. |
| CII: Yeah, go on | S: She knew I was keen, so we started by me bathing her, seeing her nude in the bathroom |
| CII: Nice, go on | S: I started just wearing a pair of boxer shorts around the flat |
| CII: This is just fantasy or for real | S: No its real. When she comes over we now started to go nude in the evenings. One thing led on from another until we both accepted we would be nude in front of each other. How does it work in your family? |
| CII: Have all grown up like this. Well not gf but she is cool now. How friendly are you with your daught now? | S: Well, we are getting closer, but not sure how it will go yet. She wants to come and live with me in the summer. |
| CII: Have you got many friends from open families | S: No |
| CII: How far do you want to go with her? | S: We only started this at Christmas. Well I can see something happening soon. She sees me getting aroused and she says she would like to help |
| CII: Nice | S: But we are both been a bit coy, do you understand. How old are yours? |
| CII: Yeah, it takes time. I have a friend from an open family |

After a short conversation, the suspect feels comfortable to share with the CII the fact that he enjoys being naked around the house with his daughter and he is teaching her to do the same. The CII shows his interest in the idea of being naked (‘Nice, go on’;
‘Yeah, go on’) but at the same time he assess if the girl is at risk of being abused: ‘This is just fantasy or for real; How far do you want to go with her?’

4.4 Sex offenders developing online communities

In both studies 1 and 2, it was found that cyberspace facilitates individuals to create fictitious characters that live in an imaginary dream world. Through these characters, individuals dissociate themselves from the demands and responsibilities they have to face offline. This is what Suler (2004) defines as dissociate imagination. Dissociative imagination refers to the belief that within the online identity individuals live in a perfectly constructed world in which there are no boundaries and where they can completely dissociate online fiction from offline fact. In this way cyberspace becomes the place in which people are allowed to live in a make-believe dimension separated from society’s rules, regulations and norms. However, this is not to say that there are no rules in their perfectly constructed world. Martellozzo (2012), studying sex offenders’ behaviour in cyberspace, found that some sex offenders are not isolated individuals but are now part of a much wider community: the online community. They create complex and impenetrable child lovers’ forums in which they find support and understanding from other like-minded individuals. Her findings were later substantiated by the European Online Grooming Study by Webster et al. (2013).

Given the lack of restrictions in cyberspace and the permissiveness of its sexual subculture, predators have a new medium to not only pursue potential contacts with children, but also unite with fellow users in a way that allows them to validate and normalise their sexual inclinations (Lanning, 1998). An example of sex offenders’ network community similar to that defined by Castell (2004) is that of the Hidden Kingdom, which was an operation observed and studied during study 2. This was a child love forum, which has now been investigated and removed by the London Metropolitan Police. The structure of this community was pyramidal, followed a clear hierarchy and was rather complex. It appears that the ‘organisation’ was more tightly knit and more closely controlled at the top of the pyramid by the chair of the ‘Hyper Court’ who was the ‘Judge of the Kingdom’. There was strong local autonomy with regents in each zone, men trusted at the top or ‘Administrators’ who were directly answerable to the top level. Like in some organised criminal organisations, a great number of personal qualities were required of members. These included honour, honesty, obedience and participation. For example, to be able to escalate to a higher level of the pyramid and to gain credibility, each individual (townsfolk) needed to post 50 posts a day. However, ‘landowners’ could choose to pay to avoid the posting but they would be looked upon with suspicion and would not be able to gain the trust and move to a higher level. Furthermore, there was a set of rules each person needed to obey to in order to protect the site from detection. These included:

- No frontal nudity
- No male interaction in any picture or video
- No trading of indecent images
- No offensive language towards the children (referred to by the participants as ‘models’).

