Macrothink Institute™

International Journal of Social Science Research
ISSN 2327-5510
2014, Vol. 2, No. 1

Communication Interception Technology (CIT) and Its Use in the Fight against Transnational Organised Crime (TOC) in Australia: *A Review of the Literature*

Peter Bell (Corresponding author)

Faculty of Law, School of Justice

Queensland University of Technology, Australia

Tel: 617-3138-7105. E-mail: p6.bell@qut.edu.au

Mitchell Congram

Faculty of Law, School of Justice

Queensland University of Technology, Australia

Received: August 3, 2013 Accepted: October 17, 2013 Published: December 4, 2013

doi:10.5296/ijssr.v2i1.4089 URL: http://dx.doi.org/10.5296/ijssr.v2i1.4089

Abstract

In recent times, technology has advanced in such a manner that the world can now communicate in means previously never thought possible. Transnational organised crime groups, who have exploited these new technologies as basis for their criminal success, however, have not overlooked this development, growth and globalisation. Law enforcement agencies have been confronted with an unremitting challenge as they endeavour to intercept, monitor and analyse these communications as a means of disrupting the activities of criminal enterprises. The challenge lies in the ability to recognise and change tactics to match an increasingly sophisticated adversary. The use of communication interception technology, such as phone taps or email interception, is a tactic that when used appropriately has the potential to cause serious disruption to criminal enterprises. Despite the research that exists on CIT and TOC, these two bodies of knowledge rarely intersect. This paper builds on current literature, drawing them together to provide a clearer picture of the use of CIT in an enforcement and intelligence capacity. It provides a review of the literature pertaining to TOC, the structure of criminal enterprises and the vulnerability of communication used by

these crime groups. Identifying the current contemporary models of policing it reviews intelligence-led policing as the emerging framework for modern policing. Finally, it assesses the literature concerning CIT, its uses within Australia and the limitations and arguments that exist. In doing so, this paper provides practitioners with a clearer picture of the use, barriers and benefits of using CIT in the fight against TOC. It helps to bridge the current gaps in modern policing theory and offers a perspective that can help drive future research.

Keywords: communication interception technology, transnational organised crime, intelligence-led policing, signals intelligence, open source intelligence

1. Introduction

The consistent development of communication technology and the subsequent growth in its usage and popularity by society has not been limited to legitimate uses. These technological advances have also been adopted by criminals to advance their own illicit goals. With transnational organised crime (TOC) much of this communication makes use of modern technology and, as such, communication interception technology (CIT) is a crucial weapon that can be utilised. However, without the placement of CIT in the correct policing framework and a viable knowledge management model, it is a weapon lacking efficiency or effectiveness.

While research exists on TOC and CIT—albeit outdated or with a primary focus on privacy concerns—these two bodies of knowledge rarely intersect to examine the effective and practical use CIT can have against TOC. It is imperative to understand how TOC groups are operating, how they are structured and more importantly, how they can be stopped. This study addresses important gaps in modern policing theory by posing the following research questions: "how effective is communication interception technology in the fight against TOC?" and "how is communication interception technology best managed in a practical law enforcement framework?"

This paper builds on existing organised criminality and CIT literature, drawing them together to provide a clearer overview of CITs use in an enforcement and intelligence capacity. It reviews pre-existing literature that guides the understanding and concepts that underpin TOC and CIT. Specifically, it examines first the defining concepts of TOC, the general work on the structure of criminal enterprises, the nature of communication within these groups and finally the legal responses that Australia has introduced in recognition of this growing threat.

2. Methodology

To answer the research questions and address the gaps in current research, this study uses a qualitative research methodology employing grounded theory; and a systematic sampling and coding strategy outlined by Strauss and Corbin (1998) to ensure that the collection and categorisation of the data provided detailed and credible information relevant to the research objectives. Document analysis was chosen as the primary method of data collection for its ability to examine subjects not easily accessible because of the dearth of research previously conducted on the topic of CIT. Triangulation and validity through the systemic sampling and coding strategies ensured the study's trustworthiness.

