The final publication is available in T. J. Holt (ed), *Crime Online: Correlates, Causes, and Context* (pp. 117-140). Durham: Carolina Academic Press.

Cybercrime trajectories: An integrated theory of initiation, maintenance and desistance

Alice Hutchings, Computer Laboratory, University of Cambridge

Technological advances have increased the reach of offenders as well as the vulnerability of potential victims. However, cybercrime offenders are a hidden and hard-to-access population. Despite the challenges involved, there are a number of innovative studies examining different samples of cybercrime offenders. This body of research indicates that cybercrime offenders are a disparate set. The theory outlined in this chapter encompasses and unites these differences to describe the two different paths that offenders make take towards committing cybercrimes that compromise data and financial security, commonly referred to as 'hacking' and 'fraud'. These pathways account for differences in cybercrime offenders, such as age of onset, technical expertise, gender and life experiences. This theory, which integrates elements from existing criminological theories, also describes why online offenders continue and escalate their behaviours, and why they stop.

Theoretical perspectives

Many cybercrimes are not unique, in that they reflect crimes that also take place in physical space. However, it is the environment, or the 'bottle', to borrow Grabosky's (2001) analogy, in which offenders operate that makes these types of offences distinctive. For example, an individual cannot necessarily engage in offending that requires a high level of technical knowledge without first obtaining that requisite

knowledge. However, it is not just the technical knowledge that is required, but information about the criminal market, and how to obtain a reward or benefit from offending.

There are a range of criminological theories that provide insights into different aspects of offending. These include innovation (for example, Merton's (1938) structural strain theory), learning and the influence of others (Sutherland's (1949) theory of differential association), how offenders perceive the wrongfulness of their actions (Sykes and Matza's (1957) techniques of neutralisation), and the drive for gain with (dis)regard for the consequences (Clarke and Cornish's (1985) rational choice theory).

Merton's structural strain theory

Merton's structural strain theory, originally developed in 1938, is based on the premise that those who are unable to achieve culturally defined goals experience strain. Goals are culturally specific, for example, 'the American Dream' (Merton, 1968, p. 190) of wealth, as are the approved means of achieving them, such as 'hard work, honesty, education and deferred gratification' (Vold, Bernard, & Snipes, 2002, p. 136). While society maintains that these goals are achievable by all, the social structure means that not everyone has equal access to the resources to achieve those goals, such as a good education and access to opportunities. Depending on their commitment to the goals and means, those who experience strain, usually members of the lower class, use one of the following five modes of adaptation: conformity, in which both the goals and means to achieve them remain important; innovation, in which goals remain important but the rules or the approved means of obtaining them do not; ritualism, which involves abandoning the goals due to their inability to be attained, and instead abiding by the institutional norms; retreatism, which involves

rejecting the cultural goals as well as the means; and rebellion, which is rejecting the goals and means and substituting them criminal behaviour is normal behaviour learnt in interaction with completely new ones (Merton, 1968).

Of the five modes of adaptation, conformity is the most common (Merton, 1968), while innovation, retreatism and rebellion are those that can lead to criminal behaviour. Innovation is considered to be the principal mode of adaptation that leads to crime (Vold et al., 2002). While still striving for their goal, such as wealth, offenders use innovative means to achieve this, such as various forms of property or white collar crime that generate income (Merton, 1968). Retreatism is reportedly the least common type of adaptation (Merton, 1968). Retreatists drop out of, or escape from, society and potentially engage in criminal behaviour such as drug use. They are reportedly the 'psychotics, autists, pariahs, outcasts, vagrants, vagabonds, tramps, chronic drunkards and drug addicts' (Merton, 1968, p. 207). Rebels, who substitute the culturally approved goals with alternative goals, may become criminally involved if associated with activities such as violent revolution or terrorism (Vold et al., 2002).

It is possible to envisage how the three modes of adaptation that could lead to crime can be applied to different types of cybercrime. For example, innovators, who aim to achieve goals by any means, could turn to computer frauds and other activities that may lead to financial gain. Similarly, rebels may be involved in hactivism and online sabotage, while retreatists, compelled to escape from the real world into the cyber realm, may become the 'computer bums, compulsive programmers' (Levy, 1984, p. 125), entangling themselves within the 'computer underground' as they do so.

Sutherland's theory of differential association

Sutherland's theory of differential association consists of nine specific points. Summarised, these points indicate that criminal behaviour is learnt in interaction with other persons in intimate personal groups. What is learnt includes both the techniques of committing crime, and motives, drives, rationalisations and attitudes (Sutherland, Cressey, & Luckenbill, 1992) either favourable or unfavourable to committing crime. Crime is committed when those definitions favourable to committing crime exceeds those unfavourable to crime (Sutherland et al., 1992).

