Crime Law Soc Change (2014) 62:1–20
DOI 10.1007/s10611-014-9520-z

Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission

Alice Hutchings

Published online: 10 June 2014

Abstract This paper examines a predominantly Australian sample of computer crime offenders involved in fraud and/or unauthorised access. This paper focuses on the extent to which offenders are involved in organised crime, the nature of the relationship between co-offending, initiation and knowledge transmission, and how the online environment facilitates organised crime and co-offending. This qualitative analysis draws from interviews with self-identified offenders, law enforcement officers who investigate these offenses, and court documents, providing a unique understanding of organised crime involving computer systems.

Introduction

Due to the hidden nature of the population who engage in offending involving computer systems, it is often unclear to what extent such activities are attributable to organised crime syndicates, sole operators, or other groups [1]. Felson [2] states that criminologists, along with the mainstream media, tend to overstate the extent that commonplace crimes are organised. However, research evidence indicates that computer crime offenders do work and collaborate together to some extent [3, 4], both on- and offline [5]. Jordan and Taylor [6] suggest that the hacker community is characterised by a fluid, informal and loosely structured membership, with a high turnover.

The computer crimes that are considered in this paper are those that compromise data and financial security. These offences affect the public greatly, including the direct cost of victimisation, emotional harm, and associated costs, such as banks passing on losses through higher fees. Many computer crimes are not reported to authorities [7], and of the small percentage of computer crimes that are reported, less than 20 per cent are likely to result in criminal charges [8]. Whilst under-reporting and under-prosecution may be typical of most crime types, computer crimes are notoriously difficult to bring to prosecution, with problems including inadequate legislation, lack of evidence, and jurisdictional difficulties [8, 9].

A. Hutchings (✉)
University of Cambridge, Computer Laboratory, William Gates Building, 15 JJ Thomson Avenue, Cambridge CB3 0FD, UK
e-mail: ah793@cl.cam.ac.uk

Nature of unauthorised access and fraud

The application of the verb 'hacking' to a variety of actions reflects advances in technology, the digitisation of data, and how behaviours that have been pursued by computer enthusiasts have been criminalised. These days, the term is applied to a variety of pursuits that compromise computer and data security [10, 11]. Both hacking and cracking refer to gaining unauthorised access to a computer system. The distinction between the terms is that "cracking" is sometimes used to refer to having another criminal motive once access has been gained [10, 11], for example, obtaining confidential information, including credit card details, or "defacing" websites. Here, the term cracking is not to be confused with software cracking, which refers to the removal of copyright protection from commercially available software to enable it to be copied and installed without authorisation ("pirated") [12]. Hacking includes the use of social engineering techniques as well as technical methods to gain access to computer systems. Misuse of legitimate access to a computer system, or insider abuse of access, occurs when hackers abuse the trust they have been given, such as an employee or contractor accessing or altering an employer's data [13]. The definition of hacking for this research is gaining unauthorised access to a computer system with or without a further criminal motive, or misuse of legitimate access to a computer system.

Computer fraud refers to dishonestly obtaining a benefit, or causing financial loss, through the use of computer systems. While computer frauds are not necessarily conducted online, the online environment does provide a forum for a large variety of computer frauds, such as identity fraud, card-not-present payment fraud, internet auction fraud, investment fraud, advance fee fraud and phishing. These may be conducted using a variety of mediums, including e-mail, social networking sites, such as chat or dating websites, and online trading sites [10, 14].

In addition, there is a relationship between the two types of offences considered in this study as unauthorised access may facilitate fraud. For example, obtaining unauthorised access to data held in servers could result in the data obtained being used to create fabricated credit cards, or for use in card-not-present transactions. Web forums provide a marketplace for malware (malicious software) and stolen data, as well as services such as the distribution of spam, web hosting, and proxy services, which may be used for fraudulent purposes [15–18]. Similarly, compromised computer systems may be connected to botnets and used to disseminate spam promoting, for example, fraudulent pharmaceuticals, work from home scams, or various advance fee frauds. Botnets are networks of 'zombies'; compromised computers that have been infected with malware so that they can be controlled remotely for purposes such as orchestrating denial of service attacks, sending spam, facilitating phishing and click fraud, conducting brute force attacks, and disseminating malware [19].

Organised computer crime and co-offending

The United Nations *Convention Against Transnational Organized Crime* ('the Convention') [20] provides the following definition of an 'organised criminal group':

> "Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of

> committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit.

A 'structured group' is defined as [20]:

> "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

A 'serious crime' is defined as an offence that attracts a penalty of at least 4 years imprisonment [20]. However, the Convention does not define a 'period of time', which could potentially be ambiguous in its application.

There has been much attention on online marketplaces and the underground online economy, in which organised cybercriminals may trade goods and services, as well as recruit skills. As, by definition, organised crime offenders are offending with others, they thus require a communication platform. Analysing these communication channels provide a rich source of data about offenders and their activities. For example, Holt and Lampke [17] analysed publicly accessible web forums, while Franklin et al. [16] analysed the black market activity on Internet Relay Chat (IRC) channels. Unlike Holt and Lampke [17] and Franklin et al. [16], Motoyama et al. [18] analysed black market forums that included private, as well as publicly accessible, messages. Holt and Lampke [17] found that the majority of goods offered for sale were dumps of stolen credit card data and banking credentials. Franklin et al. [16] found that advertising goods, such as financial data and harvested email address lists for spamming, and services, such as money laundering, was the most common type of market activity. Goods or services were promoted for sale, or as wanted advertisements. All three studies found that verification of traders' reputations on such communication channels distinguished trustworthy sellers from those who do not uphold their end of a deal, who are generally referred to as 'rippers' [16–18].

However, making inferences from these studies about organised crime offenders may result in an ecological fallacy, as these marketplaces are also frequented and utilised by sole offenders, as well as those who may actively participate in discussions but not participate in illegal activities themselves. Furthermore, organised crime groups may not necessarily operate in online marketplaces.

