In Proceedings of Third International Workshop on Critical Information Systems Research, 2008, Galway, Ireland

Citation information:
Eneman, M (2008) Panoptic Environments: How Offenders Manage the Risk of Surveillance in the Context of Digital Child Pornography, In Proceedings of Third International Workshop on Critical Information Systems Research, 2008, Galway, Ireland.

PANOPTIC ENVIRONMENTS: HOW OFFENDERS MANAGE THE RISK OF SURVEILLANCE IN THE CONTEXT OF DIGITAL CHILD PORNOGRAPHY

Marie Eneman
University of Gothenburg
marie.eneman@gu.se

Abstract

Information and Communication Technologies (ICT) have changed the conditions to consume and distribute child pornography. Child pornography is a criminal offence in many countries and therefore it is of great importance for the users to protect their identity and reduce the risk of getting caught. The technological environment, which ICT constitutes, provides powerful surveillance-mechanisms. The aim with this paper is to explore offenders' relationship towards surveillance in the context of digital child pornography. The empirical findings presented are based upon semi-structured interviews with offenders convicted of child pornography. The findings show that the offenders develop different strategies to manage the risk of surveillance. The identified strategies have been divided into technological and social. The result of this study enhances the knowledge about the offenders' ICT usage and their behaviour in their involvement in child pornography. This knowledge is of great importance to be able to develop effective combating-mechanisms, such as legislations and technological solutions. This paper contributes to previous research within the field of Critical Information Systems Research by applying Foucault's concept of panopticon on the research subject.

Keyword: ICT, Digital Child Pornography, Surveillance, Panopticon, Strategies

1 INTRODUCTION

This paper studies a specific group of criminals' use of information and communication technologies (ICT) for a criminal offence, i.e. offenders convicted for child pornography. The aim of the research is to develop knowledge that can reduce such illegal activities by analyzing and understanding both how the offenders use ICT and how they perceive ICT as a means for conducting their illegal activities. As this paper will show, ICT can act as a double-edged sword (Murray, 2006). On one side it can be used to reduce the social exposure and enhance the anonymity when carrying out undesirable and/or illegal activities, but on the other side the technology offers powerful surveillance mechanisms that can be used to monitor the same activities (Lyon, 1994, 2001, 2006). Surveillance systems in our everyday lives have become less obvious and overt, and more systematic and subtle (Lyon 2001; Haggerty, 2006). This means that people, even though they are aware of the risk of being under surveillance, seldom know exactly when they are subjects of surveillance, they are often unaware of how comprehensive others' knowledge of them actually is (Lyon, 1994). Modern societies where surveillance can take place anytime and anywhere are sometimes described as 'panoptic societies' (Jonsson, 2006).

Research (Adam, 2005; Eneman, 2006; Taylor and Quayle, 2003) shows that ICT, in some cases, provides an experienced feeling of anonymity for the users and reduces the social exposure. This has obvious consequences for criminal activities such as child pornography. Today anyone can easily, with the aid of technology, access and distribute child pornography, communicate and network with other people and initiate online contact with children without having to reveal one's real identity. Child pornography is besides being a criminal offence in many Western countries also a phenomenon, which is strongly unacceptable in society (Taylor and Quayle, 2003). People who are involved in illegal activities, such as digital child pornography, constitute a group which have a strong incitement to protect their identity, to reduce the risk of getting caught and thereby be prosecuted for the committed crime.

Digital child pornography has rarely been subject for academic research (Adam, 2005). The development of effective societal combating-mechanisms against digital child pornography, such as legislation, filtering techniques etc, must be based on adequate knowledge (Eneman, 2006). The field of surveillance studies has grown rapidly over the past decades, spurred by both rapid developments in governance and new technologies. There are a number of conceptual papers of surveillance and technology but there are few empirical studies, which investigate questions of surveillance in relation to technology (Lyon, 2006).

The purpose of this paper is to explore the offenders' relationship toward the risk of surveillance guided by following two research questions: (1) How do the offenders experience the risk of being under surveillance? (2) What strategies do the offenders develop to manage the risk of being under surveillance?

This paper contributes to the critical information systems research (CISR) field, by applying a Foucault-inspired perspective (Willcocks, 2006) on technology use. Additionally, the paper contributes to policy-making since the findings enhance the understanding of ICT and its effects regarding digital child pornography.

