

**Understanding the Expertise Required by Law Enforcement Investigating  
Cybercrime: An Exploration of Social Engineering Techniques**

Grace O. Nock

Postgraduate Forensic Psychology, University of Wellington

FPSY591

Dr. Russil Durrant

09 May 2020



## **Abstract**

Cybercrime represents a significant threat for the 21st century, a threat that traditional methods of policing cannot adequately manage. Consequently, new ways of policing utilising specialised teams have been implemented to address cybercrime proactively. One method of policing that has been relatively unexplored within academic literature is covert online investigations, wherein law enforcement creates false identities to interact with offenders from. Existing research has not comprehensively explored what tactics, techniques, and procedures law enforcement use when conducting these investigations. Accordingly, selection and training of employees presents unique challenges. Therefore, this study aims to provide a detailed evaluation of what skills are needed by law enforcement. This information can then inform future training and selection. This study examines in-depth semi-structured interviews with eight New Zealand Police investigators using Applied Cognitive Task Analysis. Data was analysed using thematic analysis. Results revealed three themes with 18 sub-themes. The first theme explored operational pre-planning, the second theme explored social engineering techniques used to gather information, and the third theme explored the wide-ranging external considerations. Finally, the discussion outlines the implications for theories of social engineering, applications for law enforcement training and recruitment, and potential future research opportunities within social engineering and police psychology.

## Table of Contents

Abstract .....	II
List of Figures .....	VII
List of Tables .....	VIII
List of Appendices .....	IX
Introduction.....	1
Literature Review.....	3
The Nature and Extent of Cybercrime .....	3
Challenges in Investigating Cybercrime .....	7
Specialized Cybercrime Units .....	11
Social Engineering .....	17
Theory of Social Engineering .....	24
Challenges within Covert Operations .....	29
Training & Hiring For Covert Investigation .....	31
Expertise and Skills of Covert Investigation.....	34
Research Aims.....	37
Methodology .....	39
Qualitative Approach of the Current Study.....	39
Characteristics of Qualitative Research .....	40
Evaluating Qualitative Research .....	43
Interviews.....	45
ACTA.....	46

Procedure.....	47
Design.....	47
Recruitment .....	48
Participants .....	48
Data Collection.....	49
Ethics .....	52
Data Analysis .....	53
Results.....	58
Data-gathering .....	59
Fabrication .....	61
Profiling .....	62
Purpose .....	63
Understanding Needs.....	63
Engaging.....	64
Building Rapport .....	65
Credibility.....	66
Reciprocity.....	67
Similarity .....	68
Scarcity .....	68
Ego Influence.....	69
Challenges .....	70

	71
Emotional Influence .....	72
Power .....	73
Curiosity .....	74
	75
External Case Considerations.....	75
Legislative Requirements .....	76
Risk Assessment .....	78
Evidential Sufficiency .....	79
Different Crime Type .....	80
Law Enforcement Community .....	81
Training .....	82
Final Comments .....	83
Discussion .....	85
Summary of Results .....	85
Situating the Research: Data-Gathering.....	89
Situating the Research: Engaging .....	94
Situating the Research: External Case Considerations .....	109
Limitations and Strengths.....	116
Future Research, Applications & Implications .....	117
Conclusion.....	122

References.....	124
Appendices.....	150
Appendix 1: Consent To Interview .....	150
Appendix 2: Information Sheet For Participants.....	152
Appendix 3: Interview Schedule: .....	155

## List of Figures

**Figure 1** *Tactics Techniques and Procedures of Covert Investigation* .....59

**Figure 2** *Social Engineering Attack Cycle as Described by Mouton et al. (2016)* .....91

**List of Tables**

<b>Table 1</b> <i>Comparison of Influence Techniques by Cialdini (1984), and Social Engineering Techniques by Workman (2008).....</i>	28
<b>Table 2</b> <i>Comparison and Similarity of Social Engineering Techniques.....</i>	105



## **List of Appendices**

<b>Appendix 1</b> <i>Consent to Interview</i> .....	150
<b>Appendix 2</b> <i>Information Sheet for Participants</i> .....	152
<b>Appendix 3</b> <i>ACTA Interview Schedule</i> .....	155

## **Introduction**

Crimes committed online, or cybercrimes, are an escalating threat to national and community safety. Cybercrime inflicts significant financial and personal hardships on victims, businesses, and society at large (Aiken et al., 2015). The industry of cybercrime is currently growing as one of the most significant illicit industries in the 21st century (Ross, 2018). Law enforcement therefore, holds a critical position in trying to reduce and combat these illegal behaviours. In particular, law enforcement is required to intercept, prevent, and prosecute individuals who engage in illicit online activity.

However, cybercrime is challenging to effectively police. Cybercrime is transnational, mostly anonymous, difficult for frontline police officers to address, and is thus dependent upon specialised skill sets (Wydra, 2015). Given the relative novelty of cybercrimes compared to other crimes, there is limited research available on the prevention and management of this illegal activity. Consequently, difficulties in training staff emerge. An emerging method of enforcement that is increasingly being utilised is covert online operations. This is a powerful method whereby law enforcement creates assumed identities in the cyberspace and interacts with offenders<sup>1</sup> through these identities. Law enforcement are then able to elicit information (Vendius, 2015). However, this method of policing is a relatively new process, and well-defined training and procedures have not been consistently outlined.

The use of these covert identities to gather information uniquely involves utilizing the skill of social engineering (Tetri & Vuorinen, 2013). Social engineering

---

<sup>1</sup> I acknowledge the negative bias around the use of the word 'offender'; however, this term has been used in the current thesis for ease of text within paragraphs, and to represent language used by NZ Police employees.

is the process of gathering information from an individual using deceptive social methods (Hadnagy, 2010). However, there remains great ambiguity surrounding the best methods of interacting with an offender (Bonino & Kaoullas, 2015; O'Leary & D'Ovidio, 2007). The present research aims to address this knowledge gap by interviewing New Zealand Police investigators using Applied Cognitive Task Analysis. This interviewing method has been developed explicitly for eliciting tacit procedural knowledge (Militello & Hutton, 1998). The current research explores the awareness of the expertise required for covert cybercrime investigations that use social engineering skills. This research is the first study aimed at understanding the expertise of social engineering tactics in covert operations. Due to its novelty, limited a-priori hypotheses regarding the knowledge of investigators can be made. However, it is expected that investigators will hold tacit expert knowledge that can be explored using in-depth, semi-structured interviews, and that some of the skills explored will parallel the skills theorised in the social engineering literature.

## **Literature Review**

### **The Nature and Extent of Cybercrime**

Developed countries have witnessed exponential growth in, and accessibility to, technology over recent decades. The expansion in access to technology has been so widespread that it has resulted in a world that operates within a global, digital economy (Sarre et al., 2018). Technology has created an interconnected society, and not only enables ease of life, but is also a critical and dependent structure of the modern environment (Broadhurst, 2017b). A consequence of this growth is that there has also been a significant increase in opportunities for individuals to commit crimes through technology (Hadlington et al., 2018; Ngafeeson, 2010; Sarre et al., 2018), following the adage that "crime follows opportunity" (Grabosky & Smith, 1998, p. 13). However, the speed with which technology has been developed has not been matched by advances within the security structures that support this environment (Brown et al., 2009), thereby creating opportunity for cybercrime to occur. The proliferation in the development of computerised devices, such as smart vehicles and smart homes, further increases the likelihood of exploitation of daily users (Broadhurst, 2017a; Rush et al., 2009). Furthermore, these gaps and vulnerabilities within technology pose threats to a country's national security such as through the threat of cyber-terrorism or cyber-warfare (Broadhurst, 2017a). Consequently, cybercrime has recently become part of many countries' critical national security concerns, as they acknowledge the seriousness of the threat posed (Armin et al., 2015).

The vulnerabilities created due to technology are so widespread that cybercrime has now become one of the most prolific and profitable forms of illicit behaviour, with an estimated global cost of USD 600 billion (Ross, 2018). This

already significant estimate is likely not capturing the real cost of cybercrime given the high likelihood of under-reporting (Caneppele & Aeibi, 2019), the overall lack of public and scientific awareness of what constitutes cybercrime, and the lack of clarity around current data (Armin et al., 2015). The breadth of the problem is exemplified when a comparison is made between current global costs and historical estimates. In 1998 cybercrime was thought to cost between \$555 million to \$13 billion (Parker, 1998), in 20 years, this figure has increased by a factor of between 50 to 1000 times. If the figure by Ross (2018) is lower than the actual cost of cybercrime, and should future progressions follow past trends, there is likely to be continued and sustained future growth in the cost of cybercrime. Accordingly, the development of management processes and preventative measures to reduce the costs and implications of cybercrime are critical global, societal goals (Gillespie, 2015; Sarre et al., 2018).

To begin a discussion into how cybercrime can be managed and reduced, one must first consider the complexity of behaviours that are covered under this term. A firm definition of any construct is required to begin the research process (Speer, 2000). From an academic perspective, how a construct is defined will influence what data is collected and analysed, and consequently, what theories can be generated (Jensen et al., 1960). Ensuring cohesion and clarity across research is necessary in order to reduce fragmentation and guide future literature. This clarity will allow for more accurate assessments of what the real nature of cybercrime is, and where additional research needs to be conducted (Armin et al., 2015). From a practical perspective, without accurate definitions for behaviour, the creation of effective criminal legislation is challenging (Chawki et al., 2015). To date, many cybercrime laws continue to be ambiguous and worded in a manner that allows for confusion and debate (Reyes et al., 2007).

Definitional issues are prominent within the literature on cybercrime (Caneppele & Aeibi, 2019), with authors debating about how to best classify and delineate what behaviours are, in fact, 'cybercrime.' At its most inclusive, a definition of cybercrime encompasses a set of illegal behaviours conducted through internet technology (IT) (Speer, 2000). However, such a definition does not capture the different variants and nuances of cybercrime, and is too broad to create a clear legal precedent (Chawki et al., 2015). McGuire and Dowling (2013) created a commonly used classification tool for cybercrime that helps in differentiating between cyber-dependent crimes and cyber-enabled crimes. In other words, crimes where the target of the crime is the IT system itself, and more traditional crimes committed through the internet, respectively (Alkaabi et al., 2010; Sarre et al., 2018).

Cyber-dependent crimes are actions where the computer system is the target (Doig et al., 2018). The classification of behaviours as cyber-dependent is incredibly extensive, with whole papers dedicated to the classification and description of the possible actions (Sabillon et al., 2016). A few examples of cyber-dependent crimes include, (a) the utilisation of malware, or malicious software that can include viruses, worms, or Trojan horses; (b) ransomware, which involves taking control of a computer system remotely and holding it for ransom; and (c) hacking, which encompasses behaviours regarding the unauthorised penetration of networks and data. In all the above examples, the behaviour could not be conducted without the computer system. The computer system is a requirement, or a dependent feature, for the crime to occur (McGuire & Dowling, 2013).

Conversely, cyber-enabled crime refers to criminal behaviours that can occur in the terrestrial environment as well as through computer technology (Sarre et al., 2018). Thus, committing the crime through IT is merely a further dimension in which

the crime can occur (McGuire & Dowling, 2013). For example, fraud, sexual crimes against children, and the selling of drugs or illegal services are all behaviours that can occur both online and offline (Kirwan, 2018). While the purpose of the crime is similar, the translation of behaviour from offline to online does produce some differences. These variances can include different methods of conducting the crime, different offender motivations, different offender demographics, and different offence-supportive cognitions within the online world compared to offline (Babchishin et al., 2010). For example online offenders against children are more likely to utilise child sexual exploitation material in the grooming process (Moore, 2011) or have greater paedophilic interest (Babchishin et al., 2010).

Another example of cyber-enabled crimes includes online marketplaces, which can provide illegal goods and services such as hacker tools, firearms, or illegal drugs (Akhgar & Brewster, 2016). Moreover, online networks, or peer to peer networks (P2P) provide an additional environment for the sharing of radicalised belief systems, which can contribute to cyber-terrorism or the planning of nation-wide disruptive activities (Dashora, 2011). These attacks against a government body are so prevalent that the Pentagon receives as many as 6 million intrusions on their cyber systems a day (Razzaq et al., 2013).

The computing system in these crimes assists or enables offenders, by providing an alternative medium with which traditional crimes can otherwise be committed (Chawki et al., 2015). Each form of cybercrime creates independent and new challenges for policy makers and investigators to control and manage (Broadhurst, 2017b). Frequently, cyber-enabled crimes require more social forms of law enforcement investigation that are transposed onto the cyber-sphere. In contrast,

cyber-dependent crimes require the expertise of computer-science and cyber-security professionals who are proficient in digital forensics (Atlam et al., 2020).

### **Challenges in Investigating Cybercrime**

The cyber-space represents a new criminal operating environment requiring unique investigative techniques. Standard policing investigation practices will experience only limited success in the online world due the many differences between online and offline environments (Jeffries & Apeh, 2020). Some of the dissimilarities between online and offline crime that are most challenging for law enforcement are the anonymity of online offending, the difficulty in evidence collection (Chawki et al., 2015) the cross-jurisdictional nature of online crimes (Urbas, 2012) and the differential skill-set required to investigate online environments (Roberts, 2008).

Research has shown that traditional investigative practices are insufficient to investigate cybercrime (Bossler & Holt, 2012). In reviewing the application of frontline policing investigative methods to the cyber-space, a US-based study by Bossler and Holt (2012) investigated 268 local patrol officers' perception of cybercrime via surveys. The results from this study found that only 18% of patrol officers believed they should be involved in the policing of cybercrime matters. In contrast, three-quarters believed cybercrime was a matter for specialized units. Hence, despite some cybercrimes representing a translation of behaviour from the physical world to the online world, with some investigative techniques being translational, many officers do not believe they hold the skills to be effectively involved in cybercrime investigations. This suggests that differences and challenges exist in policing cybercrime compared to offline crime. The recommendations reported by participants from Bossler and Holts study indicated a need for increased training in cybercrime investigation, and the need for specialized investigative units. The finding



that frontline officers do not feel adequately trained or equipped to manage cybercrime is prevalent across the literature (Davis, 2012; Wilitis & Nowacki, 2016). The current lack of training or preparation also limits the ability to study law enforcement perceptions of cybercrime, as officers do not perceive themselves as sufficiently involved. This highlights the need to develop new measures and training protocols to tackle the challenges involved, and increase officer's ability to effectively manage this growing area.

One of the biggest challenges for the investigation of cybercrime is the anonymity from which online behaviour can be committed. It is possible for individuals using a computer to conceal their identity from other users, conceal their IP address, or utilise browsers that conceal or encrypt user information, such as The Onion Browser (TOR) (Chawki et al., 2015). For example, the marketplaces most frequently utilised for access to illegal goods or services are located within the dark-net, which is principally accessed through TOR. Therefore, the identity of the user is concealed (Sabillon et al., 2016). The more technologically skilled an individual is, the more complex the methods for anonymising their identity can be, and this is often when the more serious crimes are committed (Akhgar & Brewster, 2016). Also, when an individual is utilising services that encrypt or anonymise their location and identity, law enforcement will be unlikely to receive cooperation on behalf of the company involved, given their business model is the protection of customer identity (Chawki et al., 2015). Thus, an essential technique when law enforcement is unable to identify a user through technology is to try to identify the individual through social interaction. It is in this work that social engineering techniques can become a crucial component of the investigation process, as will be discussed further in the section on social engineering.

Investigations which occur online must also deal with the distributed and transitory nature of cyberspace (Chawki et al., 2015). Information on behaviours committed online can be spread across different networks, different companies, and different countries (Chawki et al., 2015). As such, law enforcement is dependent upon the co-operation of many private companies, such as those that can provide an IP address (possible computer location) for a given suspect. This information is not guaranteed and may slow down investigation processes (Moore, 2011). Besides, given the vast amounts of information stored online, sorting through the available data to find the relevant information can be a further time-consuming part of the investigation process (Casey, 2004).

In dealing with cybercrime, law enforcement must also appropriately address the global nature of IT-based crime. For example, who is responsible for investigating or prosecuting a given crime? Is it law enforcement from where the offender has citizenship, the country from where the offender is currently residing, or the location of the victim(s) or effect(s) of the attack(s) (Brenner & Koops, 2004)? The global nature of crime is a significant challenge for law enforcement, as obtaining the required information for progressing investigations can become particularly tricky when they are only able to work within one country or state (Ayofe & Irwin, 2010). Thus, legislation must account for prosecution and investigation across borders (Roberts, 2008). Furthermore, as the definition of cybercrime is complicated and open to debate, there can often be variations in jurisdictional and legal definitions of cybercrime, further obfuscating the ability of law enforcement to effectively work together globally (Chawki et al., 2015). For example, if the individual committing the crime is located in a country that does not contain cybercrime laws, such as the Philippines, then law enforcement from other countries are not able to seek out

extradition or prosecution of the offender even if the victim is located in a country that does contain cybercrime laws, such as the United States (Chawki et al., 2015; Urbas, 2012).

The internet is an internationally connected network. Therefore, preventative measures need to similarly rely on international connectivity. These challenges in investigating cybercrime continue to increase as cybercrime grows as an industry. The growth of cybercrime is a function of the ease with which cybercrime can be committed, the increased accessibility to IT, and the likelihood that an offender will be able to evade prosecution because of the problems facing law enforcement (Ayofe & Irwin, 2010). It is therefore argued that without a global united front to tackle cybercrime, the increase in illegal behaviours will continue to develop at a rate far quicker than governing bodies can control or reduce (Bendovschi, 2015).

Consequently, steps have been taken to acknowledge the need for global cooperation, mutual legal assistance, and specialised skills and knowledge in the fight against cybercrime. Governments across the world have created specialised national and cross-national units (Council of Europe's Cybercrime Convention, UNODC, Europol, Interpol units). These task-forces have a primary role in the investigation of cybercrime internationally through intelligence sharing capabilities and creating established means of contact between law enforcement agencies (Broadhurst, 2006; Broadhurst, 2017a). Between 2000 and 2013, the use of specialized cybercrime units increased from 9% to 27.5% (Wilitis & Nowacki, 2016). Although it is not clear whether this figure is exclusive to cyber-dependent or cyber-enabled crime, the fact that growth has tripled is a significant finding. The proactive implementation of specialized groups conform with frontline officers perceptions that cybercrime

requires specialized units, as previously mentioned (Bossler & Holt, 2012; Davis, 2012).

### **Specialized Cybercrime Units**

Given the unique challenges that are involved with investigating cybercrime, unique techniques for the investigation process have been developed and implemented. The current research will specifically focus on cybercrimes that are considered cyber-enabled crime. This focus is because cyber-dependent crimes require the examination of digital forensics, and data security (Atlam et al., 2020; Harkin et al., 2018; Reyes et al., 2007), whereas cyber-enabled crimes can be investigated using social tactics (Urbas, 2010). A particularly common social technique utilised by specialized law enforcement investigating cyber-enabled crimes is that of covert operations (Urbas, 2010). Covert investigation techniques vary hugely in nature however, they have a common defining factor. The unifying variable is that the suspect under investigation is uninformed of law enforcement attention or investigation (Sharpe, 2002). Some examples of behaviour that can be considered covert include, but are not limited to: deceptive police presence, infiltration of groups, or surveillance techniques such as monitoring suspects (Loftus & Goold, 2011).

The use of covert investigations represents a change from traditional policing, from police being a visible community presence with a primary role of reacting to incidents as they arise, to being proactive and anticipatory towards current and future threats (Giollabhui et al., 2016). The use of proactive policing is considered an avenue to reduce the likelihood of future offending (Zedner, 2009). Creating a covert police presence allows law enforcement to identify offenders when the offences are known to be occurring, or to gather evidence that may indicate offences will occur in the

future (Loftus & Goold, 2011). Online covert investigation is therefore a proactive form of information-gathering.

The use of adopting false identities and interacting with offenders online has emerged as a primary method to confront cybercrime (Grabosky & Urbas, 2019). The current data available from covert operations does not allow for a detailed examination on the efficacy of these cybercrime units (Wilitis & Nowacki, 2016). However, initial research suggests specialised units can lead to significant increases in arrest rates (Mitchell et al., 2010). In the seminar conclusions of a large international cybercrime convention, the use of undercover investigative tactics was concluded to be of significant importance, and even crucial, to the battling of cybercrime in the modern age (Vendius, 2015). This success reflects modern adaption to the threat environment, the challenges involved, and tactics utilised (Razzaq et al., 2012).

Despite the growing importance of online covert investigation and the increased use of covert techniques due to the rise of IT (Harfield, 2010), the topic has been relatively unexplored within academic literature (Giollabhui et al., 2016). The lack of academic attention is unsurprising to consider given the very nature of covert investigations. Covert policing culture and operations are designed to be secretive practices (Giollabhui et al., 2016). As such, to analyse and understand the different tasks of undercover online investigations, literature from a diverse range of fields has been assessed, including criminology, security studies, psychology, and police studies. Through analysing this breadth of research, the current study will be able to provide important data as to the methods of covert investigation by specialised units.

The use of covert undercover interaction techniques has been applied to working with many different aspects of cybercrime, including counterterrorism

(Matusitz, 2006), dark-net trading (Lacson & Jones, 2016), and online sexual crimes against children (Mitchell et al., 2010). Regardless of the crime under investigation, the actions taken in these specialised operations remains alike, as outlined by Brown (2015). Firstly, law enforcement will access the relevant websites, often located on the dark-net, although sometimes within open-source websites (Maddox et al., 2015). From this, agencies can establish and observe communication with offenders via chatrooms, instant messaging services, social networking sites, dark-net forums, or P2P communication networks (Dubord, 2008). Next, using a false identity crafted for the specific crime type, law enforcement will seek to develop rapport and trust with the identified offender based upon their unique impersonated identity. Finally, investigators are then able to observe offenders commit offences as are they are happening or try to gather information on the location or identity of the offender.

In conducting these covert operations, law enforcement is utilising the same anonymity tactics that many cyber-offenders employ. The same anonymity that makes it difficult for law enforcement to identify offenders, similarly makes it difficult for offenders to determine whether the person they are communicating with is a genuine consumer of the goods being sold or the child that is the intended target (Lusthaus, 2012). By creating false identities in cyberspace, law enforcement is able to understand the environment of offending, interact with offenders, and potentially elicit information from the offender (Urbas, 2010). This strategy is not the only technique used by law enforcement in covert operations, but it has become increasingly popular to help identify offenders (Choo & Australian Institute of Criminology, 2009; Krone, 2005a; Krone, 2005b).

The effectiveness of covert techniques is highlighted in the research by Mitchell et al. (2010), which assessed the developments in investigations for online

sexual crimes against children over six years (2000-2006) in the USA. Data was analysed from information gathered under the National Juvenile Online Victimization study, which includes assessments of the characteristics of online crimes against children, and arrest rates. Further data was also collected through interviewing representative samples of frontline staff, and specialised cyber-teams that used undercover investigative tactics, at two time periods, ( $n = 612$  at T1,  $n = 1051$  at T2). Interviews included questions on arrest rates and the nature of covert operations. Results from this study identified an average overall increase of 280% in arrests from undercover investigations for all law enforcement. The largest growth in arrests was seen from specialised groups, who had an increase in arrests of 988% over the six-year period. This significant growth in arrests is indicative of successful adaptation to the challenge of cybercrime, and suggests that undercover investigations can be a unique and essential tool in the battle against cybercrime.