There are two basic elements of differential association. The first is the cognitive element, or the content of what is learnt, such as 'specific techniques for committing crimes; appropriate motives, drives, rationalisations, and attitudes; and more general definitions favourable to law violation' (Vold et al., 2002, p. 160). Sutherland did not specify the learning mechanisms, simply stating that 'the process of learning criminal behaviour … involves all of the mechanisms that are involved in any other learning' (Sutherland et al., 1992, p. 90). The second element of differential association is the associations with other people in intimate personal groups where the learning takes place (Vold et al., 2002). In explaining why different people exposed to the same social conditions may or may not conduct criminal behaviour, Sutherland claimed that it is the meanings that they give to these conditions that they experience that determines whether they violate the law. These meanings vary with the frequency, duration, priority and intensity (Sutherland et al., 1992) of the associations with criminal groups.

Hollinger (1993), while not organising his study of software piracy and unauthorised computer account access around a theoretical perspective, included variables measuring participants' friends' involvement in these types of crime, as well as self-reported involvement. Hollinger (1993) found that as the number of friends

who were involved in unauthorised access to computer accounts increase, so did the likelihood that the participant would report partaking in this activity. However, Hollinger (1993) included only one measure of friends' involvement, namely 'How many of your best friends do the following at least occasionally?' (p. 10). Hollinger (1993) also did not measure attitudes favourable to this type of crime and did not establish the time ordering sequence.

Walkley (2005) examined how well differential association explained a number of cybercrimes, including hacking and online fraud. In her analysis Walkley (2005) mainly focussed, using open source data and previously reported findings, on whether offenders interact or operate in isolation, rather than what the interaction involved, such as learning definitions favourable towards committing crime. Despite noting that hackers communicate online, at conferences and by telephone, Walkley (2005) concluded that most hackers acted alone. Walkley (2005) also concluded that differential association could not be applied to all forms of fraud as some fraudsters operate solo.

Sykes and Matza's theory of techniques of neutralisation

Sykes and Matza's (1957) theory of techniques of neutralisation is that offenders learn to use techniques to justify or neutralise acts that might otherwise produce feelings of shame or guilt, and distinguish between appropriate and inappropriate targets for deviance. Matza (1990) maintained that those that commit crime are not fundamentally different from those that do not; in fact they spend most of their time behaving in a law abiding way. Matza's (1990) claimed that most delinquents drift in and out of crime, enabled by the loosening of social control. The conditions that make this drift to criminal behaviour possible include the use of the techniques of neutralisation. These techniques are: to deny responsibility, to deny injury, to deny the

victim, to condemn the condemners, and to appeal to higher loyalties (Sykes & Matza, 1957).

Matza (1990) was particularly interested in explaining why people generally stop offending as they grow older, which he claimed was not adequately explained by other sociological theories. Therefore, his drift theory is particularly applicable to juvenile delinquency. As juveniles are uncommitted to their deviant behaviour they are free to drift between conventional and unlawful activities (Velarde, 1978). Matza (1990) clarified that the drifters, or juvenile delinquents, explained by his theory did not include all offenders, particularly those who are 'neurotically compulsive' and those that develop commitment towards offending.

Sykes and Matza (1957) argued that techniques of neutralisations were an extension of legal defences to crime, such as provocation or self-defence, which were seen as legitimate by those utilising them but not by the justice system. An interesting defence that has been raised by some defendants accused of cybercrimes, sometimes successfully, is that of addiction to computers, which they argued compelled them to act in the way that they did (Smith, Grabosky, & Urbas, 2004). Such an excuse would relate to the technique denial of responsibility posed by Sykes and Matza (1957).

McQuade (2006b) states that neutralisation theory is a sound explanation for cybercrime as the physical removal from the victim allows the offender to deny injury or deny the victim with ease:

> Since they cannot see the Internet or the people who create content, victims, if they are contemplated at all, become faceless entities, computer systems, or perhaps corporations rather than real people whose livelihoods and wellbeing are compromised… (McQuade, 2006b, p. 160).

Yar (2005) also states that hackers' self-purported motivations for offending, such as 'intellectual curiosity, the desire for expanding the boundaries of knowledge, a commitment to the free flow and exchange of information, resistance to political authoritarianism and corporate domination, and the aim of improving computer security by exposing the laxity and ineptitude of those charged with safeguarding socially sensitive data' (Yar, 2005, p. 391) may be forms of neutralisations aimed to overcoming guilt. Additional neutralisations proposed by Grabosky (2005) include blaming the victim as being deserving of attack, claiming that no harm was done by looking at the data, that corporate victims such as Microsoft could afford it, or claiming that everyone else did it.

A study by Turgeman-Goldschmidt (2009) involved in-depth interviews with 54 Israelis who engaged in hacking, software piracy and phone phreaking to determine whether they neutralised their offending behaviour. Turgeman-Goldschmidt (2009) found evidence that these offenders: deny injury by claiming that 'downloading information is copying rather than stealing' (p. 325); deny the victim by justifying their actions as revenge or targeting sites owned by the 'enemy', such as Nazis and Microsoft; condemn the condemners, such as those who prevent access to the information that they are seeking; and appeal to higher loyalties, especially the hacker ethic of freedom of information. However, Turgeman-Goldschmidt (2009) found no evidence that these offenders engaged in denial of responsibility.