The structure of this paper is organised as follows: the next section presents the theoretical framework, which includes the field of CISR and the concepts of surveillance and panopticon. This is followed by a brief presentation of the research setting, digital child pornography. Next the research strategy is presented, followed by a presentation of the empirical findings. These findings are then discussed in relation to the purpose of this paper and, in closing; brief-conclusions of this paper are presented.

2 THEORETICAL FRAMEWORK

2.1 Critical IS Research

An emerging research field within the Information System (IS) discipline, relevant for this study, is critical IS research (Howcraft and Trauth, 2005). Within IS research the discussion of the dissemination of ICT in society has mainly focused upon the benefits involved in ICT usage (Adam, 2005). This simplified approach tends to omit the fact that the technology is not one-sided and that the dissemination brings with it both pros and cons (Kling et al, 2005; Eneman, 2006). Child pornography, which is in focus in this paper, is an example of how well-established usage of ICT becomes the foundation for harmful purposes, such as digital child pornography. Critical IS research can be seen as a reaction to the mainstream IS research which tends to assume that technological innovation is 'inherently desirable' and beneficial to all (McGrath, 2005). Furthermore, this perspective is based on 'Critical Theory' as it was originally formulated and practiced by the 'Frankfurt School' (Klein and Huynh, 2004; Croon- Fors, 2006).

Critical IS researchers use a wide spectrum of critical social theories (for example ANT, Habermas, Foucault) and appropriate concepts, models and frameworks to critically question established assumptions about the technology, its use and its implications (Cecez-Kecmanovic, 2005; Willcocks, 2006). In addition to using relevant concepts the research object should be placed in a wider historical, political, social and economic context (Alvesson and Deetz, 2000). The central aim in critical research is its deep interest of emancipation. By critically questioning 'social realities' and provide insights how these 'realities' are historically, politically and socially constructed and strongly shaped by asymmetries of power in society, we are able to move beyond established definitions and assumptions and can achieve emancipation from traditional existing structures (Croon-Fors, 2006). The importance of carrying out critical studies is today frequently pointed out by several IS-researchers (Avgerou and McGrath, 2005, Howcroft & Trauth, 2005; Walsham, 2005; Willcocks, 2006). The number of studies where such perspectives are applied is nevertheless few but growing.

2.2 Surveillance and Panopticon

Surveillance is not a new phenomenon. Humans have always kept an eye on each other with purpose to control their surrounding (Lyon, 1994). One of the most important differences is that today with the use of ICT, the surveillance is more systematic, routine and often embedded in every aspect of everyday life.

One of the most unparalleled metaphors of the power of surveillance in the contemporary world is panopticon (Foucault, 1979). The panopticon was originally an architecture design developed by Bentham as a special surveillance tower for a prison (Lyon, 1994). Foucault has used panopticon as a metaphor for 'modern disciplinary societies'. It should be noted that Foucault was critical against this architecture. Panopticon can be seen as "the illusion of constant surveillance: the prisoners are not really always under surveillance, they just think or imagine that they are" (Foucault, 1979; Whitaker, 1999; Lyon, 1994). The purpose refers to discipline and control. As the prisoners fear that they might be watched, and fear punishment for transgressions, they internalize the rules (Foucault ,1979).

This paper will use the theoretical concept of panopticon to describe and analyze the offenders' relationship towards surveillance when performing their illegal activities via ICT. Willcocks (2006) argues that despite that Foucault himself wrote little directly about ICT, the work of Foucault is useful for the IS discipline in contemporary social studies of ICT. Doolin (1998) illustrates in his study how ICT can bee seen s a disciplinary technology.

Due to the mentioned fact that child pornography is both illegal in many countries and a highly unacceptable phenomenon in our society, the people involved take different measures for not getting caught. ICT constitute a risk of being under surveillance as well as offering the possibility to perform their activities. ICT can therefore be described as containing disciplinary mechanisms (Munro, 2000). These mechanisms affect people's behaviour in different contexts (Zuboff, 1988; Munro 2000). For example, Ball (2006) describes how powerful panopticon structures can give rise to resistance, where strategies to avoid surveillance are developed.