The use of these undercover ruses has historically been focused quite heavily on the online child sexual exploitation industry (Mitchell et al., 2010). This focus largely stems from the fact that the movement of the sex industry into the technological world was a rapid process with widespread acceptance among offenders (Cohen-Almagor, 2013). Although child sexual exploitation material has existed for many years, the use of modern IT led to a significant increase in the creation, distribution, and accessibility of the material (Gewirtz-Meydan et al., 2018; Moore, 2011). The focus is also a function of the multiple avenues law enforcement officers can use to identify a target. For example, law enforcement may pretend to be a child for whom a targeted offender seeks to groom or meet (Broadhurst, 2019). Alternatively, complaints from parents can alert law enforcement to a possible offender. From this avenue, police are then able to assume the identity of the child

targeted, or create another identity to interact with the offender from (Brown, 2015). This form of investigation has been described as a reactive or take-over investigation (Mitchell et al., 2011). Thirdly, investigators can pretend to be like-minded sex offenders on chat rooms and forums, either through new profiles or take-over profiles from apprehended offenders. Investigators can then direct investigations into those who download, trade or publish child sexual exploitation material. Lastly, law enforcement can pretend to be the guardian of a child with whom they want other adults to engage with sexually (Mitchell et al., 2011).

When pretending to be a child, law enforcement will often see common sequences of behaviour from the offender. These common behavioural patterns have been described in three stages, titled the Luring Communication Theory (Olson et al., 2007). By recognising common steps in the progress of communication, law enforcement is able to identify conversation progression and know when further action can be implemented. The initial stage within the Luring Communication Theory describes how the offender must first access the child, for example, through P2P communications forums or chatrooms. Secondly, the offender will then likely implement strategies designed to entice or entrap the victim. For example, offenders often initially hide mentions of sexual behaviour altogether to develop trust and formulate friendship (O'Leary & D'Ovidio, 2007). Once trust is built, then sharing child sexual exploitation material is commonly done to increase the normality of sexual behaviour for the victim (Krone, 2005a). The third stage is when the offender may seek to initiate an abusive relationship, such as through getting the victim to send photos of themselves, organising a meeting and taking photos of the victim, or through sexual abuse against the victim (Wolak et al., 2005). These three processes represent what is commonly referred to as the grooming of a child (Black et al.,



2015). Law enforcement can intervene in the first instance during covert operations to assume the identity of a child (Keyvanpour et al., 2016). Under the assumed identity, investigators can arrange a meeting with the offender and utilise the chat-logs as evidence towards indecent communication, or gather sufficient information from offender disclosure that their identity can be determined, leading to arrest and prosecution (Cohen-Almagor, 2013).

While covert investigation was initially focused exclusively on sexual crimes against children (Broadhurst, 2019), the type of cybercrime where undercover operations can be employed has expanded. As such, covert investigations have also been applied to include dark-net trading (such as drug trafficking, identity theft, selling of hacking or malware abilities or contract killing), along with the monitoring of radicalisation or terrorism groups (Brown, 2015).

Online marketplaces, commonly located on the dark-net, are inundated with illicit goods and services. Consequently these marketplaces are a further avenue from which law enforcement can conduct covert operations (Bossler & Holt 2015). The covert operations that occur on the dark-net relate to investigators pretending to be consumers or vendors of the goods being sold and then interacting with offenders to try and elicit identifying information. Alternatively, law enforcement can host fake dark-net sites and conduct covert operations on the users of the sites (Lacson & Jones, 2013; Webber & Yip, 2013). This technique has similarly been conducted with sites dedicated to child sexual exploitation material (Cohen-Almagor, 2013). These 'trap sites' create a replacement website under the same domain name, with the same features and layout of the original website and assess what information and personal details are uploaded onto the fake site (Cohen-Almagor, 2013). Law enforcement may also assume the identity of the owner of these sites, a well-known figure from the

dark-net community, and gather information on other users in this manner (Kelion, 2014).

The monitoring of cyber-terrorism is a similarly vital area to assess through covert operations. The internet has increased the ability of terrorist groups to recruit and radicalise individuals, and incite violent attacks (Gordon, 2014; Scrivens & Conway, 2020). Law enforcement can monitor any at-risk networks for information-gathering, or engage in deceptive undercover work (Klein et al., 2018). For example, in the November 2015 Paris terrorist attacks, the terrorists used TOR for encryptions and then utilised various social media platforms to communicate and plan the attack (Koch et al., 2016). Thus, the online environment is growing as an area from which radicalisation and acts of terror can be planned. If law enforcement is able to immerse themselves in this environment in the same way that they can with sexual crimes against children, this will allow for preventative measures to be implemented. The United Nations (United Nations, 2012) have outlined that there is an increase in law enforcement and intelligence agency focus upon counterterrorism online, with more sophisticated tools and techniques being continually updated. Common tactics for counterterrorism online are based upon decision making on whether to monitor, shutdown or infiltrate (conduct covert operations) a website (Theohary & Rollins, 2011). The use of covert investigation in proactive monitoring and prevention of online terrorist activity is rarely explored in academic literature, possibly due to the increased need for operational security around this work (Theohary & Rollins, 2011).

### **Social Engineering**

The use of covert identities to gather information utilises the skill of social engineering. Social engineering represents the act of using deceptive social methods in order to access an information system (Tetri & Vuorinen, 2013). The information

system can include technological systems such as websites or phones, and it can also include individuals. Mitnick et al. (2003) outlines how human traits such as trust and self-esteem offer weak points for individuals to exploit and gather information from, without the need to utilise more technical methods such as digital forensics. One of the critical challenges for cybercrime investigation can be in the collection and analysis of forensic data. Thus, if law enforcement can utilise social methods to gather the necessary information on offending, then this is a crucial skill and essential means of crime prevention. Within social engineering, the information systems, both technological systems and people, are targeted through social approaches (Tetri & Vuorinen, 2013).

The use of social engineering techniques has received support in empirical research (Tetri & Vuorinen, 2013). The success of social engineering techniques is evident in both the widespread adoption within specialised policing units (Brown, 2015) and the arrest rates based upon their use (Wolak et al., 2010). For example, research by Orgill et al., (2004) tested the ease with which an actor could access a company's network, which the actor was unauthorised to access. Through utilising techniques such as open-source assessment of data that gave him credibility, learning the correct language to use in the given setting, and developing familiarity of the environment layout, the actor was able to gain access to the network by creating a reputable false identity and getting workers to provide the relevant information.

Additional experiments within the security and information technology field have been conducted with similar success, such as getting individuals to reveal their password (Greening, 1996), and utilising phishing techniques to get access to user name credentials (Hasle et al., 2005). Further experiments within social psychology also reveal the utility of social engineering strategies, often through adopting the

technique of authority. For example, assessing participants' responses to authority figures' instructions even if the instructions are deemed socially reprehensible, illegal, or improperly authorised has been shown to lead to an increase in obedience (Russell, 2011). A typical result in these experiments is that participants will commit an action, or reveal information that they should not if the individual providing instruction assumes an identity of a higher authority (Russell, 2011).

Social engineering actions and the techniques used have been synthesised in literature by Tetri and Vuorinen (2013). Through assessing 40 articles on social engineering, they identified three principal strategies from which social engineers can exert their methods of influence. The first of these is through applying techniques such as fabrication (Latour, 2005). The second strategy identified is through using persuasion (Johnson, 2016; Workman, 2007), and finally, through data-gathering procedures (Allen, 2006; Schiller et al., 2011).

Fabrication techniques often involve the development of a situational ruse or a false identity in order to access sensitive information (Thompson, 2006). Name-dropping, utilising the correct jargon and building an impression of an in-group are also techniques that can help in fabricating an identity (Lafrance, 2004). Persuasion techniques include utilising various heuristics and manipulation tactics that try to obtain acquiescence from the target. This is done through tools such as, creating a likeable persona; creating an aura or identity of authority; creating rapport and trust between the target and the social engineer; playing on emotion or desires; or employing authoritative methods to attain obedience (Tetri & Vuorinen, 2013). Finally, data-gathering is an aspect of social engineering wherein the engineer conducts research and information-gathering via open-source platforms (Tetri & Vuorinen, 2013). This aspect of social engineering facilitates the ability to influence by

preparing the individual who will engage in the deceptive tactics. While Tetri and Vuorinen (2013) describe the three primary methods separately, they further acknowledge the overlapping nature of each technique. For example, in using a technique such as the creation of a false identity (fabrication), one may also be applying an identity of authority (persuasion), and this identity may be based upon data-gathered prior to influence, such as the target being lower in an organisational hierarchy and therefore more susceptible to authority. Accordingly, while they can be described separately, social engineering techniques are often intertwined in application.

Social engineering techniques have been most commonly associated with criminal behaviour (Tetri & Vuorinen, 2013). The most common analysis of social engineering comes from information and security studies when trying to figure out ways to reduce social engineering attacks from a cybersecurity perspective (Hatfield, 2018). Human nature remains one of the most accessible avenues for exploitation (Kombroz et al., 2015; Mouton et al., 2016). It is therefore a common technique for offenders to exploit. When an individual utilises social engineering techniques towards gathering sensitive information that is against the victims interests, it is conceptualised as a social engineering attack (Mouton et al., 2016). Many social engineering attacks utilise face-to-face communication to gather information. However, attacks can also be as simple as sending deceptive emails requesting personal information. The security threat does not arise from a weakness in technology but in the human behaviour of trust and gullibility (Junger et al., 2017). Offenders are thus able to successfully employ social engineering tactics by influencing common psychological traits (Atkins & Huang, 2013).

Researchers have developed various ontological models to assist in describing the processes of a social engineering attack. One example of a model used is analysing a compliance framework, in which the methods used to gain compliance are considered. Mouton et al. (2016) suggest the reasons for compliance to an attack are due to the manipulation of the following principles: friendship or liking, commitment or consistency, scarcity, reciprocity, social validation and authority. These principles can also be applied within another framework, described as the attack framework. The attack framework evaluates the steps taken in the attack in six sequential progressions (Mouton et al., 2016). Templates such as the attack framework have been developed through mapping and analysing the behaviour of when a social engineering attack is conducted (Mouton et al., 2016). More comprehensive templates have been formulated that consider contextual cues; however, the attack process, as outlined below, highlights the necessary steps taken by an attacker (Mouton et al., 2016).

1. The attack formulation: the initial selection of a goal and target to exploit.
2. The information-gathering phase: the attacker conducts background research on the target and the goal.
3. The preparation stage: the technique for social engineering is developed based on information gathered.
4. The relationship development stage: contact is created between the attacker and target, and rapport is built.
5. The exploit relationship phase: the engineer enacts the attack in order to gather information sought.
6. The debrief stage: the target is removed from the exploitive relationship.

Through first understanding the steps taken in social attacks, second-order preventative measures can then be researched and enacted. Due to the human factor involved with social engineering attacks, preventative measures are complicated to effectively implement, hence why research in this area is so critical. For example, some research trying to prevent social engineering attacks through warning participants has found adverse effects (Zhang et al., 2014). Conversely, other preventative measures that teach participants about the risk of social engineering attacks have been shown to have some ability in reducing susceptibility to victimisation (Aburrous et al., 2010; Bulle et al., 2016). However, this effect is often only visible in the short-term (Junger et al., 2017). Research assessing the different forms of prevention may therefore be useful in determining why there are differences in prevention success.

Junger et al. (2017) tested methods of preventing susceptibility to a phishing attack on a randomly selected group of 290 participants in the Netherlands. Participants were either placed in an experimental condition that provided a warning leaflet regarding disclosure of personal information, a priming condition that asked questions on cyber-safety, or were in the control condition. Following this, all participants were asked various questions relating to personal information, such as their email address, bank details and online shopping history. The results indicated an 80% disclosure rate, with the priming and warning condition having limited effects on reducing disclosure, and on some questions, increasing disclosure. The lack of conclusive results demonstrating an effective solution to social engineering attacks is indicative of the challenges faced in reducing cyber-security threats. The authors in this study acknowledge multiple variables that may have led to high disclosure, such

as not understanding the relevance of personal information for security threats, and the tendency for humans to trust and hold biases that contribute to vulnerability.

Additional research within cyber-security should consider the attack and compliance framework in the testing of user-safety. For example, the reason the study by Junger et al. (2017) may not have seen the effects of reduced disclosure may be due to a lack of consideration for these frameworks. Which social engineering compliance strategy is used may influence the effectiveness of the preventative measure. In the study by Junger et al., (2017) a friendly, young student researcher approached participants to ask if they wanted to participate, using the compliance strategy of likeability and, potentially, authority given it was a university backed study. If an experimental group then included warnings related to trusting people based on likeability or authority/affiliation, the researchers would have been directly tapping into the attack template and compliance strategies used by attackers. Thus, more positive results may have been discovered.

In review, social engineering represents a complex and effective method of information-gathering. These techniques have historically been used predominantly by cyber-criminals, and are very difficult to successfully prevent (Junger et al., 2017). Consequently research within social engineering has mainly focused upon the realm of cyber-security. However, social engineering tactics can also be employed by law enforcement to prevent offending. When police develop false identities on the internet, they are using social engineering strategies. In such a scenario, the offender is the identified social entry point. Law enforcement is then using deceptive social methods, such as fabrication, to access information, including the offender's identity or evidence of crimes committed.



## **Theory of Social Engineering**

To develop a theory concerning why social engineering strategies work, researchers have had to synthesise literature from many fields, including social psychology, marketing, and security studies. Why social engineering works has been briefly explored when looking at the compliance principles as described by Mouton et al. (2016). These compliance principles were based upon extensive work by Cialdini (2009), and will be discussed in more detail, along with additional, comprehensive analysis by Workman (2008).

Workman (2008) developed a theoretical model of social engineering through grounded theory. Theory development was conducted through assessing the empirical literature on social engineering success, in order to try and identify the key concepts that explain why and how social engineering works. Through this, Workman was able to identify six possible variables through which social engineering was more likely to occur and be successful. These variables were techniques by which the social engineer could exert influence upon the victim. He then employed a two-stage field study to test this further. Workman used a questionnaire to test whether specific attitudes and behaviour were correlated with an increased likelihood of providing confidential information in a social engineering ruse. This was assessed through an objective count on whether employees provided information, and self-reports on behaviour.

The first three of the six variables Workman (2008) hypothesised to increase social engineering success are related to commitment. Commitment refers to the fact that individuals are likely to engage in behaviour that is consistent with their beliefs and attitudes in order to reduce cognitive dissonance (Festinger, 1962). Commitment was divided into three variables thought to increase conformity. The first variable is

normative commitment, the second variable is continuance commitment and the third variable is affective commitment. Normative commitment describes the social behaviour of being more likely to conform to a request for information, resource or access if the person requesting the information, resource or access has previously provided something to the target. The desire to engage in a reciprocal exchange would accordingly be heightened. Continuance commitment describes the behaviour of being more likely to provide information, resource or access, if time, effort or money has already been dedicated towards the exchange with the social engineer; the individual is already invested and so will be more likely to comply. Finally, the third variable of affective commitment describes the positive associations with the in-group that one is a member of, and the desire to maintain relationships. Hence, when a social engineer highlights mutual identification with a social group, the target may be more likely to conform.

The fourth variable hypothesised to increase social engineering success relates to likeability and trust. Individuals who like someone are more likely to trust them. Thus, if the social engineer increases likeability through tactics such as developing rapport, creating friendship, or even more superficial tactics such as playing on physical attractiveness, an individual will be more likely to succumb to social engineering. The fifth variable describes how individuals often fear authority and will often engage in behaviour that complies with the instructions of an authority figure. For example, this was shown in Milgram's (1983) seminal work on obedience, where individuals were more likely to give perceived dangerous electric shocks to another participant if ordered to by an authority figure. Thus, obedience to authority can also increase the conformity to social engineering influence. Finally, if an individual is reactive versus resistant to threats upon scarcity of resource, time or freedom, they

will be more likely to experience victimisation via social engineering techniques. This is because when an object is placed under uncertainty or perceived unavailability, those who are more reactive will respond to this limitation with a greater impulsivity to attain the object.

Results from Workman's (2008) studies confirmed that each of the variables could play a key role in increasing an individual's responsiveness and conformity to manipulation via social engineering. A positive correlation was seen with all hypothesised variables, such that an increase in each one of the variables led to a corresponding increase in the likelihood of being receptive to social engineering. This correlation was significant to  $p < .001$  in all variables except reactance ( $p > .05$ ). Overall, this study suggests that utilising social engineering techniques as a method of information-gathering can be a successful method of compliance.

A further prominent researcher, who has studied the effects of influence and persuasion, is social psychologist Robert Cialdini who first published the book *Influence: The Psychology of Persuasion* in 1984. This seminal work by Cialdini (1984) is based upon observational studies into his experiences with job applications, working in car dealerships, fundraising positions and telemarketing companies. This research aimed to identify how people influence others and what techniques or language can be used to gain compliance. From this in-depth work, Cialdini was able to identify six principles: reciprocity, commitment and consistency, social proof, liking, authority and scarcity. These principles are used widely across marketing (Cialdini & Rhoads, 2001; Gamez, 2018) and have already been discussed in reference to the compliance principles described by Mouton et al. (2016).

The first principle is reciprocation. This principle dictates that people, universally (Gouldner, 1960), will feel obliged to repay in kind, favours first given to them. People feel obligated and indebted to an individual once something is provided to them, such that they will then go out of their way in order to pay it back. Secondly, is commitment and consistency, which states that humans like to maintain consistent behaviour and will do so even to the detriment of themselves. The critical factor behind how consistency works is that when someone commits to an idea, they will feel compelled to go through with it regardless of whether it is beneficial to them. The effect of commitment is related to the concept of cognitive dissonance, which states that individuals are motivated to hold consistent beliefs, attitudes and behaviours. (Festinger, 1962). Thirdly, there is the effect of social proof. Social proof is when we gather situational and behavioural cues of what to do, based on what another does. For example, canned laughter on television facilitates laughter from the intended audience. Fourth is the use of liking. People are more likely to do something for someone if they like them. This principle of liking can be enhanced further by traits such as physical attractiveness. The fifth method of influence is authority, where people will be more likely to commit an action if instructed to by an authority figure. This tool has already been discussed regarding Milgram's (1983) work. Finally, is the tool of scarcity. Scarcity, as described by Cialdini, is how "people seem to be more motivated by the thought of losing something than by the thought of gaining something of equal value" (Cialdini, 1984, p. 238).

There are many crossovers between the work by Cialdini (1984) and Workman (2008), which explain why an individual may agree to do something even if it is not in their best interest. The similarity between these social engineering techniques is shown in Table 1, which shows the comparable technique between those

identified by Cialdini and Workman. This convergence of theory suggests there may be consistent patterns in human behaviour, such that regardless of the setting in which the influence occurs, manipulation based on these factors is effective.

**Table 1**

*Comparison of Influence Techniques by Cialdini (1984) and Social Engineering Techniques by Workman (2008)*

Cialdini (1984)	Workman (2008)
Reciprocity	Normative Commitment
Commitment & Consistency	Continuance Commitment
Social Proof	Affective Commitment
Liking	Likeability & Trust
Authority	Fear
Scarcity	Reactance

Understanding how social engineering functions can be of great use and importance to law enforcement. For example, it could be that law enforcement engaging covert investigation online may utilise these tools, just as offenders (for example, when grooming a child online) apply these social engineering tactics for individual purposes (Grant & MacLeod, 2016). No current research has assessed what interactional techniques law enforcement use when interacting with offenders online. However, by understanding the mechanisms of why and how behaviour functions one is able to ensure that the techniques that are utilised are well supported by the research and can contribute significantly to the desired outcome. Thus, studies such as Workmans' (2008) provide extensive evidence to suggest that using social engineering is an important and effective method to access information

Law enforcement is required to be a step ahead of offenders in order to reduce crime. Consequently, a good understanding of the theory and techniques behind social engineering may be beneficial so that they can dynamically channel the necessary skills. Increased explicit understanding of the tools that investigators may already use could lead to benefits in several ways. If investigators were able to assess the likelihood of an offender being more prone to one of the six identified traits or attitudes by Workman (2008) or Cialdini (1984), they would be able to tailor what influence strategies are used in order to increase the likelihood of gaining the information sought. By understanding what compliance principles are more relevant for specific populations, law enforcement could then alter their strategy accordingly. For example, investigators of digital sexual crimes against children may use different tactics than those investigating other aspects of the dark-net, possibly due to differences in motivation for the offender. Within digital sexual crimes against children, offenders are more likely to seek something from individuals they are chatting to, and thus may have a different behavioural profile than offenders who are offering a service or good on the dark-net. For individuals selling or seeking illegal goods or services on an online marketplace, awareness of the risk of undercover law enforcement may reduce the likelihood of revealing information about themselves (Maddox et al., 2015). Research assessing whether online offenders differ in the identified traits compared to normative samples may provide generalisable guidance to law enforcement in how to best communicate with individuals online.

### **Challenges within Covert Operations**

In addition to the difficulties experienced within investigating cybercrime broadly, covert online investigation also introduces idiosyncratic challenges. One of the significant challenges for investigative staff is the close care and scrutiny that

must be applied when working undercover to stay within the legal powers afforded to law enforcement (Harfield, 2010). The key legal issues for undercover operations are when law enforcement tries to elicit information that will reveal who the suspect is. Law enforcement must ensure not to entrap offenders, induce offences, or gather evidence that will later be inadmissible (Urbas, 2010). Furthermore, given the relative increase in perceived or actual intrusiveness of policing powers that are demonstrated through covert investigation, further rules of governance are applied (Harfield, 2010). These additional governance restrictions are needed to reduce the chances of evidence or charges obtained being excluded from court proceedings (Harfield, 2010), as this is a particularly common problem when trying to prosecute online offending.

A further challenge for law enforcement conducting undercover investigations is related to profile development and consistent language use. For example, police must maintain the guise of being the offender that previously operated the profile. Language use is very individually stylistic, with tools available that can assess how many individuals are using one profile (Rashid et al., 2013). The use of language poses a challenge to police, as they must accurately represent the previous user of the profile to reduce suspicion in other users. Furthermore, even when not conducting an account takeover, police must still represent the assumed identity accurately, including using the language of a child or dark-net offender with consistency and ease (Tetzlaff-Bemiller, 2011).

The challenges encountered when investigating cyber-crime generally, also apply to covert investigation of cybercrime. These include the need for collaboration across nations, given the multi-jurisdictional nature of covert operations. For example, the United Nations have created the Convention on the Rights of the Child, which formulates a co-ordinated operation for allowing various countries to collaborate in

reducing the harm caused by internet crimes against children (Cohen-Almagor, 2013). Other taskforces have similarly been assembled, such as the Virtual Global Taskforce that allows officers from member countries to respond quickly and accurately to reports of online crime. Or the Comprehensive Operational Strategic Planning for police which looks at allowing police in member countries to operate in the best possible investigative manner for operations that occur trans-nationally (Cohen-Almagor, 2013).

### **Training & Hiring For Covert Investigation**

Despite the use of niche investigative techniques such as covert social engineering tactics, and the development of specialized cyber units, there remains great ambiguity surrounding the methods of investigating cybercrime (Wydra, 2015). The methods for investigation are left relatively unsaid, with significant variation in the procedures and tactics depending on the organization, the country, and the investigator (Reyes et al., 2011). Consequently, given that no definitive procedures are outlined, specific training methods are either variable in content, or non-existent (Agustina, 2012; Muncaster, 2005).

A study by Davis (2012) surveyed 127 police officers in America on cybercrime preparedness and training. Participants reported a considerable discrepancy in the level of training received, with only 26% of officers receiving training on average. The variation in training poses a significant challenge for police, and creates questions about the most effective methods and training for cybercrime broadly, and when policing different types of cybercrime. In addition, participants in the study stated that receiving training would be significantly beneficial to their working ability.



In one of the only studies identified that has researched police working on undercover investigations, Tetzlaff-Bemiller (2011) discovered several critical themes related to investigative practice. This research was conducted through semi-structured interviewing of 17 law enforcement officers who engaged in covert investigation across the United States. The first theme discussed training. Participants stated that while training was encouraged within the area of undercover chatting (i.e. social engineering), the training was sparse and often incomplete compared to other aspects of cybercrime training. Secondly, there was disagreement between personnel on which strategies were most effective when interacting with potential offenders online. This discrepancy may be due to the fact that participants in this study received incredibly diverse training, with minimal consistency. Despite this discrepancy, on the job training was reported as particularly fundamental towards conducting the role effectively. The final theme identified in this study related to the importance of knowing the legalities of procedure in order to avoid issues of entrapment. Overall, this study provides an interesting initial analysis into some of the challenges encountered by police engaging in undercover chatting. However, it focused exclusively on internet crimes against children and not on any other cybercrimes. Additionally, the themes were only briefly discussed, with limited focus on teasing out some of the expertise required for the given tasks. Importantly, this study highlighted the lack of a broad and consistent training framework for new employees, and this was particularly apparent within the realm of the social engineering skills required.

