This is an Accepted Manuscript of an article to be published by the Journal of Qualitative Criminal Justice & Criminology

Interviewing cybercrime offenders

Alice Hutchings and Thomas J. Holt

Abstract. Research on cybercrime offending and victimization has increased dramatically over the past two decades, though qualitative scholarship on more technical offenses such as computer misuse have not kept pace with this broader trend. The aim of this research is to identify potential best practices for researchers considering qualitative interviews as a method for researching computer misuse offenses, more commonly involving hacking techniques. The authors interviewed six experienced researchers who conducted qualitative examinations of active or incarcerated cybercriminals to understand their common experiences with recruitment, ways in which they interviewed research participants, ethical issues, and publishing their research. This analysis explores the difficulties associated with this area of research that are not typically discussed in the methods section of a research paper. The findings demonstrate the problems that emerge in research and the precautions researchers may need to take to protect themselves, their participants, and the research data.

Keywords: Qualitative research, cybercrime, interviewing

Introduction

Nils Christie (1997, p. 21) differentiates between 'near data', which includes information pertaining to a small number of participants while providing thousands of insights, and 'distant data', such as large datasets from official records, which may contain thousands of cases but provides little in-depth understanding. In relation to cybercrime, qualitative interviews with offenders have been a crucial method to gather such 'near data'. Accessing this population comes with unique challenges, and the number of academic researchers who have successfully carried out such work is small. In this article, we aim to provide helpful insights for researchers who are considering using qualitative interviews to research cybercrime offender populations. By learning from the experiences of others, researchers can avoid hidden pitfalls, ensure they have appropriate ethical safeguards in place, and consider how they would respond to potential situations.

Cybercrime is a relatively new topic for criminological inquiry, with the majority of published work emerging during the first decade of the 21st century (e.g. Diamond & Bachmann 2015, Holt & Bossler 2016). While the term is being used in this paper to describe computer crimes that compromise data or financial security, such as attacks against computer systems or the use or development of malicious software (malware), it is important to note that cybercrime has also been used to describe offenses ranging digital piracy to cyberstalking and

child sexual exploitation (Brenner 2010, Wall 2001). There is a relatively broad literature surrounding certain offenses like digital piracy due to the perceived prevalence of this behaviour cross-nationally (Business Software Alliance 2016, Higgins & Marcum 2011). Similarly, research examining interpersonal crimes, such as cyberbullying and on-line harassment has exploded in the last decade, with particular emphasis on interdisciplinary investigations (e.g. Patchin & Hinduja 2016, Tokunaga 2010).

Despite growing interest in cybercrime scholarship generally, studies of computer misuse which compromises data or financial security, more commonly referred to as computer hacking in popular media (e.g. Furnell 2002, Steinmetz 2015) remain relatively limited. There are definitional issues that complicate the study of this topic. For example, individuals may use their knowledge and skills to compromise computer networks with or without permission from the system owners (Jordan & Taylor 1998, Meyer 1989, Schell & Dodge 2002, Steinmetz 2015). As a result, their activities may be either criminal or legitimate depending on the individual and their relationship to the system owners (e.g. Jordan & Taylor 1998). Furthermore, those with legitimate access may misuse their privileges in an attempt to gain access to sensitive information or systems (Shaw et al. 1998). In such instances, the individual's actions are illegal but may not be immediately detected (e.g. Schell & Dodge 2002).

In addition, terms such as 'hacker' and 'hacking' are contested among various communities. While the term is often used to describe criminal actors and their activities, this is neither the original nor the only meaning of hacker (Furnell 2002, Jordan & Taylor 1998, Levy 1984). Levy (1984, p. 36) describes hackers as those that guide computers to greater heights than anyone expected,' and in computer science and engineering communities is meant as an honorific term to describe those who use innovative methods to solve complex problems, often involving computer software or hardware (Levy 1984, Taylor 1999). Thus, attempts to examine criminal hacking activities may be inherently limited due to different perceptions of the term among populations of interest.

Researchers with an interest in cybercrime, particularly those involving computer misuse to access data, often utilise qualitative research methods to examine this phenomenon, with diverse data sources ranging from interviews with offenders to posts from websites, forums, chat logs, and other on-line sources (e.g. Holt 2007, 2010, Hutchings 2013*b*, 2014, Hutchings & Chua 2017, Hutchings & Clayton 2016, 2017, Hutchings & Holt 2015, Jordan & Taylor 1998, Meyer 1989, Steinmetz 2015, Taylor 2001, Turgeman-Goldschmidt 2007). Qualitative interviews, particularly with active cybercrime offenders, can make a valuable contribution to our understanding of this offense. The offender's own words allow us to gain insights into aspects which cannot be measured quantitatively, and explore issues which we know little about. There is difficulty in accessing offender populations actively engaged in cybercrime due to the secrecy encouraged among the various communities and the relatively closed nature of their social networks (Taylor 1999). Similar issues are evident in attempts to access incar-

cerated offenders due to their involvement in criminal behaviour and concern over discussing activities with others (Hutchings 2013*b*).

Due to the inherent difficulties researchers experience in accessing cybercrime offender populations, there is a need to understand the ways that they are overcome in practice. Identifying successful methodological strategies that can be implemented in the field are vital to enhance the quality of scholarship produced, and improve the perception of researchers among the underground world of cybercrime offenders. Thus, this study analyzed a set of six interviews with criminologists who have engaged in interviews with active cybercrime offender populations to understand their personal experiences in the field. This investigation identified their successes and failures, complications throughout the research process, and recommendations for scholars new to this area of research. The methodological implications of this study were examined to provide guidance for future scholarship to improve the state of cybercrime research.

Examining the Use of Interviews in Cybercrime Research

The literature on cybercrime offenders provides insights into the challenge of developing interview samples. The 'hacker' subculture has maintained a historically antagonistic relationship to law enforcement, government, and authority figures generally (Holt 2007, Jordan & Taylor 1998, Levy 1984, Thomas 2002). They also report feeling misrepresented in popular media and academic research as criminals due to the negative connotations that surround the term 'hacking' (Holt 2007, Jordan & Taylor 1998, Schell & Dodge 2002, Steinmetz 2015). 'Hacking' has also been sensationalized and distorted in various films, such as The Matrix and Hackers, despite subject knowledge experts providing their input (Thomas 2002). Finally, some potential participants have expressed unwillingness to engage in active interviews over the risk of arrest and prosecution through cybercrime laws (e.g. Taylor 1999).