In comparison, Walkley (2005) analysed techniques of neutralisation to determine its explanatory power in relation hacking and online fraud, concluding that there was strong support for denial of responsibility and mixed support for the other techniques of neutralisation. Using open source data Walkley (2005) claimed that, when Internet addiction, as a mental health problem, has been used as a defence in

court, the defendants were neutralising their actions by denying responsibility. Walkley (2005) also stated that two defendants, who claimed that their computer had been infected with a virus or trojan which had caused the damage they were charged with, were also engaging in denial of responsibility, despite the fact that in both instances the defendants had been acquitted and therefore were found not to have been responsible at all.

Clarke and Cornish's rational choice theory

Rational choice theory assumes that offenders calculate the perceived costs and benefits of crime with the assumption that they seek some type of advantage from their actions, be it 'money, sex or excitement' (Cornish & Clarke, 1987, p. 935). Clarke and Cornish's rational choice theory looks at how offenders in particular situations make these calculations (Vold et al., 2002). The theory acknowledges that offenders' perceptions of costs and benefits can be subjective, 'constrained as they are by time, the offender's cognitive abilities, and the availability of relevant information', (Cornish & Clarke, 1987, p. 933), and therefore may not be rational at all (Akers & Sellers, 2004).

Other 'choice-structuring properties' (Cornish & Clarke, 1987, p. 935) are offence specific. For example, when offenders weigh up the type and amount of benefit likely against the perceived risk of detection and punishment, they take into consideration their skills and the skills needed to successfully commit the offence, and the availability of necessary equipment or situations (Cornish & Clarke, 1987). In addition, each of these considerations may not have equal weight. For example, a high likelihood of detection may be more influential in deterring crime than harsh punishments (Clarke, 1997).

In a study by McQuade (2006b) examining students' perceptions of being caught for a variety of technology enabled crimes, it was found that respondents believed that the likelihood of being detected was low, and that the punishment for those that were caught was not severe. Hollinger (1993) measured university students' perceived chances of being caught accessing a computer account without authorisation and found that self-reported involvement in this activity was not related to the perceived chance of being caught.

While each of these theories, on their own, provides a unique insight into the nature of online crime, none provide a complete understanding of these offenders. Hutchings (2013b) tested these theories, and others, to identify which aspects could be integrated into one theoretical model. Further developing and expanding the work by Hutchings (2013b), this chapter outlines an integrated theory, incorporating rational choice theory as well as differential association, techniques of neutralisation and structural strain theory, to explain two distinct sets of cybercrime offenders. These are *technical* cybercrime offenders, who require specialised knowledge and understanding of computer systems, and *general* cybercrime offenders, who use computers to carry out their offences, but not at an advanced level. Informed by data from active and former offenders, the theory identifies two pathways to cybercrime. The first, more general pathway, is one of strain combined with presented opportunity, such as in the workplace. The second, technical, pathway involves differential association, or the influence of others, coalesced with learning. However, maintenance and desistence from cybercrime follow similar trajectories regardless of the initial path taken.

Some of the research presented here was undertaken to directly assess a number of criminological theories, including those that were subsequently integrated

into the cybercrime trajectory theory. This work, outlined in Hutchings (2013b), involved a qualitative analysis of current and former cybercrime offenders, triangulating data from offenders, law enforcement officers, and the judiciary. However, findings by other researchers in this field also contribute to the integrated theory presented here.

Nature of *technical* and *general* cybercrimes

The cybercrimes referred to here relate to the compromise of data and financial security. These include offences commonly referred to as 'hacking' and 'fraud', as well as related offences, such as denial of service attacks and the development and supply of malware. Offences that are *solely* of an interpersonal nature, such as online stalking, accessing child sexual exploitation material, or online grooming, are not included. What may, however, be included is the compromise of computer systems for these purposes, such as gaining access to a victim's email account, or compromising a computer server for the purposes of hosting child sexual exploitation material. Also excluded from this integrated theory is the use of communication systems purely for the purpose of planning offences or communicating with co-offenders, as well as intellectual property matters, such as counterfeiting and piracy.

While the pathways for initiation are differentiated by *technical* or *general* cybercrime offenders, it is acknowledged that there are difficulties in applying these labels to offenders. While in some cases it may be clear that an offender has a particular skill set, or carried out their activities a certain way, in other cases it is less definitive. Also, the level of specialised technical knowledge that someone possesses may be subjective, depending on the knowledge of the person making that judgment. These are offences that cannot simply be defined by legislation, and in fact many may

fall outside of 'computer misuse' statutes, and instead be covered by other legislative provisions, such as fraud, conspiracy, misconduct in a public office, or money laundering.