Meyer [4] conducted what appears to be one of the first qualitative studies relating to hackers. In 1989 computer networks and BBSs were active, however the world wide web as we know it had not yet been launched. BBSs, or bulletin board systems, are personal computers that allow users to dial in using a computer and modem. BBSs are similar to online forums held on the internet, whereby users can leave messages for each other, as well as download and upload software [3]. Meyer [4] found that while offenders committed their crimes by themselves, they associated with others to discuss matters of common interest, such as performance techniques, news and problem solving. He therefore concluded that offenders have an extensive online social network.

Choo and Smith [21] differentiate between organised crime groups that engage in computer crime to facilitate their traditional activities; those that operate solely in the

online environment; and 'organised ideologically and politically motivated cyber groups' [21]. Organised crime groups that engage in computer crime to facilitate their traditional activities are primarily motivated by financial gain. Activities that traditional organised crime groups are reportedly involved in include narcotics and human trafficking, nuclear smuggling, extortion, prostitution, illegal bookmaking, unlicensed money lending, identity crimes, frauds and scams, money laundering, extortion, selling counterfeit drugs, software piracy and credit card fraud [21]. Many of these offences can easily be carried over to the cyber domain, presumably quite successfully for the criminal enterprise. For example, extortion of gambling and pornography sites has reportedly been conducted by threatening distributed denial of service attacks [22], while scams such as phishing attacks can reach a wide audience for little cost [23]. Denial of service, or DoS, attacks, involve overloading a website or computer system so that legitimate access is blocked. When using botnets this is known as a distributed denial of service, or DDoS, attack [23]. In addition to carrying out online offences themselves, traditional organised crime groups may employ professional hackers for their specialised skills, or engage money mules to launder funds, with our without their knowledge of the illegalities involved [22].

Organised crime groups that operate solely in the online environment, or 'organised cybercriminal groups' [21] are usually less structured, smaller, more likely to operate across borders, and are less hierarchical than traditional syndicates [21]. Members are also highly technically proficient, and, according to Choo and Smith [21], are likely to band together only for a limited time so as to carry out their specialised tasks. Members are also likely to know each other in the online environment only, meeting and planning with each other using the internet. In common with traditional organised crime groups, organised cybercrime groups are primarily motivated by financial gain, although groups dedicated to the dissemination of child exploitation material also fit within this typology. Compared to organised crime groups that engage in cybercrime to facilitate their traditional activities, organised cybercrime groups are more likely to be involved in targeted, rather than opportunistic, attacks.

According to Choo and Smith [21], organised crime groups of ideologically and politically motivated individuals are broadly defined into two categories depending on their specific motivation: terrorist organisations and those relating to hactivism. Critical infrastructure, such as electricity, water, communications, air traffic control and financial systems are perceived as being the targets for terrorist organisations [23]. However, while there have reportedly been no terrorist attacks using hacking abilities to target critical infrastructure to cause widespread damage [24], online crime, such as frauds, may be committed to fund terrorist organisations [22, 25, 21]. Choo and Smith [21] also point out that terrorists may use information freely available on the internet to plan their attacks, such as how to build bombs, as well as the use of legitimate information such as satellite imagery to map out terrain. Websites maintained by terrorist organisations may distribute propaganda, solicit funding and recruit members by reaching an international audience [22, 26, 21]. The internet can also be used for communication within terrorist organisations, which may extend to 'psychological warfare', which refers to deceptive communication to give the impression that an attack is imminent, therefore distracting law enforcement and intelligence services from other activities [23]. Hacktivists are traditionally motivated by ecological, political and ethical activism [27–30]. Hacktivists typically protest against perceived unfairness by conducting DoS

attacks against their targets (e.g. Anonymous) or releasing confidential information (e.g. Wikileaks).

Therefore, Choo and Smith's [21] typologies can be differentiated by a combination of factors, including the motivations of the offenders (e.g. profit-driven versus ideological), the types of behaviours undertaken (and skills required) to achieve these aims, as well as whether or not the actors are also involved in, or employed by those involved in, offline organised crime activities.

Research questions

This research examines a sample of computer crime offenders to examine their involvement in organised crime and co-offending. Therefore, the areas explored in this study include:

- To what extent are computer crime offenders involved in organised crime?
- How do computer crime offenders become involved in crime?
- What role do co-offenders play in knowledge transmission?
- How does the online environment facilitate organised crime and co-offending?

Method

A qualitative research design was selected for its ability to provide a deep understanding of the offending behaviour. Qualitative research captures nuances and provides richness to data that may not otherwise be quantifiable. In addition, qualitative research can be undertaken when the ability to meet the quantitative requirements in relation to obtaining a large, randomly selected sample size are less than ideal [31].

Computer crime offenders involved in unauthorised access and/or fraud were the unit of analysis for this research, which involved three studies. The first study was a qualitative analysis of court documents, in particular sentencing remarks and court judgments relating to prosecutions and extraditions involving computer fraud and unauthorised access in Australia, the United Kingdom, the United States, and New Zealand. A systematic review of legal databases was conducted to identify relevant cases. Only documents available on public databases were identified and retrieved. Although this resulted in a selected sample, it provides an illustration to explore the issues pertinent to this research. Of the 54 cases included in this study, 12 were female offenders, while the remaining 42 were male. The mean age of the sample for study one was calculated using either the age at the time of offending, where known (n=21), or the age at the time of the court appearance, where known (n=15). The mean age was 30.6 years, ranging from 16 to 48 years (SD=8.6). When sorted by type of offence, 44.4 % (n=24) had committed a fraud offence, 27.8 % (n=15) had committed a hacking offence, and the remaining 27.8 % (n=15) had committed offences that could be classified as both hacking and fraud.