These factors may lead cybercrime offenders to be unwilling to participate in a research study conducted by criminologists who may distort their views or unfairly portray their actions. For instance, multiple researchers have had limited interview samples, consisting of less than 20 people, despite the application of traditional data collection strategies including snowball sampling and distribution of surveys at conferences (Holt 2007, Holt et al. 2017, Hutchings 2013*b*, Kinkade et al. 2013, Steinmetz 2015). A small number of researchers succeeded in expanding their interview populations, notably Turgeman-Goldschmidt Turgeman-Goldschmidt (2007) and Jordan and Taylor Jordan & Taylor (1998). It is instructive that Jordan and Taylor's (1998) sample of 80 interviews were collected over a 10 year period, consisting of Taylor's (1993) dissertation dataset involving both electronic and face-to-face interview protocols.

Turgeman-Goldschmidt's (2007) 54 person sample illustrated the limits of multiple data collection strategies, as she employed eight different data collection strategies over two years of data collection. Snowball and chain referral techniques generated 25 interviewees, which is sizeable compared to other re-

search on this topic. This supports the argument that snowball techniques can be useful for hidden populations, such as those involved in crime and deviance (Berg 2007). By comparison, only five interviews were collected from attendees of three Israeli hacker conferences, and six from friends and family referrals. Her sample even included seven interviews as presented via media outlets on television and in magazines (Turgeman-Goldschmidt 2007).

Limited access to offender populations led scholars to utilize multiple qualitative data sources in the course of their research to triangulate their findings. Several researchers utilized participant observations at conferences and local group meetings (e.g. Holt 2007, Kinkade et al. 2013, Steinmetz 2015), posts in forums and other forms of computer-mediated communication (Holt 2007), media accounts and security vendor reports (Lusthaus 2012, Steinmetz 2015), or court documents (Hutchings 2013*a*,*b*) to better understand the activities of cybercrime offenders. Some have also combined interviews with computer security professionals and law enforcement to understand the views about offending and offenders by those in and out of the subculture (Hutchings 2013*a*,*b*, Lusthaus 2012, Taylor 1999).

The use of multiple qualitative data sets and data triangulation is somewhat debated among scholars due to the potential that the researcher may attempt to validate one form of data over another (e.g. Garfinkel 1967, Hammersley & Atkinson 1983, Silverman 2000). Comparing data that represent different versions of reality can become distorted when the phenomenon being researched is a social construct. Researchers who can avoid simply aggregating their results and instead focus on the contextual nature of the data and how it was collected can provide more nuanced analyses (Silverman 2000). To that end, studies that drew upon data collected on and off-line have been able to highlight the unique dynamics of the hacker subculture and its influence on behaviour (e.g. Holt 2007, Steinmetz 2015).

Though these studies gave substantive insights into the nature of cybercrime, they shed little light on the methodological challenges that researchers face when attempting to engage in qualitative scholarship on cybercrime offending, particularly when using interview data. These publications give minimal input as to the ethical challenges they faced before, during, or after engaging in data collection. There is also little information provided on the extent to which researchers were successful in implementing their research design, and what steps were necessary to ensure that success.

There is also a growing body of scholarship on cybercrime that eschews interviews in favour of data collected from posts in web forums and other forms of social media (see Décary-Hétu & Dupont 2012, Dupont et al. 2016, Franklin et al. 2007, Holt 2013, Holt et al. 2015, 2016, Hutchings & Clayton 2017, Hutchings & Holt 2015, Motoyama et al. 2011, Yip et al. 2013). This broad transition calls to question why and how researchers pivot from interview data to other forms of data collection and analysis. Thus, this study attempted to address all of these issues to understand the ways that researchers conducted qualitative

scholarship, how they viewed their experiences, and the ways their subsequent research changed as a function of these outcomes.

Data and Methods

The sample for this study was developed by contacting all reachable scholars who published criminological or sociological research using interview data to examine various forms of cybercrime. We focused specifically on qualitative studies exploring cybercrimes involving acts of computer misuse to acquire financial data or system access, including fraud, malware, and complex forms of cyber-trespass, to understand how they conducted their work, methodological complexities, ethical challenges, and any ways that their work has changed as a result of prior experiences. This focus excludes quantitative researchers who have used various college samples or other data sets to test traditional criminological theories with cybercrime (e.g. Bossler & Burruss 2011, Holt et al. 2012, Maimon et al. 2014).

The potential interviewees were initially contacted via email by the researchers and invited to participate in the study. Those who gave their consent were provided with an information sheet outlining the ethical protections provided by the two research ethics boards that approved the research, and then asked for permission to record the interview. In total, six researchers were interviewed, and responses analysed, which provided a 66.6% response rate. The remaining three researchers did not respond to the invitations to participate. Those interviewed ranged in experience, from doctoral students to full-ranked professors. One additional interview was conducted, however it was found that the researcher's area of expertise was outside the scope of this project, and was excluded from this analysis. Due to the small population, the authors are also research participants, and interviewed each other. While this may be unusual for qualitative interview, there are other research methods where researcher is also a participant, such as action research (Berg 2007). Theoretical saturation (Guest et al. 2006) may not have been reached. While all recently published criminological and sociological scholars were invited to participate, this study did not include those whose work has not been published recently, or computer scientists who may have a more social science research orientation. Those perspectives would benefit future research and better inform this study.

Interviews took place face-to-face, as well as using online video technology. The interviews were qualitative and semi-structured. An interview schedule was used, which outlined the topics to be canvassed, however each interview was tailored to suit the researcher, depending on their experiences. Questions explored the researcher's background and experiences in qualitatively interviewing cybercrime offenders, recruitment, ways in which they interviewed their research participants, ethical issues, and publishing their research.

Verbal consent was sought, both for the interview to be recorded and for the data to be used for analysis. The interviews took between 51 minutes and 90 minutes, with a mean time of 67 minutes. All interviews were transcribed, excluding any information identifying the researcher or specific third parties, and

the transcriptions were analysed using NVivo. To avoid confusion, the research participants for this study are referred to as 'researchers' in the following section, with the term 'participants' used to describe their research subjects.