Whether an offence is *general* or *technical* is often difficult to determine from non-descript categories. For example, 'unauthorised access' or 'hacking' includes a variety of pursuits that compromise computer security with or without a further criminal motive (Brenner, 2007; Wall, 2007). Unauthorised access may be achieved through *technical* means, such as malware or code injection. Alternatively, *general* methods include 'shoulder surfing', solely employing social engineering techniques, or misusing legitimate access to a computer system. Commonly known as 'insider abuse of access', this occurs when offenders abuse the trust they have been given, such as an employee or contractor accessing or altering an employer's data (Shaw, Ruby, & Post, 1998). Furthermore, some scams and online frauds may be relatively simple to undertake, such as selling products that do not exist (*general*), while others may be more complicated, including setting up fraudulent websites and distributing spam through the use of botnets (*technical*).

A confounding factor is that *technical* cybercrime offenders may still use *general* methods. Also, automated tools may be used to detect vulnerabilities and automate exploits. Examples include vulnerability scanners, remote administration programs, port scanners, sniffers and password crackers (Furnell, 2002). Some tools are freely available to be downloaded online, while others can be purchased from online marketplaces (Chu, Holt, & Ahn, 2010; Franklin, Paxson, Perrig, & Savage, 2007; Holt & Lampke, 2010; Motoyama, McCoy, Levchenko, Savage, & Voelker, 2011). 'Script kiddie' is a term used to refer to someone that uses others' programs to obtain unauthorised access rather than developing their own (McQuade, 2006a).

While some may scorn script kiddies, a technical understanding of computer systems is usually required to use automated tools successfully.

Methods

The integrated theory presented here was informed by qualitative analysis of a number of datasets. 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 (Berg, 2007).

Court documents

The first dataset consisted of documents for 54 court cases, in particular sentencing remarks and court judgments relating to prosecutions and extraditions involving cybercrime 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. 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. 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.

Interviews with law enforcement

The second dataset was transcripts 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, cybercrime 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 cybercrime offenders within the last five years, including offenders' characteristics and their initiation into, and desistance from, offending. 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 (Farrington, 1989). The 15 law enforcement officers who participated included 14 males and one female. The interviews ranged from 32 minutes to one hour and 16 minutes in length, with an average time of 51 minutes.

Interviews with offenders

The third dataset consisted of transcripts from 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 (Wright, Decker, Redfern, & Smith, 1992). 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 (1974, pp. 67-68) 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 asked 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' (2008) *Life Story Interview*. Additional questions enquired about additional topics, including the age

they had commenced offending, how the decision to start offending was reached, their perceptions of being caught and the penalties, how skills were obtained and improved, and, for former offenders, why they stopped offending.

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 (1990) 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.

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 began 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 (Israel, 2004).

Of the seven offenders who participated in the interviews, five were active offenders and two identified themselves as former offenders. All participants were male. The interviews ranged in length from 45 minutes to two hours and 18 minutes, with a mean time of one hour and 39 minutes. 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.

Data analysis

All interviews were transcribed verbatim, with any identifiable information replaced with pseudonyms. Coding of the data was mainly ‘concept-driven’ (Gibbs, 2007, p. 44), in that the codes used primarily arose from the literature and the theories being used. Key theoretical concepts and how these have been measured previously were identified, and the data that were collected from interviews and court documents were coded in accordance with these concepts. However, ‘data-driven coding’ or ‘open coding’ (Gibbs, 2007, p. 45) 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' (Gibbs, 2007, p. 98). NVivo, a qualitative data analysis program, was used to classify and sort the data according to the codes applied to see how the data represented the theoretical frameworks.

Initiation into cybercrime offending

The integrated theory of cybercrime trajectories identifies two distinct sets of cybercrime offenders with different pathways into the criminality. The main differentiation for these pathways is whether the offenders employ only general methods, or whether they are technical offenders, who require specialised knowledge and understanding of computer systems. In relation to initiation, general offenders begin their criminality as a consequence of the opportunities that are presented to them, often in their workplace, when they are experiencing some type of strain, such as economic problems, job loss, mental health issues, or gambling and other addictions (Hutchings, 2013b). General offenders, such as fraudsters offending in the course of their employment or on online auction sites, primarily operate alone, but their methods and inspirations can be acquired elsewhere.

This aspect of strain is based on Merton's structural strain theory; in that it is experienced by those who are unable to achieve culturally defined goals. Innovation, considered to be the most important mode of adaptation for explaining crime, is the mode of innovation that is used for this pathway to cybercrime offending. While still striving for their goal, whether it be financial success, or the gratification of other drivers, offenders use innovative means to achieve this, such as cybercrimes that provide an illicit income.