If links to pornography or nudity were posted, the person was banned from the ‘realm’ immediately and permanently and became an ‘exile’ or ‘prisoner’. Therefore,

---

6 The name of this sex offenders’ online community has been changed by the author.
if members of the forum wanted to exchange indecent images and openly discuss fantasies, they moved on to a more private site such as MSN. The aims of forums such as Hidden Kingdom are to create a global community of adults with a sexual interest in children; and to provide online support to help individuals who are seeking to come to a fuller understanding of their attraction and love for children. Here they meet to discuss and share their love for children and their fantasies and to exchange information such as non-indecent pictures of young people. The Hidden Kingdom site can be compared to a virtual castle where different rooms, towers and secret passages were created to accommodate everybody’s desires. For example, there were rooms where pictures of girls in red skirts, riding bikes or in school uniforms were posted. Through the creation of this ‘dream world’, individuals dissociated themselves from the real world and its rules and freely expressed their ideas and feelings towards children with other group members. One member, for example, stated:

Member 15: The last and most profound is the fact that there have been a rash of criminals, who uncaringly force themselves on the object of their passions. These ass holes care nothing for anyone except themselves and attack the very creatures we adore. They desire, they assault and they destroy. The things that separate us from them is as old as time itself. It is called honor. It is called respect, and it is called love. Love instead of lust, which is what drives these animals that hurt and kill children, for self-gratification.

Member 16: Not perverts, we are all perfectly normal people who have a timeless love that has always existed and always will do, someday society will see that – but it will be an enlightened society and not this one we currently have.

Some offenders, perhaps unconsciously, perceive their online life as a game from which they can gain pleasure and gratification and to which they can return to any time they feel the need to abandon their daily life to re-immerse themselves into this fantasy world.

Sex offenders are using the dark web to communicate with other sex offenders and share ‘best practice’ about how to gain access to potential victims and create new material and high quality material. These online communities, like the Hidden Kingdom, contribute to the normalisation of child abuse by sharing experiences and justifications. Furthermore, they share best practices on how to abuse a child and ensure that no traces are left behind, by silencing the victim. The analysis of how sex offenders behave online, their grooming techniques and the way they socialize with other sex offenders in safe online communities, leaves us wondering how the police can monitor and possibly control this growing problem. The remaining part of this paper focuses on how the British police respond to this problem and some of the challenges they face.

5. Policing challenges

Undercover investigations of the types described in this article come with a number of challenges. First of all, there is an incredible amount of preparation that a CI needs to do prior to any communication with a potential online groomer. If the investigator is pretending to be a child or an adult with interest in children, he/she needs to set up a profile that is credible and does not put anyone at risk. It is not easy for undercover
officers to reach credibility, however. Their success depends on the credibility of the profile, which in turn depends on the legend created, which in turn relies on the availability and the quality of the images. When undercover Internet investigations were still at their infancy, police officers needed, first of all, to obtain a picture of a child, generally online, and change it with the aid of technology, so to protect the identity of the child. In selecting the image they needed to take into account of the age of the child in the picture. As this officer explains:

‘I believe, and probably the rest of the team believe, that a child under 13 will add more weight at court when it comes to sentencing because a child they think they are going to abuse is aged under 13. But if I am targeting a particular individual then I will create a profile as near to what I think that person’s interest is.’ (Police Officer ID: 3)

What complicates matters further is that one image is no longer sufficient to make a profile credible. The techniques used by undercover officers when creating a child profile less than a decade ago would not work today, given the changes in online behaviours among children and young people. As prices for portable devices are becoming more affordable and online communication is free of charge (via WiFi), children and young people have a considerable freedom to access the Internet from any location they may be. A recent study suggests that the number of children who go online when ‘out and about’ has doubled in most countries (Vincent, 2015) and because of the increase in the use of social media, there is an high expectation be always available to respond to the notifications on WhatsApp, Twitter or Instagram instantly (ibid., 2015: 4). There is also the expectation for profiles to be regularly updated with new pictures, notifications, places visited, new friends, comments on photographs etc. With these changes in mind, undercover investigators would not be able ‘to be’ children living in a mobile digital online world. They do not have enough resources to create credible profiles that can be used to engage with potential sex offenders or monitor all the social networking platforms where children are most at risk. And even when a profile is created, officers are faced with further challenges. For example, the most cautious sex offenders are aware of the police operating undercover and, as a result, constantly test that they are communicating to a real child. Therefore, they want to speak to the child and ultimately they want to see the child via a webcam. This clearly represents a limitation for the police:

‘As technology progresses our job is going to become incredibly hard because the expectation of the bad guy or the suspect is that we would have access to all the facilities that would allay their fears: things like being on the web cam, having a mobile phone, being contactable. These things that we have to now use our initiative to negate, phone calls, covert messages that we do to get through this I think it will get to a stage where between the publicity that we give ourselves, and the technological advances you have to be thick to get caught by us. I give it a couple more years I think the average Internet top proper paedophile will not waste time.’ (Police Officer: ID 7)

As confirmed by the officer, cautious sex offenders could possibly be ‘the most dangerous, they are not easy to identify and lie from start to finish’ (Police Officer: ID 2). Cautious groomers are so concerned about being caught that they are not willing to furnish details about themselves until completely sure. This type of offender may
insist on viewing the potential victim on webcam, hearing her voice over the phone and receiving more photographs. Eventually, when they feel they are chatting to someone real, they start grooming the child. However, this is not always the case. If they do not feel comfortable in establishing a closer relationship because of a lack of credentials, they may decide to move on to the next victim. This contention was supported by the majority of the police officers working in the field:

‘Hyper-cautious online groomers are the ones that we don’t know how dangerous they are, we don’t know if they’re paedophiles, we don’t know anything about them because we don’t have the tactics or technology to go up against them. We’re not able to prove at a very early stage that we are an authentic child and they switch off and go elsewhere and quite possibly go elsewhere to real children.’ (Police Officer: ID 20).

These findings may question how computer generated avatars such as Sweetie could possibly convince the most hyper cautious and dangerous offenders that she is a real girl.

6. Conclusions
Over the past ten years online child sexual abuse has brought about some innovative changes to combat problems, certainly in the legal context but also in the way cyberspace is policed. Sex offenders now create online networks and communities where they can meet to share fantasies, exchange indecent images of children or find new young victims to abuse.

Before children in the world’s wealthy countries became the main digital citizens of cyberspace, police forces were primarily concerned about the viewing, possessing and distribution of indecent images. However, it became clear that sex offenders were using the Internet also to groom child victims to sexually abuse them. Since the Sexual Offences Act 2003, the concept of ‘grooming’ has been recognised in the UK and several other countries are still following the UK lead and have criminalized grooming behaviour. Police forces have been able to train officers to become Covert Internet Investigators, who are able to pro-actively police the Internet by portraying themselves as children or as adults. However, new technological innovations, such as the dark web where users enjoy total anonymity, are constantly threatening the safety of cyberspace. This article has presented a number of police successes, but as technology advances, there is a need to improve police responses to the issue of online safety. A crucial question that remains unanswered: Are undercover police investigators tactics targeting individuals that pose real risks to children or are they targeting the least dangerous? This is a key question that needs to be addressed in order to effectively improve police practice. Child sexual abuse online is not an easy problem to police as the Internet is constantly developing and new social networking groups attract more children and like-minded people.

Furthermore, social networking sites are by definition designed to let people meet new people online. These sites encourage and enable people to exchange information about themselves, share pictures and videos, and use blogs and private messaging to communicate with friends, and share interests, either with individual contacts or all site users. This means that shared information in the right hands is welcomed. However, moral panic occurs when it gets into the wrong hands and the potential for great harm to a vulnerable child occurs. This indicates that law enforcement agencies and academia need to maintain a critical level of awareness
concerning the possible risks that come with online social networking sites. Undoubtedly policing online abuse will always be a challenging task even for the most developed and equipped police forces. It is important to continue to develop innovative and creative technical solutions combined with proactive undercover police strategies that will help protect the most vulnerable and innocent in our society.

**Bibliography**


Child Abuse and Neglect, 14 (1), 29-45.


FKBKOK.net: University of Central Lancashire.
NEWS, 41, April , 17-21.