O'Leary and D'Ovidio (2007) also outlined several crucial issues with training for investigators of cybercrime, particularly those who primarily utilise covert investigative tactics. Firstly, accessing high-quality or standardised training is very

difficult. This access to training applies to both generalised knowledge of digital forensics and investigations, and more niche aspects related to investigating certain crime types such as online exploitation of children. The training that is offered to investigators is often unclear in regards to which course is best for the unique job role and crime type being investigated, and which order to do the courses in. Out of the training offered, there is usually a lack of focus on the more practical skills needed, such as undercover chatting; a finding that was also identified in research by Tetzlaff-Bemiller (2011). Finally, the monitoring of training processes, as well as precise assessments of law enforcements abilities, strengths and weaknesses, and capabilities, has not yet been conducted in order to improve upon procedures and increase the likelihood of successful prosecution.

Further challenges for training are present due to the low-visibility of the covert teams (Harkin & Whelan, 2019). Based on pre-gathered anonymous survey data with 66 specialist cybercrime investigators in Australia, Harkin and Whelan (2019) were able to identify that training and skill retention was a problem among specialist units, and this was reported by participants to be due to the low visibility of the units. Thus, it may be that not only is specialized training required by investigators, but a more significant shift towards transparency and understanding by senior managers and the policing community is also required.

Additional research by Harkin et al. (2018) using the same data-set as Harkin and Whelan (2019), concluded that a lack of training for specialized cyber-units was a significant problem for both new employees and existing employees who needed to up-skill. The development of training for staff should, therefore, not only consider basic teaching for new employees, but also consider how experienced staff can benefit from more education. A lack of training by cybercrime investigators is reported

consistently across Western nations, with a need for more training being similarly identified in the UK, based on interviews with 45 police staff (Schreuders et al., 2018). The need for training is not an isolated requirement, and considering the trans-national nature of cybercrime, implementing more standardised measures would be incredibly beneficial.

### **Expertise and Skills of Covert Investigation**

Cybercrime investigation appears to have evolved as a field of specialist expertise that is experience-based, particularly within the use of covert operations and social engineering (Loftus & Goold, 2011). For optimal success, the skills for covert investigation appears to require socialization and training that occurs from working on cases and operations, as well as directed instruction (Loftus & Goold, 2011). The use of a covert police presence requires law enforcement to understand the common environmental regularities and irregularities of offences and offence related behaviour (Loftus & Goold, 2011). The knowledge and expertise required are not necessarily abilities that can be taught via classroom instruction, but instead require more abstract skills such as problem-solving when encountering operational dilemmas, utilizing the correct language for different contexts (Loftus & Goold, 2011) and the need for heightened awareness when working covertly (Giollabhui et al., 2016). These skills are not easily imparted, articulated, or easy to identify as heightened skill areas in potential investigators. Consequently, limited research exists that explores what skills are necessary for covert investigative staff.

Brown (2015) has hypothesized some skills that may be required by undercover investigators. These include critical inquiry, interpersonal aptitude, the ability to establish fact from fiction, and the ability to influence conversation (Brown, 2015). However, the description of these traits as being critical is not based upon

empirical assessment, and is instead merely assumed necessary by researchers (Brown, 2015; Loftus & Goold, 2011).

A further skill that could be important for law enforcement conducting covert operations may be in understanding the language used, and the order of communication. To assess this, researchers have used linguistic analysis to examine the conversations between offenders online (Black et al., 2015). From this, the recurring language used and the typical steps in the process can be explicitly identified and act as a guide for directing communication. For example, research by Black et al. (2015) analysed the grooming process when offenders were chatting to a decoy child, and the language examples at each stage of the grooming process. This analysis could be a particularly useful tool for investigators of online crimes against children, principally in the initial period of conducting undercover operations.

The usefulness of forensic linguistics is determined by the ability of law enforcement to impersonate an individual, engage in undercover chatting realistically, and interpret progression within communication (Black et al., 2015). Linguistic training may advantage law enforcement by explicitly teaching what language cues to be aware of that may reveal information on the offenders' identity (Orebaugh et al., 2014). Within the UK, police officers conducting undercover investigations are often offered a two-day course in linguistic analysis, language theories, and practical skills such as the patterns of turn-taking, subject approach, and development (Grant & MacLeod, 2016). However, further evidence-based skill identification is needed and should be used to make training and recruitment recommendations.

Various skills identified within the current literature on social engineering and social psychology could also be relevant for investigators. For example, in

constructing false identities, fabrication is a necessary component of the covert investigation process. Accordingly, the skills and techniques of fabrication, such as crafting a profile that is appropriate for the given situation, learning the language of the environment or establishing a contact base, could potentially be important for law enforcement. The nuances of persuasive discourse and data-gathering could also be necessary in order to build relationships effectively and influence the offender (Tetri & Vuorinen, 2013). Likewise, the techniques outlined by Workman (2008) may also be adopted by law enforcement in order to shape and influence the direction of the conversation to gather the necessary evidence effectively and efficiently. However, as this has never been explored in the literature, the specific skills used are difficult to postulate.

A thorough evidence-based review of the critical skills and competencies has not yet been conducted, which means researchers are not able to provide recommendations for training or skill development that maintain high levels of reliability and validity. Consequently, if hiring or training individuals depended upon the selection or development of skills that had not follow rigorous scientific processes, there is no guarantee that it would lead to a proficient investigator. The concepts cannot be deemed empirically valid for the role and are thus, unreliable constructs from which to base decisions on (Marcum et al., 2010). The lack of training identified by covert investigators may in part be due to the lack of research that can guide the development of an appropriate training program. The assessment of necessary competencies should therefore evaluate the job or the individual who is working in the job to uncover the strategies required for successful daily operating. This information could then inform training and selection decision making, as well as contribute to the literature on social engineering processes.

## **Research Aims**

The current research seeks to understand and promote the awareness of the expertise required for covert investigations of cybercrime that use social engineering skills. This will be done through interviewing law enforcement officers using a method developed explicitly for eliciting tacit knowledge. This research will deepen our understanding of the knowledge and skills required for covert cybercrime investigations. It will also provide a cross-comparison of skills required for investigating different types of cybercrime. As this will be the first study aimed at understanding the expertise of social engineering tactics in covert operations against cybercrime, it is exploratory. As such, no specific hypotheses regarding the knowledge of investigators can be made. However, it is expected that investigators will hold tacit, expertise knowledge that can be explored using in-depth, semi-structured interviewing. Furthermore, it is predicted some techniques discussed within the security studies on social engineering techniques may be identified within law enforcement, such as the skills used in fabrication, or data-gathering. Alternatively, skills identified within social psychological research on influence, such as authority or reciprocity may also be applicable for participants.

The primary aim of the present study is, therefore, to develop a greater understanding of the tacit expertise that investigators of cybercrime hold. This research will seek to elicit investigators' tacit knowledge through Applied Cognitive Task Analysis (ACTA) interview methodology (Militello & Hutton, 1998). ACTA can assist in identifying and articulating the cognitive processes involved in investigative procedures, and is an efficient means of extracting and describing the methods experts use in undertaking complex cognitive tasks. Through an explicit

understanding of these skills, more directed training programs for investigators could be developed in the future.

The primary research questions for the current study are as follows:

1. What are the skills, knowledge and techniques utilised by law enforcement when engaging in an undercover online investigation?
2. Are there any differences in the skill sets required for investigators of covert cybercrime operations, depending upon the crime being investigated?

## **Methodology**

Minimal research exists on how law enforcement conducts covert investigations online. As such, like other studies that have sought to develop an initial understanding of cybercrime investigation (Harkin & Whelan, 2019; O’Leary & D’Ovidio, 2007; Tetzlaff-Bemiller, 2011), understanding the work from the perspective of law enforcement is a critical first step. This study aims to develop the evidence-base on what skills are needed to investigate cybercrime in covert operations. This evidence will then be able to inform training, assessment and selection of employees.

The method section will be organised in the following way. First, the qualitative research design will be introduced; this will place the current study within the broader literature on qualitative methodology. The use of interviews will then be explored in order to state why this method of research design has been employed. The process of data collection, an interviewing procedure called Applied Cognitive Task Analysis (ACTA), will then be described and evaluated. The research procedure, including ethical considerations, will then be considered in full. Finally, the framework for data analysis will be presented.

### **Qualitative Approach of the Current Study**

The need for qualitative research has grown in line with the appreciation for environmental diversity and methodology that emerged from post-positivist perspectives (Willis et al., 2007). Qualitative research considers context, experience and the broader conditions of social life, in order to arrive at information that enhances a holistic understanding of phenomena. This is in contrast to making statistical linkages and predictions as seen in quantitative research (Golafshani, 2003). Qualitative research methods can potentially portray a broader assessment of the



complexities of psychology that might otherwise be missed with more traditional methods (Flick, 2018).

Qualitative research typically works within different ontological paradigms than quantitative research (Ponterotto, 2005). The experience of events is not considered an objective reality that can be transposed from laboratory experiments with little external validity. Nor is it always appropriate to generalise a single set of results widely, as everyone experiences life through a perspective that is unique to them and their background (Croker, 2009; Kraus 2005). Hence, any meaning that is attributed to events is based on an individual's creation of meaning; humans construct their reality, and this reality is strictly inimitable (Kraus, 2005). A diverse range of philosophical perspectives guide qualitative research. However, most relevant for the current research are approaches that typically have the underlying assumption of relativism (Bryman, 2012; Cupchik, 2001; Ponterotto, 2005).

Both forms of methodology, qualitative and quantitative, are valuable approaches. When trying to cognise a complex phenomenon or appreciate participant experience and knowledge of an event, qualitative research is typically the most appropriate choice (Elliot et al., 1999). Qualitative research is often useful when there is a lack of understanding about the nature and scope of the phenomenon under investigation (Bryman, 2012). Therefore, when trying to explicate the skills and processes used by law enforcement in social interactions with offenders, qualitative research is the more relevant research choice.

### **Characteristics of Qualitative Research**

Common approaches for conducting qualitative research exist (Bryman, 2012). A key characteristic of qualitative research is that it is inductive (Merriam &

Grenier, 2019). In comparison to quantitative research where prior theory guides the development of a hypothesis, qualitative research is guided by the data collected.

Qualitative research can be considered a *bottom-up* approach, whereas quantitative research is often a *top-down* approach (Bogdan & Biklen, 1997). The bottom-up approach is particularly relevant for the current study, as the lack of prior research means that it is difficult to state in advance the expected findings with any degree of precision. The findings and assessments that will be described are based on the cumulative appreciation of participant experience, as seen through this study, and cannot be predicted on the basis of pre-existing theories.

Qualitative research also requires the researcher to be active and embedded within the data collection process. The active participation by the researcher allows for rich and detailed reporting of participant experience (Crocker, 2009). Researcher involvement and relationship building is supported within qualitative research (Sutton & Austin, 2015). Quality interview data requires more than an interviewer asking the participant questions (Patton, 1980). The present research has conducted in-depth interviews which thoroughly traversed the challenges and details of the role, this then allowed for truly descriptive data.

A further component of qualitative research is the communication of findings in a descriptive, detailed and transparent way (Bogdan & Bilken, 1997). The descriptive process is designed to create meaning out of the data (Kraus, 2005), which is a continuous process. Critically, the researcher must always maintain a viewpoint that they are the vehicles for participants' voices. Hence, throughout the collection, analysis, and reporting of data, the research must maintain the speakers world view, thoughts and experiences (Sutton & Austin, 2015). This study aimed to present the characteristics of the job as accurately as participants described. The results have

sought to be detailed and vibrant, easy to make sense of, and true to the experience of the participants.

Another component of qualitative research describes how qualitative approaches are useful methods when trying to develop a theoretical and comprehensive understanding of unexplored phenomenon (Flick, 2018). Qualitative research offers the opportunity for more exploratory research; qualitative studies can produce entirely new ideas and concepts (Croker, 2009). Consequently, strict research questions or hypotheses are not always required, and can even impede the data collection process through applying a restrictive framework to the data, rather than allowing the data to provide the framework itself (Croker, 2009). Cybercrime and online covert investigation, both represent a niche and emerging environment. The research questions developed for the current research were designed to give a fundamental guide on how to gather information, but no specific hypotheses were made.

Finally, due to the comprehensive information gathered through qualitative research, large sample sizes are not always a requirement, hence the current research has eight participants. Rather, the goal of qualitative research is data saturation (Marshall et al., 2013). Data saturation, also termed ‘information power’ by Malterud et al. (2016), is where the level of information gathered from participants dictates the number of participants required. Judgement by the researcher as to the suitable number of participants necessitated in order to reach data saturation is an iterative and flexible process (Bryman, 2012).

## **Evaluating Qualitative Research**

The most pervasive criticism of qualitative research comes from the position that research gathered through qualitative approaches has few means of demonstrating validity and reliability, and is consequently less able to provide useful information to the scientific community (Merrick 1999). However, these ideas are conceptualized differently in qualitative research (Merrick, 1999). In qualitative research, rather than using validity and reliability to determine the quality of research, credibility and dependability are used instead (Gregory & Russell, 2003). Credibility refers to the trustworthiness of the data and the extent to which it represents the data gathered (Nowell et al., 2017). Trustworthiness of information in qualitative research is more aptly considered to be having regard for the ability of the researcher to understand and translate a collective participant meaning (Merrick, 1999; Williams et al., 2012). Dependability is another way qualitative research is evaluated. Dependability can be seen as similar to quantitative conceptualisations of reliability (Golafshani, 2003), which considers the consistency of the results and the replicability of them over time (Koch, 2006).

Procedures exist that can assist researchers in enhancing the dependability of the research. Primarily, this can be achieved through triangulation, and methods for audit checking. Triangulation is the use of multiple forms of data or sources to assess the research issue or question from various stances (Flick, 2004). These sources can be researchers, data collection tools, methodology, or theory (Bryman, 2012). The most relevant form of triangulation for the present study has been that of theoretical triangulation, which involves exploring how the results of a given study are similar to or consistent with previous theoretical work (Russell & Gregory, 2003). While no research or comprehensive theory of online covert investigators work exists, if there

are parallels between the present results and ideas in previous literature, it would be a positive form of theory triangulation. Another relevant avenue of triangulation for the present study is method triangulation (Casey & Murphy, 2009). Consistency within participant responses provides a way of measuring the dependability of the materials used, and the accuracy of the data gathered (Stevenson & Mahmut, 2013). Finally, reliability can also be increased through audit checking, such as through providing participants with the option to review their transcript to check that it is representative of what they sought to convey, or following rigorous processes for analysis and data-logging (Carlson, 2010). Both of these forms of review were conducted for the present study.

Best practice guidelines for increasing the trustworthiness of research require employing strategies that will inform the reader that the results are representative of information gathered (Bryman, 2012). The use of multiple data sets or participants that point to similar findings (triangulation of data) is a valuable tool to display convergence of meaning (Lincoln & Guba, 1985). Furthermore, the findings should be written in a manner that provides clear descriptions, allowing the reader to become immersed in the environment of exploration, similar to the researcher (Bryman, 2012). This includes displaying quotations of participant experience that capture the essence of the themes identified (Cope, 2014). This transparency allows for a more in-depth understanding by the reader, and also promotes trust that the data is presented correctly. Finally, the trustworthiness of qualitative research can be increased through the minimisation of bias by the researcher as best as possible (Carlson, 2010). Complete objectivity by the researcher is not expected (Pope, 2002). The researcher's perspective and individual contribution can be a positive and beneficial aspect of qualitative work (Sullivan, 2002). However, this positive effect of subjectivity

requires active self-reflection on the part of the researcher in order to understand any potential biases that could influence the research (Merrick, 1999).

Qualitative research is a powerful tool to employ when trying to examine the more intricate patterns of social life and behaviour (Erikson, 2012). Qualitative research allows for a depth of understanding that is often missed within deductive methods of analysis (Soiferman, 2010). The multifariousness and nuance of detail uncovered through qualitative work will see qualitative research persevere as a robust research method strategy (Erikson, 2012). However, in the continued use of qualitative approaches, acknowledgement of the limitations and processes to mitigate them is crucial.

## **Interviews**

Within qualitative work, interviews are the most prevalent form of data-gathering (Cassell & Symon, 2004). The goal of using interviews is to gather rich, substantial, and raw information that represents an event or phenomenon from the perspective of the participants (Cassell & Symon, 2004). Therefore, flexibility in structure and questioning is vital in order to be able to fully interact with all topics that are uncovered during the interview process. The flexibility of interviews allows for a diverse range of epistemological paradigms to utilise the data-gathering technique, ranging from realist to radical constructionist philosophies (Cassell & Symon, 2004).

The current research will take both a constructivist and realist approach. This is an ontological paradigm that has been only selectively discussed within the research (Cupchik, 2001; Jackson & Nexon, 2004; Iofrida et al., 2014; Sterling-Folker, 2002). While usually considered opposing paradigms (Bryman, 2012), the present research

acknowledges how social perspectives will influence the experience of working covertly, and the perception of techniques used. However, the research also recognises that the description of online covert work by investigators will be an honest and authentic depiction of the real-life working environments for New Zealand (NZ) Police covert investigators. The goal of this study has been to synthesise the different perspectives, backgrounds and life experiences expressed into a credible and trustworthy description of engaging in the role of covert online investigator.

Interviews can be utilised as a structured, semi-structured or unstructured tool (Gill et al., 2008; Jamshed, 2014). The present research followed a semi-structured interviewing method. This interview approach means that the questions were pre-determined and acted as a guide for the interview. However, questions were predominantly open-ended, allowing for the exploration of new ideas and topics as they arose (Jamshed, 2014). The interviews conducted in this research used the ACTA method as a guide for questioning across participants.

## **ACTA**

The purpose of the ACTA interviewing technique is to uncover the cognitive demands and skills required for various sub-tasks of a given job (Militello & Hutton, 1998). This form of interviewing was utilised due to the following considerations. It is in-depth and so facilitates a cross-comparison of answers due to the completeness of data, or information power gathered. ACTA also does not require extensive interviewer training (Hoffman et al., 2002; Hoffman et al., 1998). Finally, ACTA has a strong theoretical and empirical basis and has been applied successfully to many diverse settings such as intelligence analysis (Hutchins et al., 2007), firefighter training (Okoli et al., 2016), US Navy operations (Bisantz et al., 2003), and investigative profiling procedures (Knabe-Nicol & Alison, 2008).

ACTA identifies the skills, strategies, and processes used by experts in particular tasks. ACTA can also highlight any gaps in a process, and opportunities for error. All of this data is then able to inform selection, training, and policy and procedure development (Militello & Hutton, 1998). As with other expert domains, eliciting this expertise can speed up an otherwise experience-based process, which requires extensive time (Schraagen et al., 2000). Allowing for this wait continues to leave a significant knowledge gap within academia and policy. Therefore, this study's use of ACTA seeks to identify and understand this expertise and make an important contribution to theory and practice.

ACTA is composed of three sections: the task diagram, the knowledge audit and the simulation interview (Militello & Hutton, 1998) (appendix 3). The task diagram seeks to broadly synthesise ideas about the tasks required for a job, and highlight the problematic cognitive portions of the task. The knowledge audit then explores aspects of expertise required for a specific task or subtask. As each aspect of expertise is uncovered, it is probed for concrete examples in the context of the job, cues and strategies used, and why it presents a challenge to inexperienced persons. The simulation interview then allows the interviewer to probe the cognitive processes within the context of a specific scenario. The use of a simulation or scenario provides job context that is difficult to obtain via the other interview sections. Therefore, the simulation interview allows additional probing around issues such as situational assessment and common errors.

## **Procedure**

### **Design**

The current research utilised an inductive, exploratory design, using comprehensive semi-structured interviews based on constructivist, realist



perspectives. This approach allowed for flexibility in questioning all necessary facets of behaviour, along with the representation of participant ideas as demonstrative of their work.

## **Recruitment**

Participants for this study were NZ Police employees, selected from the Online Covert Group (OCG), and the High-Tech Crime Group (HTCG). Participants were recruited through the primary researcher providing an information sheet along with a consent form (appendix 1 and appendix 2), to the managers of both the OCG and the HTCG. These forms were then distributed to all employees who have engaged in online interaction. Covertly interacting with offenders is not an exclusive role of all police in OCG and HTCG. Therefore, participants recruited for this study were required to have experience in discreet covert operations. Any participants who volunteered for this study informed their managers. The managers then informed me of the contact details of relevant participants. From this information, I then contacted participants with the information sheet, consent form and interview schedule (appendix 1, 2 and 3, respectively) and instructions on how to review and complete the relevant sections before the interview.

## **Participants**

The sample for this research was determined through a purposive sampling process (Russell & Gregory, 2003). Participants for this research were six workers from the OCG and two workers from HTCG. Collectively, eight participants were interviewed. Due to the small sizes of the teams, this was considered representative of their workgroups. No demographic data was collected. This was in order to protect the anonymity of workers, considering any further identifying information may reveal who was interviewed.

## **Data Collection**

Participants were contacted by their managers with an information sheet and consent form. The information sheet detailed who I was, what the research was concerning, including the background and the purpose, and what their participation would involve. The consent form highlighted any risks involved, and also included information regarding the ethics approval from the Victoria University Human Ethics Committee. Any participant interested in participating could advise their manager, who then provided me with a list of email addresses and dates on which the interviews were able to occur.

Contact between myself and participants was then made to provide all documentation to participants. This included providing the ACTA template, the consent form, and the information sheet. All three forms are included as appendices: appendix 1, appendix 2 and appendix 3. Participants were then told what each of the forms was, and in preparation for the interview, to complete part one and two of the ACTA forms. Participants were informed that part three (the simulation interview) could be left exclusively for the interviewing process. These forms were provided one week in advance of interviews and completion of the necessary sections was required before the interview. The interview location, confirmation of timing, and an offer of contact if any questions arose while completing the forms was also provided.

Interviews were conducted at NZ Police premises in a private office. First, the research goals and risks outlined in the consent form were described to participants. Participants were then asked if they gave permission for notes to be taken and the interview to be recorded. This was to ensure participants fully understood the purpose, risks and confidentiality involved, and consent was made knowingly and voluntarily.

All participants agreed to this process and acknowledged that they could stop the recording or process at any point.

The interviews sequentially ran through each of the components in the ACTA interview process: the task diagram, the knowledge audit, and the simulation interview. Participants had already completed some sections of the task diagram and knowledge audit to varying degrees prior to the interview. This familiarity aided participant understanding regarding the purpose and direction of the interview. Participant responses to these sections also guided the flow of the interview. Their answers were discussed in more detail along with new areas of questioning arising organically throughout the interview process.

The task diagram broadly synthesised the components of covert investigation into between one and five subtasks as determined by the participants. The purpose of the task diagram is to break down the complex role of covert investigation into conceptualised skills or subtasks. Each subtask identified by participants was discussed to gain an understanding of the role and the context without more directed questions. These subtasks then formed the basis of additional, more detailed discussion in the knowledge audit.

The knowledge audit explored the most important subtasks, as identified by participants in the task diagram. Participants are asked about examples, challenges, and strategies used for the given skill area. Nine areas for questioning are covered under the knowledge audit: perceptual skills, anomalies, past and future, the big picture, tricks of the trade, improvising or noticing opportunities, self-monitoring and adjustment, information, and a scenario from hell. Thus, the subtasks are comprehensively probed in a nine by three matrix (the interview schedule is included

within appendix 3). The knowledge audit assessed what strategies are used as online investigators, as well as what the most considerable difficulties for novices are. The knowledge audit was the primary focus of the interview as this was the section where the most detail was gathered on covert job processes.