Technical offenders, while they may also be considered 'innovators', have a different pathway to offending, namely through differential association. Technical offenders primarily operate with others. There are many well-developed online communities, which are used for learning and sharing information and ideologies, recruiting others to commit offences, and trading tools (Hutchings & Holt, 2015). With an interest in computers, technology or gaming, would-be-offenders begin by communicating online, during which they learn the techniques to commit cybercrime as well as share the definitions and techniques of neutralisation that enable offending to occur. This part of the theory integrates Sutherland's (1949) key points from differential association, that criminal behaviour is normal behaviour learnt in interaction with others (Vold et al., 2002). To illustrate, one law enforcement officer spoke about his experiences seeing young offenders becoming exposed to online criminality through online gaming communities (Hutchings, 2013b, p. 150):

> I know that if you have teenage kids these days, especially boys, you see a lot of them play online games. And, 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.

The techniques of neutralisation proposed by Sykes and Matza (1957) that Hutchings (2013b) found in use by technical offenders include denial of injury (as there is no loss to individual victims) and denial of the victim (as they do not secure their

systems, are undertaking questionable activities, or are perceived to have done them wrong). Offenders sometimes avoid targets when they are seen as undeserving of victimisation or there is the potential for innocent parties to be harmed (Hutchings, 2013a). Use of condemnation of the condemners as a technique of neutralisation is evidenced where it is accused that the victim has caused harm to others, for example, if a military site is being attacked. Offenders also appeal to higher loyalties when their actions are believed to be for the common good, such as increasing transparency or revealing vulnerabilities. However there is little evidence of denial of responsibility, for example, participants advise that they consider themselves to be addicted to computers, however they do not perceive this as warranting a legal defence.

These trajectories explain the gender imbalance found in cybercrime offending. For example, more females are involved in opportunistic fraud (general offending) than technical offending. This may be due to the types of opportunities that are presented to them. Females are more likely to travel along the first (general) pathway to offending, and, in comparison to their male counterparts, many have experienced substantial strain prior to their offending (Hutchings, 2013b). The second (technical) pathway is male-dominated. Explanations for this centre upon social stereotypes, and the nature of the online social communities where differential association and learning takes place, which tends to be less accepting of those that identify as female. One young male offender, who was engaged in both unauthorised access and fraud, spoke about the reception females received in these communities (Hutchings, 2013b, p. 110):

> So what happens is that when you get a girl that says she can do these things, she gets scrutinised more, people will work against her, because they hold such prejudices against her. So it's just not worth it. So the girl can either crack the

> shits or say nah, this isn't worth it, or she'll just have to keep slugging it out. And she'll have to be better than the boys. It's probably why a lot of them just go no… It's way harder. They have to work. Like, to be a girl doing that sort of stuff, not only do you have to deal with dickheads that are constantly hitting on you, dickheads that think you're a dickhead, or just ragingly rude people that make grossly inappropriate statements that it's just not, ok, eventually you'd just have to say it would probably have been easier to pretend to be a guy, and then say that. And it's just weird.

At first glance, there is a wide disparity in the age of cybercrime offenders (Chantler, 1995; Smith et al., 2004; Turgeman-Goldschmidt, 2005). However, the two trajectories also assist in our understanding of the age differences in offence types, as general offenders are normally older than technical offenders (Hutchings, 2013b). Advancements in age corresponds with greater exposure to scenarios that may induce strain, and a larger range of presented opportunities (Hutchings, 2013b). In relation to the second pathway to offending, young males are exposed to a subculture of gaming and online interaction that relates to their age (Hutchings, 2014).

Holt and Bossler (2014) provide an overview of research into cybercrime offenders, and identify commonalities with the research findings put forward by Hutchings (2013b). These include the subculture and online communication for those involved in technical offending, as well as the pathways provided through the gaming culture (Holt, 2007; Jordan & Taylor, 1998).

Maintenance

Common to both trajectories, offending behaviour is maintained not only because of the benefits accrued by the offenders, but also because of the low level of risk.

Offenders generally perceive the likelihood of being detected as low, and this holds greater weight than the harshness of available punishments. A young male offender, who had previously been involved in unauthorised access, advised (Hutchings, 2013b, p. 197):

> Um, it is hard to get caught. The penalties are severe but, I mean, the chances of getting caught are quite low, especially if you take the proper precautions.

This supports other research into cybercrime offenders that finds that the likelihood of detection has a greater deterrent effect than harsh penalties (Hollinger, 1993; Skinner & Fream, 1997). Benefits obtained from general offence types are mainly financial, while those engaged in technical offences enjoy a greater range of benefits. These include skill development, fun and excitement, social status, power and sexual gratification (Hutchings, 2013a). Maintenance integrates rational choice theory, in that offenders weigh up the apparent costs and against the type of benefits that they seek to achieve (Cornish & Clarke, 1987).