Even though the panopticon is a strong metaphor to conceptualize and understand surveillance it has been criticised for its limitations to adequately understand contemporary technological societies (Lyon, 2006; Bauman, 1992; Bogard, 1996). The critique is based upon the argument that we must 'move beyond' Foucault to understand modern technology-dependent societies. It is however difficult to discern what this mean in reality (Lyon, 2006). The panopticon concept refuses to go away despite the critique. The reasons for this are manifold but clearly one of them is that panopticon is such a rich multifaceted concept (Lyon, 2006). It can be used for interpretation in a number of ways and in different contexts. Lyon (2006) argues that it is impossible to evade some interaction with the panopticon, either historically or in today's analyses of surveillance. Boyne (2000) suggested that it is best to 'accept the panoptic presence, even if only as the ghost lurking within the post-panoptic world.

Surveillance is a controversial topic. Lyon (2001) claims that surveillance has 'two faces', both negative and positive aspects. Surveillance technologies can discipline and control unwanted behaviour, such as illegal activities, but at the same time the technology facilitate such illegal activities.

The concept of panopticon has been used in the analysis of different contexts such as prisons (Foucault, 1979), workplaces (Zuboff, 1988; Doolin, 1998; Jonsson, 2006; Ball, 2006) and in other public spaces (Koskela, 2006). Adam (2002, 2005) has applied a similar surveillance and control perspective in her studies of cyberstalking and Internet pornography. Adam's focus is upon the offenders' possibility to carry out surveillance on potential victims in this technological environment. This paper applies the concepts of surveillance and panopticon (Foucault, 1979; Lyon, 2006; Willcoks, 2006; Jonsson, 2006; Brooke 2002), to explore offenders' relationship towards surveillance in the context of digital child pornography.

3 DIGITAL CHILD PORNOGRAPHY

The term digital child pornography, which is used in this paper, refers to child pornography where ICT (Knights and Murray, 1994) has been used as a medium. This section will illustrate the use of ICT for child pornography. First, ICT simplifies the production of child pornography and enables it to be conducted at a low cost (Taylor and Quayle, 2003). By using digital technology, images and films can easily and quickly be produced and stored. The development of ICT has enabled non-technically skilled users to record, store and manipulate images in a way which was previously only available to people with the requisite technical skills and costly equipment (Hughes, 2002). Therefore, today even non-technically skilled users can record their abuse of children and thereafter easily distribute the material through ICT. Similarly ICT have affected the volume of material which it is now possible to distribute and consume (Taylor and Quayle, 2003). The technology offers features to manage large amounts of data easily, rapidly, at low cost and is readily available without a high level of technical knowledge (Hughes, 2002). Computer networks also allow people interested in child pornography to create online communities (Adam, 2005). The communities function as places where these people can share and trade information and material. These communities allow them to meet other like-minded. Together in the community they can legitimise their interests and establish important contacts. (Eneman, 2006; Taylor and Quayle, 2003).

While legal definitions of child pornography can differ greatly between jurisdictions, it is possible to discern a generally accepted definition of the term. One such generally accepted definition is: representations where a child is engaged, or appears to be engaged, in some kind of sexual act or situation (Wolak et al, 2005). The content can vary from posing pictures to physical sexual abuse of children (Taylor and Quayle, 2003). The current Swedish legal position criminalises the production, distribution and possession of child pornography. Swedish legislation has proven to be inadequate in parts (Gillespie 2004; Eneman 2005).

4 RESEARCH DESIGN

One of the challenges with engaging in CISR is that the guidelines for how to conduct CISR are scarce and sketchy. Critical IS researchers have focused on defining what it means to be critical, but largely ignored to explicitly define how criticality can be achieved in IS research (McGrath, 2005). McGrath (2005) argues that CISR has not yet reached a position where theory and practice of critical research inform each other. CISR, as a field, would benefit if its researchers become more explicit in their approach, especially when carrying out empirical studies. The importance of using empirically based material when studying social consequences of ICT has been pointed out by Kling (2001).

Researching the area of digital child pornography involves certain difficulties. This is due to the fact that many actions surrounding the phenomenon constitute criminal offences and are, at the same time, considered highly unacceptable in society. Due to the illegal dimension of the studied phenomenon, research approaches that involve participation were not an alternative for this paper. An alternative approach used in this paper has been to explore how the people who were part of this ‘’world’ make sense of it and what they did (Taylor and Quayle, 2003).