Finally, the simulation interview was designed to explore any further job requirements that had not yet been examined. During this section, participants were asked to think of a recent case and to describe what critical steps were taken from the start of the process to the conclusion of the investigation. The simulation interview was the most concise section of the interview, as most of the detail had previously been explored throughout the knowledge audit. Each component of the interview schedule was addressed sequentially with participants, starting with the task diagram and finishing with the simulation interview.

Due to the complexity of covert investigation, the interview schedule was considered a guide versus a strict process. This allowed for flexibility to explore new topics as they arose, skip areas where it was not considered as relevant to their work, or move through different sections of the knowledge audit in a variable order depending on how a topic arose. The interview was designed to be an organic process, rather than a structured and rigid process as depicted in the interview schedule. Participants had pre-completed the forms to a varying degree, so additional flexibility was required, along with different cueing for questions being necessary depending on participant familiarity with the ACTA forms. The length of the interviews varied between 80-120 minutes. Upon finishing the interviews, participants were thanked for their time and informed of the next steps in the research process.

## **Ethics**

Ethics approval for the research was obtained from both the Police Research Review and Access committee, and the Victoria University Psychology Sub-Committee of the Human Ethics Committee (0000027248). The critical ethical considerations that were acknowledged and accounted for will now be discussed.

Firstly, it was essential to ensure that all participation was voluntary, had no impact on work performance or requirements, and remained confidential. Participants were provided with an information sheet outlining all relevant information, and a consent form to sign prior to participation. Within the consent form, participants were assured of confidentiality. All identifying information was removed from data transcription, so no identifying information was stored electronically. Within the completed research, pseudonyms were used to reference any quotes.

Participants were offered a chance to review their transcript to allow for the removal of any quotes they did not approve of, or clarify any points that did not reflect intended meaning. Furthermore, to ensure operational security of tradecraft, the managers of OCG and HTCG were also provided with a chance to review any quotes that were used in the results. Further security of information was ensured through communicating to participants that all information discussed must offer no identifying information as to any cases or offenders. If any information was mentioned that contained identifying information, this was removed or anonymised from findings.

The research was perceived as unlikely to cause distress to any of the participants, given it related to tasks performed daily. However, participants were informed that they had the right to withdraw at any moment in the interview with no

repercussions. Interviewer distress was also not anticipated. However, if any distress was experienced, a path was in place to reduce emotional harm through frequent supervision contact, and the option to seek counselling via student help if required.

Data security within the study was maintained through several steps. Firstly, after all interviews were transcribed, the recordings were destroyed. Secondly, access to the data was restricted to primary researchers. Written documents and the recording device were transported in a locked and secured case between pre-designated locations. Recordings were stored on a password-protected drive which had restricted access. Transcriptions were also password protected on the secure drive. All physical copies of documents were physically destroyed via secure shredding.

Participants were not selected or excluded based upon culture or ethnicity, rather, the selection of participants was based purely upon skill expertise. Also, no demographics of participants were recorded or reported upon in the study. Moreover, very little research presently states demographic characteristics of cybercrime offenders, with no NZ specific research. As such, the results of the research will not negatively affect outcomes for Māori as an ethnic group nor any other cultures or minority groups. Instead, the implications aim to contribute to the training of police positively, and consequently enhance community safety. Finally, the interview schedule does not assess any cultural aspects of behaviour. Had there been any culturally relevant information discussed, steps were in place to consult a cultural adviser to understand how to best manage any conflicts.

### **Data Analysis**

Thematic analysis was used to explore the data. Thematic analysis seeks to locate and analyse the themes within a given data set by identifying meaningful

patterns (Braun & Clarke 2012). Themes in this context refer to clusters of shared experiences across participants which highlight unique patterns. The identification of themes seeks to answer any pre-determined research questions and guide the development of new research questions (Braun & Clarke, 2012). Thematic analysis is an incredibly flexible process without the requirement of preconceived theoretical assumptions that are necessary with other qualitative analytic approaches, such as grounded theory (Braun & Clarke, 2006). Thematic analysis is a process best used when seeking to maintain the detail in the raw data set and then translate and report this information into meaningful categories (Braun & Clarke, 2006). Thus, it is an excellent method to utilise when evaluating complex and meticulous data.

Due to these characteristics of thematic analysis, it was chosen as the most appropriate form of analysis for the present research. Specifically, inductive, semantic thematic analysis was employed, following a realist constructivist epistemological paradigm (Braun & Clarke, 2006). An inductive approach was decided upon as there is a distinct lack of theoretical guidance in the field of covert investigation. Therefore, an inductive approach was regarded as more appropriate to represent the description of skills as described by participants. The process of theme development was conducted at a semantic perspective in order to provide themes that were accurate and descriptive of participant experience. Given the complexity within social engineering and covert operations, an analysis process is needed that acknowledges and seeks to understand the breadth of the phenomenon. Finally, a realist constructivist epistemological position was followed, as it is considered that the work as described by participants is an accurate representation of the actions and skills required. The approach to thematic analysis followed the six-phase process as described by Braun and Clarke (2006). The six-stage process was followed because outlining the steps

explicitly allows for an increased ability to audit the research, and improve credibility and dependability.

The six-phase approach to thematic analysis identified by Braun and Clarke (2006) is described more in detail below. This approach allows for an intensive analysis of the data and can provide enlightening findings, without limiting the flexibility afforded to thematic analysis (Braun & Clarke, 2006). The stages are not conducted in a linear sequential direction; rather, the analysis is a recursive process. Swapping between the stages or having stages merge is accepted (Braun & Clarke, 2006).

1. Phase one involves familiarisation with the data set. Active and in-depth engagement with the data by the researcher is needed. This familiarisation helps in shaping ideas for the themes and codes prior to the coding process.
2. Phase two involves generating initial codes. After developing ideas on codes to utilise in phase one, the researcher must then formalise this and conduct the coding process. Codes are a far more superficial analysis of the data than generating themes, and are used as building blocks for theme generation.
3. Phase three is when the themes are assessed. The codes are looked at more broadly and holistically to try and find meaningful patterns among the codes. Codes may be combined and merged as they fit together, along with potentially creating a cluster of codes that do not seem to fit anywhere.
4. Phase four involves a review of the themes. This review entails assessing whether there is enough data to support codes and whether any further categories require merging. A two-stage analysis is suggested here. Firstly, a more focused scale of assessing the quotes used and the relevance to the



theme, and secondly, a more holistic assessment of reviewing the themes as they relate to the whole data set (Patton, 1980).

5. Phase five is the process of defining and naming themes. Phase five is when an analysis of each theme is conducted in order to accurately designate a name that succinctly captures what the theme is describing. Additionally, a comprehensive explanation of the theme content, meaning, and importance are written to describe to the reader the relevant and noteworthy findings.
6. Finally, phase six involves creating the report. The report should explain the themes in the researcher's writing, with participant extracts used throughout to highlight the representation of the themes.

The six-phase analytic approach was followed in the current research. Firstly, all interviews were transcribed in order to produce a data-set that could be reviewed and read for familiarisation. The primary researcher completed all the transcribing. Transcripts were read twice, further increasing familiarity with the dataset. Next, each interview was read and analysed several times to begin the official coding process. Some preliminary codes had been identified in the familiarisation procedure of stage one. However, most of the codes generated for the data were based upon the creation of new codes identified during the repeated reading of transcripts in stage two. Stage two was conducted using NVivo software, by collating all quotes that most appropriately fit into a given coding group. The third stage of analysis involved reviewing the current codes to see where common ideas may allow for some codes to be merged. It emerged at this juncture that there would likely be several categories, each with unique sub-themes within them. At this point, a diagram was created to conceptualise the findings visually. The themes were then assessed for the quotes contained within them, with some quotes being removed if others more accurately and

vividly portrayed the themes. The themes were also organised structurally to fit with one another. Themes were then provided names that accurately captured what was included within the category along with a brief description. This description was then supplemented with more detail in stage six during the final write-up process. A summary of the themes generated, including the relevant quotes, were provided to both the managers of OCT and HTCG, along with my supervisor to ensure they were accurate and representative.

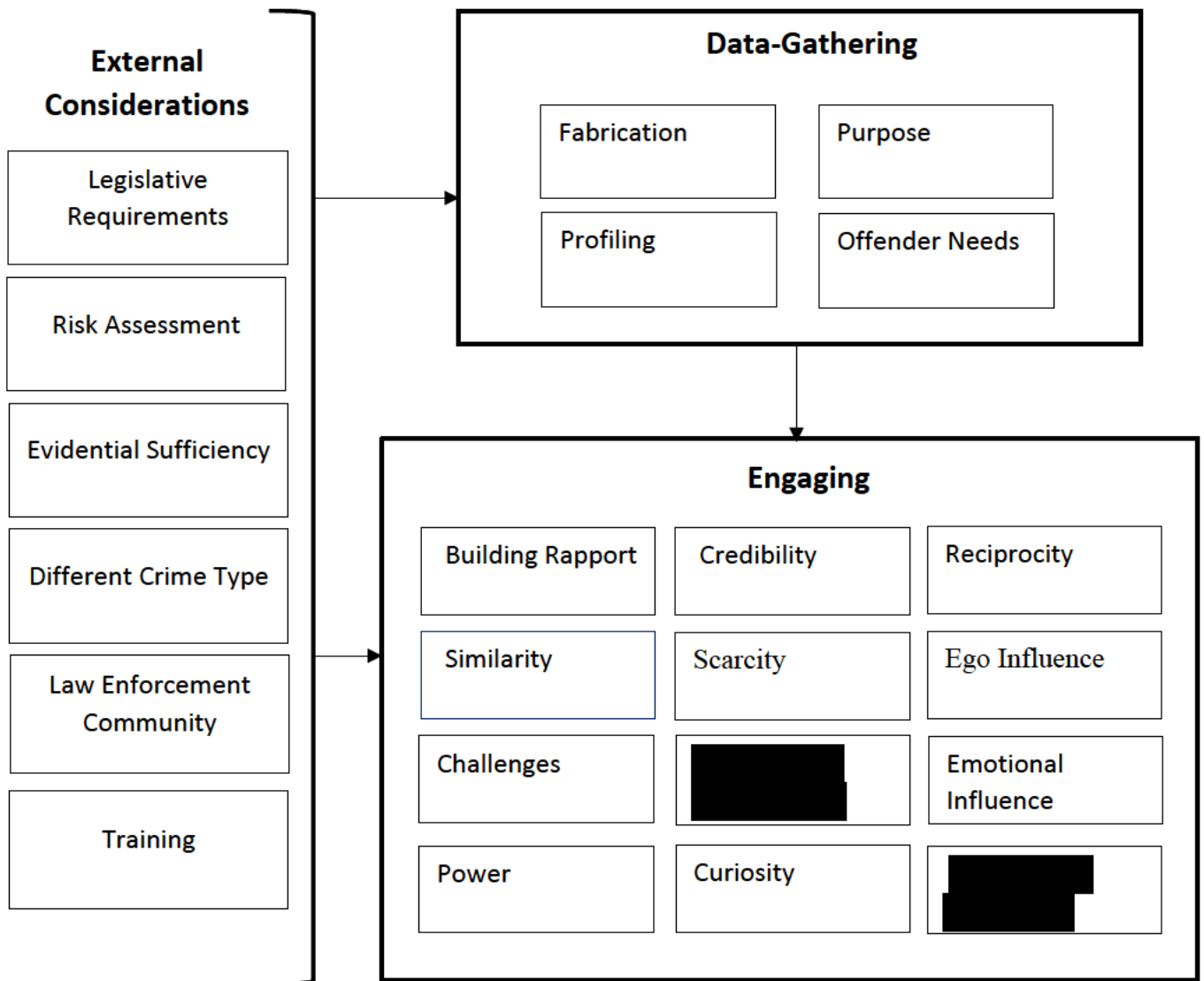
## Results

The thematic analysis led to the formation of three overarching themes and 18 sub-themes (see Figure 1 below). This figure displays both the sequential and recursive process of covert interaction. Each of the themes are discussed individually with quotes provided that highlight participant experience. Confidentiality of participants was ensured through the use of pseudonyms instead of participant names.

A summary of the results have been developed into a visual representation shown in Figure 1. This figure demonstrates how an undercover investigation proceeds. Beginning with the *Data-Gathering* stage, investigators complete each sub-theme in preparation for the initiation of social interaction. *Data-gathering* informs the *Engaging* process, which is where the critical social engineering techniques are located. *Data-Gathering* steps must be done prior to *Engaging*; however, the information gathered in the *Engaging* processes updates and informs the *Data-Gathering* themes. The third primary theme is *External Case Considerations*, which includes sub-themes that inform areas of awareness for both the planning and execution of covert interaction. These themes will be discussed in more detail below.

**Figure 1**

*Tactics, Techniques and Procedures of Online Covert Investigation*



### **Data-gathering**

The theme *Data-Gathering* represents a critical process whereby participants collected widespread available background information to help inform a successful covert interaction. This process involves an analysis of the environment, the suspect, possible strategies for information collection, and the development of an identity in

order to accurately prepare for covert interaction. Without an initial *Data-Gathering* process, interactions would lack preparation, resulting in challenges in accurately and reliably engaging the suspect. The investigator has to take the initiative to explore and obtain as much information as possible during the *Data-Gathering* stage:

[REDACTED]

[REDACTED]

[REDACTED]

Examples of background information that may be useful to an investigation include, but are not limited to:

- [REDACTED]
- [REDACTED]
  - a review of any posting online by the suspect;
  - any background information on the suspect;
- [REDACTED]
- [REDACTED]
  - [REDACTED]
    - accurate terminology;
    - any background information for an investigator's profile that may arise in conversation.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]


### *Fabrication*


*Fabrication* is the first sub-theme of *Data-Gathering*, and describes the development of an identity to utilise throughout the specific investigation. Participants reported the technique of *Fabrication* as a crucial process because all interaction between the investigator and the suspect occurred through the fabricated profile. The identity created is determined by the investigators, and is specific to the circumstance, crime, and environment:

While *Fabrication* is necessary to engage the suspect in covert interaction, the challenge and requirement for success is to fabricate a personality that will appeal to the suspect:



### *Profiling*

The second sub-theme, *Profiling*, is when investigators develop an idea of who a suspect is. 

. *Profiling* can be formal such as a structured analysis of the suspect, or informal such as brainstorming on likely traits:



This process allows for a greater understanding of the suspect, potentially resulting in a more accurate ability to predict and influence behaviour:



*Profiling* is critical as a pre-planning stage, and a process that should be continually updated throughout the interaction as more information on the suspect is gathered.

### *Purpose*

The third sub-theme of *Data-Gathering* that arose from the data is *Purpose*.

*Purpose* refers to clearly pre-defining the goal of what is required from the interaction. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Depending on the goal, the questioning style and relationship building will vary:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### *Understanding Needs*

The final sub-theme under *Data-Gathering* is the importance of *Understanding Needs*. [REDACTED]

[REDACTED]

This understanding allowed them to shape the likelihood that the suspect will engage:

[REDACTED]


[REDACTED]





### Engaging

The second primary theme identified in the research was *Engaging*. *Engaging* represents the skills and processes that participants utilised during covert social interaction. *Engaging* occurs during the stage of covert online work where an investigator is actively talking to the suspected offender using a false identity. The engaging process utilises diverse and unique techniques that aid in eliciting information from a suspect:



It requires the use of many social psychology principles relating to influence and persuasion, such as reciprocity, methods of liking, the effect of ego, and uniqueness. These will all be described in more depth below. These psychological principles generally typify what is thought of as social engineering. While not all the 12 tools identified within the theme of *Engaging* will be relevant in each conversation, they remained useful tactics that could be drawn on by an investigator in order to meet previously defined end goals. Using the appropriate social engineering strategies for

an interaction is critical for building relationships and guiding the conversation to the desired outcome:

[REDACTED]

### ***Building Rapport***

The first sub-theme identified within *Engaging* is the skill of *Building Rapport*. *Building Rapport* refers to being able to create clear communication with a suspect that engages them in conversation. Strong interpersonal skills and the ability to quickly draw another individual into conversation are critical for establishing a relationship and gathering information:

[REDACTED]

Investigators must be able to start and maintain conversations with incredibly diverse individuals, who are often very paranoid, and in a complex environment. This communication is also devoid of non-verbal cues such as body language, which are typically critical in providing information in conversations. Thus, the challenge for investigators is not only being able to develop rapport as a broad skill, but in being able to develop rapport through a screen, while maintaining the guise of another person. Being able to *Build Rapport* and get another individual invested in a conversation quickly is critical for successful interactions:

[REDACTED]

[REDACTED]

[REDACTED]

The early development of an effective profile is critical in the *Rapport Building* stage, along with maintaining the character created for the interaction.

[REDACTED]

### ***Credibility***

The sub-theme of *Credibility* considers how investigators must follow unspoken rules of the online environment. [REDACTED]

[REDACTED]

[REDACTED] which creates further challenges in trying to gather information:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Maintaining a consistent profile is also critical in helping to build a credible identity. Participants described how *Credibility* could aid in eliciting information or reassuring a suspect should they become suspicious. If a profile is credible, then it enhances the trust of the suspect and the likelihood that they will continue engaging with an investigator. [REDACTED]

[REDACTED]. Crucially, *Credibility* can only be maintained [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### *Reciprocity*

The sub-theme of *Reciprocity* considers how participants may provide information about themselves to try and trigger a response from the suspect or establish a debt of information:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The key is building a noticeable discrepancy in the information provided, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### *Similarity*

Participants reported the collective experience of how if the *Similarity* [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

If an investigator creates and enhances a level of *Similarity* [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### *Scarcity*

This sub-theme considers how creating a sense of *Scarcity* [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Participants reported the importance of first identifying what is sought by the offender in order to fabricate perceived *Scarcity*. Once this is achieved, the suspect will be more likely to comply with the investigator:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### ***Ego Influence***

Complimenting and building the *Ego* of the suspect was reported as a useful strategy [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Through increasing positive feelings towards the investigator, the suspect will be more likely to continue engaging with the false identity and may be more likely to provide information:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### *Challenges*

When presented with a *Challenge* or protest to an idea or belief held, the suspect may respond to that *Challenge* to disprove any allegations. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Finally, investigators can *Challenge* a suspect's identity, which for many individuals, is a fiercely protected ideal. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[illegible]

### *Emotional Influence*

Participants also utilised the tool of *Emotional Influence*. Influencing emotion included increasing positive feelings such as appreciation, debt, or gratitude and also inducing negative feelings such as anger, insecurity, or fear.

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### *Power*

Use of the sub-theme *Power* could be employed in two ways. Firstly, by making the suspect feel like they are in control and influential in the situation. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

A second way of using *Power* [REDACTED]

[REDACTED] in order to increase the suspect's respect towards the investigator, and potentially their level of compliance:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Which strategy to use is dictated by the situation and the person under investigation. Conducting comprehensive data-gathering strategies first indicated to participants which aspect of *Power* and control to use:

[REDACTED]

### *Curiosity*

Enhancing *Curiosity* in a suspect was reported as a useful skill through increasing the desire and interest of the suspect. The suspect is motivated to disclose information by a perceived reward. An investigator is playing on common responses in human behaviour:

[REDACTED]

The increased *Curiosity* would often make the suspect more likely to doing something, or reveal information about themselves that they otherwise would not do without the incentive of having their *Curiosity* needs met:

[REDACTED]

Finally, the sub-theme of [REDACTED] emerged as a common useful strategy for investigators when engaging with suspects online. [REDACTED]

Useful tactics include open questions, allowing for a pause in the conversation, mimicking, repetition as cues for further information, and summarisation to continue the conversation. These skills form the basis of active listening:

The use of reflection or mimicking works [REDACTED], and can also have the effect of building the ego, increasing familiarity, similarity or enhancing rapport as people may feel more heard and understood:

### **External Case Considerations**

The third primary theme identified in the research was *External Case Considerations*. This theme describes the additional skills required for online

investigation, including the knowledge and techniques that are needed to monitor investigative process and respond to the unique online environment. The following sub-themes are components of online investigation that are continually monitored throughout the different phases of *Data-Gathering* and *Engaging*. Each of the sub-themes discussed are related to one another only in the sense that they broadly apply to due process in an online covert investigation. *External Case Considerations* is a category intended to capture essential themes that became apparent in the analysis process that were not as conceptually linked together as sub-themes within *Data-Gathering* and *Engaging*:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### ***Legislative Requirements***

The sub-theme *Legislative Requirements* emerged as critical to investigative awareness. Covert online investigation requires constant monitoring of what is said, to avoid becoming agent provocateur. Legislation dictates that investigators cannot encourage behaviour that would not already occur without their presence. The consequences of not adhering to legislation around agent provocateur can be severe, in that a suspect may not be prosecuted if methods of obtaining evidence are not within the necessary legal boundaries:

[REDACTED]

[REDACTED].



[REDACTED]

[REDACTED]

[REDACTED]

The extensive legal requirements imposed upon investigators who work covertly online, places comprehensive cognitive demands on participants.

### ***Risk Assessment***

The sub-theme of *Risk Assessment* describes how participants explained that a constant awareness of the risk a suspect poses to themselves or others was vital to monitor continually:

[REDACTED]

[REDACTED]

[REDACTED]

Gathering information on a suspect's identity or previous crimes becomes secondary to preventing a crime occurring:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. *Risk Assessment* of the suspect throughout the whole interaction is, therefore, a crucial component in covert online investigations:

[REDACTED]

[REDACTED]

[REDACTED]

### ***Evidential Sufficiency***

When engaging with a suspect, participants have to be aware of what level of information is required in order to progress the investigation (search warrants, arrest, prosecution). Investigators are seeking identifying information and information relating to offences. When collecting this detail, investigators must know when they have reached various thresholds relating to *Evidential Sufficiency*:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Participants emphasised the need to be forward-thinking, [REDACTED]

[REDACTED], and ensuring the desired outcome for the investigation.

### *Different Crime Type*

The sub-theme of *Different Crime Type* identified the need for participants to develop further crime-specific knowledge depending on what crimes they were investigating. While similarities in the critical skills required are present throughout the *Engaging* and *Data-Gathering* process, specific knowledge is required on the area an investigator is directly working within. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The same techniques, tactics and procedures as described throughout *Data-Gathering* and *Engaging* can still be utilised regardless of crime type:

DP: You need a base level of skills but then specific skills for your area.

However, through changing the subject matter, an investigator may have to change what kind of offender needs are analysed, and what the appropriate ways to steer a conversation are, amongst other considerations:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

□ □ □ □ □

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### *Training*

Finally, the sub-theme *Training* became apparent because participants reported a lack of formalised training for the role. As such, participants often came from varied backgrounds wherein they could utilise other skills that had been gathered throughout their policing careers:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The limited preparation did not hinder the current employees or workgroups, particularly given participants all had extensive backgrounds within the police:

[REDACTED]

However, formalised *Training* would be useful to cover the more nuanced topics of the role. Having a formulated set of skills that are taught to new individuals would also be useful for the selection and testing of new employees:

[REDACTED]

### **Final Comments**

The analysis of the data for the present research was guided by the two research questions that sought to understand 1) the skills used by online undercover investigators, and 2) whether any variable skills were required depending on the crime type. The skills utilised by online investigators are described through each of the themes and sub-themes. Varied and extensive skills are required, which fit under pre-planning, operational action and cognitive considerations. The second research

question was answered within a sub-theme inside *External Case Considerations*, *Different Crime Type*. This sub-theme identified that there were indeed different knowledge requisites for investigators. The ‘how’ of the investigation remained extant across crime types, however, the ‘what’ of understanding changed. Investigators needed detailed knowledge of the nuances of the crime specific environment and offending behaviour.