Findings

The findings of this study are presented thematically to highlight the rationale for research, past experiences with active research in the field, the publishing experience, and lessons learned from their experiences. Quotes are provided from the interviewees when appropriate to situate the experiences of the researchers in their own words.

Why Interview Cybercrime Offenders?

Unsurprisingly, all researchers believed that qualitative interviews are particularly valuable for researching cybercrime offenders. Reasons for qualitatively interviewing cybercrime offenders were broadly classified as: correcting misunderstandings; providing a deep understanding; identifying new lines of inquiry; accessing a hidden population; providing a voice; and perceiving quantitative approaches as being insufficient. Researchers also stated that the methods used should depend on the type of questions being posed, with qualitative interviews being particularly appropriate for explorative research.

In relation to correcting misunderstandings, one researcher spoke about the 'myth and mythology' surrounding cybercrime offenders. For instance, the researcher described how cybercrime offenders are often depicted as 'the lone computer hacker pulling a ski mask over his face, pecking away behind the computer' (R001), while they were instead interested in the human elements, particularly group dynamics. As well as correcting misunderstandings, qualitative interviews were seen as providing a deep understanding to matters that were poorly understood. It was felt that interviews lead to new themes and topics that had previously not been thought about, or at least not in any amount of detail. As cybercrime is a relatively new phenomenon, qualitative interviews were seen as particularly useful, as they could open up new lines of inquiry:

> Cybercrime's a new topic, trying to get a sense of what's going on, I think qualitative is a very appropriate method, and I think that would be the case for a number of kind of, newish fields where you're still trying to get a feeling for the landscape. I think qualitative is also good for a very micro-level of understanding of what's going on, the mechanisms, how people, individuals... as soon as you start getting up to different levels, and trying to answer different types of questions, then different methodologies become more appropriate (R004).

Particular aspects relating to cybercrime offenders were also seen as especially conducive to research using qualitative interviews. This included the illegal nature of their activities, the removal from physical interaction with targets and

victims, and the small size of the population, which make them particularly hidden and hard to access. It was noted that the cybercrime offender population could also be mischievous, as well as untrusting. However, with careful recruitment methods, research involving qualitative interviews could break down those barriers. Through this process, it was felt that an objective researcher allows the population to have a voice, to have their experiences and views expressed in a safe and anonymous way.

The final rationale for qualitative interviews related to concerns about some quantitative approaches. It was felt that by reducing observations down to numbers, a lot of the richness inherent in the data was lost, and that nuances, meanings, norms, and values were not quantifiable. Another researcher pointed out that while some may criticise qualitative research for being subjective, often quantitative approaches suffered the same shortcomings, such as deciding what to measure, and how. Qualitative interviews were perceived as being more appropriate than quantitative surveys when there was a need to tailor the experience to the particular experiences of the participant. Trust was another important concept, with researchers agreeing that the personable approach required for qualitative research helped their research participants open up to them, but also that they could have more confidence in the responses, compared to what they might receive in surveys.

Recruitment

The researchers were asked to reflect on their experiences in recruiting cybercrime offenders to take part in their research. The main locations that researchers had recruited, or attempted to recruit, participants from were online forums, Internet relay chat (IRC), email distribution lists, customer-facing websites operated by potential participants, conferences, and events organised or attended by relevant communities. These may be considered 'cold' recruitment methods, where there was no intermediary to introduce the researcher. Other recruitment strategies included researchers gaining access to their research participants by way of personal introductions through contacts, and referrals from other participants ('snowball sampling'). The main differences in the 'cold' recruitment strategies were whether they were on- or offline, and whether it was directed at a mass audience, or if there was a more selective approach, such as invitations issued to just one individual or a small group.

Some of the most discussed challenges related to building trust and perceived legitimacy with potential participants. The researchers felt that cybercrime offenders tended to be quite 'sceptical' and 'wary of outsiders':

> I mean, we're talking about people who generally tend to be a little sceptical, who are wary of outsiders, and may be unwilling to disclose everything about themselves, because they're never quite sure what that person's up to (R001).

For example, cybercrime offenders could be concerned that the researcher is actually from law enforcement or intelligence services. Researchers suggested

ways to build trust, including blending in with others in the environment, staying natural, learning and understanding the language being used, having a relevant online presence (such as a university webpage), being honest and open about the research being conducted, and demonstrating a willingness to learn. Things to avoid included deceiving potential participants, using stereotypical definitions, showing ego, and inappropriately claiming expertise. Trust is also multi-directional, with researchers avoiding potential research participants when they felt it might have lead to an unsafe situation for themselves or others. This was exemplified in the following quote from Respondent 001:

> There have been a few people that I've thought could do [negative things] and would do that, and I've heard have done that. And those are people that I've learned about through my key informants, and I sort of talked to them, but I never made them a formal part of my research, knowing full well what they could do. And it's not that I cared that they would do stuff to me, I was more worried about there being a fallout for other people in the group if I got involved. So there was a little bit of that, like, navigating the waters in the subculture to keep myself safe, but more to keep other people safe.

Building trust was seen as especially challenging when recruiting potential participants through online environments. Online interactions are usually text-based, and some researchers have had trouble in being taken seriously. This was less of a challenge when recruiting cybercrime offenders in-person. However, while recruiting cybercrime offenders in-person was generally seen as more feasible in terms of getting agreement to participate, the main challenge is being able to get access to the specific population that is relevant to the researcher. Researchers often felt that attendees at 'hacker' conferences, for example, were more 'deviant' than criminal, and being finding the relevant people to make introductions to highly skilled offenders was difficult.

Recruiting in online interactions where multiple individuals receive the same message, such as forums, IRC, or email distribution lists, can lead to what was referred to as 'flameballs' (a play on 'snowball' and 'flaming', which refers to 'the hostile expression of strong emotions and feelings' in online communication (Lea et al. 1992, p. 89)). One researcher advised that a call for participants sent on an email distribution list relevant for the population being researched, while being successful in recruiting some subjects, had met with an initial negative reaction. This resulted in an escalation of negative exchanges on the same list. Another experience resulted in forum moderators deleting posts that attempted to recruit participants, and threatening to delete accounts, as they apparently violated the terms of service of the site.