Source documents (such as academic journals, periodicals, scholarly books, legal statutes, reports by law enforcement agencies, etc) on such topic areas as; organised crime, transnational crime, intelligence theory and intelligence practice, as well as communication interception technology and models of policing transnational organised crime, were critically examined during the course of this research.

3. Literary Review Findings

3.1 Understanding TOC

TOC is defined by the United Nations as: "structured groups of three or more persons acting together, over a period of time, with the aim of committing one or more serious crimes committed in more than one State, or has significant effect on another state, or elements of planning, preparation, direction or control occur in another State" (United Nations, 2000, pp.25-26).

Whilst TOC can be viewed as a broad spectrum of activity, LEAs note a range of specific 'organised' activities, including money laundering, drug trafficking, sex/human trafficking, people smuggling, arms trafficking, endangered species trafficking, cybercrime and most notably over the past decade, terrorism (Grennan & Britz, 2006; Borger, 2007; Davies, 2007; Lyman & Potter, 2007; Australian Crime Commission, 2009; Abadinsky, 2009;).

Unlike many 'habitual' forms of crime, TOC defies 'tradition' and exploits the reactive crime control techniques currently utilised by LEAs (Andreas & Nadelmann, 2006). From this, there has been substantial disagreement over the ability to succinctly define such an adaptable assortment of crimes and groups. This paper uses the definition put forward by Conklin (2009, 73) who, sharing similar definitional notions put forward by Abadinsky (1994; 2007), and Grennan and Britz (2006, p.12), describes organised crime as:

> "*Criminal activity by an enduring structure or organization developed and devoted primarily to the pursuit of profits through illegal means...organized crime has the characteristics of a formal organization: a division of labor, coordination of activities through rules and codes, and an allocation of tasks in order to achieve certain goals. The organization tries to preserve itself in the face of external and internal threats*" (Conklin, 2009, p.73).

3.2 Structure of TOC groups

The structure of organised crime networks, domestic or transnational, have long since been viewed as highly organised hierarchical structures, with groups such as the Sicilian Mafia, popularised in novels and film, influencing common perceptions. In reality crime groups have modified their structures into what Cressey (1997, p.3) and Williams (2001, p.70) describe as "fluid, dynamic and loosely structured networks that are highly flexible and possess the ability to adapt to relevant influences, designed with an intention to confuse authorities and protect their organisation".

The organisational structure of crime groups are highly debateable. However research by the United Nations (2002) led to the development of five TOC organisational structures: standard

hierarchy; regional hierarchy; clustered hierarchy; core group; criminal network (United Nations 2002). Lyman and Potter (2007) note that not all TOC groups fit specifically within the boundaries of the five structures, however the basic typologies provide a basis for understanding (Malkin, 2007).

It is argued that the first three hierarchical structures are those closest to "traditional" notions of organised crime, whereas the final two structures are closest to organisations emerging in the current global climate. The latter two are described here in more detail.

3.2.1 Core Group

The core group is a structure that consists of several individuals who form a tight and structured group to conduct business, surrounded by a loose structure of associate members or networks who are used to carry out business depending on the core group's intended criminal activities. Core groups generally limit their activities to one or only several ventures, acting in a more horizontal structure rather than hierarchical. The group exists solely for the profit motivation of individuals and shifts business activity to whichever venture generates the greatest profit. The core group is arguably one of the most readily emerging forms of organised crime structure and in some cases is the result of continued law enforcement pressure and as part of the groups adaptation to more sophisticated means (United Nations, 2002, pp.39-41; Lyman & Potter, 2007, pp.13-14).