Desistance

Desistance from offending also follows a rational choice theory (Clarke & Cornish, 1985) perspective. Offenders desist from cybercrime when they no longer receive benefits from offending or when the costs outweigh the benefits (Hutchings, 2013b). For example, some offenders stop when they no longer experience excitement or obtain a sense of achievement from their activities. The costs to offenders are not limited to the punishments metered out by the criminal justice system. As offenders believe that the likelihood of detection is low, costs associated with offending are mainly social in nature, including the amount of time they are engaged online, which interferes with legitimate employment or intimate relationships. One offender advised

that he had stopped offending due to other commitments in his life, including his relationship (Hutchings, 2013b, p. 145):

> Um, no real reason to be honest. Nothing really happened that I thought I'd better stop doing this. I just kind of started spending my time doing other things… Hanging out with people in real life a lot more. Um, when I moved to [the city] I started seeing my girlfriend a lot more, so I didn't really feel the need to do it as a pastime.

Costs could also include feelings of guilt or shame, which may have previously been mediated by the Internet, as offenders are not in physical contact with victims. However, once stopped, offenders may return to the maintenance stage and resume their activities if the balance of costs and benefits is in favour of the latter. This integrated theory is presented in Figure 1.

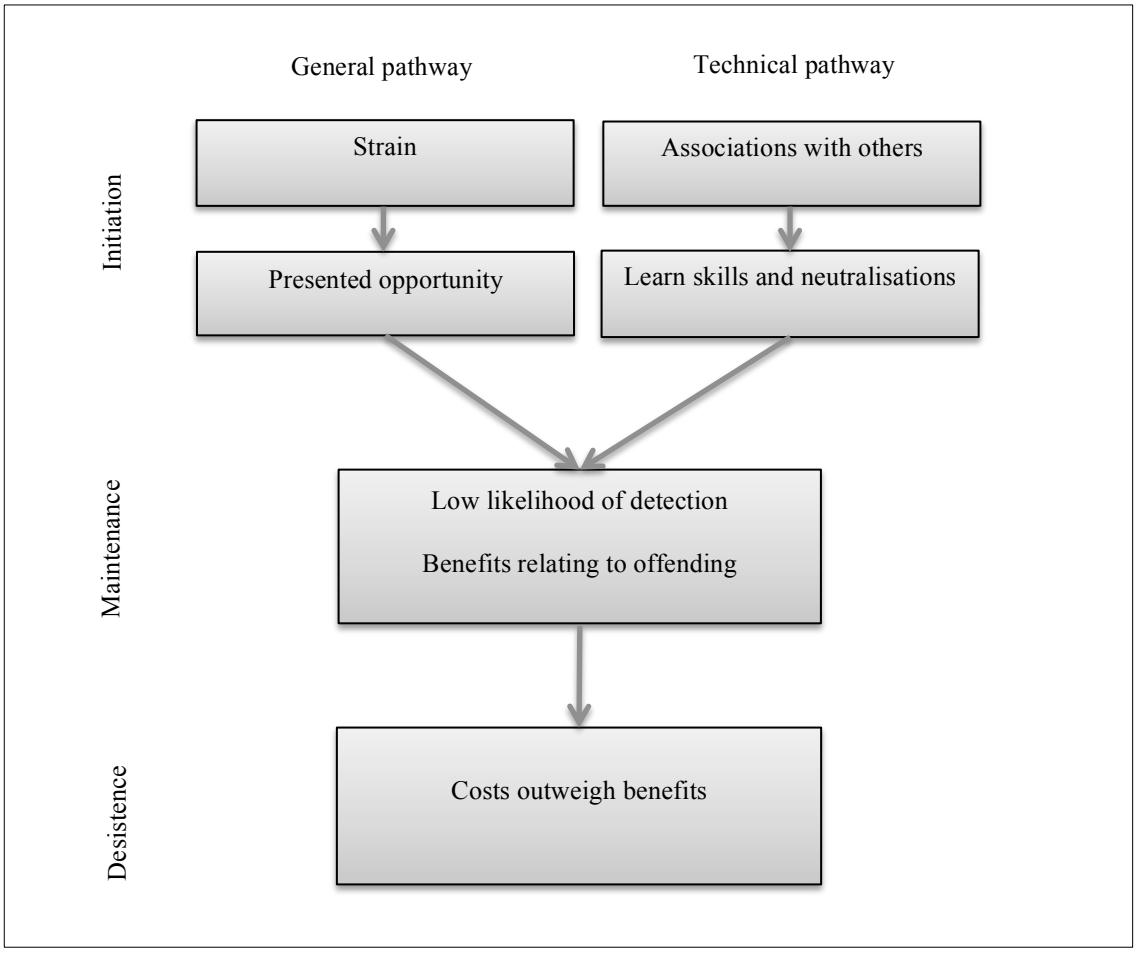

Figure 1. Initiation, maintenance and desistence

Assumptions

Prompted by Walsh (2014), we consider the assumptions that underpin this integrated theory. This is particularly important with integrated theory, which may inherit differing assumptions from the original theories. This is the case in the first assumption considered here, that of free will and determinism. According to Walsh (2014), the operating assumption of strain and learning theories is determinism, while the assumption of rational choice theory is free will. Therefore, the assumption of this integrated theory is that free will and determinism are compatible. While offenders may find themselves at the initiation stage due to deterministic factors, their decision as to when to offend, and when to stop offending, is a matter of choice, noting that these choices may be influenced by factors outside of the control of the individual, and limited by reasoning abilities.