The benefits of being introduced, either through snowballing or other personal introductions, are not having to continually prove credibility, and being put in contact with to hard-to-access participants. However, one researcher felt that cybercrime offenders might prefer to being approached through 'cold' methods, as it reduces the number of people who were aware that they had taken place in

the research, and the type of information that the researcher had about them. This may help explain why most researchers advised that, for cybercrime offenders, snowball sampling is often not a very successful technique. Respondent 005 succinctly explained:

> I've tried to use snowball sampling mostly, and I wouldn't describe it as being necessarily successful, a lot of the hackers I've talked to would maybe connect me with one other person, at most, but even there those connections would fail probably 25 to 30 percent of the time, I don't know how that compares to the offline rates.

Many of the researchers found that those being interviewed will not introduce the researcher to other potential participants, or when introductions do happen, they do not result in an interview. One researcher believed that this was due to risk. Their research subjects may have taken the risk on themselves to speak to them, but can be unwilling to spread that risk to others. There could also reputational risks to someone who had made a misjudged introduction, so not making an introduction feels safer and comes at no cost.

None of the researchers had used referrals from the criminal justice system. Therefore, for accessing cybercrime offenders, none of the researchers had used 'formal' gatekeepers, such as law enforcement or prison staff. However, for many researchers there existed informal gatekeepers, who could either pave their way and introduce them to potential participants, or shut them out, hindering them from being able to access particular groups. Opening the gate was often seen as key in assisting the researcher develop trust within particular communities, or gaining access to closed forums. Similar to snowballing, being a gatekeeper requires a certain level of responsibility, so while it does happen, such relationships are not easily fostered and are relatively rare. One researcher paid a 'professional recruiter', a consultant who had access to a specialised population of interest. The recruiter not only gained access to the participants, but also interviewed them on behalf of the researcher as part of a formal agreement.

One aspect of recruitment involves explaining to potential participants the subject that is being researched. It was evident that researchers have preferred terms that they used, and that the meanings of these terms are not necessarily uniformly shared among other researchers, or their various participants. For example, terms such as 'hacking' and 'hacker' reflect the divergent uses more broadly within society. Researchers had a number of tactics to broach the research subject with their participants, while also allowing for differences in terminology. One researcher described to their potential participants how some people define the research subject, allowing them to respond with their own definition, or (dis)agreement, and therefore progressing the conversation:

> So, I have, my strategy is that I usually defer to them as the experts. So I say, so, you know, a lot of people describe hacking as this, so I'll give like a text book definition, and you can see them roll their eyes, but when you frame it in that way, they don't say, they automatically

> sense that you're a little sceptical of it, so they're willing to give their full definition, and then I allow them to define it, and then our conversation proceeds from there (R001).

Other researchers preferred to have very general definitions, and to let their participants outline what they think cybercrime is, only setting out clear parameters of what they are not including within the scope of their research.

Interviewing

The various ways researchers interviewed their participants, as well as the associated benefits and problems, were explored. Interview methods included interviews face-to-face with the participants, conversations that took place over email, online interactive chat sessions, online video, as well as by phone. While the researchers did not necessarily advocate for one method over another, they recognised that each had their weak and strong points. In-person interviews were generally preferred, but it was acknowledged that they were often more difficult to organise, particularly when participants were not geographically close to the researcher.

One of the benefits of interviewing participants in-person included being able to develop a good dynamic. This was seen as being instrumental in breaking down barriers quicker and easier than methods in which the researcher was physically removed from the participant. It was felt that in-person interviews tended to go for longer, and the participants opened up more. One researcher described in-person interviews as being beneficial as it took the participant outside the type of environment that they are used to, and removed from their offender persona. Online, offenders can wear a mask of anonymity, which is stripped away during an in-person interview. Furthermore, as their normal environments are ones where manipulating information is the norm, it was believed that this could be advantageous for gaining accurate insights, as noted by Respondent 003:

> I think in person interviews, it's kind of easier to make contact with the person, it's a particular form of communication, it's easier to mediate, and it gets hackers slightly away from the kind of habitual sock puppet manipulation of information environments that they're used to.

However, it was recognised that there was also value in online interviews, as it placed the researcher in the communicative environment that the participant was used to. One of the main problems with interviewing in-person was the cost and time-intensive travel that was sometimes required, for the researcher and/or their participants.

A number of benefits of online text communication were identified. First, there is no need to transcribe the interview, which means it takes less time to prepare for analysis, and there is less scope for mishearing what was said, or introducing typographical errors. Also, cybercrime offenders may feel more

comfortable talking to researchers online, as it could be perceived as being less risky than meeting in-person. And finally, for interviews over email, participants are able to take part in the research at a time that is convenient for them.

One of the concerns that researchers had about conversations that took place over email or through interactive chat sessions was they are solely based on text communications. Therefore, these methods miss many cues, such as changes in facial expressions, body language, silences and pauses, or tone of voice, that are used to impart meaning. For example, cues can signal to a researcher that they may want to ask further questions about the topic being addressed, and can identify further avenues of inquiry. Furthermore, Respondent 003 advised that there was the possibility for collusion when interviewing participants through interactive chat sessions, recounting an event where users of an online forum had coordinated their answers when being interviewed by a journalist:

> There's some of the accounts of the Anonymous hackers where [...] they grouped in a chatroom, when they had a journalist, interviewing them, and they all grouped in a separate chatroom and coordinated their answers, to try and effectively just to have fun. [...] I think they were aware, but I don't think that they'd fully taken in that their interview was going to be in a newspaper, but they were just trying to take the piss out of a journalist who they thought was being pompous, I think that's the way that they presented it (R003).

This researcher also advised that it was possible that one individual may operate more than one online presence to manipulate the conversation.

Interviewing which took place by video or telephone was described as mimicking in-person interviews. Audio or video interviews come with the convenience of breaking down geographic boundaries and logistical problems, and being able to hear the voice of the participant. In the case of video communication, the researcher also has access to non-verbal cues. One researcher felt that a downside of video or telephone interviewing, compared to in-person, was that the participant was more likely to want to fit it around their schedule, which sometimes meant changing pre-arranged times and dates, while they were more likely to keep an in-person appointment, and instead reschedule their diary around that commitment.