3.2.2 Criminal Network

The criminal network is the clearest example of the globalisation of TOC and illustrates the measures that individuals and groups have taken to avoid detection and interference by LEAs (Cressey, 1997; Malkin, 2007). Criminal networks are the loosely organised, highly adaptable, fluid networks of individuals that engage themselves in illicit activities with regularly shifting alliances (Cressey, 1997, p.3; Williams, 2001, p.70; United Nations, 2002, p.41; Lyman & Potter, 2007, p.14). The network's shape, organisation and membership continually changes depending on the individuals, attributes and/or skills required.

The lack of predefined identity and structure makes it difficult for LEAs to infiltrate or dismantle the network. Whilst key individuals may exist, their association is usually distanced. This ensures that even if LEAs successfully target and prosecute one individual the network will still remain connected and operational (United Nations, 2002, p.41-43; Lyman & Potter, 2007, pp.14-15). As noted by the Australian Crime Commission (ACC) in their Annual Organised Crime Report (2009, p.6), the organised crime groups that pose the most serious threat are those that are fluid and adaptable, and are resilient to interventions, rebuilding quickly after disruption. It is for these reasons that this form of criminal network is emerging as the new forefront of TOC structures (Lyman & Potter, 2007).

3.3 Vulnerabilities of TOC

It is noted that there is minimal research on the weaknesses and vulnerabilities of TOC groups. Current research largely focuses less on the vulnerabilities of criminal enterprises and

more on the vulnerabilities of victims and subsequent propositions as how to reduce these vulnerabilities.

However, by understanding the structure of criminal enterprises it is possible to identify a core vulnerability: communication (Malkin, 2007). Criminals require instantaneous communication that spans the globe amongst their networks of contacts, and as such the very sophistication and complexity that dictates their business activities also makes it highly susceptible to high quality intelligence attack.

Grabosky and Smith (1998, p.188) argue that the use of telecommunications by criminals is categorised into four basic methods: coordinating and planning criminal activities; marketing and distribution of illicit services or products; sustaining the organisational structure; and obstruction of law enforcement investigations (Grabosky & Smith, 1998, p.188). Through the identification of these contact and communication points by LEAs, vital information can be acquired and subsequent intelligence developed to facilitate operational response strategies.

While Grabosky and Smith (1998) note a variety of communication strategies used by criminal enterprises, since their research the use of technology has advanced significantly. Mobile phones and Short Message Service (SMS) text messages, electronic mail (email), message forums, instant chat services and Voice Over Internet Protocol (VoIP) telephony services (Jackson et al., 2007) are now increasingly prevalent. Criminals have been found to programme mobile phones to send or receive from specific phone numbers and are known to exploit the easy availability and poor identity checks of mobile phone prepaid SIM (Subscriber Identity Module) cards along with access to cheap handsets. This allows them to reduce the risk of detection and interception and limits their links to other criminals (Jackson et al., 2007; Waters, Ball & Dudgeon, 2008).

The internet provides access to a growing multitude of free and temporary email accounts that require no identification and can transmit messages with relative anonymity (Waters, Ball & Dudgeon, 2008). The growing availability of encryption devices also allows criminals to either encode whole messages or messages within an attachment such as an image, document or link. (Bakier, 2007). Otherwise known as steganography, this technique is designed to ensure message content appears innocent if intercepted. Whilst “off the shelf” products are readily available for use by criminals they are also available to LEAs for decryption purposes (Jackson et al., 2007). To combat this, criminal enterprises—particularly those in Eastern Europe—have been known to develop their own software and methods (Abadinsky, 2009).

Despite the available research, Malkin (2007, p.18) notes that there is a distinct lack of research examining the social structures of criminal enterprises and both verbal and non-verbal communication that occurs within criminal networks. Much of the existing research focuses solely on the flow or path of the communication, rather than the ‘how’ and ‘what’ of the actual communication (Malkin, 2007, pp.18, 22). This highlights another gap surrounding the concepts of CIT and the ability to identify its effectiveness and most practical use.