As well as outlining the facts of the matter, the nature of the harm caused, and details about the lead up to the offence(s), the documents typically included factors of

relevance when sentencing offenders, including mitigating and aggravating circumstances. Within Australia sentencing statutes are applicable in each jurisdiction that set out what these factors may be. These typically include the offender's criminal history, their level of remorse, their attitude and the level to which they cooperated with the criminal justice system, the effect that various punishments may have on the offender and the family, such as the ability to maintain employment [32].

Study two consisted of interviews with law enforcement officers within computer crime or fraud specialist units from four policing agencies in Australia, namely the Australian Federal Police, the Queensland Police Service, Western Australia Police, and Victoria Police. These interviews focused on officers' experiences with, and perceptions of, offenders who have been identified by the criminal justice system. The interviews were one-on-one, open-ended, and semi-structured.

Participants were asked about their experiences with offenders within the last 5 years. It was expected that recall would be fairly accurate given the limited number of cases available. It was considered appropriate to gather information using law enforcement officers as third parties due to the nature of the offender population, which is generally considered to be hard to access. Gathering data from third parties is consistent with prior research relating to offenders, for example, the Cambridge Study in Delinquent Development, which included interviews with parents and questionnaires completed by teachers [33]. The 15 law enforcement officers interviewed in study two included 14 males and one female. The interviews ranged from 32 min to one hour and 16 min in length, with an average time of 51 min.

Study three consisted of face-to-face interviews with active and former offenders. Participants were recruited within Australia using snowball sampling, a non-random, purposive method. Initial recruitment used informal networks. Those known to the researcher who worked and/or studied in the IT industry were encouraged to source participants. The benefit of such an approach is that such recruiters are able to assure potential participants that the researcher is legitimate [34]. Participants were also encouraged to approach additional potential participants. Recruitment consisted of advising potential participants about the research and what it entailed and providing the contact details of the researcher. In this way, participants self-identified as being members of the target population and because the participants had to contact the researcher, they were in control of the amount of personal information that they provided. Participants were offered a gift voucher for a national chain of electronic gaming stores as a thank you for being interviewed.

Studying active offenders has many benefits over studying a prison sample as active offenders may be characteristically different in their frequency, nature and severity of offending, as well as their skill levels and abilities. Supporting this, Sutherland and Cressey [35] state:

> Those who have had intimate contacts with criminals "in the open" know that criminals are not "natural" in police stations, courts, and prisons, and that they must be studied in their everyday life outside of institutions if they are to be understood… In this way, [s]he can make observations on attitudes, traits, and processes which can hardly be made in any other way. Also, [her] observations are of unapprehended criminals, not the criminals selected by the processes of arrest and imprisonment.

Participants were first asked if they had been involved with hacking, computer fraud, or both, and whether they identified themselves as current or former offenders. The answers to these questions allowed the remainder of the interview to be tailored to the participant. For example, former offenders were asked additional questions about why they ceased offending, as well as what their situation was at the time that they were offending. The interviews were one-on-one, open-ended, and semi-structured, based on a modified version of McAdams' [36] *Life Story Interview,* with additional questions covering relevant topics.

It is possible that the data obtained are not an accurate depiction, i.e. that the information provided is not truthful. This may occur because the participant had trouble with recollection, misinterpreted the question or preferred not to give an honest answer. It may be asked how the researcher can believe the accounts of those who, due to the subject matter, may be untrustworthy. However, Wright and Bennett [37] have examined the literature relating to the truthfulness of accounts given by offenders during qualitative interviews. They conclude that much information provided during interviews is consistent with official records, and that, after agreeing to be interviewed, offenders perceive lying to be pointless as they may as well not have consented at all. In addition, during the interviews with active and former offenders, time was spent checking for distortions and exploring the participants' responses with them to seek clarification. Some questions were also asked in more than one way in order to compare the responses.

Ethical clearance was granted for this research, and the studies were conducted in accordance with the approved protocols. A number of potential ethical considerations arose out of the research design, including potential harm to participants and the researcher, researching illegal behaviour, maintaining confidentiality and anonymity, and keeping data secure. As the interviews in study three covered aspects such as home life, upbringing, friendships, social activities, etc., there was the potential for some level of psychological harm to participants (for example, remembering or talking about a bad experience). To minimise this risk participants were provided with the details of freely available psychological services that they could contact. Participants were also able to withdraw from the study at any time. There was also the potential risk of harm to the researcher while interviewing participants face-to-face. Therefore, interviews were conducted in a public area, and the researcher's advisor was informed when interviews were to take place and when they had been concluded.

The researcher determined an appropriate course of action if faced with information concerning offences that were in progress, offences that were intended to be committed, or if court ordered or subpoenaed to provide evidence about participants. While the research involved people that had engaged in illegal behaviour it did not relate to the specifics of individual events, nor was it intended to expose criminal behaviour. However, there was the potential for the researcher to be told about current illegal activities or those that involve serious harm. While the researcher was not under any contractual, professional or legal obligation to disclose illegal behaviour, there was a moral question to consider relating to elective disclosure. To mitigate this risk to participants, they were informed at the beginning of the interview that they should not divulge any current activities, and they would be reminded of this if they begin to do so.

There was a possibility that the researcher may be compelled by law enforcement or a court to disclose information. However, as the data were not collected in an identified form and remained anonymous the researcher could not disclose any identifiable

information about any participants if such a circumstance arose. This means that it would have been difficult for a law enforcement or other agency to identify that data with an individual. This technique is consistent with other research relating to self-reported criminal behaviour [38].