Researcher Effects

Researchers were cognisant that during the recruitment and interview process, their individual characteristics could have an effect on their participants' behaviour and responses. Respondent 001 noted:

> So, I'm a straight white male in America, there are certain populations that are going to be easier for me to get access to, and certain ways that I can behave that might not be accessible to a black woman, or whoever.

The age and gender of the researcher were discussed as being the most salient characteristics, particularly as participants tend to be younger men. 'Hacker' conferences could be intimidating for women or older attendees, and some researchers who appeared different to the 'norm' had been challenged on their attendance. It was felt that there had been a recent positive shift away from this direction, as the research population aged, and more women became involved.

Self-presentation was also felt to affect the researcher/participant dynamic. As was previously discussed in relation to recruitment, trust is a large factor in having participants agree to be interviewed, as well as provide thoughtful responses. One researcher thought that being open and easy-going, rather than cagey or guarded, was an essential way to present themselves to their potential participants. In some cases, it would be improper to provide an answer to a question, such as wanting to know what someone else had said to the researcher. However, in this type of situation the best response was felt to be reminding the participant that their responses would be kept confidential.

The researcher's institutional affiliation and title may also have an impact on how they are perceived by their participants. One researcher recalled that a potential participant had responded more positively once they realised that they were a faculty member, rather than a graduate student. Another researcher found that their connection to the university's criminal justice program had been a barrier to recruitment, as potential participants had mistakenly believed that they were affiliated with law enforcement.

In addition to the characteristics of a researcher having an effect on the research process, it was noted that the research process itself could have an impact on the population being researched. One researcher felt that through the interview process, researchers could potentially 'interfere with natural behaviour because of what's involved' (R002).

Technical Knowledge

One theme that arose often when speaking with the researchers was whether they should have technical knowledge about cybercrime offending. All those that raised the topic felt that they should, however the reasoning for this varied. One researcher felt that having some technical expertise would be useful when it came to developing trust, as well as being able to probe further into some responses. Respondent 001 noted:

> Don't pretend like you are an expert, and this is going across most things, but most people in cybercrime, to some extent, have a level of technical expertise that's going to be beyond you, and you're not going to be able to guess your way through it, be willing to turn off the ego, and most people are willing to respond to someone who wants to learn. [...]

Another researcher expressed similar sentiments, but also believed that in the process of learning technical skills, a social scientist would develop a better

understanding of the 'norms, values, and social structure' (R002) of the research population.

Being familiar with different ways that potential participants might choose to communicate was an additional reason for acquiring technical knowledge. This included the use of encrypted communication methods. The researcher who raised this also cautioned that researchers who came across as 'a complete technoclutz' (R003) may be viewed with suspicion, and could even become a target for mischief.

Differences By Cybercrime Type

Researchers were conscious of a range of factors that might have an impact on the experience of interviewing cybercrime offender participants. One salient factor is the type of cybercrime the participant is involved in. For example, one researcher found that politically motivated offenders tended to be open to participation, as it was seen as a way of disseminating their message. On the other hand, another researcher noted that there was very little qualitative research involving interviews with active cybercrime offenders from countries with a reputation for being home to particularly virulent cybercriminals. It was speculated that there would be very different challenges in gaining access to these populations.

Researchers noted that some of the more potentially interesting members of the research population may be those who are the most secretive, as they have the most to lose. Conversely, focusing only on the more visible and loudest groups, although easier to access, may mean that the researcher misses crucial pieces of information, or develops a skewed perspective if attempting to generalise findings. This was noted by Respondent 003:

> You can get in a very voluble group of hackers and find out that actually, you know, they haven't really done anything, or hacked anything, they're just, you know, kind of just a very loud group in a forum.

For this reason, many of the researchers used additional qualitative and quantitative methods, to supplement, or instead of, qualitative interviewing. Some researchers also interviewed other specialists who investigate different aspects of cybercrime, such as law enforcement and those that work in the computer security industry.

Ethics

The researchers were asked what they perceived to be the main ethical concerns for cybercrime research. Most researchers felt that the confidentiality and anonymity of their participants and the participants' data as being the main concern. Related to this was the need to protect participants from law enforcement as a result in participating in the research. Additional principal concerns included the potential to cause harm to the participants by causing psychological

distress, as well as researcher safety, and having informed consent information that was set out in clear terms.

Anonymity was believed to be particularly important for cybercrime offender participants, due to the nature of their illegal activities. Furthermore, Respondent 001 noted that 'most of these people, as guarded as they are, have a larger than average online presence' (R001), therefore there was a risk that information about participants could be used to re-identify them indirectly.

Steps that researchers took to try to maintain anonymity included de-identifying interviews at the point of transcription, including deleting any specific information that could be linked back to an individual. Furthermore, while excerpts of interviews were frequently published, researchers did not allow others to have access to the whole transcripts, in case the amalgamation of the data could be used to identify who was spoken to. Some researchers avoided the use of emails to correspond with participants, or used a throwaway email account that was deleted soon afterwards. However, one researcher advised that some of their participants had wanted to be identified, at least by their moniker, as they were active in social movements and political activists. In some cases, potential participants had declined due to the anonymity provisions offered:

> I know I've lost research participants in social movements and hacktivists because I've said, you know, I think you should be anonymous, and they say no, unless I can attach myself to this, then I don't want to talk to you, that's part of my political activism, to do this (R003).

Closely related to anonymity was data security. Researchers used a variety of methods to secure data, including encrypting files, locking disks in filing cabinets, and airgapping computers that held data so they were not connected to the Internet. Some researchers also ensured that they checked the logs of their firewalls, and scanned their computers regularly with anti-virus software. Some researchers deleted data that were no longer necessary for the research. For example, one researcher described how they transcribe the interviews themselves, ensuring that any potentially identifiable information was omitted, then deleted the audio file.

Another concern has arisen following 'open data' requirements from funders, in which researchers are to provide de-identified data to an archival service. The amount of information that qualitative interviews can reveal about a person means that de-identification is problematic. This is particularly challenging with sensitive subject matter such as cybercrime offending. To comply, one researcher specified that the data were not to be made freely available online, however could be viewed in-person at the archives.