3.4 Legal Responses within Australia

Over the past decade Australia has introduced a variety of reforms to assist in the combat of transnational criminal activities occurring on and off shore (Hughes, 1999, p.10). Cornall (2005, p.62) and Irwin (2001, pp.5-6) identify that policy and operational responses are two key facets required to challenge this societal threat. Administrative arrangements have strengthened Australia's fight through the expansion of agreed extradition treaties, mutual assistance agreements, Memorandums of Understanding with Asian neighbours and the establishment of international cooperation groups responsible for establishing laws, agreements and treaties (Cornall, 2005, p.62). Since the terror acts of September 11, 2001 on US soil, and the Bali Bombings of October 12, 2002, stringent legislation has been introduced to further the prevention of similar attacks within Australian borders. Legislative measures introduce definitions and offences for transnational criminal activities and further assist combating these crimes. This has included an expansion of powers such as the ability to seize and freeze assets identified as proceeds of criminal activities and an increase powers and responsibilities regarding investigation and arrest to law enforcement and intelligence agencies such as the Australian Federal Police (AFP) and the Australian Security Intelligence Organisation (ASIO). Australia has also promoted their involvement with the Organisation for Economic Cooperation and Development with attempts to ratify the Financial Action Task Force on Money Laundering's 40 recommendations and nine special recommendations against money laundering and terrorism financing (Cahill & Marshall, 2004, pp. 52-66).

Cornall (2005, p.62), Irwin (2001, p. 7), Wardlaw and Boughton (2006) and Chalk and Rosenau (2004, p. 38) all note that attempts to increase knowledge sharing through the interweaving of law enforcement and intelligence agencies, including the creation of the Australian Crime Commission, National Threat Assessment Centre and Transnational Crime Coordination Centre. The importance of including the private sector in intelligence sharing as a means of protecting crucial infrastructure as a major step in the right direction has also been recognised.

In addition to policy responses, operational responses have been important in the fight against TOC. The extent of AFP's international deployment and operations has enhanced intelligence gathering and diplomatic ties between nations, namely Indonesia, Papua New Guinea and those in the Pacific Islands. Glenn, Gordon and Florescu (2008) argue that whilst Australia has instigated significant changes to recognise the growth of TOC, where 'transnational' underscores organised crime, the need for a comprehensive, integrated global counter-strategy is required.

Whilst crime groups are vulnerable to detection and disruption because of their communications, in addition to policy and operational responses, LEAs need a method and framework that allows them to combat these crimes efficiently and successfully. The next section examines the modern policing methodologies, their appropriateness in fighting TOC and their ability to effectively utilise technology that can exploit criminal communications.

4. Policing Methodologies

4.1 Models of Policing

In an ever changing world driven by a media-fuelled obsession of demanding best practice in crime reduction, policing methodologies have developed into their own research niche as attempts to develop a 'perfect solution' come and go. Ratcliffe (2008a; 2008b) and Weisburd and Eck (2004) contend that there are five primary models: traditional policing, community-orientated policing, problem-orientated policing, computer statistics and intelligence-led policing. Each model has its own differing concepts of strategic goals and possesses its own strengths and weaknesses.

Weisburd and Eck (2004, p. 44) argue that the traditional model of policing can be seen as a "one size fits all" arsenal of reactive strategies to suppress crime regardless of the nature, level or other variations of crime within the jurisdiction. These strategies include rapid response to callouts, random community patrols, follow up investigations and occasional intensive enforcement and arrest policies (Weisburd & Eck, 2004, pp. 44-45). Eck and Rosenbaum (1994) and Conser et al. (2005, pp. 329-330) similarly argue that traditional policing has four primary functions: control crime, provide immediate response, arrest and serve justice, and provide 'non-emergency' services. As such the model relies solely on law enforcement powers to prevent crime (Conser et al., 2005; Eck & Rosenbaum, 1994). Subsequently, Goldstein (1987) and Ratcliffe (2008b, p. 271) both argue that the primary drawback with this methodology is that this "enforcing the law" attitude results in a distinct ineffectiveness in promoting long term crime control, arguably the result of being a reactive tactic rather than a proactive strategy (Goldstein, 1987; Ratcliffe, 2008a, p. 271). It is important to note that arguments made against the traditional methodology contain a source of bias resulting from their primary objective to provide support for an alternate policing methodology. However, there is also a distinct lack of empirical evidence or explanation supporting the reasoning for successes of the traditional model.