Another assumption of this theory is that crime, law, money, and property are social constructs (Durkheim, 2014). It is because society has tacitly agreed that money exists, that people can have ownership over property, that individuals have rights, and that governments that make laws have the power to do so, that we have legislation that criminalises certain behaviours. Therefore, what is considered to be a crime can vary across time and jurisdiction, as is the case with crimes involving computers, which cannot occur without the advancements in technology which have provided computer systems, networks and the Internet, along with concepts related to ownership over accounts and digital data.

Understanding the power elements in how crime is constructed is important to our understanding of why crime is committed, by whom, and which crimes are

pursued by the criminal justice system. To illustrate, Sutherland's differential association theory was designed to explain law breaking behaviour by the rich and the poor alike. Sutherland argued that criminological theories that relate to poverty and the conditions related to poverty are 'inadequate and invalid' (Sutherland, 1949, p. 5). This is because '…the theories do not consistently fit the data of criminal behaviour [and] the cases on which these theories are based are a biased sample of all criminal acts' (Sutherland, 1949, p. 5). Blaming crime on poverty does not take into account that the actions of the poor may be more likely to be defined as criminal than actions of the powerful. Revelations that nation states are engaging in cybercrimes (see Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014) may also fit the integrated theory presented here, whether it be initiating new offenders, or recruiting existing offenders.

This integrated theory of cybercrime offending aligns with Garland's (1996) concept of 'criminology of the self'. Rather than offending behaviour arising from some pathological state of the offender, it is assumed that offending behaviour can commence, and cease, depending on the particular circumstances surrounding an individual. These circumstances may include what access they have to technology, the types of influences they experience, their opportunities, both legitimate and illegitimate, and the community that they are in contact with, both online and in physical space.

Discussion and conclusion

This chapter has set out an integrated theory of crime that explores the criminal trajectories for general and technical cybercrime offenders. This theory has only been developed for cybercrimes that compromise data and financial security, although it is

noted that there are many offence types, including terrestrial crimes, that may have similar trajectories, and this integrated theory may be useful in providing insight into the pathways of other crime types.

In addition to technical levels, differentiating factors for online offenders include age, gender, opportunities, and life experiences. At first glance, the age ranges for online offenders, when not differentiated by type of offence, appear to be similar to those of other criminal populations. The age-crime curve shows that the prevalence of offending increases from late childhood, peaks in late adolescence and decreases in adulthood (Loeber & Farrington, 2012). However, this is not true for every offence type. It is the more high-volume types of crimes that young offenders are usually involved in, such as graffiti, vandalism and shoplifting. In contrast, homicide, sexual offences and white collar crimes, which are lower in volume, but high in impact, are usually committed by adults (Richards, 2011).

Cybercrime offenders cross a range of ages; however it is the younger, male, offenders that are likely to be involved in technical crimes, compared to general cybercrime offences. While males are also more likely to commit general cybercrime offences than females, females are more likely to commit general offences than technical offences. Older offenders are more likely to commit general, opportunistic cybercrimes. Technical offenders, through an interest in gaming and technology, are initially exposed to online communities that provide information about how to commit crime, as well as a marketplace for hacking tools and stolen data. Females, however, struggle in gaining acceptance into such communities, limiting their exposure and the subsequent development of technical expertise. These extensive online communities, including online gaming communities, can lead to cybercrime through association and the influence of other offenders.

The differences found for the skilled and unskilled offenders reflect the *who* and *what* they are exposed to, and what opportunities come their way. The Internet allows offenders to further the reach of their social groups, interacting with others across jurisdictions that they otherwise are unlikely to come into contact with. Therefore, definitions that are favourable towards offending, as well as the necessarily technical knowledge and skills, can reach a greater audience.

The majority of young offenders are likely to mature out relatively early in their life when confronted with career and relationship choices. This occurs when the costs start to outweigh the benefits that were actually obtained, as well as those that were perceived to be achievable. The benefits for general cybercrime offenders are mainly financial gain, particularly when this is used to feed drug and gambling addictions. Technical cybercrime offenders gain additional benefits, including retribution and revenge, testing their skills, and pleasurable feelings arising from excitement, power over others, and social status. Although offenders perceive the potential penalties as severe, they have a low opinion about the ability of law enforcement to investigate these matters and therefore see the chance of detection as being low, as there are steps that can be taken to hide or mask someone's identity and to launder funds in order to obfuscate the money trail. Therefore, it is the likelihood of detection, rather than the severity of punishment, that is likely to have the greatest effect on offending. Offenders cease their activities when they gain meaningful work or enter a relationship, reflecting the increased cost of their actions on their lives.