## Discussion

This study sought to gain an understanding of what skills are necessary to conduct covert online investigations for NZ Police investigators. These specific skills, tactics and techniques used by covert investigators have been revealed more closely through the use of in-depth interviews. Due to the limited research available on covert investigation, this study sought to address a significant knowledge gap in how covert investigations are undertaken, including the internal and external resources required. Furthermore, as the lack of training in the area of specialist cybercrime investigations has been reported across the Western world (Hinduja, 2004; O'Leary & D'Ovidio, 2007; Tetzlaff-Bemiller, 2011), this research has been able to develop the foundations for what training should incorporate and consider.

Through thematic analysis, three overarching themes became apparent in the research project. [REDACTED]

[REDACTED]

[REDACTED]. A descriptive summary of the findings will now be explored. Following this, the findings will be situated within the broader research base on social engineering, police psychology and social psychology. The present study will then be critically reviewed for the relevant strengths and weaknesses. Finally, the broader applications of the research will be considered, specifically in the context of enhancing police covert knowledge, along with the implications for continued research within this area.

## Summary of Results

The first theme that emerged from the analysis was *Data-Gathering*. This theme predominantly considered the steps and processes conducted before engaging with an offender online. This theme was then further broken down into four specific

sub-themes, including *Fabrication*, *Purpose*, *Profiling* and *Offender Needs*. The sub-themes were not ordered sequentially, but were equally essential considerations when preparing for an investigative process. Importantly, investigators had to consider the suspect they were speaking to and adapt the first interaction accordingly. Thus, knowledge of how best to approach a suspect (*Profiling and Fabrication*), consideration of the unique personality of the offender (*Offender Needs*), and understanding the intention of the interaction (*Purpose*), combined to inform the *Data-Gathering* process. Investigators had to conduct comprehensive and detailed pre-planning and engage in extensive forethought.

The second theme, *Engaging*, covered the strategies that could be used by law enforcement when interacting with an offender. This theme was further broken down into 12 sub-themes. These sub-themes collectively made up the toolbox of conversation tactics that investigators could utilise in order to try to gather information from the offender. Not all tactics are relevant for every conversation. However, they represent common strategies investigators relied on, whether implicitly or explicitly, to develop a dialogue and influence the conversation towards their own goals. *Engaging* distinctly covers skills and procedures used during the undercover conversational phase of the investigation. Therefore, *Engaging* follows the *Data-Gathering* stage as a sequential process, yet the information uncovered through *Engaging* can, and should, update the information that informs *Data-Gathering* decision making.

The third theme, *External Case Considerations*, included six sub-themes. These sub-themes were not conceptually related to each other in the way that the sub-themes within *Engaging* and *Data-Gathering* are. Instead, the third theme describes the external background knowledge that a police officer must understand as an

investigator in the covert and legal community. Investigators must be aware of these sub-themes throughout the investigation process, and use it to inform their process and behavior throughout the entire investigation. The sub-themes contained within *External Case Considerations* are critical for ensuring the protection of the victims and officers involved, and the security of the case itself. Furthermore, this theme also details the broader care that must be considered in understanding the online covert environment, and how to take precautions to adapt the strategies for *Engaging* and *Data-Gathering* as needed.

The results from this study suggest that the process for conducting covert online investigations is complex and multifaceted, necessitating extensive cognitive demands be upon the investigators. As this was an exploratory study, broad research questions guided the data collection process. The first research question sought to understand what skills and procedures were used by investigators when engaging in a covert online investigation. This research question was evaluated throughout the analysis process, with all three themes and sub-themes providing data that describe how online investigators conduct their work. The skills needed by investigators are predominantly learned through experience rather than directed instruction. These skills include (a) how to initiate and maintain contact with offenders; (b) how to uniquely tailor conversational approaches in order to influence an offender and guide them towards one's goal; (c) how to understand the offender and the unique online environment from which offending occurs; and, (d) how to stay within the complex and rigid legal boundaries surrounding officers. The vast number of themes and sub-themes required to capture and describe these skills is an indicator of the breadth of knowledge required by online investigators.



The second research question aimed to understand whether any differences in skills were applied based on the crime type under investigation. This was reported by participants as a sub-theme within *External Case Considerations*, 'Different Crime Type'. The results reveal that regardless of the crime type, all investigators reported using the same skill set, as discussed throughout *Engaging*, *Data-Gathering* and *External Case Considerations*. However, which strategy or skill would be more beneficial changed slightly depending on the crime type. Investigators had to adapt their skills for different types of investigation. [REDACTED]

[REDACTED]

[REDACTED]. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] By in large however, the majority of skill sets were extensively transferrable. For an investigator to move from one crime type to another, they are required to undertake a familiarization period within the new online environment [REDACTED]

[REDACTED]

[REDACTED] Moving between crime types would not require a completely new approach on how to investigate crimes online. Rather, investigators would simply need to research and familiarize themselves with the nuances of the new crime type.

### **Situating the Research: Data-Gathering**

This study is the first of its kind to comprehensively explore the skills and processes utilised by online investigators. The results revealed are consistent with existing research and theory. These consistencies with theoretical literature can be found between *Data-Gathering* and theories of social engineering, between *Engaging* and social psychological theories of influence, and between *External Case Considerations* and police psychology research.

The process of *Data-Gathering* represents an essential set of skills and behaviours whereby investigators planned how to interact with a suspect. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. These skills display many parallels with existing literature on social engineering behaviours, including social engineering attacks. Social engineering efforts seek to gather information through utilizing deceptive guises or behaviours, principally from a social source, such as conversing with an individual (Tetri & Vuorinen, 2013). [REDACTED]

[REDACTED]

*Data-Gathering* skills revealed in the current research show similarities with those used for social engineering attacks. In their research into the behaviours used by individuals conducting social engineering attacks, Tetri and Vuorinen (2013) identified data-gathering as a key behavioural cluster wherein the engineer actively researches the target of the attack through online based open-source research, or methods of physical intrusions. These behaviours provide the engineer with important information that can be used to tailor an approach to the target and thereby gain access to what is needed. The importance of this is outlined in the start of the

discussion on data-gathering by Tetri and Vuorinen where they state “every attack requires knowledge about the target” (Tetri & Vuorinen, 2013, p. 1017).

Likewise, every covert interaction by law enforcement requires knowledge about the suspect. When investigating crimes online, law enforcement are not committing attacks on individuals in the way that the sample literature by Tetri and Vuorinen (2013) are. However, as can be seen, the principle remains the same. Investigators must know about the suspect whom they are to interact with, in the same way an attacker must know about their target. For the attacker, this phase involves obtaining information from open-source data, stealing, eavesdropping, or various technical means of stealing information, e.g. loggers. The purpose of this stage is to reduce the likelihood of a failed attack (Tetri & Vuorinen, 2013). Similarly, *Data-Gathering* represents [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]. However, the purpose of data-gathering for the two groups appears to be incredibly similar.

A further theme identified by Tetri and Vuorinen (2013) is fabrication, which was equally considered one of the fundamental aspects of social engineering attacks. The sub-themes *Fabrication* and *Profiling* were also revealed in the current study to be important to investigators conducting online covert operations. Fabrication by Tetri and Vuorinen is considered a subtle, deceptive influence of the environment.

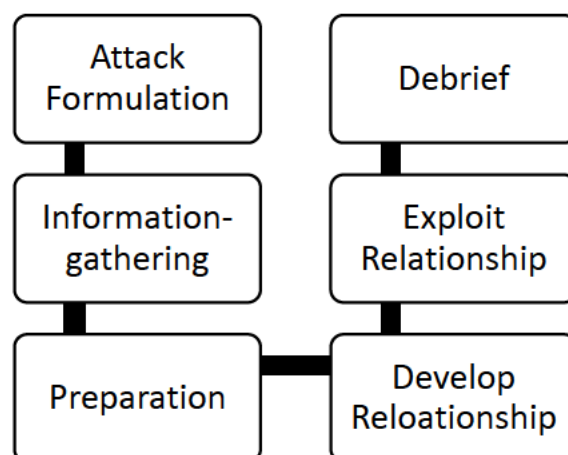
Fabrication analyses the setting of the victim and the most appropriate way it can be influenced while remaining unnoticed. For example, the use of the correct terminology is a simple way to fabricate a personality so the person being deceived would be less likely to question what is happening. This is in line with the sub-theme *Fabrication*, which outlines how careful development of a profile is conducted to reduce the likelihood of being identified as out of place. [REDACTED]

[REDACTED]. The use of *Profiling* is also important, as it is through the identification of the suspect's [REDACTED]

Further similarities between the sub-themes in *Data-Gathering* and previous research can be seen within research by Mouton et al. (2016). Mouton et al. assessed the key behaviours in a social engineering attack (see Figure 2).

**Figure 2**

*Social Engineering Attack Cycle as described by Mouton et al. (2016)*



The first stage in the social engineering attack framework by Mouton et al. (2016) is the attack formulation. Attack formulation is defined by Mouton et al., as the development of a goal and the identification of a target. This phase is very similar to the sub-theme, *Purpose*, found in the current research, wherein investigators must identify what the end goal of the interaction is. The use of formulating a goal for the deceptive interaction, either through an attack formulation or through *Purpose*, provides a framework to situate the task and direct the best strategies. Without first highlighting what is sought from the interaction it is difficult for law enforcement or attackers to tailor an effective approach for communication.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The second stage of the attack framework by Mouton et al., (2016) is information-gathering. According to Mouton et al., this process involves sourcing information about the target using a number of methods, including from other people, online sources, technical means, or physically going through their information (e.g., dumpster diving). This is similar to the theme of *Data-Gathering* found in the current research and data-gathering by Tetri & Vuorinen (2013), as discussed. The purpose of gathering the information and the importance of doing thorough background research is critical for both investigators and social engineers. Thus, having a comprehensive

understanding of the suspect regardless of the context is critical for increasing the probability of developing a relationship that will lead to high levels of information-gathering.

Finally, the third phase of the attack framework as described by Mouton et al., (2016) is the preparation stage, where the attacker may formulate a pretext or backstory that is developed based upon the target information. They may also identify the mechanism for interaction, and which psychological compliance principles to implement. This is consistent with the two sub-themes of *Data-Gathering*, identified in the present study, *Fabrication* and [REDACTED]. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Overall, investigators follow a very similar data-gathering process to that of social engineers as identified by Tetri and Vuorinen, (2013) and Mouton et al. (2016). The process may not be as sequential as described by Mouton et al. yet the key phases to consider in the pre-planning of interaction has many crossovers and similarities. Investigators and attackers alike must conduct extensive planning prior to the execution of engaging with the suspect. Importantly, it appears that regardless of the goal of engaging with an individual to gather information, be it legal and in the name of community protection, or illegal and in the name of personal gain, similar processes and steps are required in order to increase the likelihood of success. The theory of social engineering described by Mouton and colleagues applies to law enforcement covert investigation within the first three stages. This finding is

noteworthy because it suggests that there is a standardised process that must be adhered to in the preparation phase.

### **Situating the Research: Engaging**

The second theme that emerged from the data, *Engaging*, is also consistent with existing literature. Extensive similarities exist between theory and research on social psychology and social engineering, and the skills located within *Engaging* (Cialdini, 2009; Workman, 2008). The convergence of ideas indicates a standard method from which influence can be exacted upon individuals, regardless of their characteristics.

These sub-themes of *Engaging* comprise behavior that is considered exploitative or manipulative within social engineering literature (Atkins & Huang, 2013; Krombholz et al., 2015). While negative connotations are associated with the word ‘manipulate’, the use of social influence or the ability to cleverly control a situation are acts of manipulation (Hahnagy, 2010). The difference between investigators and offenders is that, for investigators, the influence is conducted without exploitative or harmful overtones. Furthermore, the goal of investigators is to protect and help the community at large. Thus, *Engaging* reflect the use of manipulation for beneficial purposes.

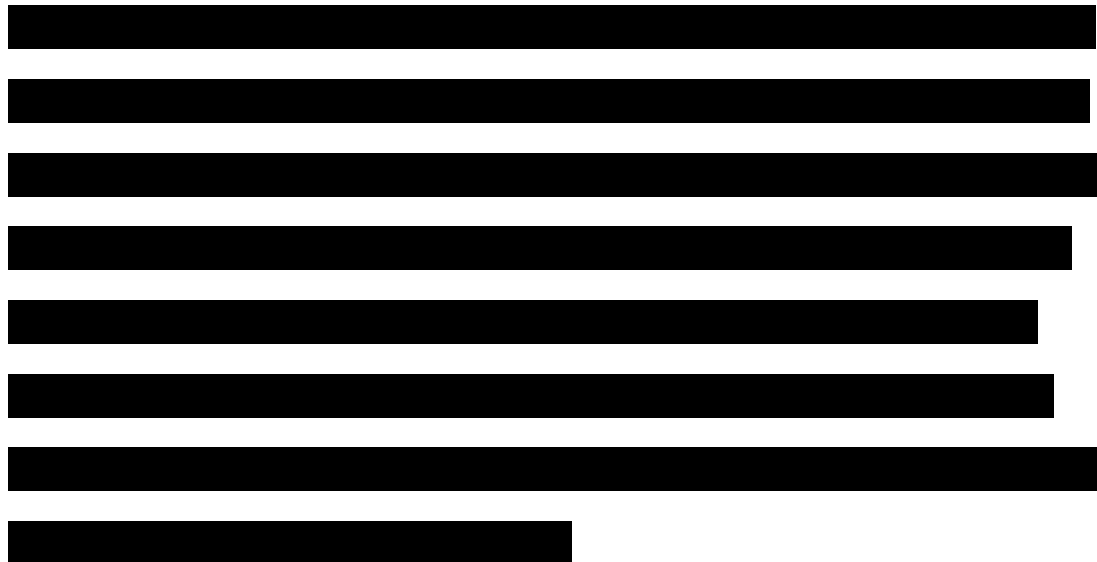
*Engaging* contains 12 sub-themes which describe how investigators talk to offenders online. [REDACTED]

[REDACTED] The

[REDACTED]

[REDACTED]

[REDACTED]



The skills of *Engaging* within the present study show resemblances to the theme of persuasion within Tetri and Vuorinen's (2013). Social engineers utilise various methods of persuasion to try to get their target to reveal information or comply with requests. Interestingly, the goal is to gain acquiescence from the target, so compliance is voluntary rather than due to threats. Threatening behaviour would be a separate manner of accessing information not constituted under a method of social engineering, as the free will of the person is removed (Perloff, 2016). Tetri and Vuorinen (2013) describe persuasion as a technique that requires active and purposeful interaction between the engineer and the target, for example, through direct conversation. The skills involved in persuasion as outline by Tetri and Vuorinen are: utilizing authority, validating the target, reciprocity, drawing on emotion, likeability, building rapport and the use of subversion. These techniques are notably similar to the skills found in the present research. *Reciprocity*, *Building Rapport*, and *Emotional Influence* are all directly comparable to reciprocity, building rapport, and drawing on emotion, respectively. Further resemblances can be seen between authority, subversion and the theme of *Power*, and likeability and the theme of *Similarity*. Thus, while it is difficult to analyze these similarities with more



distinction, it would seem many skills are certainly transferable and have been previously identified in relation to social engineering techniques. However, the present study identified a further seven skills that were not mentioned by Tetri and Vuorinen.

Some of these additional skills and sub-themes were discovered in research by Mouton et al. (2016). Mouton et al. used the concept of ‘compliance principles’ in their social engineering attack frameworks. Compliance principles are both explanations for why an individual may comply with instructions when they know they should not, and are also techniques that can be used by the social engineer in order to gain conformity. These compliance principles are based upon Cialdini’s (2009) work into six key psychological principles that can be influenced in order to gain obedience from an individual. Cialdini’s work appears repeatedly within the research on social engineering and thus, is highly influential (Archer, 2017; Bullee et al., 2015; Hadnagy, 2010; Mouton et al., 2016). As mentioned in the literature review, these six principles are reciprocity, commitment and consistency, social proof, liking, authority and scarcity.

#### Comparison **and** *Similarity of Social Engineering Techniques*

represented on page 105 provides a comparison of the sub-themes of the present study as compared to the persuasive properties of research by Cialdini (1984) and Workman (2008). These will also be discussed further below.

Reciprocity (Mouton et al., 2016) is when favours and requests are more likely to be adhered to by the target if the engineer has acted favourably to them previously. It is based upon the engineer creating a sense of obligation (Archer, 2017). Regardless of whether the favour is requested or desired, the individual who receives it will feel a sense of debt that increases the likelihood of returning the favour (Cialdini, 2009). Cialdini (2009) has postulated that this is mostly a universal rule of human behaviour. Similarly, the present research identified *Reciprocity* as an essential method in gathering information from offenders. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

A second compliance principle of Cialdini's (1984) work that is comparable to the current research findings, is liking. The principle of liking simply states that an individual may be more willing to comply with a request if they like the person who is asking for the favour (Mouton et al., 2016). Liking can be increased by physical attractiveness, similarity, providing compliments to someone, familiarity, and association, some of which work entirely unconsciously (Cialdini, 2009). Thus, it is a potent tool in which to exert influence. Investigators in the current study used some of these methods to enhance likability, including *Similarity* and providing compliments (*Ego Influence*), in addition to other methods such as *Emotional Influence* and *Rapport Building*.

The technique of *Similarity* incorporated the use of reflecting talking styles, which created a sense of positivity on behalf of the suspect, and also enhanced a sense of comfort and familiarity by creating and highlighting commonalities between one another. [REDACTED]

[REDACTED] Providing compliments can be seen in the sub-theme *Ego Influence* which was also used to enhance likability. [REDACTED]

[REDACTED] *Emotional Influence*, when used in a manner to increase positive feelings, would also increase a sense of liking by the suspect, as a further positive link would be created. Finally, *Building Rapport* may also contribute to a sense of liking by the offender, as when one can talk to someone effectively and build a conversational flow, a sense of positive regard, appreciation or comfort may be created. For many investigators, the anonymity of the online environment means physical attractiveness may not always be relevant. However, some investigative roles can directly play on this. Usually, the creation of a physically attractive individual is developed before the initial conversation and therefore is more related to pre-planning *Fabrication* than within the *Engaging* strategies. The factors therefore involved in why one might like someone fit under several distinct sub-themes identified within the present research. Using these likability tactics should enhance liking and friendship development which in turn increases the likelihood that an offender will comply with a request. Investigators can capitalize on this by building a positive relationship first, before seeking information relating to identity, or access to images.

*Scarcity* is a further principle identified by Cialdini (2009), which corresponds to a sub-theme of *Engaging* within the present work. Cialdini reports that scarcity has the direct effect of increasing value. That is, the rarer an item or possession is, the more it will be sought after. This effect is due to individuals creating a mental shortcut between what is hard or challenging to acquire being of higher value. Further, the use of scarcity places restrictions on our options and freedoms. When there is restriction directed upon our freedom to access choices, the desire to enhance individual autonomy can lead to the decision to seek what is being restricted (Brehm, 1966).

[REDACTED]

The final technique identified in both the work of Cialdini (2009) and the current research is authority. The use of authority is based on the idea that people will comply with requests if the individual requesting the information is in a position of authority (Mouton et al., 2016). Authority corresponds to the sub-theme *Power*. However, the current research expands on this idea of holding authority by suggesting that investigators can use different positions of power to influence a desired outcome.

[REDACTED]

[REDACTED]

The sub-theme *Challenges* also relates to authority, [REDACTED]

[REDACTED]

The final two principles identified by Cialdini (2009) were social proof and commitment and consistency. However, these were not found as prominent ideas in the current research. Social proof or validation is the tendency for people to comply with an action if they believe other people are, or if it is considered the social norm in the scenario (Cialdini, 2009; Mouton et al., 2016). Given conversations happen in relative isolation for most investigators, there is little opportunity to use group compliance or social norms. Therefore this principle is less applicable, given the anonymity of the online environment.

Commitment or consistency details how once an individual is committed to an action, they will be more likely to continue to behave in a manner consistent with their attitude (Archer, 2017). Influencing commitment and consistency was not a tactic that came through in much detail from interviews with investigators, however, drew some similarities with the sub-theme *Challenges*. This technique shows similarity to commitment and consistency through influencing the desire for an individual to be consistent with their perceived identity. Therefore, when a confrontation to that identity is stated, they may be more likely to reject claims that challenge their perception of themselves. Challenging identity specifically was not reported upon frequently enough to merit its' own consideration as a sub-theme. Rather, *Challenges* as a sub-theme encapsulates the various methods through which an alleged offender could be challenged.

Further research directly probing the techniques used within the theme of challenges would be beneficial in highlighting any additional relevance to the concept of commitment and consistency. For example, it would be interesting to assess whether more directed use of commitment and consistency applies to online investigation. Commitment and consistency could be applied through the investigator asking the offender their opinion on sharing photos or personal details. If the opinion provided were one of openness, then the investigator would be in a prime position to ask for the information. This would be because the suspect has already verbally expressed open-mindedness to sharing, accordingly, they may feel a measure of pressure to act consistently with an attitude they have expressed.

Workman (2008) has similarly completed research into what psychological principles may affect social engineering success. As such, his work can be contrasted against the present research to see whether further techniques appear in the broader

literature, or whether they are unique to the investigation of online covert operations. Workman's (2008) theory of social engineering also looked at six factors that would influence persuasive ability, and employed a field study to test the six variables. These variables included normative commitment, continuance commitment, affective commitment, trust, fear, and reactance. All factors significantly increased susceptibility to social engineering ( $p < .001$ ), with the exception of reactance, which showed a positive but not significant relationship ( $p > .05$ ). Interestingly, each of these factors is similar to that of Cialdini's (2009) principles, with slight variation (see Table 1 in the literature review).

Normative commitment describes the feeling of obligation to reciprocate an action due to a perception of customary response or responsibility (Workman, 2008). Normative commitment is consistent with both Cialdini's principle of reciprocity (2009) and with *Reciprocity* in the current study. This suggests that creating feelings of obligation and reciprocity are stable and pervasive human traits that can be used reliably in conducting online investigations.

The second principle, continuance commitment, describes how an individual seeks to maintain equilibrium between attitudes and behaviours (Workman, 2008). This idea is similar to commitment and consistency by Cialdini (2009). However, Workman expands this concept to include time spent as evidence of a commitment. Thus, if investigators were to invest time in pursuing a suspect, the time expended by the suspect in return would be a commitment that could then be used to try to gather information. Likewise, affective commitment can be compared to the concept of social proof described by Cialdini. Affective commitment explores the way that an individual may generate their self-identity based upon social connections, which can then form a social identity that is protected. Affective commitment leads to further

effort and attachment towards those who share similarities. These two principles did not emerge as distinct within the current research. This was due to the more isolated nature of the online environment, and the inability to determine social norms. As affective and continuance commitment appear to be influential human traits though, they should be applied and tested more thoroughly in future research.

The third principle is trust. The concept of ‘trust’ by Workman (2008), describes how social engineers can build rapport and a sense of friendship by influencing the needs of the target. Those who have higher levels of trust will be easier to influence. This concept of trust relates to many of the sub-themes of *Engaging* in the current research. [REDACTED]

[REDACTED]. However, tenuous forms of trust and relationships can be cultivated. When doing so, [REDACTED]

[REDACTED]

[REDACTED] Other methods of trust development include *Fabrication* techniques for developing profiles that would be attractive, [REDACTED]

[REDACTED]

[REDACTED] These tactics may culminate in the net effect of increased liking and consequently, trust.

A further principle by Workman (2008) is fear. This relates to the principle of authority identified by Cialdini (2009), as they both increase the ability to induce obedience in a target. However, while achieving comparable goals, the focus is slightly different. Workman focuses on the emotions that are being targeted (fear) whereas Cialdini focuses on the position used to induce this. Increasing or decreasing the threat level can enhance or reduce the fear in the suspect, which in turn influences



compliance. The sub-themes of *Power*, *Challenges* and *Influencing Emotion* found in the current research are consistent with these principles [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Finally, while not shown to be significant in Workman's (2008) study, reactance is still an intriguing facet to explore, especially considering the direct association to the use of scarcity by Cialdini (2009) and investigators in the present study. Workman (2008) proposed that the more reactant a person is to the depiction of scarcity or shortage of supplies, the more quickly they can be influenced. Workman (2008) does not explain why this hypothesis was not significant; however, further research within the use of scarcity has highlighted it as a crucial skill in influencing individuals (Cialdini, 2009; Jung & Kellaris, 2004). Therefore, perhaps a replication of Workman's research is needed to provide further reliability to the results, particularly given their importance in the present research and additional literature, as stated.