4.1 Data Collection

The research data was collected through semi-structured interviews with 15 offenders convicted for child pornography, where ICT has been used as a medium. Contacts with the respondents have been enabled through the prison psychologists. All the respondents were given information about the study prior to the interview and gave their consent (Brantsaeter, 2001). The interviews, each lasting between 1,5-2 hours, were in eleven cases tape recorded and later transcribed. In four cases, where the respondents didn't want the interview to be recorded, field notes were taken and carefully written out after the interview (Silverman, 2005). Noak and Wincup (2004) argue, that in those cases where the use of recording equipment is not possible, the researcher will have to rely on the more traditional method of note taking.

Since this study is part of a wider ongoing research project exploring the use of ICT for child pornography, the data collection covered more issues than the surveillance related ones. During the interviews the respondents were asked questions regarding their relationship towards surveillance and how this affects their involvement in digital child pornography. Depending on the respondent's answers follow-up questions were asked during the interview. All the interviews took place inside the prison, either in the visiting room or in the prison psychologist's office.

4.2 Data Analysis

The data analysis consisted of three stages. The first stage started with the transcription of the material. The transcription process offers the opportunity for reflection on the data and attention to emerging themes and should be seen as an integral part of the analysis process (Silverman 2005). The material was then read and re-read through. Some initially notes were also taken to comment the material. In the next stage the material was structured and coded manually into different broader themes (for example 'developed strategies'), which emerged from the material relevant to the purpose of this study. During the last stage subjective meanings were searched and differences and similarities were identified among the themes identified during stage two (Silverman, 2005).

4.3 Ethical Consideration

An important consideration for this study has been to ensure the anonymity for all the participants. All identifying information has been removed or changed to ensure anonymity. The respondents have also been informed of how the material will be used and stored. As described above this paper is part of a wider ongoing project, which explores the role of ICT, its use and its effects in relation to child pornography. The project is ethically approved by the Ethical Committee of Göteborg University.

5 FINDINGS

5.1 Offenders Experience of the Risk of Being Under Surveillance

During the interviews a recurring theme was the tension between how to be able to conduct the desired activities at the same time as avoiding being revealed. The findings show that surveillance and anonymity are considered as important and serious issues among all the respondents who were interviewed in this study. In the interviews the offenders expressed concern about the risk of being under surveillance when carrying out child pornography activities. It is considered important among the offenders to protect their identity and to reduce the risk of being revealed. One respondent expressed his concern of surveillance as follows:

> "Yes, one always thinks about it. Every time you put on the computer. You notice how it blinks like hell and one starts to wonder who the hell it is, sometimes one wonders if it is the cop. Of course one thinks that, every time one is out there ." (Interview C)

This illustrates a constant awareness over the risk of being under surveillance. It also highlights the uncertainty of not knowing who the other persons are in the environment. The other respondents confirmed this constant worrying. They are well aware that their involvement in child pornography is a criminal offence according to Swedish legislation and therefore they assume that they can be monitored at any time. The following quotation illustrates how the awareness of the risk of surveillance is expressed:

> "Of course I have felt chased. Sometimes I have felt jittery, when it has been a lot of raids all round. Then it is only a matter of time, one can be totally jittery. But then one thinks that it won't happen to me, but that's what everybody says". (Interview J)

The anxiousness of being monitored appears in different ways. Common issues that are expressed by both the quotations above are feelings of being chased, feeling jittery and being under stress. The later quotation adds another dimension, which illustrates an interesting conflict. The respondent describes the feeling of being chased and that it is only a matter of time before getting caught and at the same time he thinks that it won't happen to him. However, the awareness of the risk of surveillance doesn't seem to refrain the offenders from their involvement in the illegal activities. One the one hand they express serious concern of the risk, but on the other hand they seem to persuade themselves that it won't happen to them, i.e. being revealed and getting caught.

As this section has shown the awareness of the risk of surveillance affects the offenders. It does however not seem to act as a deterrent for not carrying out child pornography activities. To handle the risk of surveillance and to protect the anonymity, different counter-strategies have been developed.

5.2 Developed Counter-Strategies

The result shows that the offenders have developed different counter-strategies to manage the risk of surveillance, with the purpose to reduce the risk of being under surveillance and to protect their identity. Three different categories of counter-strategies have been identified in the material: (1) technological strategies, (2) social strategies and (3) a combination of technological and social strategies.