Of the seven offenders who participated in study three, five identified as hackers and two as both hackers and online fraudsters. Five were active offenders and two identified themselves as former offenders. All participants were male, aged between 18 and 49, with a mean age of 29.7 years at the time they were interviewed (SD=10.7). The age they reported that they had started hacking ranged from 11 to 25 years (M=16.6, SD=5.2). The interviews ranged in length from 45 min to two hours and 18 min, with a mean time of one hour and 39 min. With the researcher vouched for, the participants were cooperative and obliging. They appeared to be truthful and forthcoming during the interviews. All the interviews were conducted in public places chosen by the participant, typically a coffee shop.

All interviews were transcribed verbatim, with any identifiable information replaced with pseudonyms. Coding of the data was mainly 'concept-driven' [39], in that the codes used primarily arose from the literature. However, 'data-driven coding' or 'open coding' [39] was also utilised when other key themes arose during the analysis. Notes were made about all the possible meanings of each code to enable a more reliable and stable coding system and to avoid 'definitional drift' [39]. NVivo, a qualitative data analysis program, was used to classify and sort the data.

Results

Question 1: To what extent are computer crime offenders involved in organised crime?

Of the 54 cases in study one, 11 (20.4 %) operated within a group of at least three offenders. While the number and role of offenders was not always known, the largest group included at least 23 offenders in total. One additional case was suspected to have involved co-offenders, but the number potentially involved and the role that they had played was unknown (Case #26, male fraudster, age unknown). Co-offenders were not necessarily locally based, and coordination across jurisdictions was common:

> In addition, from time to time, you sent money to people who were not apparently family in Nigeria and others, including … Benin, … Singapore, … Ivory Coast, … Ghana, … Malaysia and … Thailand… Clearly, you did not act alone, but rather in concert with others (Case #18, male fraudster, aged 29 at time of offence).

Of the seven participants interviewed in study three, three (42.9 %) had offended with others in groups of three or more (Interview #1, male hacker and fraudster, aged 27; Interview #4, male former hacker, aged 49; Interview #5, male hacker and fraudster, aged 22). For example:

> Oh, it was only, there was only about four of us. That I remember particularly. I mean, there were, yeah, there was a whole group of people that we sort of knew, but it was pretty, it was pretty loose (Interview #4, male former hacker, aged 49).

The number of people that offenders worked and communicated with varied from small groups of one or two others, up to hundreds:

> Probably hundreds, two hundred people. Cause I was a member of three different trading groups… Ah, there's one that I will see when I'm on a holiday that I'm going on soon. Or two. None of the rest are close friends… Acquaintances, yeah (Interview #1, male hacker and fraudster, aged 27).

All of the law enforcement officers in study two advised that they had been involved in investigations that included aspects of organised crime:

> Oh definitely, the big organised ones that come in that run some of the serious money making schemes are a business. They are a top-down business and, you know, they're well, the information that you see, it's out there in a lot of papers and stuff as well, they are sort of setup like a business. They have their own sectors and little areas, they know what they're doing and have a certain job, and they outsource certain things, like if one part of it can't do, you know, x, they will outsource to another group that can do that (Law Enforcement Officer #14).

> More the organised crime aspect. They recruit, recruit people with skills in certain areas and they sort of use them to commit the crime on their behalf… Um, I really wouldn't put it past organised crime to control a few forums themselves just from a recruitment point of view (Law Enforcement Officer #5).

However, it was noted that when offenders worked together it was not always considered to be organised crime, particularly with younger, less experienced offenders. Sometimes it was 'just dudes hanging out':

> Oh definitely, it's just dudes hanging out… Um, well, for, just because it's fun, it's something to do, because they get on and they chat and it is, a lot of the time, it is a social network as well. You know, these other guys, or guys and girls, whatever it is, that you find online have similar interests to what you do, be it, you know, hacking websites, stealing credentials, whatever it is, you start talking to them and you get on there and chat to them as you would to your friends. And as you chat to them you will, you know, you'll be chatting about your day as well as about whatever, you know, websites you've found that are vulnerable to whatever exploits or how many credit cards you've got, that sort of stuff. It's just a social thing… Um, I've never personally seen them in the same location but, it makes total sense that they would, you know, you go over to your mate's place to play video games don't you, so you probably go to your mate's place to hack… It is the same thing, you know, they don't see it as a criminal activity per se, it's just having fun with your mates (Law Enforcement Officer #14).

> We see them as young as 13, 14… But they tend to be just inquisitive I suppose, for want of a better word. They're involved in gaming sites or social networking sites talking to people all over the world, other kids, and they share information and some of that ends up being criminal information. They commit other

> offences, hack each other's accounts, commit online fraud and also, we even have kids sharing botnet remote control servers with each other. So, they might attack the school, attack the school website. So, yeah, it can start quite young. That's just the nature of the internet I think, the information sharing's out there, and if you're inquisitive and you're interested in that sort of thing, it tends to be a bit of a cool interest and a thing for the kids online to dabble in without ever thinking about the consequences, that they are actually committing a criminal offence… Yeah, kids. So in terms of, a lot of kids get involved with keylogging on public computers, so they can do internet banking rips and stuff like that. They tend to share stuff offline with mates, you know, physically passing thumbdrives with, um, details on, either data from keylogs or, you know, information on how to do certain things online. But, um, we've seen instances where kids sort of share that information. You know, share information on vulnerabilities on websites and things like that amongst each other (Law Enforcement Officer #2).

Question 2: How do computer crime offenders become involved in crime?

Of the 11 cases in study one that involved an offender that had offended in a group of at least three or more, all fit within Choo and Smith's [21] 'traditional organised criminal groups' typology. All of these were motivated by financial gain, and seven did not necessarily require high-level skills in order to carry out the offence. Not all of the offences took place solely online, and some offenders were also facing charges for other crimes, such as drug trafficking (Case #8, male fraudster, age unknown). The following example describes a case in which property offences escalated into identity crimes:

> She was a member of an organised group who had acquired or stolen items of identity, manipulated computer records or processes, and represented identity and acquired, or attempted to acquire, financial advantage through the knowledge and documentation possessed (Case #39, female hacker and fraudster, aged 28 at time of offence).