Acknowledgements and funding

Much of this chapter arises from my doctoral thesis, which would not have been possible without the support of my supervisors, Dr Hennessey Hayes, Associate Professor Janet Ransley, Professor Simon Bronitt, and Professor Peter Grabosky, and the assistance of the School of Criminology and Criminal Justice and the ARC Centre of Excellence in Policing and Security at Griffith University. This chapter was written while supported on a grant from the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131]. The opinions, findings, and conclusions or recommendations expressed are those of the author and do not reflect those of the aforementioned agencies.

References

Akers, R. L., & Sellers, C. S. (2004). *Criminological Theories: Introduction, Evaluation and Application* (4th ed.). Los Angeles: Roxbury Publishing Company.

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

Brenner, S. W. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), *Crime Online*. Devon: Willan Publishing.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1-20.

Chantler, A. N. (1995). *Risk: The Profile of the Computer Hacker.* Doctor of Philosophy, Curtin University, Perth.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examing the Creation, Distribution and Function of Malware On-Line*: Technical report for the National Institute of Justice.

Clarke, R. V. (1997). Introduction. In R. V. Clarke (Ed.), *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Monsey: Criminal Justice Press.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice, 6*(1985), 147-185.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933-947.

Durkheim, E. (2014). *The Rules of Sociological Method* (W. D. Halls, Trans.). New York: Free Press.

Farrington, D. P. (1989). Early predictors of adolescent aggression and adult violence. *Violence and Victims, 4*(2), 79-100.

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.

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

Garland, D. (1996). The limits of the sovereign state. *The British Journal of Sociology, 36*(4), 445-471.

Gibbs, G. (2007). *Analyzing Qualitative Data*. London: SAGE Publications Ltd.

Grabosky, P. (2005). The global cyber-crime problem: The socio-economic impact. In R. Broadhurst & P. Grabosky (Eds.), *Cyber-Crime: The Challenge in Asia* (pp. 29-56). Aberdeen: Hong Kong University Press.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social Legal Studies, 10*(2), 243-249.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorised account access. *Security Journal, 4*(1), 2-12.

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., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40.

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.

Hutchings, A. (2013a). Hacking and fraud: Qualitative analysis of online offending and victimization. In K. Jaishankar & N. Ronel (Eds.), *Global Criminology: Crime and Victimization in the Globalized Era* (pp. 93-114). Boca Raton: CRC Press.

Hutchings, A. (2013b). *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., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*(3), 596-614.

Israel, M. (2004). Strictly Confidential?: Integrity and the Disclosure of Criminological and Socio-Legal Research. *British Journal of Criminology, 44*(5), 715-740.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757-780.

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

Loeber, R., & Farrington, D. P. (2012). Introduction. In R. Loeber & D. P. Farrington (Eds.), *Juvenile Delinquency to Adult Crime* (pp. 3-13). New York: Oxford University Press.

Matza, D. (1990). *Delinquency & Drift*. New Brunswick: Transaction Publishers.

McAdams, D. P. (2008). The Life Story Interview. Retrieved November 12, 2009, from http://www.sesp.northwestern.edu/docs/LifeStoryInterview.pdf

McQuade, S. C. (2006a). Technology-enabled crime, policing and security. *The Journal of Technology Studies, XXXII*(1), 32-42.

McQuade, S. C. (2006b). *Understanding and Managing Cybercrime*. Boston: Pearson Education, Inc.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review, 3*(5), 672-682.

Merton, R. K. (1968). *Social Theory and Social Structure*. New York: The Free Press.

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.

Richards, K. (2011). *What makes juvenile offenders different from adult offenders? Trends & Issues in Crime and Criminal Justice no. 409*. Canberra: Australian Institute of Criminology.

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.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*(4), 495-518.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber Criminals On Trial*. Cambridge: Cambridge University Press.

Sutherland, E. H. (1949). *White Collar Crime: The Uncut Version*. New Haven: Yale University Press.

Sutherland, E. H., & Cressey, D. R. (1974). *Criminology* (9th ed.). Philadelphia: J. B. Lippincott Company.

Sutherland, E. H., Cressey, D. R., & Luckenbill, D. F. (1992). *Principles of Criminology* (11th ed.). Lanham: General Hall.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664-670.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8-23.

Turgeman-Goldschmidt, O. (2009). The rhetoric of hackers' neutralisations. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet*. New Jersey: Pearson Education, Inc.

Velarde, A. J. (1978). Do delinquents really drift? *British Journal of Criminology, 18*(1), 23-39.

Vold, G. B., Bernard, T. J., & Snipes, J. B. (2002). *Theoretical Criminology* (5th ed.). New York: Oxford University Press, Inc.

Walkley, S. (2005). *Regulating Cyberspace: An Approach to Studying Criminal Behaviour on the Internet.* Doctor of Philosophy, The Australian National University.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Walsh, A. (2014). *Criminological Theory: Assessing Philosophical Assumptions*. Waltham: Anderson Publishing.

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.

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.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal, 44*(4), 387-399.