5.2.1 Technological Strategies

Technology Choice

All the respondents state that it is important to use secure technology and consequently it is also important to avoid insecure technologies. The respondents express that they are careful in their choice of technology. The technology choice is based on their belief that it is a more secure technology to use, i.e. that it would be difficult for law enforcement to monitor their activities. When talking about the use and security level among different types of ICT one respondent expressed his experience of choosing secure technology like this:

> "One quickly learns which technology one should use to not be visible." (Interview F)

This illustrates that the offenders view certain technologies as insecure and others as more secure, and that this is something they learn quickly. The technologies that are considered more secure, make the user more invisible and act as a shield for surveillance systems. When talking about insecure and secure technologies the respondents were unanimous in their attitude against WWW. One respondent expressed his concern as follows:

> "Web pages are not to think of, they are too insecure." (Interview B)

This quotation shows that the respondents exclude certain technologies since they are considered to be insecure to use. This quotation indicates that this particular technology, WWW, is not even an alternative due to the insecurity. The concern of using insecure technology is confirmed in the following quotation, but this quotation also shows the offenders awareness of the consequences of using insecure technologies.

> "And yet one knows that if one use for example WinMX [freeware peer-to-peer file sharing program], and if one meets the wrong person on the other side one is screwed up. If loading up to a board without encryption, one is totally screwed up. If I start downloading from a news server, I am logged everywhere. Sometimes one doesn't think about it." (Interview E)

What is shown here is the offenders' awareness of the risk of using insecure technology, and consequently that the risk of getting caught is increased by using insecure technology. The quotation also illuminates the fear of not knowing whom the other person really is that the respondent is exchanging material with. Awareness and concern are expressed over being logged, i.e. that data is collected about the respondent's activities when using insecure technology. It is however interesting to note that despite the awareness of the risks, the respondent says that he sometimes doesn't think about the risks but just do it.

Advice and Recommendations

Users, who initially don't possess adequate knowledge about which technology that is preferable to use to enhance the security, can obtain advice and recommendations from other users.

> "During one of the first occasion when I was out looking for something to download, I talked with a person who had greater experience of this than me. He gave me tip of which technology I should use and which to avoid". (Interview N)

This supports the idea that people involved in child pornography advice each other regarding technological issues, with the purpose to enhance the protection of their identity. The inclination to help each other can be explained by the fact that advising other in their environment can also be seen as a protection of themselves. This is due to the fact that the involvement in child pornography is a criminal offence in many countries, and if one is caught several others also risk to get caught if there are any traceable connections.

Obligatory Rules

Besides the advice and recommendations there are a further dimension, with obligatory rules which the user is obliged to follow. Within this network it was obligatory to follow the guidelines in the manual regarding the technology use. It is interesting to note that the members actually are forced to use certain types of technology, otherwise they risk to be excluded from the network. The purpose with these obligatory rules is to ensure a high level of security for the members.

> "Everything is built from the ground, all these boards had programmers. One chap who writes the scripts and who is responsible for it. There was another chap who was responsible for a manual with guidelines which everybody was forced to use, about secure technology". (Interview K)

Another interesting aspect shown here is how the network is organized with certain persons responsible for different aspects. Within this particular network there were for example programmers responsible for the scripts. Another person was responsible for the manual. Respondents who have been member in other networks confirmed that it is common with this kind of organisation.

5.2.2 Social Strategies

Personal Information

Besides the technological strategies the findings show that the offenders also have developed different social strategies. The awareness of the surveillance risk and the incitement to protect the identity have influenced the offender's behaviour when interacting with other. One approach that is commonly practiced among the respondents is to be careful with revealing personal information about oneself when interacting with others. This is due to the fact that they almost never can be sure who the other person really is. One respondent expressed it like this:

> ”I have never revealed my real identity and I know that nobody else does it either, it's the way it is you don't think about it." (Interview G)

This statement shows that the offenders are careful with revealing personal information that can reveal their offline identity. It also shows that this approach is considered to be generally accepted among the users.

Use of Alias

One effect of being careful with personal information is that the offenders use several different alias instead, to enhance the protection of their offline identity. The risk of getting caught is considered to be reduced when using several alias instead of always using the same alias. The use of different alias is illustrated in following quotation:

> "I have different names. A sometimes, B sometimes, C sometimes, it varies. One just picks a name. Unfortunately, I can't remember all the names right now, they are too many. No, I can't say that I have used any specific name more than the other." (Interview O)

This respondent claims that he doesn't use any particular alias more than the other. This is however not a common approach among the other respondents, instead they state that they have one or two alias that they use more frequently.