The potential for law enforcement to request access to the researcher's data was a concern. Some researchers had experienced this, while the majority had not. For those that had experienced requests, they had come in two forms. The first type of request was general in nature, suggesting that the researcher might have information that could be of use to police, and could they gain access to it:

> So, I've had [...] very kind of general, fishing requests, so, oh you have data on this, we'd like to look at it, can you provide us with a copy. It's not targeted to a particular person, but it's just potentially been of interest to them. And I've been able to just flatly say no, not at all (R006).

The second type of request was more targeted, requesting data about a particular individual. For example, one researcher had been contacted by law enforcement advising that someone who had been arrested was claiming to have been interviewed by them, and could they provide the interview data. The researcher had clearly outlined in the application seeking ethics approval, and the informed consent information provided to participants, that they would only provide data to law enforcement if they were legally required to do so (for example, on receipt of a subpoena), and that all data would be de-identified. Therefore, they had a clear basis for refusing these informal requests for access to the data. Furthermore, as the data was de-identified, the researcher was unable to confirm or deny that they had interviewed the suspect. They made it clear that even if law enforcement had access to the research data, it would not be possible to link the information contained to an individual, and no further requests were received.

Another concern that researchers raised was when they might have a moral, if not legal, responsibility to let law enforcement know about something that they had been told during an interview. One researcher addressed this concern by advising their research participants not to tell them about any activities being planned, or that might have a serious impact, and reminded them of this during the interview if required. Another possible strategy that was suggested was to interview former offenders. Respondent 004 felt that law enforcement realised the importance of academic research in this field:

> Nobody has ever formally requested, and in fact, [...] I've been pretty impressed with [law enforcement] realising the importance of academic research in this area, and understanding that they have their job, which is law enforcement, and I'm doing research, and that research might be useful in the end to them, in a broad sense. [...] And I think it's great that a lot of these agents are open to that, and are aware of academic research, and are happy to help, and they've never once suggested that, you know, I hand over information, or that they would even be interested in that. They're kind of like, you know, I've got my own investigations, I'm busy enough, there's enough cybercriminals out there, I don't need yours.

The researcher whose experience being contacted by law enforcement about a specific person was outlined above had mainly been concerned about the potential impact on their research participant. However, a related concern was the possibility of retaliation if they had provided data. This falls under the concerns about researcher safety. Overall, researchers did not hold grave fears that

their research put them in an unsafe position (although some said they would be concerned about inexperienced researchers with no knowledge of the field conducting interviews).

The researchers used a number of precautions to avoid potential risky situations. For in-person interviews, researchers tended to use public spaces, or areas where others were around, such as cafes, universities, and group spaces in libraries. Some let others know where they were going, and what time they were due to finish. Other tactics included limiting the places where personal addresses and telephone numbers were held, including having an anonymous electoral roll registration. One researcher found the risk assessment process required by their university to be useful, such as thinking about who they would get in touch with in different local contexts if they did experience difficulties.

While no one reported feeling unsafe as a result of their research, some had experienced electronic pranks and attacks. These included accessing a school database and inserting the researcher's phone number in place of the parents for a frequently truant child, so they received a telephone call whenever the student was absent. Another had experienced a denial of service attack, but this had been thwarted by the university's network. Sometimes, the research participants can actually be helpful. A potential participant had contacted one researcher, supplying a list of places where their university may be vulnerable to attack. It appears that the most harm this caused was to the university's security team's weekend, which they spent fixing the vulnerabilities.

For qualitative research, the construction of a narrative, and the presentation of research findings, particularly for large amounts of rich data, is a particular challenge. It was also identified as being an ethical issue, as how research findings are presented can impact the research population. This may also affect the researcher's ability to recruit participants in the future, and even other researchers doing similar work. As well as ensuring that participants could not be identified through information provided in publications, the researchers spoke about ensuring that they were objective as possible when presenting their findings.

The researchers were asked if they provided incentives to participants, and what the ethical issues were in relation to this practice. Most researchers did not provide incentives. Those that had provided incentives did not do so for all their research projects. One pragmatic reason for not providing incentives was due to limited budgets. However, researchers also felt that it could be unethical or have negative impacts on the research process in some situations. One researcher had refused to pay potential participants who had demanded a fee, and found that they had sometimes participated anyway. There was a feeling that turning the research process into a transaction changed the dynamic, and could impact the responses that were received. Researchers were concerned that, particularly for cybercrime offenders, providing incentives created a 'gameable transaction', potentially allowing the researcher to be scammed. Respondent 001 stated 'I want people to be there because they want to talk to me, not because they want to get a reward out of it.'

On the other hand, researchers that had offered gift vouchers found that generally, their participants had been reluctant to accept the incentive. Instead, participants seemed to be incentivised by non-monetary rewards, such as having a medium in which to safely have their voice heard, and having access to the published work. Another ethical issue related to the digital trail that could be used to identify participants, such as linking a gift voucher with the researcher's credit card, and then, for redeeming online, identifying the IP address used, and any delivery address, or reviewing security camera footage for physical redemptions.

One concern to some researchers was the possibility that the interview process may have a negative psychological impact on their participants. One researcher noted that they provided information about counselling services on their information sheet provided to potential participants. While they also advised participants that they were not a psychologist, a number of participants told the researcher that they felt better for having done the interview, and it had felt like a therapy session. However, in one situation the researcher had been concerned after their participant had started crying in the interview. In this case, the participant's offending had negatively impacted their relationship with their family, to the point that they were estranged. The researcher was concerned that they had caused psychological distress, at least temporarily, and felt providing counselling service information had been justified.

Respondent 006 summed up the ethical challenges present in conducting cybercrime research quite succinctly, stating:

> Don't under-estimate the importance of ethical review, they'll help make sure nothing goes wrong, and have your back if it does. But, first and foremost, you need to protect your research participants and ensure no harm comes about as a result of your research.

Publishing

Overall, researchers had mainly positive experiences when it came to publishing their work. There was a feeling that as cybercrime was a relatively new phenomenon, editors were more open to exploratory qualitative methods. The main problems experienced related to peer review, particularly as there has been a rather limited field of potential reviewers. Researchers recounted experiences where they felt reviewers had expertise in relation to qualitative methodologies, but not cybercrime, or conversely, had subject matter expertise, but were biased against the methods used. The latter was particularly experienced when trying to publish in outlets that crossed the computer science/social science divide:

> Because I'm trying to publish both in computer science and in criminology, computer science, they go qualitative, this is rubbish, it's just a bunch of anecdotes, it's no good, when you go to peer review, it's just really really hard (R006).