There is extensive consistency between ideas in this research and previous literature. The culmination of in-depth social psychological work by Cialdini (2009), the experimental studies by Workman (2008), and the present research, provides converging evidence on standard techniques that can be used to influence an individual across varying environments. Table 2 provides a comparison of the relevant sub-themes of the present study as compared to the persuasive properties of research by Cialdini (1984) and Workman (2008).

**Table 2***Comparison and Similarity of Social Engineering Techniques*

Current Study	Cialdini (1984)	Workman (2008)
Reciprocity	Reciprocity	Normative Commitment
<i>Challenges - Challenging Identity</i>	Commitment & Consistency	Continuance Commitment
	Social Proof	Affective Commitment
Ego Influence Emotional Influence Building Rapport Similarity	Liking	Trust
Power Challenges	Authority	Fear
Scarcity	Scarcity	Reactance

*Note.* When the themes have been italicized in the Current Study column, this is due to a more tenuous association with the concepts outlined by Workman (2008) and Cialdini (2009).

Many of the previously identified techniques of influence appear to be relevant

[REDACTED], [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Not only do offenders who are conducting social engineering attacks use these skills (Tetri & Vuorinen, 2013), but also sales

consultants, marketers (Cialdini, 2009) [REDACTED] This study, therefore, offers further support to a prevailing theory of persuasion and influence.

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] Rather than influencing the individual, investigators are influencing the flow and method of conversation. However, *Credibility* and *Curiosity* are more psychologically-based technique to gather information, like those of the compliance principles. Thus, it is interesting that these were not found in either of Cialdini's or Workman's research. These findings appear to be unique in the context of social psychology. This study therefore contributes meaningful new findings to the research on social psychology influence. However, some of these skills do appear within additional research on law enforcement investigation, as is discussed below.

Hadnagy (2010) is a further researcher who has done extensive work into prevalent methods of social engineering and how to understand the techniques used. Within his book, Hadnagy explores the use of interviewing and interrogation within law enforcement. He argues that interviewing and interrogation are critical skills needed by a social engineer as they both lead to elicitation, which is often the goal of a social engineer. These skills involve paying careful attention to word use, wording questions in a manner to elicit a response, pre-planning what the response of the suspect will be and wording a question accordingly, mirroring or reflecting, utilizing active listening and open-ended question. All of these techniques were described by

investigators as useful in the present research, under the sub-theme *Interviewing Techniques*. There is thus consistency between the present research and Hadnagy's work. This consistency may be due to the fact that Hadnagy chose to first analyse the typical behavior of frontline law enforcement and then apply that to social engineering. He therefore captured a broader degree of possible avenues from which social engineering can apply. Similarly, this current research focused on a subset of law enforcement where previous training as a constable could be applied.

In addition to interview skills, framing is a further technique revealed by Hadnagy (2010) to be a critical to social engineering. Framing, as described by Hadnagy is the choosing of words selectively in order to invoke specific mental ideas or precepts, and is consistent with the skills described by the present research under [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. Preloading is a further skill explored by Hadnagy, which is also supported within additional social engineering literature (Mitnick, 2002; Mouton et al., 2016). Preloading, as described by Hadnagy, is a method of conversation management wherein one primes ideas before introducing them. While not directly referred to by name in the present study, the skills within the sub-theme [REDACTED]

[REDACTED] refer to this idea. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

---

<sup>2</sup> 'fap to' is a common colloquialism in the online environment as a reference to masturbating.

Finally, Hadnagy (2010) emphasises the importance of credibility to the social engineer. One must understand the environment and the specific cues in the environment to be successful. A social engineer can also highlight this credibility in building trust and eliciting further information. This effect is very similar to how law enforcement in the present study were able to use *Credibility* to their advantage. Hadnagy also expresses the importance of several other skills that have already been described as being important to both the current research and other previous research (Cialdini, 2009; Workman, 2008). These include building rapport, outlining the goal of the interaction, reciprocity, obligation, scarcity, authority, commitment, social proof, influencing the ego of someone, and influencing emotion. This consistency offers further support to the prominence and reliability of social engineering methods.

The only *Engaging* sub-theme identified within the present research that has not been found in previous research is *Curiosity*. [REDACTED]  
[REDACTED]  
[REDACTED]. This finding is a unique technique unexplored in the present literature on social engineering or social psychological methods of influence. The only reference to curiosity in relation to cybercrime was found through a comparison to technical means of intrusion (Krombolz et al., 2015) which relate to cyber-dependent crimes, and are not as relevant in socio-psychological processes. The novelty of *Curiosity* adds to the literature on what techniques can be used by social engineers. Consequently, this finding provides interesting opportunities for further research. For example, *Curiosity* may not have emerged as a useful technique in previous literature because it is [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Based on the above discussion, it appears that the findings identified within the theme of *Engaging* are largely consistent with previous literature. Many of these similar skills are reported across varied and diverse literature (Archer; 2017; Cialdini, 2009; Hadnagy, 2010; Mitnick et al., 2003; Mouton et al., 2016; Workman, 2008). Widespread agreement within the literature for the current findings substantiates the reliability and validity of the current results, and provides interesting findings to suggest that methods of influence may be universal. [REDACTED]

[REDACTED] Consequently, these results are novel and important findings for the population assessed, but also consistent with previous research in similar areas. Finally, these results would indicate that methods currently used by law enforcement within NZ represent evidence-based techniques even if limited training is provided.

### **Situating the Research: External Case Considerations**

The final theme of the present study, *External Case Considerations*, represents a collection of ideas that are externally relevant to online covert investigations. This theme draws several similarities to previous research into online covert investigation, with the addition of several novel findings. *Training*, *Legislative Requirements*, and *Law Enforcement Community* are all sub-themes that frequently appear within the literature (Broadhurst, 2019; Marcum et al., 2010; Powell et al., 2014; Tetzlaff-Bemiller, 2011). However, *Risk Assessment*, *Evidential Sufficiency* and *Different Crime Type* are new ideas the current research has uncovered concerning covert investigation.

Firstly, training for individuals within online covert investigation can be incredibly variable, as previously discussed. Notably, there has been a significant lack of training reported, for both cybercrime more broadly and for more specialized cybercrime units. Harkin et al. (2018) identified a lack of training as a key finding in their study of Australian cyber units. While their study considered cyber-units that included both cyber-enabled and dependent crimes, a similar pattern was found within both groups. Similarly, a study by Schreuders et al. (2018) that conducted an expansive needs assessment in the UK identified that further training of cyber-staff was required. Where training is available to staff, this is often variable between investigators, not always a requirement, and did not always cover essential topics such as undercover chatting (Tetzlaff-Bemiller, 2011).

These findings are similar to the results found in the present study under the sub-theme *Training*. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. However, a formalized and structured program is not currently in place. [REDACTED]

[REDACTED]

[REDACTED]

Despite the poor reporting of training within the literature, the training of these cyber-units and undercover teams are critical for combatting cybercrime (Hinduja, 2004; Marcum et al., 2010). The development of a more standardised tool of training would be beneficial for ensuring equal skill level within an organization, and consistency between organizations that work together.

A second emerging sub-theme consistent within the literature is the importance of community and cooperation on both a local and global scale, shown through *Law Enforcement Community*. Cybercrime is a global problem, and thus, necessitates a global strategy and approach. Communication between teams internally and externally, including networking globally, is critical for successful prevention and proactive response (Broadhurst, 2006; Broadhurst 2019; Buono, 2016). The importance of international co-operation and communication was reported as a critical component of fighting cybercrime in the present study and is repeatedly shown to be necessary within existing literature (Broadhurst, 2006; Broadhurst, 2017; Neumuller, 2017; Wainwright, 2017). Reflective of this need for global law enforcement is the development of many international specialized organizations aimed at developing measures and methods for international co-operation (Broadhurst, 2006).

The need for co-operation not only sits at an international level, but also within the nation and the organization itself. Participants in the present study indicated that brainstorming within their teams for strategies was a useful method of developing ideas when they were struggling with a situation. Given the focus within the literature to assess global co-operation, it appears that the processes for internally assisting co-workers have been left relatively overlooked. Further research to examine the present finding of brainstorming should be explored.

A further key finding that occurs within both the present study and the literature is the importance of understanding the legislative boundaries that law enforcement are operating within. In the current research, this falls under the sub-theme *Legislative Requirements*. While this is important for all police officers, a heightened awareness is required for those conducting online covert investigations, as every sentence typed must not be considered agent provocateur. Every participant emphasized adherence to



legislation and the constant mindfulness of agent provocateur. This constant balancing act between legislative adherence and information-gathering creates additional challenges for law enforcement, such as requiring a constant alertness to every message sent. This is particularly relevant for new employees. The significance of a thorough understanding of what legal boundaries are present is a function of the consequences if not followed. Tetzlaff-Bemiller (2017) reported a similar theme in her sample of participants. Understanding the legal requirements of the role was a necessary and challenging aspect of online undercover work. The importance of good legislation is critical to protect the valuable work that is conducted by law enforcement, while also protecting citizens from entrapment.

An additional theme found in the current research that has not been identified within previous literature is *Evidential Sufficiency*. Participants reported that forward-thinking regarding what evidence is necessary for the progression of a case was an additional cognitive demand. Evidence gathered during an investigation is later used for prosecution. Therefore, investigators must constantly monitor the collection of evidence in order to be confident that certain thresholds for evidential sufficiency are met (Bell, 2002; Roscini, 2015). This requirement is standard across law enforcement investigative awareness. In the context of online covert investigation, *Evidential Sufficiency* represents a translation of a skill that has already been developed through frontline policing. The assessment of whether the monitoring of evidential sufficiency is different between online and traditional forms of investigation could be studied in future to provide more definitive guidelines on investigation progression.

Similarly, the importance of *Risk Assessment*, as discovered in the present study, has not been reported upon in previous literature. This refers to the way in which covert investigative staff had to be constantly aware of the risk that the offender

posed, and any changes that could increase risk. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. Constant

monitoring of risk could be a skill translated from traditional policing. However, a more comprehensive understanding of how risk assessment is conducted in the online environment would be helpful, given the limited cues available to the investigator.

Further research into the process of *Risk Assessment* could also inform the use of risk assessment tools for online investigators. The constant requirement to mentally monitor the risk of the suspect is an additional cognitive burden that could potentially be better managed through having a simple risk assessment tool. For example, key risk factors that would require a situation to be brought to a supervisor's attention could be outlined and presented as a simple traffic light system matrix. This system would also manage accountability for decision making on the rare occasion of any significantly grave outcomes. While an investigator is in the green, the conversation can continue as usual, if a potential risk factor for an offence occurring was mentioned, such as a suspect indicating access to children, then an investigator could know to flag this development for discussion. If it becomes apparent that a suspect is unequivocally about to offend, then an investigator would know to act upon that information instantly. As reported within the findings, being risk aware and cautious is crucial in the role. Having this tool may not be as necessary to use for investigators who are more experienced, but for new employees, it would provide a buffer and assurance of how to respond to a very new situation appropriately.

The final theme within *External Case Considerations* was *Different Crime Types*. This sub-theme presented novel findings on how investigators conducted covert operations in different crime environments. This sub-theme also answered the second research question into whether any differences existed between skills used depending upon the crime under investigation. As reported, the skills were similar regardless of crime type, but familiarisation of crime-specific knowledge was required in order to utilise the skills most appropriately and effectively. Considering the sparse research available that assesses online undercover investigation broadly, no research has been found that considers online undercover investigations for differing crime types. This is a significant result, as no one has previously been able to suggest or provide evidence that describes how covert skills are used in different online environments. The present research suggests that while skillsets are similar, different knowledge is required.

This novel and noteworthy finding can be used for guidance on a practical level, such as within training programs in law enforcement agencies. For instance, this finding suggests that the main induction course for covert operations could include all investigators. Further crime specific training could then be done over a shorter period, as a practical placement, or incorporated into the main program where possible. Thus, training programs could be structured to facilitate all online investigators, with an understanding that minor content changes will be required depending on the crime type. This finding is useful information that law enforcement agencies can use in recruitment and training internationally.

Understanding the key differences in knowledge is essential. This cannot always be prescriptively taught, however, highlighting the importance of some of the key differences would enhance online investigative practice. For example, by learning

some shared attitudes, such as sex offenders believing children can consent

(Kettleborough & Merdian, 2017), [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. Based on the present research,

identifying unique environmental knowledge is the only difference in investigating different crime types. Future research could therefore investigate and explicitly pinpoint exactly what unique knowledge is required. Such research would broaden the understanding of online covert investigation, and further help in the development of training materials for new staff.

Some of the additional skills relevant to online covert operations that were discussed within the Literature Review, such as linguistic analysis, did not appear as a necessary skill for online investigators in the present study. However, it has been reported as an essential tactic in other nations that are quite similar to NZ, such as the UK (Grant & MacLeod, 2016). Further research by a forensic linguist could assess the relevance of linguistic analysis to covert work within the NZ context. If it were found to be an important skill to the work, then it would suggest that future training should additionally consider the importance of linguistic analysis. For example, the basics of linguistic analysis could be taught in a program to provide valuable insights into understanding language, how to notice variations or consistency in language, cultural differences, and conversational control.

## **Limitations and Strengths**

The present research has presented a novel and unique exploratory study into the skills and processes used by online covert investigators in NZ. No such research has previously been conducted in this area, and therefore, this study provides new findings to expand the research base on forensic policing psychology. The results from this research will be able to inform new research, as well as possible policy change within law enforcement. These applications and implications will be explored more fully in the following section. The research template used was an in-depth interview with extensive empirical-support, and therefore established a rich and detailed level of data from which to explore. Furthermore, the method of analysis followed a framework that has been well supported within the literature on thematic analysis (Maguire & Delahunt, 2017; Terry et al., 2017). Consequently, the dependability of the research is enhanced. Many of the results identified also showed consistency with existing theory and research, further enhancing research dependability and trustworthiness.

Despite the numerous strengths to the present research, it is important to highlight where there may also be weaknesses present. The sample size for the present research was small. While this was indicative of the personnel who worked within covert online for NZ Police, additional research is needed to assess for any differences within larger police departments overseas, as well as within other cultural environments. Secondly, the interview template used was originally created for more rigid and structured interviews. Consequently, for the present research the template was adapted into a semi-structured format. This adaptation to the interview process was due to the length of the worksheets, and the varying degrees of familiarity with the worksheets by participants. ACTA allowed for a high degree of information-

gathering. However, the practicality of filling out all the textboxes for each participant was not feasible within the time allowed, nor was it always feasible for participants to dedicate extensive time to interview preparation. A shortened form of ACTA would be beneficial for future research and to maintain replicability in the interview process.

Finally, due to the sensitive nature of the research, the research was not able to be discussed in depth with others. This limited the degree of triangulation and reflectivity that could occur. While bias was minimised as much as possible through recording notes of any potential bias, the possible impact of researcher worldviews is acknowledged. Furthermore, due to the sensitivity of the data, it was not possible to conduct any form of inter-rater examination of the analysis. Given the multitude of themes and ideas identified, future research should incorporate this form of triangulation, in order to enhance the dependability of the results. Nonetheless, given the consistency with existing literature, the present research appears to represent a high level of credibility and trustworthiness. Finally, as the themes and sub-themes were present across the majority of participants, the results appear to accurately reflect the participant's responses and skills. However, given it is a secretive role, further techniques may be commonly used that were not allowed to be discussed. To offer more utility for law enforcement, further research that is conducted by police employees may offer more information as to whether any additional skills are utilised that cannot be more publicly recognised.

### **Future Research, Applications & Implications**

This study contains many practical applications for the training, selection and testing of law enforcement within online covert investigation. Training for investigators entering the role of covert online investigations is limited or variable, and does not currently follow a formulated program. The lack of a standardised

platform for training development was repeatedly identified by investigators and the literature as being a major problem for online covert investigators. Given the growth of cyber-crime globally, and the need for internationally equitable skills and co-operation, there is the increasingly urgent need to develop a standardised training program. The current research offers a guide to the essential skills that are needed by investigators, and thus, what could be taught to new investigators. Law enforcement would then be able to directly train new employees on the most effective methods of information-gathering. The findings could also be adapted to develop selection tools from which to choose new employees that may be best suited for the role.

The key topics for a training program could include the themes and sub-themes identified in the present research. For example, the skills of *Profiling*, as identified within *Data-Gathering*, could be incorporated into a training program with the use of practical examples and scenario-based learning. A trainee could be provided with some fabricated information on the pretend suspect, based on what information is commonly available before *Engaging*. From this information, the trainee could develop a hypothetical profile of who the suspect may be, and how they would develop an identity that would be most relevant for the scenario (practicing the skills *Fabrication* and *Profiling*). This task could again be a standardised process, with the opportunity for marking, feedback, and comparison. [REDACTED]

[REDACTED] This training would provide investigators with a greater understanding of the personality, motivations, and needs of whom they are speaking to. Furthermore, such training may lead to greater accuracy in influencing a suspect, and also increased knowledge of how to emulate an individual if required, leading to greater *Fabrication* accuracy. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Similarly, the sub-themes covered under *Engaging* would be highly beneficial in a training curriculum. Each of the techniques outlined relates to social psychological principles that have backgrounds within evidence-based research. Training on how to employ each technique and why they can be useful will assist in building a potential investigator's toolbox of tactics for engaging with suspects. Training within *Engaging* techniques would enable critical skills to be practised and refined, improving investigative success. These skills could also be outlined within a handbook for existing investigators. This handbook would be a quick reference guide that could reduce the pressure and cognitive load of investigators when trying to think about how to proceed with online interaction. This training would ensure each new investigator understands the requirements and can act as effectively as possible.

The benefits of a systematic training process are as follows. (a) When recruiting and selecting employees for online covert interaction, testing could be done to see if there is a natural aptitude [REDACTED]

[REDACTED] (b) Upon the conclusion of selection and training, law enforcement could test new employees on the skills needed to assess a baseline expected level of entry, and understand what the most challenging techniques to learn are. (c) When a new employee or even an experienced investigator is engaging with an offender [REDACTED]

[REDACTED]

[REDACTED] (d) It



would assure investigators that they are maintaining the legal boundaries of what they can and cannot say to avoid agent provocateur. (e) It would provide a structured platform from which future research can be conducted in this area, as currently, the literature is very scattered and difficult to comprehensively assess. Research opportunities would then be more readily accessed.

As this study is the first of its' kind to assess the skills in online covert interaction, it has provided a platform from which future research can build on. Further qualitative work into the existing themes and sub-themes, such as the specific skills within conversation management, would provide interesting and new findings as to the specific techniques used. From this, quantitative research can then be applied. For instance, quantitative research could assess how frequently various skills are used, or importance ratings through likert-charts could be tested to understand more nuanced information as to the tactics, techniques and procedures used by online covert investigators. Additional areas for future research have been highlighted throughout the assessment of findings within the Discussions section. For example, comparing the different knowledge bases required depending on the crime, the development and experimental evaluation of a risk assessment tool, and an analysis of whether there is a difference in evidential sufficiency between online versus offline crimes.

In addition to future research and practical applications, the present study offers interesting theoretical implications. Of note, is how the skills for *Engaging* could be conceptualized into what emotions are influenced, rather than what skill is used. Each of the techniques could be hypothesized to influence a particular emotion. For example, power and scarcity may influence fear, likeability and ego influence may influence happiness. If this is the case, then an integrated theory of social

engineering could be developed based upon an analysis of what emotions are generated relating to what specific actions. Rather than breaking down the skills for social engineering into the constituent actions, skills for social engineering could instead be broken down based on the thematic consideration of emotion.

Conceptualizing social engineering in this manner could provide greater information on how to implement the techniques in order to heighten the emotion being influence. This theory could be tested through experimental manipulation, or priming of emotion prior to the application of social engineering tactics to see whether they are connected to the emotion being considered. Alternatively, testing social engineering techniques on people experiencing alexithymia or blunted emotional responses would indicate if they are based upon emotional influence. The present research has therefore opened up many avenues of further research by providing a base understanding of how online investigative work is conducted.

Another implication of the present research is the opportunity to organise the current research on social engineering and persuasion. Given the consistency between the present research and previous research, a more unified theory of how to influence another, or engage in social engineering could be developed. The present research in conjunction with previous research appears to suggest a similar method of social engineering is conducted regardless of who the suspect or engineer is, or what the motivation for influence is. A unified system could be very important for law enforcement, as it could guide the processes and organisation of covert investigations units. Such a guide would be founded upon evidence-based techniques to utilise when interacting with offenders, instead of solely relying on experience base.

Therefore, the present research has significant practical applications to the law enforcement community, from a local to an international level. Furthermore, the

knowledge and skills that the current research highlights will continue to grow in their use and importance as cybercrime investigation increases. The present study also contributes theoretically to the knowledge base of social engineering and social influence, building on the work of previous researchers. This research has provided an in-depth description of online investigative work that provides a platform for future research and increased exploration of this important area.

## **Conclusion**

As the online criminal operating environment grows, so too do the requirements for a robust and established covert online investigations team. The present study sought to understand the skills and techniques used in covert online investigation. This is an important research area that has not been previously assessed. Interviews with eight investigators were performed to assess how they conduct their investigations, and how it varies depending upon the crime under investigation. The results found three themes of *Data-Gathering*, *Engaging* and *External Case Considerations*, which all meaningfully contribute to the literature on social engineering, covert operations, and training development.

The observations and recommendations of the current study would contribute greatly to a bespoke candidate assessment criteria and training curriculum for covert investigators. Furthermore, the present research can also contribute to the development of: the efficient selection of suitable candidates for the role of covert online investigator; formalized training and assessment of candidates; and greater opportunities for collaboration and cross-training with the global law enforcement community and other NZ Government agencies. Implications for the theory of social engineering, compliance and persuasion are also outlined, representing an opportunity for a unified theory. Additionally, a theory could be developed that conceptualizes

social engineering based upon emotional influence. Overall, the present research is a novel study into a significant and growing offending environment. The findings from this study, and the implications and applications discussed, offer significant contribution to operational success and safer communities.