Community-orientated policing (COP) is grounded in the notion that through community interaction and support, crime and fear of crime can be controlled. Police act in a role as a facilitator within the community as they establish a balance between police duties and community responsibilities. Contact with the community in a means of establishing why crime is occurring rather than a simple response to calls for service is promoted as a fundamental purpose of COP (Goldstein 1987). However, in their own review of COP research, Adams, Rohe and Arcury (2002), and Eck and Rosenbaum (1994) argue that there is a clear lack of clarity as to what exactly passes as community policing and that the benefits and impact COP has on crime have been mixed during research evaluation. The disagreement as to what actually constitutes and defines community policing thus makes evaluation difficult, but adoption and proclaimed use by an LEA easy (Ratcliffe, 2008b, p. 70).

Problem-orientated policing (POP) is an approach that involves examining and analysing clustered incidents to determine an underlying cause of crime and implement strategies specifically to address the problem. POP focuses on the use of new preventative responses that engage the wider community when their contribution can potentially help to reduce the

problem (Goldstein, 1990; Centre for Problem Oriented Policing, 2009). This approach is similar to situational crime prevention strategies (Goldstein in Scott, 2000, p.5) however, rather than being a specific policy as in the case of situational crime strategies, POP guides the LEA's whole doctrine in crime prevention. John and Maguire (2003), and Braga and Weisburd (2006) note there is a clear structural difficulty in implementing POP in practice, with an evaluation of numerous studies indicating a disconnect from POP's articulated aims and the realistic practices of LEAs.

Computer Statistics (COMPSTAT) is a management philosophy that utilises geographical information systems for crime mapping to identify problems and approach crime reduction and resource management in line with relevant problem areas. Due to the primary focus on statistics, critics such as Weisburd et al. (2003) and Manning (2005) claim that COMPSTAT's effectiveness is minimal due to the ability to misconstrue data and the subsequent ability to greatly under-represent crime. Criticism further extends with Manning (2005) claiming that COMPSTAT goes so far as to regenerate and reinforce the hierarchical and methodological guides of traditional policing, a structure that COMPSTAT along with COP and POP were designed to eradicate.

A common factor, and subsequently a negative consequence, presented in these four methodologies, is their specific focus on addressing localised and 'minor' crime. As such they fail to possess the qualities required to address the more serious threat of TOC.

Whilst over the past two decades there has been a noticeable shift in the culture and strategies within most, if not all, Australian LEAs towards using a more proactive policing approach for tackling all forms of criminal activity, the traditional reactive model of policing still exists as the primary methodology (Chan, 1997; Ratcliffe, 2008a). This has been precipitated by the increasing sophistication of criminal enterprises, which has made it imperative to work towards the disruption and demolition of the network structures instead of merely arresting individual criminals within organised groups (Robertson, 1997; Wardlaw & Boughton, 2006). The attempts to break up criminal networks will fail until all available information is developed, analysed and transformed into an intelligence product suitable for use by law enforcement personnel. As such there needs to be a shift within the law enforcement environment that views intelligence as a precondition to effective policing, rather than as a supplement. To encourage this change there is a need to break down intelligence 'obstacles' as LEAs enter the new era of the ILP methodology (Wardlaw & Boughton, 2006, p. 135).