The offender in this case claims to have been pressured by others to commit the offences:

> Most of the crimes, if not all, involved accomplices… She claimed that she had been stood over by someone. She had only received between $1,500 and $2,000 for her own use, the rest going to the other person… She described herself as "the button presser", doing what other people told her to do (Case #39, female hacker and fraudster, aged 28 at time of offence).

The results for study two were varied, with three law enforcement officers describing matters that fit within the 'traditional organised criminal groups' typology, seven describing matters fitting within the 'organised cybercriminal groups' typology, and one describing both typology one and two. Just one participant described organised crime that would fit within the typology

'organised ideologically and politically motivated cyber groups'. The three remaining law enforcement officers did not provide enough detail to classify the organised crime that they were aware of.

It was identified that organised crime groups that operated solely in the online environment used online portals in order to recruit the services of other offenders for specific tasks, and that the players did not necessarily know who else is involved:

> In fact, you can go to some of these channels where they share online and trade, but there's a genuine sort of underground economy in that they bandy it around. If I wanted to get involved in, whatever the case may be, if I wanted to get involved in phishing a bank or something that everybody knows, but I don't know how to write the actual page, someone will write it for me online and reasonably cheaply I can ask them to do it. And if I'm not too sure how to host it, they'll host it for me on one of the bots for a part payment. And if I don't want to get involved in cashing out and receiving the money because that's a little bit too risky, there's guys doing cash out services all over the world who you can talk to and meet online. There's a whole community out there of thousands of people that can solve any one of the problems online or make up any link of the chain if you don't want to get involved […] And it's when they start working together like that detection's much harder. And of course the internet being what it is these guys can score worldwide. They don't necessarily need to be local. And in fact, it would be uncommon, it would be, if not, you'd never seen all the components occurring in this state (Law Enforcement Officer #1).

Working with others like 'links in a chain' not only made the work easier for offenders, but also assisted offenders in evading detection:

> Um, probably because it's harder to track, you know, money is going all over the place, if one person puts the ad, another person takes the money and forwards it, another person receives it, the more links in the chain there are, the harder it is to get caught. And put it all together, and be held responsible for the entire fraud. So I think it's a mitigation, circumstance, and it's also a spreading of the workload. Because there is a bit of workload involved in online fraud. You know, you've got to create ads, you've got to set up bodgy names, set up bodgy accounts, you've got to set up bank accounts, you've got to arrange money mules to transfer money around, that's if you don't want to get caught. There's a fair bit of organising involved, so I think many hands make light work, and it's also it's a mitigation of the workload and also a mitigation of getting caught and culpability (Law Enforcement Officer #8).

Law enforcement officers advised that online organised crime groups that specialised in fraud also shared victims to perpetuate their activities:

> [T]he West Africans and Eastern Europeans […] they tend to be networked to a fairly high degree in not only sharing information but sharing victims. So shunting victims on, sharing information that victims might give them, so you can create further profiles. But just bringing each other into the offence, so you

> might, you might get a victim online, […] and you might work with that victim up to needing a solicitor in London, then you would contact me and get me caught into the deal as the solicitor, and we all sort of share the takes from that […] And you end up in the situation where victims are being scammed by multiple networked groups, where they've either overplayed or sold them or they needed someone to come in (Law Enforcement Officer #2).

> If you fall for one scheme you'll fall for another. And they'll sell it amongst each other. And there's people who are specialised in various parts of the scam. Or, um, people specialise in victims who have run out of money, and they have a special skill for getting even more money out of them, so they might buy the victim off another offender who's taken the scam so far (Law Enforcement Officer #9).

By crossing jurisdictions offenders were also able to complicate matters for law enforcement:

> But if you want to successfully, be more successful in getting involved in online fraud or financial crime online, you want to specifically avoid your local jurisdiction because you can complicate matters considerably (Law Enforcement Officer #1).

> Yeah, you know, multiple jurisdictional makes it, unfortunately, police across the world haven't caught up, you know, criminals don't have jurisdictional boundaries, we do, and we operate within them. And they know that, so, they know that a way to avoid getting caught is to distribute the network and distribute the offences across jurisdictional boundaries (Law Enforcement Officer #8).

One officer indicated that while organised crime groups accounted for the vast majority of computer crimes, they were not often detected and prosecuted, which could explain why none of the cases in study one fit the organised crime groups that operate solely in the online environment typology:

> Um, [organised crime] would account for the vast majority of crime, it would not be as common as the detection and prosecution of them, that'd be far less […] But they're still making up the lion's share of the offending. They're just not so well represented on the prosecution. Not that we're not looking at them, we do (Law Enforcement Officer #1).

In contrast to study one, all of the participants in study three would be classified as fitting into Choo and Smith's [21] typology 'organised cybercriminal groups'. One offender described how he had initiated 25 to 40 others by teaching them how to hack, and that he had communicated with over two hundred others. He advised that he offended 'always with different people' (Interview #1, male hacker and fraudster, aged 27). There was one point of difference with Choo and Smith's [21] typology, however, with all three participants advising that they had, at least to a minor extent,

communicated with co-offenders in person, in addition to online. One participant also advised that he had worked with others in the physical environment installing hardware keyloggers on computers located in university computer labs (Interview #5, male hacker and fraudster, aged 22).

The influence of others was identified as one of the ways offenders became initiated into computer-related offending:

> I know that, um, if you have, um, teenage kids these days, especially boys, and um, you see a lot of them play online games. And, um, you see what they get up to, and they're teaching each other. It starts with fun and games online, you know, tricking people to give up their identities or to give you property within the game and run away with it, so it all starts with fun and games. And then you find a friend who's, guess what I did the other night, so they start talking about it, and then gee, that sounds great, and how did you do that? So they start teaching each other and it escalates. So what was fun and a game, as they get older they realise well, what I was doing here, why can't I use this out here and make a bit of coin out of it. So, kids are learning. Kids know how to get around school systems… Or they'll sit there and they'll take photos of, um, the Wi-Fi devices and find out how to monitor the activity on it, and how to, they'll go and find out the default access details, try that, see if anyone's changed the default access, if they haven't, well they're in. So they're forever trying and learning and sharing that information (Law Enforcement Officer #10).