Rules for Interaction

Rules for interaction constitute a further dimension of social strategies that are used within closed networks. The purpose with the rules is to enhance the collective security for the users within the network. Following quotation exemplifies what sort of interaction that the rules attempts to regulate:

> "It's just the way it is, there has to be certain rules for how it should work, what is allowed and what is not. It is the main administrators that create the rules. For example, there are rules, which forbid buying and selling, payment is never allowed. If one is to sell or buy

> material, there has to be some personal information and then it is a risk of being revealed in some way. We are in fact not allowed to exchange names and telephone numbers and stuff like that, but people do that anyway after a while." (Interview L)

Rules are considered necessary for the network to work. Once again, we see example of the social organization of these networks. Main administrators are responsible for creating the rules. Technological rules were presented earlier, which purpose is to regulate the technology used among the users to enhance the security. In this example the rules attempt to regulate what interaction that are allowed respectively forbidden in the network. Buying and selling are forbidden, since such transactions often require a certain amount of personal information and consequently enhance the risk of being revealed. It is also possible to discern a conflict here since the respondent express that the users do not always follow the rules.

5.2.3 Combination of Technological and Social Strategies

The third strategy is a combination of the technological and social strategies. The offenders use this kind of strategy to carry out counter-surveillance towards their environment, with the purpose to reduce the risk of being under surveillance. All the offenders in this study are aware of the possibility to carry out surveillance as a counter-strategy. They also state that they have used ICT to monitor different social behaviour of others in the environment. The following quotation shows how the use of language is monitored:

> "At least he is English-speaking, it 's obvious in the way he writes. Most writes in English, but you notice that some make spelling mistakes. Germans don't master English, its obvious. They write really badly, Frenchmen as well. They mix terribly. One can tell directly that English is not their mother tongue." (Interview I)

The respondent is attentive and observes another user's language usage during their interaction. What is observed is how well the user master the English-language, by spelling correctly. Based on this observation the respondent draws certain conclusions regarding the nationality of the user. This constitute an interesting example of how the offenders are able to discern further information about the other users during their interaction, besides the information actually written. Besides the possibility to observe the language usage, other behaviour has also been observed among the offenders:

> "I'm quite sure that it was the same person. We were several that suspected that. Well, the way these two persons loaded up stuff. Sometimes it is the same places and everything. It is to similar for two different persons to do exactly like that." (Interview I)

This is an illustrative example of how the technology is used to monitor another user's behaviour when uploading material. The offenders are attentive and suspicious of certain behaviours in their environment. Furthermore, what is shown is that several users have observed this particular user's behaviour and they have also talked about this user and the behaviour.

6 DISCUSSION

ICT can be described as a disciplinary technology containing powerful panopticon structures (Doolin 1998), which facilitates surveillance (Lyon 2006, Ball 2006). The purpose with panopticon is to mediate a feeling of constant surveillance, where the persons may not really be exposed to surveillance, they just think or imagine that they are (Foucault 1979, Lyon 1994, 2006). This feeling of constant surveillance is confirmed by the offenders in this study. The findings indicate that the offenders are aware of the risk of surveillance, and think about it almost constantly. The awareness doesn't seem to act as a deterrent for the offenders in their involvement in child pornography. Which can be explained by the strong incentive that motivates the offenders in their technology use when downloading this type of material.

As this study has shown, disciplinary technologies such as ICT are not exclusively constraining (Doolin 1998). They can also evoke new spaces of action such as the development of strategies in this study. The offenders have developed different counter-strategies to reduce the risk of surveillance and to protect their identity. Ball (2006) describes how the knowledge about the risk of being under surveillance can evoke active resistance among those who believe that they might be under surveillance. Three different types of counter-strategies have been identified within this study: technological strategies, social strategies and a combination of technological and social strategies. The developed strategy, 'obligatory rules', is an illustrative example of internalization of rules (Foucault, 1979). These rules seem to engender a degree of self-discipline regarding the offenders' behaviour (Lyon, 1994; Willcocks 2006).

The offenders also carry out counter-surveillance as a counter-strategy, which is facilitated by the panoptic structure in the technological environment (Zuboff, 1988). The offenders view the technology as both a risk and a possibility, which confirms that ICT can be seen as a double-edged sword (Murray, 2006).