4.2 ILP Methodology

Whilst the use of intelligence has been common practice within the military arena for centuries, its application as a proactive rather than a reactive strategy within Australian LEAs is still a relatively new concept. ILP has no universally accepted definition, however it is identified by the core idea that policing, from tactical to strategic levels and beyond to government policy, should be informed by relevant and actionable intelligence analysis. It is developed as a model that uses intelligence to guide and shape policy, strategy and operations, rather than simply solving or supporting singular investigations (Wardlaw & Boughton, 2006, p.135).

A central precept of the ILP methodology is to focus on the prolific and persistent offenders who commit a majority of the crime with the requirement to "tackle and incapacitate" the primary offenders of serious crime (Flood, 2004; Ratcliffe, 2008b, p.167; Flood & Gasper, 2009, p. 51). Through the development of an ILP grounded system, the ability to manage this criminality can be identified.

As Flood and Gasper (2009, p. 57) note, the primary difficulty that LEAs face is simply trying to visualise and understand the criminal environment. They argue that whilst on the surface it is initially confusing, chaotic, complex and ever changing in both its impact and character, there always remains an area that is stable and enduring (Flood & Gasper, 2009, p. 57). It is the identification of this area by the collection, collation and analysis of data and subsequent development of intelligence that reveals a systematic and comprehensible environment. This understanding enables the basis for a "highly impactive strategy" that can at the very least, provide a starting point for dealing with the bigger picture. Meeting this requirement, ILP is the most suitable methodology for combating TOC (Flood & Gasper, 2009, p. 57).

The current lack of evaluation of ILP, along with a requirement for additional research and development of a model of best practice for implementation of ILP into new jurisdictions is clearly acknowledged within the literature (Ratcliffe, 2002; 2008a). This is in part due to the difficulty to effectively evaluate business models. Within Australia, the use and slow integration of ILP has been used with limited, and in some cases, flawed evaluation of its effectiveness. Heldon (2009) and Ratcliffe (2008b) discuss the effectiveness and limitations of Operation Anchorage, a short term ILP operation carried out by the AFP in response to a spike in property crime in the Australian Capital Territory in 2001. Whilst the operation was deemed effective following its closure and resulted in a 21 per cent decrease in burglaries combined with a residual effect lasting 45 weeks, its unsustainability resulted from limited resources and high costs. Heldon (2009, pp. 128-129), argues that the operation was flawed in its use of the ILP methodology—whilst offender targeting was present, it failed to address the underlying causal factors a primary focus on tactical intelligence meant that the strategic and long-term ideals were forgotten. As such Heldon (2009, pp. 130) theorised that had the AFP embraced ILP as a whole and addressed these issues, it is likely a more robust result could have been achieved.

There is also an apparent gap in literature regarding the specific discussion of intelligence collection. Whilst Ratcliffe (2008a; 2008b) frequently encourages the use of covert means of intelligence collection and briefly discusses the use of informants, he, along with a multitude of existing literature, fails to examine the covert means in depth. In addition, there is an obvious disconnect in the literature between the use of CIT and ILP as a whole.

Of all the policing methodologies ILP is uniquely positioned to effectively combat TOC. For example: the United Kingdom's (UK) Serious Organised Crime Agency (SOCA) (SOCA, 2010) argues that the majority of current LEAs are structured for bureaucratic efficiency. The operational focus is on individual crime types to satisfy the priorities and objectives of a government led by the media advancing community concern. Conversely, criminal

enterprises rarely think or deal in terms of isolated and singular crime areas. Instead, they simply see the opportunities available to them for making money if they possess the relevant criminal capability, and frequently amalgamate crime types into their enterprise as a means of maximizing profits whilst ideally minimizing detection (Serious Organised Crime Agency, 2006, p. 15; Flood and Gasper, 2009, p. 57).