> Why they get involved. Again, that could be from a number of different reasons. If you're talking about the advance fee fraud side of things, from what I've seen, it just tends to be just a, I suppose, a regional sort of thing for those types of offenders, in that they tend to mix with those people who are involved in those sorts of offences, so they are exposed to it and become involved like that. The lower end sort of offenders that we see, they're day-to-day sort of stuff. Being exposed to it, someone knows somebody who's involved in those sort of offences and, um, yeah, they gain the knowledge through the hand and then, again, removed from the consequences so they become involved in it… They seem to be a little removed from that physical social network. Basically. They make friends online and then that therefore creates a door into criminal activity (Law Enforcement Officer #2).

While offenders associated with others online, it did not necessarily lead to co-offending. The following participant in study three advised that he operated alone, however became involved in offending through associating with others:

> Um, no, I got onto hacking by, I guess it all started, I was just hanging around at an image board, it is quite seedy area of the Internet, ah, and I guess kind of started to make acquaintances with people. You start to talk to them a bit and, um, that's basically how I learnt, just by talking to other people and them sharing their

> experiences and basically teaching me how to do it (Interview #6, male former hacker, aged 18).

Question 3: What role do co-offenders play in knowledge transmission?

In addition to initiating others into online crime and communicating with co-offenders, online portals and communication channels were used to learn and to teach others how to hack and commit fraud:

> Ah, I probably just learnt about it through IRCs, you know. I got on IRC and just learnt how to do it and ah, because I had a computer and things like that I wanted to make the most of my time… (Interview #1, male hacker and fraudster, aged 27).

> …if I want to get involved in armed robbery and I'm not too sure how to do it, I can't walk down the street and, excuse me mate, you done any stickups before and I was just wondering, what happens if they put the screen up at the bank and what should I do? You can't do that, oh, you haven't done any, oh sorry mate, I'll go and ask someone else what he knows about stickups. You haven't got the medium to do that. If you go online to an IRC channel and look at online fraud, there's a myriad of people you can ask, exchange ideas and information and tools and, it's all there for you to get involved. And you start communicating and the next thing you become, you know, the second, third, fourth time, and the next thing you're giving advice and your paypal and your money there's laundering going on and you're into business. Because it's there. And I think it's probably unique in that crime type (Law Enforcement Officer #1).

> They can, ah, send you complete instructions. Or, it's like MSN or instant chat, you can sit there and talk, you can post a comment. So even if they're not there, you can say listen, such and such, I'm having troubles with this, it's not working. I've done this, any suggestions, and they'll write back and they'll just talk them through on how to set up (Law Enforcement Officer #10).

> More the, when you're talking young you're taking more script kiddies, who, ah, just like to sort of play with code and do very basic command-prompt, DDoS attacks, which really don't do much damage. But, um, what happens is they get into these forums and they start speaking with other hackers and, you know, they start learning, you know, through these international forums and, ah, to a point some people even purchase code, you know, so they can sort of see, you know, cause it's, obviously code for hacking software is a valuable resources, you know, people actually buy it… Um, and some of them get on it late in life. You know, there's forty year olds who've never touched a computer before and they discover Facebook, and then they discover forums and then they start learning, and then they speak to people, people tell them how to hide IP addresses and different things like that, and it just escalates, so you've got a forty-five, fifty year old with

> some basic knowledge of how to evade the police and to do something which may be illegal (Law Enforcement Officer #5).

Question 4: How does the online environment facilitate organised crime and co-offending?

Offenders worked together for a variety of purposes, including the actual commission of offences:

> Yeah, um, uni mates, when we were getting the keylogger together. The keylogger cost twenty bucks. And we had to get it from Hong Kong. And we all got together and were like oh, this is a bit much, first year uni, everyone's broke, no one's got any brains, yeah, let's just try it. So there were a couple of us that eventually got it… oh, [the university] got slammed. No one paid for internet that semester. Everyone got it. So, yeah, there were about, a small group, four or five of us that would actively try and go to the labs together and try and not look sussed while we're keylogging people's stuff, but eventually about thirty people were probably finding out (Interview #5, male hacker and fraudster, aged 22).

There was a perception among law enforcement officers that offenders worked together as a way to frustrate police investigations or provide legal defences:

> …we've seen them working in groups, because it allows for a long list of defences around the mental element of the offence, i.e. the person taking the money out, who is closest to the offence, the first step in the chain, then has a defence of, well, it's not my money, I was, you know, doing a favour for Bob. You go to Bob and he says, you know, well Tom owed me money, and I don't know where he got the money from. So there's built in defences straight away when they're starting to deal with those proceeds (Law Enforcement Officer #13).

In addition to being places to learn how to offend and share knowledge, portals were identified as being a marketplace for code used to commit offences and compromised data arising from hacks that could be used for fraudulent purposes, and as a place to recruit particular skill sets:

> So, they deal in underground portals. So they all know each other. They may not have ever met each other, but they all know their own tags, and they know who's who in the zoo, and there tends to be a camaraderie between them, and there's also a, um, a pecking order so to speak. They know who's in charge. So they go and meet online at these various portals and they trade in stolen data, they trade in information, they write their own codes, their own malware, they deal in malware. Um, and you can buy and sell (Law Enforcement Officer #10).

> The last type of offending relates to selling software that had the capability of doing what you did. You advertised and promoted this software on a particular

website which is described as an "Internet criminal bazaar dedicated to largely hacking and information stealing, as well as the online trade in stolen personal information". You advertised and offered for sale proscribed data, being malicious software designed to compromise computers and manage or control compromised computers (Case #54, male hacker, aged 19 at time of offence).