## References

- Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2016). A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, 11(4), 373-391. <https://doi.org/10.1080/21582041.2015.1117648>
- Agustina, J. R. (2012). Book review of cyber criminology: Exploring internet crimes and criminal behavior. *International Journal of Cyber Criminology*, 6(2), 1044-1048.  
[https://www.researchgate.net/publication/293170855\\_Book\\_review\\_of\\_cyber\\_criminology\\_Exploring\\_internet\\_crimes\\_and\\_criminal\\_behavior](https://www.researchgate.net/publication/293170855_Book_review_of_cyber_criminology_Exploring_internet_crimes_and_criminal_behavior)
- Akhgar, B., & Brewster, B. (Eds.). (2016). *Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Springer International Publishing. <https://doi:10.1007/978-3-319-38930-1>
- Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Experimental case studies for investigating e-banking phishing techniques and attack strategies. *Cognitive Computation*, 2(3), 242-253. <http://dx.doi.org/10.1007/s12559-010-9042-7>.
- Atkins, B., & Huang, W. (2012). A study of social engineering in online frauds. *Open Journal of Social Sciences*, 1(3), 23-32. <https://doi:10.4236/jss.2013.13004>
- Atlam, H. F., Alenezi, A., Alassafi, M. O., Alshdadi, A. A., & Wills, G. B. (2020). Security, Cybercrime and Digital Forensics for IoT. In S. L. Peng, S. Pal, & L. Huang (Eds), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm* (pp. 551-577). Springer. [https://doi.org/10.1007/978-3-030-33596-0\\_22](https://doi.org/10.1007/978-3-030-33596-0_22)

- Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2010). Dealing with the problem of cybercrime. In C. Vielhauer (Ed.), *Conference Proceedings of 2nd International ICST Conference on Digital Forensics and Cyber Crime* (pp. 1–18). Springer International. [https://doi:10.1007/978-3-642-19513-6\\_1](https://doi:10.1007/978-3-642-19513-6_1).
- Allen, M. (2006). *Social engineering: A means to violate a computer system* [White Paper]. Sans Institute: Information Security Reading Room.  
[http://www.sans.org/reading\\_room/whitepapers/engineering/529.php](http://www.sans.org/reading_room/whitepapers/engineering/529.php)
- Archer, A. K. (2017). *"I Made a Choice": Exploring the Persuasion Tactics Used by Online Romance Scammers in Light of Cialdini's Compliance Principles*. [Publication No. 823] [Master's Thesis, All Regis University] Regis University Theses. <https://epublications.regis.edu/theses/823>
- Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). *2020 Cybercrime economic costs: No measure no solution*. 2015 10th International Conference on Availability, Reliability and Security. Conference Publishing Services. [https://doi:10.1007/978-3-319-38930-1\\_8](https://doi:10.1007/978-3-319-38930-1_8)
- Ayofe, A. N., & Irwin, B. (2010). Cybersecurity: Challenges and the way forward. *Computer Science and Telecommunications*, 6(29) 56-70.  
[https://www.researchgate.net/publication/265121167\\_CYBER\\_SECURITY\\_CHALLENGES\\_AND\\_THE\\_WAY\\_FORWARD](https://www.researchgate.net/publication/265121167_CYBER_SECURITY_CHALLENGES_AND_THE_WAY_FORWARD)
- Babchishin, K. M., Hanson, K. R., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse: A Journal of Research and Treatment*, 23(1), 92–123. <https://doi:10.1177/1079063210370708>
- Bell, R. E. (2002). The prosecution of computer crime. *Journal of financial crime*, 9(4), 308-325. <https://doi.org/10.1108/eb026030>

- Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. 7th International Conference on Financial Criminology. *Procedia Economics and Finance*, 28, 24–31. [https://doi:10.1016/s2212-5671\(15\)01077-1](https://doi:10.1016/s2212-5671(15)01077-1)
- Bisantz, A. M., Roth, E., Brickman, B., Gosbee, L. L., Hettinger, L., & McKinney, J. (2003). Integrating cognitive analyses in a large-scale system design process. *International Journal of Human-Computer Studies*, 58(2), 177-206. [https://doi:10.1016/s1071-5819\(02\)00130-1](https://doi:10.1016/s1071-5819(02)00130-1)
- Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behaviour in an increasingly computer-mediated world. *Child Abuse and Neglect*, 44, 140–149. <https://doi:10.1016/j.chiabu.2014.12.004>
- Bogdan, R., & Biklen, S. K. (1997). *Qualitative research for education: An Introduction to Theory and Methods* (3rd ed.). Allyn & Bacon. [http://math.buffalostate.edu/dwilson/MED595/Qualitative\\_intro.pdf](http://math.buffalostate.edu/dwilson/MED595/Qualitative_intro.pdf)
- Bonino, S., & Kaoullas, L. G. (2015). Preventing political violence in Britain: An evaluation of over forty years of undercover policing of political groups involved in protest. *Studies in Conflict & Terrorism*, 38(10), 814-840. <https://doi.org/10.1080/1057610X.2015.1059102>
- Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbooks in psychology. APA handbook of research methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and*

- biological* (pp. 57–71). American Psychological Association.  
<https://doi.org/10.1037/13620-004>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101. <https://doi:10.1191/1478088706qp063oa>
- Brehm, J. W. (1966). *A theory of psychological reactance*. Academic Press.
- Brenner, S. W., & Koops, B. J. (2005). Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, 4(1), 1-46.  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=786507](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507)
- Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408–433. <https://doi:10.1108/13639510610684674>
- Broadhurst, R. G. (2017a). Cybercrime in Australia. In A. Deckert, & R. Sarre (Eds.), *The Palgrave Handbook of Australian and NZ Criminology, Crime, and Justice* (pp. 221–235). Palgrave Macmillan. [https://doi:10.1007/978-3-319-55747-2\\_15](https://doi:10.1007/978-3-319-55747-2_15)
- Broadhurst, R. (2017b). *Cybercrime: thieves, swindlers, bandits and privateers in cyberspace*. SSRN Electronic Journal. <https://doi:10.2139/ssrn.3009574>
- Broadhurst, R. (2019). Child Sex Abuse Images and Exploitation Materials. In R. Leukfeldt, & T. Holt, (Eds.), *Cybercrime: the human factor of cybercrime* (pp. 310-336). Routledge. <https://doi.org/10.4324/9780429460593>
- Brown, I., Edwards, L., & Marsden, C. (2009). *Information security and cybercrime* (3rd ed.). Research Gate. <https://ssrn.com/abstract=1427776>



- Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9(1), 55-119. [https://doi: 10.5281/zenodo.22387](https://doi.org/10.5281/zenodo.22387)
- Bryman, A. (2012). *Social research methods* (4th ed.). Oxford University Press. [https://www.academia.edu/35174091/Alan\\_Bryman\\_Social\\_Research\\_Methods\\_4th\\_Edition\\_Oxford\\_University\\_Press\\_2012\\_](https://www.academia.edu/35174091/Alan_Bryman_Social_Research_Methods_4th_Edition_Oxford_University_Press_2012_)
- Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: an international journal of police strategies & management*, 34(1), 165-181, <https://doi.org/10.1108/13639511211215504>
- Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge. <https://doi.org/10.4324/9781315775944>
- Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of experimental criminology*, 11(1), 97-115. [https://doi:10.1007/s11292-014-9222-7](https://doi.org/10.1007/s11292-014-9222-7)
- Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016). Telephone based social engineering attacks: An experiment testing the success and time decay of an intervention. In A. Mathur, & A. Roychoudhury (Eds.), *Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016* (pp. 107-114). IOS Press. <https://doi.org/10.3233/978-1-61499-617-0-107>
- Buono, L. (2016). Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. *Journal of the Academy of European Law*, 17(3), 343-353. <https://doi.org/10.1007/s12027-016-0432-5>

- Caneppele, S., & Aebi, M. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, 13(1), 66–79. <https://doi.org/10.1093/police/pax055>
- Carlson, J. A. (2010). Avoiding traps in member checking. *The Qualitative Report*, 15(5), 1102-1113. <https://nsuworks.nova.edu/tqr/vol15/iss5/4>
- Casey, E. (2004). *Digital Evidence and Computer Crime* (3rd ed.). Elsevier Academic Press. <https://www.elsevierdirect.com/companions/9780123742681>
- Casey, D., & Murphy, K. (2009). Issues in using methodological triangulation in research. *Nurse Researcher*, 16(4), 40–55. <https://doi:10.7748/nr2009.07.16.4.40.c7160>
- Cassell, C., & Symon, G. (Eds.). (2004). *Essential guide to qualitative methods in organizational research*. Sage Publications. <http://dx.doi.org/10.4135/9781446280119>
- Cialdini, R. B. (1984). *The psychology of persuasion*. William Morrow.
- Cialdini, R. (2009). *Influence* (Rev. edition). HarperCollins Publishers. [http://elibrary.bsu.az/books\\_400/N\\_232.pdf](http://elibrary.bsu.az/books_400/N_232.pdf)
- Cialdini, R. B., & Rhoads, K. V. (2001). Human behavior and the marketplace. *Marketing Research*, 13(3), 8-13. <https://search.proquest.com/docview/202675039>
- Chawki, M., Darwish, A., Khan, M., & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer International Publishing. <https://doi:10.1007/978-3-319-15150-2>

- Choo, K. K. R., & Australian Institute of Criminology. (2009). *Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences* (Research and public policy series no. 103). Australian Institute of Criminology.  
<https://aic.gov.au/publications/rpp/rpp103>
- Cohen-Almagor, R. (2013). Online child sex offenders: Challenges and counter-measures. *The Howard Journal of Criminal Justice*, 52(2), 190–215.  
<https://doi:10.1111/hojo.12006>
- Cope, D. G. (2014). Methods and meanings: credibility and trustworthiness of qualitative research. *Oncology nursing forum*, 41(1), 89-91. <https://doi:10.1188/14.ONF.89-91>.
- Crocker, R. A. (2009). *Qualitative research in applied linguistics*. Palgrave Macmillan.  
[https://doi:10.1057/9780230239517\\_1](https://doi:10.1057/9780230239517_1).
- Cupchik, G. (2001). Constructivist realism: An ontology that encompasses positivist and constructivist approaches to the social sciences. *Forum: Qualitative Social Research*, 2(1), Article 7. <https://dx.doi.org/10.17169/fqs-2.1.968>
- Dashora, K. (2011). Cybercrime in society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences*, 3(1), 240-259.  
[https://www.japss.org/upload/11.\\_Dashora\[1\].pdf](https://www.japss.org/upload/11._Dashora[1].pdf)
- Davis, J. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management*, 35(2), 272–284.  
<https://doi.org/10.1108/13639511211230039>

- Doig, A., Gundur, R., Wall, D., & Williams, M. (2018). *The Implications of Economic Cybercrime for Policing*. Cardiff: City of London Corporation.  
[https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/London\\_Economic-cybercrime-Summary-Report.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/London_Economic-cybercrime-Summary-Report.pdf)
- Dubord, P. (2008). Investigating Cybercrime. In J. J. Barbara (Ed.), *Handbook of Digital and Multimedia Forensic Evidence* (pp. 77-89). Humana Press Inc.  
[https://doi:10.1007/978-1-59745-577-0\\_6](https://doi:10.1007/978-1-59745-577-0_6)
- Elliott, R., Fischer, C. T., & Rennie, D. L. (1999). Evolving guidelines for publication of qualitative research studies in psychology and related fields. *The British Journal of Clinical Psychology*, 38(3), 215–219.  
<https://doi:10.1348/014466599162782>
- Erickson, F. (2012). Qualitative research methods for science education. In B. Fraser, K. Tobin, & C. McRobbie (Eds.), *Second International Handbook of Science Education*, (pp. 1451-1469). Springer International Handbooks of Education.  
[https://doi:10.1007/978-1-4020-9041-7\\_93](https://doi:10.1007/978-1-4020-9041-7_93)
- Festinger, L. (1962). *A theory of cognitive dissonance*. Stanford University Press.
- Flick, U. (2004). Triangulation in qualitative research. In U. Flick, E. V. Kardoff, & I. Steinke (Eds.), *A Companion to Qualitative Research* (pp. 178-183). Sage Publications.  
[https://www.researchgate.net/profile/Stephan\\_Wolff2/publication/305496229\\_Wolff\\_in\\_Flick\\_et\\_a/links/5792046008aec89db77fca3c/Wolff-in-Flick-et-a.pdf#page=193](https://www.researchgate.net/profile/Stephan_Wolff2/publication/305496229_Wolff_in_Flick_et_a/links/5792046008aec89db77fca3c/Wolff-in-Flick-et-a.pdf#page=193)
- Flick, U. (2018). *An introduction to qualitative research* (5th ed.). Sage Publications Limited. <http://dx.doi.org/10.4135/9781526416070>

- Gamez, J. (2018). *Persuasive design and the web: How Cialdini principles are used in online successful companies*. (Corpus ID: 145934980) [Master's Thesis, International Hellenic University]. Semantic Scholar.  
<https://www.semanticscholar.org/paper/Persuasive-design-and-the-web%3A-How-Cialdini-are-in-Gámez/690f78d7bb03a0ec40f76eb595504ef8f096e863>
- Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect*, 80, 238-248. <https://doi:10.1016/j.chiabu.2018.03.031>
- Gillespie, A. A. (2015). *Cybercrime: Key issues and debates*. Routledge.  
<https://doi:10.4324/9781315884202>
- Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, 204(6), 291-295. <https://doi:10.1038/bdj.2008.192>
- Giollabhui, S., Goold, B., & Loftus, B. (2016). Watching the watchers: conducting ethnographic research on covert police investigation in the United Kingdom. *Qualitative Research*, 16(6), 630–645.  
<https://doi:10.1177/1468794115622529>
- Gordon, R. (2014). *Privacy, Security and the Cyber Dilemma: An Examination of NZ's Response to the Rising Threat of Cyber-attack*. [Unpublished Master's thesis]. Victoria University of Wellington. <http://hdl.handle.net/10063/3565>
- Grabosky, P. N., & Smith, R. G. (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Transaction Publishers.  
<https://doi:10.4324/9780203794401>

- Grabosky, P., & Urbas, G. (2019). Online undercover investigations and the role of private third parties. *International Journal of Cyber Criminology*, 13(1), 38-54. [https://doi: 10.5281/zenodo.3383885](https://doi:10.5281/zenodo.3383885)
- Grant, T., & MacLeod, N. (2016). Assuming identities online: Experimental linguistics applied to the policing of online paedophile activity. *Applied Linguistics*, 37(1), 50–70. <https://doi:10.1093/applin/amv079>
- Greening, T. (1996). Ask and ye shall receive: a study in ‘social engineering’. *ACM SIGSAC Review*, 14(2), 8–14. <https://doi:10.1145/228292.228295>
- Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4), 597-607. <https://nsuworks.nova.edu/tqr/vol8/iss4/6>
- Gouldner, A. W. (1960). The norm of reciprocity: A preliminary statement. *American Sociological Review*, 25(2), 161-178. <https://doi:10.2307/2092623>
- Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2018). A qualitative exploration of police officers’ experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*, 19(6), 519-536. <https://doi:10.1093/police/pay090>
- Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking* (1st ed.). Wiley. [http://index-of.es/Varios/The\\_Art\\_of\\_Human\\_Hacking.pdf](http://index-of.es/Varios/The_Art_of_Human_Hacking.pdf)
- Harfield, C. (2010). *The Governance of Covert Investigation*. Melbourne University Law Review, 34(3), 773. <http://www5.austlii.edu.au/au/journals/MelbULawRw/2010/27.html>

- Harkin, D., Whelan, C. and Chang, L. (2018). The challenges facing specialist cyber-crime units: an empirical analysis. *Police Practice and Research*, 19(6), 519–536. <https://doi:10.1080/15614263.2018.1507889>
- Harkin, D., & Whelan, C. (2019). Exploring the implications of “low visibility” specialist cyber-crime units. *Australian & NZ Journal of Criminology*, 52(4), 578–594. <https://doi.org/10.1177/0004865819853321>
- Hasle, H., Kristiansen, Y., Kintel, K., & Snekenes, E. (2005). Measuring resistance to social engineering. In R. H. Deng, F. Bao, H. Pang, & J. Zhou (Eds.). *ISPEC: International Conference on Information Security Practice and Experience* (pp. 132–143). Springer. [https://doi:10.1007/978-3-540-31979-5\\_12](https://doi:10.1007/978-3-540-31979-5_12)
- Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102–113. <https://doi:10.1016/j.cose.2017.10.008>
- Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management*, 27(3), 341–357. <https://doi:10.1108/13639510410553103>
- Hoffman, R. R., Coffey, J. W., Carnot, M. J., & Novak, J. D. (2002). An empirical comparison of methods for eliciting and modeling expert knowledge. *Human Factors and Ergonomics Society Annual Meeting Proceedings*, 46(3), 482–486. <https://doi:10.1177/154193120204600356>
- Hoffman, R. R., Crandall, B., & Shadbolt, N. (1998). Use of the critical decision method to elicit expert knowledge: A case study in the methodology of

- cognitive task analysis. *The Journal of the Human Factors and Ergonomics Society*, 40(2), 254–276. <https://doi:10.1518/001872098779480442>
- Hutchins, S. G., Pirolli, P. L., & Card, S. K. (2007). What makes intelligence analysis difficult? A cognitive task analysis. In R. R. Hoffman (Ed.), *Expertise Out of Context: Proceedings of the Sixth International Conference on Naturalistic Decision Making* (pp. 281-316). Psychology Press.  
<https://www.crcpress.com/Expertise-Out-of-Context-Proceedings-of-the-Sixth-International-Conference/Hoffman/p/book/9780805855104>
- Iofrida, N., De Luca, A. I., Strano, A., & Gulisano, G. (2014). Social life cycle assessment and participatory approaches: A methodological proposal applied to citrus farming in Southern Italy. *Integrated Environmental Assessment and Management*, 11(3), 383–396. <https://doi:10.1002/ieam.1611>
- Jamshed S. (2014). Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, 5(4), 87–88.  
<https://doi:10.4103/0976-0105.141942>
- Jackson, P. T., & Nexon, D. H. (2004). Constructivist realism or realist-constructivism? *International Studies Review*, 6(2), 337-341.  
[https://doi:10.1111/j.1521-9488.2004.419\\_2.x](https://doi:10.1111/j.1521-9488.2004.419_2.x)
- Jensen, B. T., Terebinski, S. J., & Ellis, W. R. (1960). The importance of criterion definition. *Journal of the American Society of Training Directors*, 3-7.
- Jeffries, S., & Apeh, E. (2020). Standard operating procedures for cybercrime investigations: a systematic literature review. In Benson. V., & Mcalaney. J (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 145–162). Elsevier. <https://doi:10.1016/b978-0-12-816203-3.00007-1>



- Johnson, T. J. (2016). *Professions and Power*. Routledge.  
<https://doi:10.4324/9781315471372>
- Jung, J. M., & Kellaris, J. J. (2004). Cross-national differences in proneness to scarcity effects: The moderating roles of familiarity, uncertainty avoidance, and need for cognitive closure. *Psychology & Marketing*, 21(9), 739-753.  
<https://doi:10.1002/mar.20027>
- Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75-87. <https://doi:10.1016/j.chb.2016.09.012>
- Kelion, L. (2014, February 12). Five arrested in Utopia dark net marketplace crackdown. *BBC News*. <https://www.bbc.com/news/technology-26158012>
- Kettleborough, D. G., & Merdian, H. L. (2017). Gateway to offending behaviour: Permission-giving thoughts of online users of child sexual exploitation material. *Journal of sexual aggression*, 23(1), 19-32.  
<https://doi:10.1080/13552600.2016.1231852>
- Keyvanpour, M., Ebrahimi, M., Nayeibi, N. G., Ormandjeva, O., & Suen, C. Y. (2016). Automated identification of child abuse in chat rooms by using data mining. In Isafiade, O. E., & Bagula, A. B. (Eds.), *Data Mining Trends and Applications in Criminal Science and Investigations*, (pp. 245–274). IGI Global. <https://doi:10.4018/978-1-5225-0463-4.ch009>
- Kirwan, G. H. (2018). Dispelling the pseudopsychology of cybercrime. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 71–72.  
<https://doi:10.1089/cyber.2017.29100.ghk>

- Klein, B. R., Gruenewald, J., Chermak, S. M., & Freilich, J. D. (2018). A mixed method examination of law enforcement investigatory strategies used in jihadi and far-right foiled terrorist plots before and after 9/11. *Journal of Qualitative Criminal Justice & Criminology* 7, 29-58.  
<https://www.jqcjc.org/documents/v7i2.pdf#page=32>
- Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process and offender characteristics. *Trauma, Violence & Abuse*, 15(2), 126–139. <https://doi.org/10.1177/1524838013511543>
- Knabe-Nicol, S., & Alison, L. (2011). The cognitive expertise of Geographic Profilers. In Alison. L., & Rainbow. L., (Eds), *Professionalizing offender profiling: Forensic and investigative psychology in practice*, (pp. 143-176). Routledge. <https://trove.nla.gov.au/work/38617744>
- Koch, T. (2006). Establishing rigour in qualitative research: The decision trail. *Journal of Advanced Nursing*, 53(1), 91–100. <https://doi.org/10.1111/j.1365-2648.2006.03681.x>
- Koch, R., Golling, M., & Rodosek, G. D. (2016). How anonymous is the tor network? A long-term black-box investigation. *Computer*, 49(3), 42-49. <https://doi.org/10.1109/MC.2016.73>
- Krauss, S. E. (2005). Research paradigms and meaning making: A primer. *The qualitative report*, 10(4), 758-770. <https://nsuworks.nova.edu/tqr/vol10/iss4/7>
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E.R. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22(C), 113-122. <https://doi.org/10.1016/j.jisa.2014.09.005>

- Krone, T. (2005a). *International police operations against online child pornography*. (Trends and Issues in Crime and Criminal Justice ; No. 296). Australian Institute of Criminology. <https://aic.gov.au/publications/tandi/tandi296>
- Krone, T. (2005b). *Queensland police stings in online chat rooms*. (Trends and Issues in Crime and Criminal Justice; No. 301). Australian Institute of Criminology. <https://www.aic.gov.au/publications/tandi/tandi301>
- Lacson, W., & Jones, B. (2016). The 21st century DarkNet market: Lessons from the fall of Silk Road. *International Journal of Cyber Criminology*, 10(1), 40-61. <https://doi: 10.5281/zenodo.58521>
- Lafrance, Y. (2004). *Psychology: a precious security tool*. [White Paper] Sans Institute. [http://www.sans.org/reading\\_room/whitepapers/engineering/1409.php](http://www.sans.org/reading_room/whitepapers/engineering/1409.php)
- Latour, B. (2005). *Reassembling the social. An introduction to actor-network-theory*. Oxford University Press. [http://townsendgroups.berkeley.edu/sites/default/files/reassembling\\_the\\_social\\_selections.pdf](http://townsendgroups.berkeley.edu/sites/default/files/reassembling_the_social_selections.pdf)
- Lincoln, Y. S., & Guba, E. G. (1990). Judging the quality of case study reports. *International Journal of Qualitative Studies in Education*, 3(1), 53–59. doi:10.1080/0951839900030105
- Loftus, B., & Goold, B. (2011). Covert surveillance and the invisibilities of policing. *Criminology and Criminal Justice*, 12(3), 275–288. <https://doi:10.1177/1748895811432014>

- Lusthaus, J. (2012). Trust in the world of cybercrime. *Global crime*, 13(2), 71-94.  
<https://doi:10.1080/17440572.2012.674183>
- Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2015). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital ‘demimonde’. *Information, Communication & Society*, 19(1), 111–126.  
<https://doi:10.1080/1369118x.2015.1093531>
- Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *The All Ireland Journal of Teaching and Learning in Higher Education*, 9(3), 3351-33514.  
<http://ojs.aishe.org/index.php/aishe-j/article/view/335>
- Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative health research*, 26(13), 1753-1760. <https://doi:10.1177/1049732315617444>
- Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cyber crime. *International Journal of Police Science & Management*, 12(4), 516-525. <https://doi:10.1350/ijps.2010.12.4.201>
- Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A Review of Qualitative Interviews in is Research. *Journal of Computer Information Systems*, 54(1), 11–22.  
<https://doi:10.1080/08874417.2013.11645667>

- Matusitz, J. A. (2006). *Cyberterrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them* (Publication No. 3207541) [Doctoral dissertation, University of Oklahoma] ProQuest Dissertations & Theses Global.  
<https://search.proquest.com/openview/e32be6b49bacf94905c06b3971973177/1?cbl=18750&diss=y&pq-origsite=gscholar>
- McGuire, M., & Dowling, S. (2013). *Cybercrime: A review of the evidence: Summary of key findings and implications*. U.K Home Office Research Report.  
<https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence>
- Merriam, S. B., & Grenier, R. S. (Eds.). (2019). *Qualitative research in practice: Examples for discussion and analysis*. John Wiley & Sons.
- Merrick, E. (1999). An exploration of quality in qualitative research. Are "reliability" and "validity" relevant? In M. Kopala & L. A. Suzuki (Eds.), *Using qualitative methods in psychology* (pp. 25–36). Sage Publications.  
<https://doi.org/10.4135/9781452225487.n3>
- Milgram, S. (1983). *Obedience to authority: An experimental view*. Harper-Collins.
- Militello, L. G., & Hutton, R. B. (1998). Applied cognitive task analysis (ACTA): A practitioner's toolkit for understanding cognitive task demands. *Ergonomics*, 41(11), 1618-1641. <https://doi.org/10.1080/001401398186108>
- Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2010). Growth and change in undercover online child exploitation investigations, 2000–2006. *Policing & Society*, 20(4), 416–431. doi:10.1080/10439463.2010.523113

- Mitchell, K. J., Wolak, J., Finkelhor, D., & Jones, L. (2011). Investigators using the internet to apprehend sex offenders: Findings from the Second National Juvenile Online Victimization Study. *Police Practice and Research*, 13(3), 267–281. <https://doi:10.1080/15614263.2011.627746>
- Mitnick, K. D., Simon, D., & Wozniak, S. (2003). *The art of deception: controlling the human element of security*. John Wiley & Sons.  
<https://pdfs.semanticscholar.org/9974/68975ffba55ada70b3ac3a13b5ae6853a80f.pdf>
- Moore, R. (2011). *Cybercrime: Investigating high-technology computer crime*. Anderson Publishing. <https://doi:10.4324/9781315721767>
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186-209.  
[doi:10.1016/j.cose.2016.03.004](https://doi:10.1016/j.cose.2016.03.004)
- Muncaster, P. (2005). Police fail to cope with e-crime: Firms expected to improve their own security. *Computing*.  
<https://www.computing.co.uk/news/1816053/police-fail-cope-crime>
- Neumüller, A. S. (2017). *Cybercrime Centres: Analysis and Recommendations* [Unpublished Master's thesis], University College Dublin.
- Ngafeeson, M. (2010). Cybercrime classification: a motivational model. *Proceedings of the South West Decision Sciences Institute*, 1201.  
[http://swdsi.org/swdsi2010/SW2010\\_Preceedings/papers/PA168.pdf](http://swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf)
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1-13. <https://doi:10.1177/1609406917733847>

- O'Leary, R., & D'Ovidio, R. (2007). *Online sexual exploitation of children*. International Association of Computer Investigative Specialists.  
<https://docplayer.net/3133696-Online-sexual-exploitation-of-children-the-international-association-of-computer-investigative-specialists-robert-j-o-leary-robert-d-ovidio.html>
- Okoli, J. O., Weller, G., & Watt, J. (2016). Information processing and intuitive decision-making on the fireground: Towards a model of expert intuition. *Cognition, Technology & Work*, 18(1), 89-103.  
<https://doi:10.1007/s10111-015-0348-9>
- Olson, L. N., Daggs, J. L., Ellevold, B. L., & Rogers, T. K. (2007). Entrapping the innocent: Toward a theory of child sexual predators' luring communication. *Communication Theory*, 17(3), 231–251. <https://doi:10.1111/j.1468-2885.2007.00294.x>
- Orebaugh, A., Kinser, J., Allnutt, J., & Mason, G. (2014). Visualising instant messaging author writeprints for forensic analysis. *ADFSL Conference on Digital Forensics, Security and Law*, 8, 191-214.  
<https://commons.erau.edu/adfsl/2014/thursday/8>
- Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy education to counter social engineering attacks on secure computer systems. *Proceedings of the 5th conference on Information technology education*, 177-181. <https://doi:10.1145/1029533.1029577>
- Parker, D. (1998). *Fighting Computer Crime: For Protecting Information*. John Wiley & Sons.
- Patton, M. Q. (1980). *Qualitative evaluation methods*. Sage Publications.