The UK's Audit Commission (1993) noted that the targeting of known and recidivist offenders, criminal leaders and criminal innovators is the cornerstone of any proactive policing model. A central precept of the ILP methodology is to focus on the prolific and persistent offenders who commit a majority of the crime with the requirement to 'tackle and incapacitate' the primary offenders of serious crime (Flood, 2004; Flood and Gasper, 2009, p. 51; Ratcliffe, 2008b, p. 167). Through the development of an ILP grounded system the ability to manage this criminality can be identified. As Flood and Gasper (2009) note, the primary difficulty that LEAs face is simply trying to visualize and understand the criminal environment. They argue that whilst on the surface it is initially confusing, chaotic, complex and ever changing in both its impact and character, there always remains an area that is stable and enduring (Flood and Gasper, 2009). It is the identification of this area by the collection, collation and analysis of data, and subsequent development of intelligence, that allows the development of a clearer understanding of what once appeared complex and haphazard, and reveals a systematic and comprehensible environment. This understanding enables the basis for a 'highly impactive strategy' that can, at the very least, provide a beneficial starting point for dealing with the bigger picture. These requirements are answered by the ILP philosophy, characterizing it as the most suitable methodology for combating TOC (Flood and Gasper, 2009).

It has well been documented that the key resolve to TOC is a comprehensive, integrated global counter-strategy that involves the continual cooperation, support and knowledge sharing of law enforcement and intelligence agencies worldwide (Glenn, Gordon, & Florescu, 2008). A point that then resonates is that without intelligence, the required case for cooperation among countries and agencies cannot be made in the first place, the priorities of the LEA cannot be identified and the threats posed cannot be tackled.

The literature illustrates that the proactive nature of ILP is the most beneficial framework that can fight criminal enterprises and support CIT appropriately, as will be discussed in the following section.

5. Communication Interception Technology (CIT)

In line with the development and growth of communication technology, there has been an increasing requirement for the use of interception technologies. This 'popularity' has resulted in frequent debate regarding the most appropriate definition (Branch, 2003; Starey, 2005; Electronic Frontier Australia, 2006). The term 'communication interception technology' (CIT) resulted from the preconceived notions attached to the definition of 'telecommunications'—largely associated with solely traditional telecommunication methods, such as telephone calls. Conversely, CIT implies a broader scope for all forms and methods of communication and is subsequently used to reference the interception methods and related

technology. It is important to note that concerning CIT, under both the Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act) and Telecommunications (Interception) Amendment Act 2006 (Cth), communications are divided into two distinct categories: live communications and stored communications.

'Live communications' addresses the category of communication that passes over a telecommunication system, such as voice telephony. The 'live' aspect concerns the fact that during a telephone call, the recipient instantly receives the message being communicated in 'real time' (Starey, 2005; Ahmed, 2007). Starey (2005) argues the key aspect personifying live communication is that without interception (listening or recording) there is no record of the conversation once communication ceases.

Conversely, stored communication or communication stored in transit covers communication that during the course of its transmission is stored on one or more pieces of equipment of a carrier or service provider before being retrieved and accessed by the recipient. Starey (2005) and Ahmed (2007) both state that the concept of stored communication applies to most forms of electronic communication. During the transmission of electronic communication—such as email, SMS text messaging, voice mail, internet chat or instant messaging software and VoIP telephony—the data packets transmitting this information are stored, at least momentarily, on various service provider servers and computer equipment. This information can therefore be intercepted prior to the intended recipient actually receiving the message (Starey, 2005; Ahmed, 2007). It is argued that this breakdown is especially important with regards to legislative definitions and subsequent abilities to intercept communications, where interception is the act of listening to, recording or reading through any means a communication without the knowledge of the person making the communication (Starey, 2005; Telecommunications (Interception) Amendment Act Cth, 2006; Ahmed, 2007).