Oh, anything. Any illegal activity. Whether it be carding, malware, um, buy and sell… you can buy and sell your own DDoS attacks, like you can, they trade in malware, so you can go there. It's like a one stop shop. You can, if you're interested in getting into some sort of illegal activity, criminal activity, on the net, all you've got to do is find one of these websites, become a member, and you can go in and they'll give you complete how to's. You can download certain programs, you can buy other programs, and they'll give you complete instructions on how to operate them. If you can't do it yourself you can get people to tune it for you, to fix it up. You can, if, and something we have seen a couple of times, if that if you have a um, ex-employee again, um, left the company and hired a DoS attack from the Russians. So he's obviously been to one of these underground networks and hired a, um, an individual or a group to do a DoS attack on his ex-employer. And that was sustained, that I'm aware of, for at least four to six weeks. So, they couldn't use their systems and they just kept getting attacked. And generally it starts with, um, you've been a naughty, something along the lines of you've been a naughty boy, you've upset a friend of mine, because of that, um, cop this (Law Enforcement Officer #10).

It was apparent that most of the communication with other offenders took place online rather than face-to-face, which allowed them to remain anonymous:

Yeah, I think maybe that happens, you know, it's not face-to-face and it's all online. Quite often they have never even met these people too. They've never met them for real. Oh, it's this bloke, you know, [name], this is his handle online. Never met them. They may have been involved, been in business for a couple of years together, and swapped a load of money and all the rest, never met (Law Enforcement Officer #1).

And online forums are probably the primary way, there may be people who go to school together and so forth, but generally it's the online forums because you have got that added anonymity (Law Enforcement Officer #12).

In the study with law enforcement officers it was identified that many online trading portals took steps to control access so as to minimise law enforcement infiltration and disrupt investigations:

Particularly, a lot of these forums, you have to be vouched for. You can be police. You need to get vouched for to by a member of this group. To do so you probably have to commit crimes to get vouched for by another member… There's a number of reasons for credibility of members, but it stops the law enforcement interaction with them, and all those reasons. So, depending on what group you

want to go, you know, if you can get involved in the vouched for groups it's much better creed (Law Enforcement Officer #1).

Um, but if you don't commit wholeheartedly, well then they start to be concerned. Because police work eight hours a day, you're, you know, there's certain hours, they're not living on it. So they get suspicious of people who aren't giving as much um, attention to the portal as what everyone else is… Like, if you buy and sell and you get a bad reputation, people can post and say, you know, watch out for such and such, he's failed to deliver on this, or the product he provided was crap. They have their own feedback for each other as well. So, it goes up in rankings (Law Enforcement Officer #10).

There's hacker groups out there who, as an entrance exam to get into these forums, you have to produce some code. You know, and it's, if the code's good, then you might get in, you know. And that's just how it works (Law Enforcement Officer #5).

Hard to say. Um, when you start sort of breaking them down into charts, it's surprising, you have your inner group and your inner groups sprouts off maybe another group of twenty, and that group can sprout off another group of twenty, you know. Where do you draw the line, you know, do you just say it's the first group of twenty, but then you've got, you know, other contacts (Law Enforcement Officer #5).

It was identified that there was a level of control over how people communicated on the information sharing sites:

And they love to assert their skills over other people, you know. Someone not as knowledgeable asks a dumb question or if there's, you know, postings by somebody who's off their mark in their knowledge or whatever, they tend to flame them fairly quick you know (Law Enforcement Officer #2).

Yeah, there was another case I have dealt with, he was on, he was on sites, discussion sites, but, um, he was, it was quite bizarre, because he was on these discussion sites, but from what I saw of it, they were actually hanging a lot of crap on him himself (Law Enforcement Officer #4).

Discussion

This research demonstrates the importance of data triangulation and the impact that research design can have on outcomes. Study one, which consisted of a sample of offenders that had been detected and processed by the court system, were more likely to fit Choo and Smith's [21] 'traditional organised crime groups' typology. In contrast, offenders that operated with others in study three would be considered 'organised cybercriminal group' members. These more technologically developed offenders were

seen by law enforcement as having the skills to evade detection, and by operating across borders, created hurdles that lessened the likelihood that there activities would be policed. However, the offenders did not necessarily fit the Convention's definition of organised crime, particularly in relation to the conceptualisation of 'a period of time', as offenders may only be transiently involved in their part of the offence/s, and different offenders may be involved at various times for particular tasks.

As the pathways to computer crime offending involve learning from, and communicating with, others, there is the potential for offenders' behaviours to be perceived, and indeed labelled, as organised crime. Whether it is classified as 'organised crime' or 'just dudes hanging out', these results indicate that computer crime offenders are highly networked and cooperate with each other to commit offences. This networking and coordination reflects the ways in which offenders become involved with offending in the first place; through the influence of others. Other offenders provide the knowledge and subject matter expertise, taking on specific tasks to commit offences. This takes place on online marketplaces, which enable and facilitate organised crime through the sale of code to conduct attacks, the data obtained from hacking and fraud, such as compromised credentials, and services offered by skilled specialists.

There was little data that fitted the third typology described by Choo and Smith [21], namely 'organised ideologically and politically motivated cyber groups'. This paper does not argue that such offenders do not exist, but rather that the sampling methodology was more likely to capture data that related to offenders that were driven by profit, rather than ideology.

Limitations of the research design

It is noted that a number of limitations may arise due to biases within the research design. For example, as noted by Smith, Grabosky and Urbas [40], the limitations of using court documents include the fact that many matters are heard in the lower courts where judgments may not be published, and that it is difficult to determine which matters involve computer crime due to the classification of offenses. Another limitation that is relevant to study one is that cases brought before the courts are unlikely to be representative of the larger population of hackers and computer fraudsters who are not apprehended or prosecuted. Interviewing active and former offenders mitigated this limitation.