The identified strategies should however not be seen as isolated strategies used by the individual offender. The strategies must be placed in a wider context to fully understand the offenders' behaviour. The strategies have been created and shaped in different networks, which are socially organized. This means that the social organizations constitute the basis for the offenders' behaviour and that it is crucial to understand these social organizations as well as the developed strategies if we are to obtain an adequate picture of the studied phenomenon.

The reason why it is important to understand how this specific group of user use the technology and behave within the technological environment is due to the fact that the development and use of different combating-mechanisms in society, for example legislation and technological solutions such as certain Internet Service Providers (ISP) use of filtering techniques (Eneman 2006), must be based on adequate knowledge about the user and the use. Otherwise these combating-mechanisms tend to be rather ineffective.

Despite its critique, and the call to 'move beyond' panopticon (Lyon, 2006; Haggerty, 2006), the concept of panopticon can be used as a powerful concept to understand complex issues of surveillance in contemporary society. The concept has been useful for this study to illuminate the different dimensions of surveillance in the context of digital child pornography.

The possibility for the offenders to use technology to resist surveillance can in this context be seen as a form of emancipation (Cecez-Kecmanovic, 2005). In this context, emancipation from societal control- and discipline-mechanisms that attempts to regulate the involvement in child pornography.

It is important to be critically aware of the consequences of the used material (Alvesson and Deetz, 2000). The findings in this paper are based on interviews with convicted offenders. This raises an interesting question – could it be that those who have not been convicted use other forms of counter-strategies to reduce the risk of surveillance? Despite the limitation of the empirical material, it provides a rich source of information to understand the offenders' relationship towards surveillance.

7 CONCLUSION

This paper has explored the offenders' relationship towards surveillance in the context of digital child pornography. This paper has shown how the technological environment, which can be seen as a powerful panopticon structure, evokes resistance among the offenders to reduce the risk of surveillance. The offenders have developed different technological and social counter-strategies to reduce the risk of being under surveillance and to protect their anonymity. Counter-surveillance has also been identified as a strategy to reduce the own risk of being exposed to surveillance. The counter-strategies should however not be studied isolated from the social organizations, which constitute the contexts where the strategies are created and shaped. This paper contributes to the field of CISR and to the professional communities by providing knowledge about this specific group of users, how they use the technology and how they behave within the technological environment. This understanding is decisive to enable social change, which is the ultimate goal with this research as well with the CISR agenda.

References

Adam, A. (2002) Cyberstalking and Internet Pornography: Gender and the Gaze. In Ethics and Information Technology 4(2).

Adam, A. (2005). Gender, Ethics and Information Technology. Palgrave Macmillan.

Alvesson, M. and Deetz, S. (2000). Doing Critical Management Research. Sage.

Avgerou, C. and McGrath, K. (2005). Rationalities and emotions in IS innovation. In Handbook of Critical Information Systems Research (Howcroft, D. and Trauth, E. eds.). Edward Elgar.

Bain, P. and Taylor, P. (2000) Entrapped by the Electronic Panopticon? Worker Resistance in the Call Centre. In New Technology Work and Employment, 15(1).

Ball, K. (2006). Organization, Surveillance and the Body: Towards a Politics of Resistance. In Lyon, D. (ed) Theorizing Surveillance: The Panopticon and Beyond. Willan Publishing.

Bauman, Z. (1992). Intimations of Postmodernity. London, Routledge.

Bogard, W. (1996). The Simulation of Surveillance. Cambridge University Press.

Boyne, R. (2000). 'Post-Panopticism'. In Economy and Society, 29(2), 285-307.

Brantsaeter, M. (2001) Möter med menn dömt för seksuelle overgrep mot barn. Doctoral Thesis, Report 3:2001, Institutt for Sosiologi og Samfunnsgeografi, Universitetet i Oslo.

Brooke, C. (2002). What Does it Mean to be 'Critical' in IS Research?. In Journal of Information Technology, 17(2).

Cecez-Kecmanovic, D. (2005). Basic assumptions of the critical research perspectives in information systems. In Handbook of Critical Information Systems Research (Howcroft, D. and Trauth, E. eds.). Edward Elgar.