As well as unfamiliarity with qualitative methods, the computer sciences generally have different publishing styles and methods compared with the social sciences, disseminating their research findings through published conference papers rather than journals or books. However, the social sciences had previously not been very receptive to the unfamiliar terminology and concepts associated with cybercrime, although it was believed that this was improving.

Discussion and Conclusion

Though the body of criminological scholarship on cybercrime research has increased dramatically over the last two decades (Holt & Bossler 2016), there is still a relatively limited corpus of study on cybercrime offenders. The majority of these studies are qualitative, though quantitative scholarship has increased over the last few years. This begs the question as to why qualitative scholarship has slowed, and the experiences of qualitative scholars in the field generally. This study attempted to address these issues through an analysis of a series of six interviews conducted with experienced scholars who have conducted and published qualitative studies of those who have engaged in cybercrime offending.

The findings provide several valuable insights into the process of interviewing cybercrime offenders. Specifically, researchers reported utilizing multiple avenues to access potential interviewees on and off-line. There was some agreement that so-called cold call/contact methods were preferred, but made it difficult to establish trust with potential interviewees. Researchers also felt that conferences had some potential to facilitate connections, though the population was primarily composed of those engaged in deviant, rather than criminal, behaviours. This may limit the potential utility of the findings to understand criminal practices of the cybercrime offenders.

There was, however, agreement that snowball sampling techniques were largely ineffective to obtain a sample of interviewees. This is surprising given the majority of qualitative research on various forms of traditional offending populations utilize snowball sampling techniques to acquire large populations of respondents (e.g. Cherbonneau & Copes 2006, Jacobs 1996, Miller & Decker 2001, Wright & Decker 1997, 1994). Further study is needed to understand the dynamics that affect the development of cybercrime offender studies, and the extent to which this issue may be evident with other forms of online criminal activities. In turn, we may better understand the differences between cybercriminality and real world offending.

Researchers also noted that their attempts to interview active online offender populations may lead them to be targeted for minor forms of cyberattack or compromise. Qualitative researchers have noted the risk of victimization and violence that may accompany attempts to study active offender populations, whether associated with armed robbery (Wright & Decker 1997), drug sales (Jacobs 1996), or gang activity (Miller & Decker 2001). The risk associated with studying cybercrime may not, however, be evident to young scholars who are unfamiliar with research area. Thus, there is a need to better communicate the

ways that scholars need to protect themselves and their institutions in the event of retaliatory attacks or pranks that cybercriminals may perform as a function of their involvement in a research study.

This research also demonstrates the importance of ethical review to avoid harm to the researcher and their participants. Precautions that have been taken to minimise harm have been found to be useful, particularly when it comes to de-identifying data. A related concern is the ever-more common requirement from funding bodies and publishers for 'open data'. There are admirable philosophies in support of open data requirements. However, for sensitive topics such as cybercrime, where qualitative data may hold clues about who it was that was spoken to, however well it has been sanitised, it can be problematic to comply with these requirements while also being in a position to protect participants. In some cases, funders will acknowledge such restrictions, and may have exemptions in place (for example, the UK Engineering and Physical Sciences Research Council has an exemption for personal and sensitive data).

Taken as a whole, this study demonstrates the need for future scholars to continue to use qualitative methodologies to better understand the evolution of cybercriminality. The depth of information that can be developed from robust interview protocols can improve our understanding of the practices of actors, their motivations, and decision-making processes. This sort of research can also improve our understanding of the ways that the practices of offenders evolve, and differ by place (e.g. Holt et al. 2017). Without such inquiry we will be unable to move beyond the limited results that can be produced from quantitative studies of college student samples and honeypot data that provides limited insights into offender behaviour (see Holt & Bossler 2016).

Funding

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) [grant EP/M020320/1, to A.H.] for the University of Cambridge, Cambridge Cybercrime Centre.

Bibliography

Berg, B. L. (2007), *Qualitative Research Methods for the Social Sciences (6th ed.)*, Boston: Pearson Education, Inc.

Bossler, A. M. & Burruss, G. W. (2011), *The general theory of crime and computer hacking: Low self-control hackers*, Information Science Reference, Hershey, pp. 38–67.

Brenner, S. W. (2010), *Cybercrime: Criminal Threats from Cyberspace*, Santa Barbara: ABC-CLIO.

Business Software Alliance (2016), '2016 BSA Global Software Survey: Seizing Opportunity Through License Compliance'.
URL: *http://globalstudy.bsa.org/2016/index.html*

Cherbonneau, M. & Copes, H. (2006), ''Drive it like you Stole it': Auto theft and the illusion of normalcy', *British Journal of Criminology* **46**(2), 193–211.

Christie, N. (1997), 'Four blocks against insight: Notes on the oversocialization of criminologists', *Theoretical Criminology* **1**(1), 13–23.

Décary-Hétu, D. & Dupont, B. (2012), 'The social network of hackers', *Global Crime* **13**(3), 160–175.

Diamond, B. & Bachmann, M. (2015), 'Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology', *International Journal of Cyber Criminology* **9**(1), 24.

Dupont, B., Côté, A.-M., Savine, C. & Décary-Hétu, D. (2016), 'The ecology of trust among hackers', *Global Crime* **17**(2), 129–151.

Franklin, J., Paxson, V., Perrig, A. & Savage, S. (2007), An inquiry into the nature and causes of the wealth of Internet miscreants, *in* 'Proceedings of the ACM SIGSAC Conference on Computer and Communications Security'.

Furnell, S. (2002), *Cybercrime: Vandalizing the Information Society*, London: Pearson Education Limited.

Garfinkel, H. (1967), *Studies in Ethnomethodology*, New York: Prentice Hall.

Guest, G., Bunce, A. & Johnson, L. (2006), 'How many interviews are enough?: An experiment with data saturation and variability', *Field Methods* **18**(1), 59–82.

Hammersley, M. & Atkinson, P. (1983), *Ethnology: Principles in Practice*, New York: Tavistock.