However, the sample of active and former offenders was not chosen at random; therefore it may be argued that the participants are not representative of the offender population. In addition, those who agree to be interviewed may differ from the typical offender. However, although this sample is not likely to include offenders who have worked for, or are part of, for example, a terrorist organisation, it may include more mainstream offenders who, collectively, may cause significant damage or fear of victimisation. Again, this limitation was also minimised by comparing offenders who have been identified by the criminal justice system and those who have not.

Acknowledgments I would like to thank those who participated in this study and the assistance provided by the Australian Federal Police, the Queensland Police Service, Western Australia Police, and Victoria Police. I also appreciate the support of my supervisors, Dr Hennessey Hayes, Associate Professor Janet Ransley,

Professor Simon Bronitt, and Professor Peter Grabosky, and acknowledge the assistance of the School of Criminology and Criminal Justice and the ARC Centre of Excellence in Policing and Security at Griffith University in undertaking my doctorate.

References

1. Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime, 14*(1), 52–60.
2. Felson, M. (1998). *Crime and everyday life* (2nd ed.). Thousand Oakes: Pine Forge Press.
3. Chantler, A. N. (1995). *Risk: The Profile of the Computer Hacker*. Curtin University.
4. Meyer, G. R. (1989). *The Social Organization of the Computer Underground*. Northern Illinois University.
5. Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behaviour, 28*(2), 171–198.
6. Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757–780.
7. Yar, M. (2013). *Cybercrime and society* (2nd ed.). London: SAGE Publications Ltd.
8. AusCERT. (2006). *Australian 2006 computer crime & security survey*. Brisbane: AusCERT.
9. Smith, R. G. (2001). *Trends & issues in crime and criminal justice No. 202: Cross-border economic crime: The agenda for reform*. Canberra: Australian Institute of Criminology.
10. Brenner, S. W. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), *Crime online*. Devon: Willan Publishing.
11. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.
12. Goode, S., & Cruise, S. (2006). What motivates software crackers? *Journal of Business Ethics, 65*, 173–201.
13. 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.
14. Finch, E. (2007). The problem of stolen identity and the Internet. In Y. Jewkes (Ed.), *Crime online*. Devon: Willan Publishing.
15. Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the Creation, Distribution and Function of Malware On-Line*: Technical report for the National Institute of Justice.
16. Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). *An inquiry into the nature and causes of the wealth of internet miscreants.* Paper presented at the ACM Conference on Computer and Communications Security (CCS), Virginia, October 29-November 2
17. Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies: A Critical Journal of Crime, Law and Society, 23*(1), 33–50.
18. Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). *An analysis of underground forums.* Paper presented at the 2011 ACM SIGCOMM conference on Internet measurement, Berlin, November 2–4
19. Choo, K.-K. R. (2007). *Trends & issues in crime and criminal justice No. 333: Zombies and botnets*. Canberra: Australian Institute of Criminology.
20. United Nations Office on Drugs and Crime. (2004). *United Nations convention against transnational organized crime and the protocols thereto*. Vienna: United Nations Office on Drugs and Crime.
21. Choo, K.-K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology, 3*(1), 37–59.
22. Choo, K.-K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in Organized Crime, 11*(3), 270–295.
23. Grabosky, P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, Law & Social Change, 47*(4–5), 201–223.
24. Theohary, C. A., & Rollins, J. (2011). *Terrorist use of the internet: Information operations in cyberspace*. Washington, DC: Congressional Research Service.
25. Smith, R. G., McCusker, R., & Walters, J. (2010). *Trends & issues in crime and criminal justice No. 394: Financing of terrorism: Risks for Australia*. Canberra: Australian Institute of Criminology.
26. Seib, P. (2008). The Al-Qaeda media machine. *Military Review, 88*(3), 74–80.
27. Barber, R. (2001). Hackers profiled - who are they and what are their motivations? *Computer Fraud & Security, 2*(1), 14–17.
28. Chantler, A., & Broadhurst, R. (2006). *Social engineering and crime prevention in cyberspace - technical report*. Brisbane: Queensland University of Technology.
29. Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. London: Pearson Education Limited.

30. Taylor, P. A. (1999). *Hackers*. London: Routledge.
31. Berg, B. L. (2007). *Qualitative research methods for the social sciences* (6th ed.). Boston: Pearson Education, Inc.
32. Edney, R., & Bagaric, M. (2007). *Australian sentencing: principles and practice*. New York: Cambridge University Press.
33. Farrington, D. P. (1989). Early predictors of adolescent aggression and adult violence. *Violence and Victims, 4*(2), 79–100.
34. Wright, R. T., Decker, S. H., Redfern, A. K., & Smith, D. L. (1992). A snowball's chance in hell: doing field research with residential burglars. *Journal of Research in Crime and Delinquency, 29*(2), 148–157.
35. Sutherland, E. H., & Cressey, D. R. (1974). *Criminology* (9th ed.). Philadelphia: J. B. Lippincott Company.
36. McAdams, D. P. (2008). The Life Story Interview. http://www.sesp.northwestern.edu/docs/LifeStoryInterview.pdf. Accessed November 12 2009.
37. Wright, R., & Bennett, T. (1990). Exploring the offender's perspective: Observing and interviewing criminals. In K. L. Kempf (Ed.), *Measurement issues in criminology* (pp. 138–151). New York: Springer-Verlag New York Inc.
38. Israel, M. (2004). Strictly confidential?: integrity and the disclosure of criminological and socio-legal research. *British Journal of Criminology, 44*(5), 715–740. doi:10.1093/bjc/azh033.
39. Gibbs, G. (2007). *Analyzing qualitative data*. London: SAGE Publications Ltd.
40. Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.