Croon-Fors, A. (2006). Being-With Information Technology: Critical Explorations Beyond Use and Design. Doctoral Thesis, Department of Informatics, Umeå University, Umeå, Sweden.

Doolin, B. (1998). Information Technology As A Disciplinary Technology: Being Critical in Interpretive Research in Information Systems. In Journal of Information Technology, 13(4).

Eneman, M. (2005). The New Face of Child Pornography. In Klang, M. and Murray, A. (eds) Human Rights in the Digital Age. Cavendish Publishing.

Eneman, M. (2006). Child Pornography & ICT: Reflections on the Need for an IS Research Agenda. Proceedings of IFIP-TC9, HCC7 Conference, Nova Gorica, Slovenia, September 21-23.

Foucault, M. (1979). Discipline and Punish: The Birth of the Prison. Vintage.

Gillespie, A.A. (2005). Indecent Images of Children: The Ever-Changing Law. Child Abuse Review. 14. Published online in Wiley InterScience (www.interscience.wiley.com)

Haggerty, K. D. (2006). Tear Down the Walls: On Demolishing the Panopticon. In Lyon, D. (ed) Theorizing Surveillance: The Panopticon and Beyond. Willan Publishing.

Howcroft, D. and Trauth, E. M. (2005). Handbook of Critical Information Systems Research: Theory and Application. Edward Elgar.

Hughes, D. (2002). The Use of New Communications and Information Technologies for Sexual

Exploitation of Women and Children. In Hastings Women's Law Journal, 13(1).

Jonsson, K. (2006). The Embedded Panopticon: Visibility Issues of Remote Diagnostics Surveillance. In Scandinavian Journal of Informatin Systems, 18(2).

Klein, H. and Huyhn, M. (2004). The Critical Social theory of Jurgen Habermas and its Implications for IS Research, in Social Theory and Philosophy for Information Systems edited by Mingers, J and Willcocks, L, John Wiley & Sons, Ltd.

Kling, R., Rosenbaum, H. and Sawyer, S. (2005). Understanding and Communicating Social Informatics: A Framework for Studying and Teaching the Human Contexts of Information and Communication Technologies. Information Today, Inc.

Kling, R. (2001) Social Informatics. In The Encyclopaedia of LIS. Kluwer Publishing, Amsterdam.

Knights, D and Murray, F. (1994) Managers Divided: Organizational Politics and Information Technology Management. Wiley, Chichester.

Koskela, H. (2003). "Cam Era": The Contemporary Urban Panopticon. In Surveillance and Society, 1(3) 292-313.

Koskela, H. (2006). 'The Other Side of Surveillance': Webcams, Power and Agency. In Lyon, D. (ed) Theorizing Surveillance: The Panopticon and Beyond. Willan Publishing.

Lyon, D. (1994). The Electronic Eye: The Rise of Surveillance Society. University of Minnesota Press.

Lyon, D. (2001). Surveillance Society: Monitoring Everyday Life. Open University Press.

Lyon, D. (2006). Theorizing Surveillance: The Panopticon and Beyond. Willan Publishing.

McGrath, K. (2005). Doing critical research in information systems: a case of theory and practice not informing each other. In Information Systems Journal. 15, 85-101.

Munro, I. (2000). Non-Disciplinary Power and the Network Society. In Organization, 7(4).

Murray, A. (2006). The Regulation of Cyberspace: Control in the Online Environment. Routledge Cavendish.

Noaks, L. and Wincup, E. (2004). Criminological Research: Understanding Qualitative Methods. Sage Publications.

Silverman, D. (2005). Doing Qualitative Research. SAGE Publications.

Taylor, M. and Quayle, E. (2003). Child Pornography: An Internet Crime. Routledge.

Thomas, D. and Loader, B. D. (2000). Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Routledge.

Walsham, G. (2005). Learning about being critical. In Information Systems Journal. 15. 111-117.

Whitaker, R. (1999). The End of Privacy. New York: The New Press.

Willcocks, L. (2006). Michel Foucault in the Social Study of ICTs: Critique and Reappraisal. In Social Science Computer Review, 24 (3).

Wolak, J., Finkelhor, D and Mitchell, K. (2005) The Varieties of Child Pornography Production.

In Viewing Child Pornography on the Internet, (eds) E. Quayle and M. Taylor. Russell House Publishing.

Zuboff, S. (1988). In the Age of the Smart Machine: The Future of Work and Power. Basic Books.