Higgins, G. E. & Marcum, C. D. (2011), *Digital Piracy: An Integrated Theoretical Approach*, Durham: Carolina Academic Press.

Holt, T. J. (2007), 'Subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures', *Deviant Behavior* **28**(2), 171–198.

Holt, T. J. (2010), 'Examining the role of technology in the formation of deviant subcultures', *Social Science Computer Review* **28**(4), 466–481.

Holt, T. J. (2013), 'Exploring the social organisation and structure of stolen data markets', *Global Crime* **14**(2-3), 155–174.

Holt, T. J. & Bossler, A. M. (2016), *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*, Oxon: Routledge.

Holt, T. J., Bossler, A. M. & May, D. C. (2012), 'Low self-control, deviant peer associations, and juvenile cyberdeviance', *American Journal of Criminal Justice* **37**(3), 378–395.

Holt, T. J., Freilich, J. D. & Chermak, S. M. (2017), 'Exploring the subculture of ideologically motivated cyber-attackers', *Journal of Contemporary Criminal Justice* .

Holt, T. J., Smirnova, O., Chua, Y. T. & Copes, H. (2015), 'Examining the risk reduction strategies of actors in online criminal markets', *Global Crime* **16**(2), 81–103.

Holt, T. J., Smirnova, O. & Hutchings, A. (2016), 'Examining signals of trust in criminal markets online', *Journal of Cybersecurity* **2**(2), 137–145.

Hutchings, A. (2013*a*), *Hacking and fraud: Qualitative analysis of online offending and victimization*, CRC Press, Boca Raton, pp. 93–114.

Hutchings, A. (2013*b*), *Theory and Crime: Does it Compute?*, PhD Thesis, Griffith University, Brisbane.

Hutchings, A. (2014), 'Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission', *Crime, Law & Social Change* **62**(1), 1–20.

Hutchings, A. & Chua, Y. T. (2017), *Gendering cybercrime*, Taylor & Francis Group, Oxford, pp. 167–188.

Hutchings, A. & Clayton, R. (2016), 'Exploring the provision of online booter services', *Deviant Behaviour* **37**(10), 1163–1178.

Hutchings, A. & Clayton, R. (2017), Configuring Zeus: A case study of online crime target selection and knowledge transmission, *in* 'APWG Symposium on Electronic Crime Research (eCrime)'.

Hutchings, A. & Holt, T. J. (2015), 'A crime script analysis of the online stolen data market', *British Journal of Criminology* **55**(3), 596–614.

Jacobs, B. A. (1996), 'Crack dealers and restrictive deterrence: Identifying narcs', *Criminology* **34**(3), 409–431.

Jordan, T. & Taylor, P. (1998), 'A sociology of hackers', *The Sociological Review* **46**(4), 757–780.

Kinkade, P., Bachmann, M. & Bachmann, B. (2013), *Hacker Woodstock: Observations of an off-line cyber culture at the Chaos Communication Camp 2011*, Carolina Academic Press, Raleigh, pp. 27–53.

Lea, M., O'Shea, T., Fung, P. & Spears, R. (1992), *'Flaming' in computer-mediated communication: Observations, explanations, implications Contexts of Computer-Mediated Communication*, Hertfordshire: Harvester Wheatsheaf.

Levy, S. (1984), *Hackers: Heroes of the Computer Revolution*, Garden City: Anchor Press/Doubleday.

Lusthaus, J. (2012), 'Trust in the world of cybercrime', *Global Crime* **13**(2), 71–94.

Maimon, D., Alper, M., Sobesto, B. & Cukier, M. (2014), 'Restrictive deterrent effects of a warning banner in an attacked computer system', *Criminology* **52**(1), 33–59.

Meyer, G. R. (1989), *The Social Organization of the Computer Underground*, Master of Arts, Northern Illinois University, DeKalb.

Miller, J. & Decker, S. H. (2001), 'Young women and gang violence: Gender, street offending, and violent victimization in gangs', *Justice Quarterly* **18**(1), 115–140.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S. & Voelker, G. M. (2011), An analysis of underground forums, *in* 'Proceedings of the ACM SIGCOMM Conference on Internet Measurement, Berlin'.

Patchin, J. W. & Hinduja, S. (2016), *Bullying Today: Bullet Points and Best Practices*, Thousand Oaks: Corwin Press.

Schell, B. H. & Dodge, J. L. (2002), *The Hacking of America: Who's Doing It, Why, and How*, Westport: Greenwood Publishing Group Inc.

Shaw, E., Ruby, K. G. & Post, J. M. (1998), 'The insider threat to information systems: The psychology of the dangerous insider', *Security Awareness Bulletin* **98**(2), 1–10.

Silverman, D. (2000), *Doing Qualitative Research: A Practical Handbook*, London: Sage.

Steinmetz, K. F. (2015), 'Craft(y)ness: An ethnographic study of hacking', *British Journal of Criminology* **55**(1), 125–145.

Taylor, P. (2001), *Hacktivism: In search of lost ethics?*, Routledge, London, pp. 59–73.

Taylor, P. A. (1993), *Hackers: a case-study of the social shaping of computing*, PhD Thesis, University of Edinburgh.

Taylor, P. A. (1999), *Hackers*, London: Routledge.

Thomas, D. (2002), *Hacker Culture*, Minneapolis: University of Minnesota Press.

Tokunaga, R. S. (2010), 'Following you home from school: A critical review and synthesis of research on cyberbullying victimization', *Computers in Human Behavior* **26**(3), 277–287.

Turgeman-Goldschmidt, O. (2007), 'Meanings that hackers assign to their being a hacker', *International Journal of Cyber Criminology* **2**(2), 382.

Wall, D. S. (2001), *Maintaining order and law on the Internet*, Routledge, London, pp. 167–183.

Wright, R. & Decker, S. (1994), *Burglars on the Job: Streetlife and Residential Break-ins*, Boston: Northeastern University Press.

Wright, R. & Decker, S. (1997), 'Creating the illusion of impending death–armed robbers in action', *Harry Frank Guggenheim Review* **2**, 10–18.

Yip, M., Webber, C. & Shadbolt, N. (2013), 'Trust among cybercriminals? Carding forums, uncertainty and implications for policing', *Policing and Society* **23**(4), 516–539.