- Perloff, R. M. (2016). *The dynamics of persuasion: Communication and attitudes in the 21st century* (6th ed.). Taylor & Francis. [https://doi:10.4324/9781315657714](https://doi.org/10.4324/9781315657714)
- Ponterotto, J. G. (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. *Journal of counseling psychology*, 52(2), 126–136. [https://doi:10.1037/0022-0167.52.2.126](https://doi.org/10.1037/0022-0167.52.2.126)
- Pope, C. (2002). Qualitative methods in research on healthcare quality. *Quality and Safety in Health Care*, 11(2), 148–152. [https://doi:10.1136/qhc.11.2.148](https://doi.org/10.1136/qhc.11.2.148)
- Powell, M., Cassematis, P., Benson, M., Smallbone, S., & Wortley, R. (2014). Police officers' strategies for coping with the stress of investigating internet child exploitation. *Traumatology: An International Journal*, 20(1), 32–42. <https://doi.org/10.1037/h0099378>
- Rashid, A., Baron, A., Rayson, P., May-Chahal, C., Greenwood, P., & Walkerdine, J. (2013). Who am I? Analyzing digital personas in cybercrime investigations. *Computer*, 46(4), 54–61. [https://doi:10.1109/mc.2013.68](https://doi.org/10.1109/mc.2013.68)
- Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, (1), 1-6. [https://doi:10.1109/isads.2013.6513420](https://doi.org/10.1109/isads.2013.6513420)
- Reyes, A., O'Shea, K., Hansen, J., Jean, B., & Ralph, T. (2007). *Cybercrime investigation: Bridging the gaps between security professionals, law enforcement, and prosecutors*. Syngress Publishing Inc.



<https://epdf.pub/cyber-crime-investigations-bridging-the-gaps-between-security-professionals-law-28931.html>

Roberts, L. (2008). Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An analysis on cyber stalking. *International Journal of Cyber Criminology*, 2(1) 271-285.

<https://www.researchgate.net/publication/242074185>

Roscini, M. (2015). Evidentiary issues in international disputes related to state responsibility for cyber operations. *Texas International Law Journal*, 50(2), 233-273. <http://ssrn.com/abstract=2611753>

Ross, G. (2018, February 23). *The Cost of Cybercrime*. Internet Society.

<https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime/>

Rush, H., Smith, C., Kraemer-Mbula, E., & Tang, P. (2009). *Crime online: Cybercrime and illegal innovation*. Nesta Innovation Flourish.

[https://johnbessant.org/wp-content/uploads/2019/08/Crime\\_Online.pdf](https://johnbessant.org/wp-content/uploads/2019/08/Crime_Online.pdf)

Russell, N. J. C. (2011). Milgram's obedience to authority experiments: Origins and early evolution. *British Journal of Social Psychology*, 50(1), 140-162.

<https://doi:10.1348/014466610X492205>

Russell, C. K., & Gregory, D. M. (2003). Evaluation of qualitative research studies.

*Evidence-Based Nursing*, 6(2), 36-40. <https://doi:10.1136/ebn.6.2.36>

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, 4(6), 165-176.

<https://doi:10.1109/icccf.2016.7740434>

- Sarre, R., Lau, L., & Chang, L. (2018). Responding to cybercrime: Current trends. *Police Practice and Research*, 19(6), 515–518.  
<https://doi:10.1080/15614263.2018.1507888>
- Schiller, C., Fogie, S., DeRodeff, C., & Gregg, M. (2011). *InfoSecurity 2008 Threat Analysis*. Elsevier.  
<https://www.sciencedirect.com/book/9781597492249/infosecurity-2008-threat-analysis>
- Schraagen, J. M., Chipman, S. F., & Shalin, V. L. (Eds.). (2000). *Cognitive task analysis*. Psychology Press. <https://doi:10.4324/9781410605795>
- Schreuders, Z. C., Cockcroft, T. W., Butterfield, E. M., Elliott, J. R., & Soobhany, A. R. Shan-A-Khuda, M.(2018). *Needs assessment of cybercrime and digital evidence in a UK police force* [Unpublished Submission]. Leeds Beckett University. <http://eprints.leedsbeckett.ac.uk/5076/>
- Scrivens, R., & Conway, M. (2020). The roles of “old” and “new” media tools and technologies in the facilitation of violent extremism and terrorism. In R. Luekfeldt. & T. J. Holt. *The Human Factor of Cybercrime* (pp. 286-306). Routledge. [http://library.oapen.org/bitstream/id/6dbdcb14-86a4-4dd5-98b8-6dcd623c9268/9781138624696\\_oachapter13.pdf](http://library.oapen.org/bitstream/id/6dbdcb14-86a4-4dd5-98b8-6dcd623c9268/9781138624696_oachapter13.pdf)
- Sharpe, C. (2002). Covert surveillance and the use of informants. In McConville, M., & Wilson, G. P (Eds.), *The handbook of the criminal justice process*. Oxford University Press.
- Soiferman, L. K. (2010). *Compare and Contrast Inductive and Deductive Research Approaches* (ED542066). ERIC.  
<https://files.eric.ed.gov/fulltext/ED542066.pdf>

- Speer, D. L. (2000). Redefining borders: The challenges of cybercrime. *Crime, Law and Social Change*, 34(3) 256-273. [https://doi: 10.1023/A:1008332132218](https://doi.org/10.1023/A:1008332132218)
- Stevenson, R. J., & Mahmut, M. K. (2013). Using response consistency to probe olfactory knowledge. *Chemical Senses*, 38(3), 237–249. [https://doi:10.1093/chemse/bjs139](https://doi.org/10.1093/chemse/bjs139)
- Sterling-Folker, J. (2002). Realism and the constructivist challenge: Rejecting, reconstructing, or rereading. *International Studies Review*, 4(1), 73-97. [https://doi: 10.1111/1521-9488.t01-1-00253](https://doi.org/10.1111/1521-9488.t01-1-00253)
- Sullivan, G. B. (2002). Reflexivity and subjectivity in qualitative research: The utility of a Wittgensteinian framework. *Forum Qualitative Social Research* 3(3), Article 20. <http://dx.doi.org/10.17169/fqs-3.3.833>
- Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, 68(3), 226. [https://doi:10.4212/cjhp.v68i3.1456](https://doi.org/10.4212/cjhp.v68i3.1456)
- Terry, G., Hayfield, N., Clarke, V. & Braun, V. (2017). Thematic analysis. In C. Willig & W. Rogers (Eds.). *The SAGE Handbook of qualitative research in psychology* (pp. 17-36). Sage Publications. [https://doi: 10.4135/9781526405555](https://doi.org/10.4135/9781526405555)
- Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour and Information Technology*, 32(10), 1014–1023. [https://doi:10.1080/0144929x.2013.763860](https://doi.org/10.1080/0144929x.2013.763860)
- Tetzlaff-Bemiller, M. J. (2011). Undercover online: An extension of traditional policing in the United States. *International Journal of Cyber*

*Criminology*, 5(2), 813-824.

<http://www.cybercrimejournal.com/mellisal2011julyijcc.pdf>

Theohary, C. A., & Rollins, J. (2011). *Terrorist use of the internet: Information operations in cyberspace*. Congressional Research Service.

<https://fas.org/sgp/crs/terror/R41674.pdf>

Thompson, S. T. C. (2006). Helping the Hacker? Library Information, Security, and Social Engineering. *Information Technology and Libraries*, 25(4), 222-225.

<https://doi.org/10.6017/ital.v25i4.3355>

United Nations Office on Drugs and Crime (2012). *The Use Of The Internet for Terrorist Purposes*. United Nations.

[https://www.unodc.org/documents/frontpage/Use\\_of\\_Internet\\_for\\_Terrorist\\_Purposes.pdf](https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf)

Urbas, G. (2010). Protecting children from online predators: The use of covert investigation techniques by law enforcement. *Journal of Contemporary Criminal Justice*, 26(4), 410–425. <https://doi.org/10.1177/1043986210377103>

Urbas, G. (2012). Cybercrime, jurisdiction and extradition: The extended reach of cross border law enforcement. *Journal of Internet Law*, 16(1), 7-19.

<https://link-gale-com.helicon.vuw.ac.nz/apps/doc/A296379271/AONE?u=vuw&sid=AONE&xid=0a932080>

Vendius, T. T. (2015). Proactive undercover policing and sexual crimes against children on the internet. *European Review of Organised Crime*, 2(2), 6-24.

[https://curis.ku.dk/ws/files/150989358/Vendius\\_pp6\\_24\\_EROC.pdf](https://curis.ku.dk/ws/files/150989358/Vendius_pp6_24_EROC.pdf)

- Wainwright, R. (2016). *Trends and challenges for law enforcement training and education*. European Law Enforcement Research Bulletin, Europol, (3), 11-19. <https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/254/218>
- Webber, C., & Yip, M. (2012) Drifting on and off-line: Humanising the cyber criminal. In, S. Winlow, & R. Atkinson (Eds.), *New Directions in Crime and Deviancy* (pp. 191-205). Routledge Taylor & Francis.  
<https://doi.org/10.4324/9780203102657>
- Williams, E. N., & Hill, C. E. (2012). Establishing trustworthiness in consensual qualitative research studies. In C. E. Hill (Ed.), *Consensual qualitative research: A practical resource for investigating social science phenomena* (pp. 175–185). American Psychological Association.
- Willis, J. W., Jost, M., & Nilakanta, R. (2007). *Foundations of qualitative research: Interpretive and critical approaches*. Sage Publications.  
<https://doi:10.4135/9781452230108>
- Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies*, 29(2), 105-124.  
<https://doi:10.1080/1478601x.2016.1170282>
- Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2010). Online “predators” and their victims: Myths, realities, and implications for prevention and treatment. *Psychology of Violence*, 63(2), 13–35. <https://doi:10.1037/2152-0828.1.s.13>
- Wolak, J., Mitchell, K., & Finkelhor, D. (2005). The varieties of child pornography production. In M. Taylor, & E. Quayle (Eds.), *Viewing child pornography on*

*the Internet: Understanding the offence, managing the offender, helping the victims* (pp. 31-48). Russell House.

Workman, M. (2007). Gaining access with social engineering: an empirical study of the threat. *Information Security Journal: A Global Perspective*, 16(6), 315–331. <https://doi:10.1080/10658980701788165>

Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662–674. <https://doi:10.1002/asi.20779>

Wydra, C., Rota, D., Cellante, D., & Kohun, F. (2015). The evolution of criminal procedure for law enforcement in western Pennsylvania and the northern west Virginia with emphasis of cybercrime (Publication No. 10092230). [Master's Theses, Point Park University]. ProQuest Dissertations and Theses Global. <http://search.proquest.com/docview/1779975777/>

Zedner, L. (2009). *Security*. Routledge -Cavendish. <https://doi.org/10.1080/17440570903478042>

Zhang, B., Wu, M., Kang, H., Go, E., & Sundar, S. S. (2014). Effects of security warnings and instant gratification cues on attitudes toward mobile websites. *Proceedings of the 32nd annual ACM conference on human factors in computing systems - CHI '14*. <https://doi.org/10.1145/2556288.2557347>

## Appendices

### Appendix 1: Consent To Interview



### *Understanding the Expertise Required for Law Enforcement Investigating Cybercrime: An Exploration of Social Engineering Techniques*

This consent form will be held for 5 years.

Researcher: Grace Nock, School of Psychology, Victoria University of Wellington.

- I have read the Information Sheet and the project has been explained to me. My questions have been answered to my satisfaction. I understand that I can ask further questions at any time.
- I agree to take part in an audio recorded interview.

I understand that:

- I may withdraw from this study at any point before 01/09/2019 and any information that I have provided will be returned to me or destroyed.
- The identifiable information I have provided will be destroyed on 31/06/2019.
- Any information I provide will be kept confidential to the researcher and the supervisor.

- I understand that the results will be used for a Master's Thesis, a report to the Police, academic publications or presented to conferences.
- My name will not be used in reports, nor will any information that would identify me.
- I would like a copy of the transcript of my interview: Yes ☐ No ☐
- I would like a summary of my interview: Yes ☐ No ☐
- I would like to receive a copy of the final report, and have added my email address below. Yes ☐ No ☐

Signature of participant: \_\_\_\_\_

Name of participant: \_\_\_\_\_

Date: \_\_\_\_\_

Contact details: \_\_\_\_\_



## Appendix 2: Information Sheet For Participants



### *Understanding the Expertise Required for Law Enforcement Investigating Cybercrime: An Exploration of Social Engineering Techniques*

You are invited to take part in this research. Please read this information before deciding whether or not to take part. Please note, the decision to participate in this research project or not is entirely voluntary and has no impact upon your employment requirements. Any information provided as part of the research will additionally have no impact upon your employment.

#### **Who am I?**

My name is Grace Nock and I am a Master's student in the Forensic Program at Victoria University of Wellington. This research project is work towards my Master's Thesis.

I have been working for and with the Police in the Research and Evaluation Centre for 18 months, starting on a student volunteer placement, progressing to full-time work for a fixed-period; currently while I complete my study, I am working on a casual basis. It was through my first placement in 2018 that the topic of studying cybercrime was discussed and has since advanced to the interview stage now.

#### **What is the aim of the project?**

This research aims to understand how specialized units investigating cybercrime conduct their covert operations. Currently, very minimal literature has explored this area, with no known research looking at the components of social engineering within covert investigation. This research therefore seeks to interview Police staff who engage in online covert investigations within NZ.

The method of interviewing follows Applied Cognitive Task Analysis. Applied Cognitive Task Analysis will seek to discover the cognitive expertise necessary to perform undercover investigations into cybercrime through identifying the skills, strategies and processes used by experts in a particular task. This research will offer insights into current practice and expertise within law enforcement groups, and gather important data that can help shape future training programs for Police.

This research has been approved by the Victoria University of Wellington Human Ethics Committee [0000027248].

### **How can you help?**

You have been invited to participate because a part of your job requires you to interact with offenders online. If you agree to take part I will ask for the completion of pre-interview worksheets, and an interview with you at your workplace. I will ask you for a broad overview of the tasks and skills required to interact with an offender online, along with asking for further details on specific tasks or subtask. As each aspect of expertise is uncovered, it is probed for concrete examples in the context of the job, cues and strategies used, and why it presents a challenge to inexperienced people.

The interview will take 60-90 minutes, along with a further time spent on the worksheets prior to the interview. I will audio record the interview with your permission and write it up later. You can choose to not answer any question or stop the interview at any time, without giving a reason. You can withdraw from the study by contacting me at any time before 20/06/2019. If you withdraw, the information you provided will be destroyed or returned to you. You will also have a two-week opportunity to review your transcript and interview worksheet in order to amend or remove any information you do not approve of.

### **What will happen to the information you give?**

This research is confidential. This means that the researchers named below will be aware of your identity, but the research data will be anonymised and your identity will not be revealed in any reports, presentations, or public documentation.

Only my supervisor (Russil Durrant) and I will have access to the interview data. The interview transcripts, summaries and any recordings will be kept securely. Hard copies of the data will be destroyed on the 31/06/2019, and electronic copies will be destroyed at the completion of my thesis, to be stored on Police serves only.

Given the potentially sensitive nature of the research, any quotes used in my thesis will be approved by the manager of your work group. While your name will not be provided with these quotes, given the small sample of participants, it is possible your manager will be able to identify you via these quotes.

### **What will the project produce?**

The information from my research will be used in my Master's Thesis, in any academic journals or professional publications that I write, in a Police report summarising my thesis and in any additional professional presentations.

**If you accept this invitation, what are your rights as a research participant?**

You do not have to accept this invitation if you don't want to. If you do decide to participate, you have the right to:

- choose not to answer any question;
- ask for the recorder to be turned off at any time during the interview;
- withdraw from the study before 20/06/2019;
- ask any questions about the study at any time;
- receive a copy of your interview transcript;
- read over and comment on a written summary of your interview;
- be able to read any reports of this research by emailing the researcher to request a copy.

**If you have any questions or problems, who can you contact?**

If you have any questions, either now or in the future, please feel free to contact me:

**Student:**

Name: Grace Nock

Email: [nockgrac@vuw.ac.nz](mailto:nockgrac@vuw.ac.nz)

**Supervisor:**

Name: Russil Durrant

Role: **Co-Director** School of Social and Cultural Studies

School: School of Social and Cultural Studies

Phone: 04 4639980

[Russil.durrant@vuw.ac.nz](mailto:Russil.durrant@vuw.ac.nz)

**Human Ethics Committee information**

If you have any concerns about the ethical conduct of the research you may contact the Victoria University HEC Convenor: Dr Judith Loveridge. Email [hec@vuw.ac.nz](mailto:hec@vuw.ac.nz) or telephone +64-4-463 6028.

## **Appendix 3: Interview Schedule**

### **Applied Cognitive Task Analysis (ACTA)**

The ACTA process consists of three stages:

1. *Task Diagram*: this provides the interviewer with a broad overview of the task and highlights the difficult cognitive portions of the task to be probed further.
2. *Knowledge Audit*: this surveys the aspects of expertise required for a specific task or subtask. As each aspect of expertise is uncovered, it is probed for concrete examples in the context of the job, cues and strategies used, and why it presents a challenge to inexperienced people.
3. *Simulation Interview*: this allows the interviewer to probe the cognitive processes of experts within the context of a specific scenario. The use of a simulation or scenario provides job context that is difficult to obtain via the other interview techniques, and therefore allows additional probing around issues such as situation assessment, how situation assessment impacts a course of action, and potential errors that a novice would be likely to make given the same situation.

### **Instructions for completion of the ACTA templates**

- To provide a basis for further discussion during the interview, please complete what you can of the following templates.
- Please work through the Task Diagram, Knowledge Audit, answering each question in turn. Don't worry if you cannot answer all of the questions, simply leave that section blank and we will discuss it during the follow-up interview.
- The Simulation Interview will be completed in the interview, so do not complete that during the pre-interview preparation.
- Note: Please do not include any identifying information.

**1. Task Diagram**

Think about what you do when you are talking with offenders online. Can you break this task down into 3-6 steps or subtasks? These subtasks can be judgements, assessments, problem-solving, decision-making and thinking skills required for covert interaction with offenders.

Subtask 1	Subtask 2	Subtask 3	Subtask 4	Subtask 5

**2. SUBTASK: \_\_\_\_\_ From Task Diagram**

	EXAMPLE(S)	CUES & STRATEGIES	WHY DIFFICULT?
		What cues or strategies do you use in this situation?	Why is this task hard for novices?
<b>1. Perceptual Skills</b> Experts detect cues & patterns & make discriminations that novices can't see. Have you had any experiences where part of a situation just 'popped out at you', where you noticed things that others didn't catch?			
<b>2. Anomaly</b> Experts can notice when something unusual happens. They can quickly detect deviations, or notice when something that should happen doesn't. Can you think of any examples here? Can you think of a time when you spotted that something was amiss?			
<b>3. Past &amp; Future</b> Experts can guess how the current situation arose and they can anticipate how the current situation will evolve. Is there a time when you looked at a case or investigation and knew exactly how it happened and where things were headed?			
<b>4. Big Picture</b> Experts tend to see the big picture quickly. What are the major elements you have to know or keep track of? What is important about the big picture for this task?			
<b>5. Tricks of the Trade</b> Experts tend to be more			

	EXAMPLE(S)	CUES & STRATEGIES	WHY DIFFICULT?
efficient, but without cutting corners. E.g. ways of combining procedures. Are there ways of working smart or accomplishing more with less that you have found useful?			
<b>6. Improvising or noticing Opportunities</b> Experts tend to improvise, see what works in a particular situation, and are comfortable shifting direction to take advantage of opportunity. Can you recall a situation when you noticed that following the standard procedure wouldn't work?			
<b>7. Self-monitoring &amp; Adjustment</b> Experts notice when their performance is sub-par, and can often figure out why this is happening (e.g. high workload, fatigue, boredom, distraction) in order to make adjustments. Can you think of a time when you realised you would need to change the way you were working to get the job done?			
<b>8. Information</b> Unless you're careful, misinformation can mislead you. Novices tend to believe whatever the information says. Can you think of examples where you had to rely on experience to avoid being fooled by misinformation?			
<b>9. Scenario From Hell</b> If you were going to give someone a scenario to teach someone humility – that this is a tough job – what would you put into that scenario?			

### 3. ACTA Simulation Interview

Please reflect on your most recent case, and try to think about the decisions and judgments you made in engaging with an offender online.

Note: Please do not include any identifying information.

	Event/ Decision/ Judgement	Situational Assessment	Actions	Critical Cues	Alternative	Potential Errors
	Major events / crucial points in the investigation.	What's your assessment of the situation at this point in time?	What actions, if any, would you take at this point in time?	What pieces of information led you to this situational assessment / action?	Are there any alternative ways you could interpret this situation?	What errors would a novice be likely to make?
1						
2						
3						
4						
5						