5.1 Signals Intelligence

Signals intelligence (SIGINT), has had a long history of use by military forces around the world ever since the tactical use of both wired and wireless communication technologies. Richelson (1999, p. 167) claims that traditionally, signals intelligence is considered one of the most important and sensitive forms of intelligence able to provide a vast amount of information. Whilst traditionally utilised by foreign governments or groups, the expansion into criminal groups has slowly developed over the years. Communication Intelligence (COMINT) and Electronics Intelligence (ELINT) form the majority of CIT relevant to law enforcement and can be used in conjunction with open source intelligence (OSINT).

COMINT, the interception of signals between people, broadly corresponds to live communications such as telephone calls, while ELINT, the interception of signals between machines, corresponds to stored communication mediums such as email or SMS.

Whilst the DSD plays a pivotal role in intelligence collection and analysis within the Australian Intelligence Community (AIC), its membership and subsequent framework with the AIC limits its functions to a national security oriented position. Section 4 of the Australian Security Intelligence Organisation Act 1979 (Cth) outlines security as including

espionage, sabotage, politically motivated violence, the promotions of communal violence, foreign interference, attacks on Australia critical infrastructure and defence systems and also includes carrying out of Australia's responsibilities to any other foreign country in relation to threats to security with a particular focus on politically motivated violence. This is further exemplified restrictions imposed under the *Intelligence Services Act 2001 (Cth)*. Section 11 of the Act in particular, explicitly details that "the agencies' functions do not include: (a) the carrying out of police functions; or (b) any other responsibility for the enforcement of the law."

This effectively prohibits DSD from intercepting signals originating from within Australia and requires a "double up" of resources as Australian LEAs must purchase, maintain, operate and analyse their own interception technology. This is coupled with the need to go through the rigorous process of requesting appropriate intercept warrants and attempting to maintain a quality level of information sharing between multiple agencies. This separation of intelligence, law enforcement and also foreign and domestic intelligence is a significant obstacle to the overall success of effective transnational crime fighting (Chalk & Rosenau, 2004; Bhaskar & Zhang, 2007; Brady, 2008; Ratcliffe, 2008b; Chalk et al., 2009).

Recent developments in the United States regarding the interception of private communications by the National Security Agency (NSA) in support of the war on terror, has practitioners and academics engaged in a comprehensive debate surrounding Fourth Amendment rights to privacy, under the US Constitution.

Under US law, intelligence agencies are not required to obtain a warrant in order to collect information on foreign adversaries and terrorists with communications that occur outside the US. When electronic communications either transit or occur within the US, however, intelligence officials must use the Foreign Intelligence Surveillance Act (FISA). To use FISA, the government must show probable cause that the target of the surveillance is a foreign power or agent of a foreign power (Bazan, 2009). Following the events of 911 President Bush enacted Executive Powers enabling the NSA to intercept communications domestically in response to an ongoing terrorist threat. Supported by Congress in this instance, there was agreement that greater flexibility with regard to the interception of communications was needed. Congress also passed amendments to the FISA legislation in the USA-Patriot Act in 2001. This Act significantly reduced the standard required of a federal officer to apply for intelligence collection under the FISA framework. In addition to this Congress also amended FISA in the Protect America Act of 2007 and the FISA Amendments Act of 2008 (Bazan, 2009).

The ability to operate a warrantless surveillance program (of communications) was initiated by President Bush in 2005, and became known as the Terrorist Surveillance Program (TSP) or "warrantless wiretapping" (Risen & Lichtblau, 2005). With reports of the surveillance program slowly finding their way to the public domain, some argued that the program was necessary to intercept al-Qaeda – related communications more quickly than the FISA process allowed. Further to this, supporters of the program claimed that the FISA process did not allow them to gain valuable intelligence on the terrorist group in a timely manner (Liptak,

2007). While others argued that the President has overstepped the bounds of his authority by spying on Americans and that the President could not completely bypass the FISA process because Congress explicitly intended FISA to be the exclusive means for authorising this type of surveillance. Furthermore, some argued that the program failed to offer sufficient protections to prevent the government from monitoring communications of innocent Americans and that the program lacked sufficient oversight (Risen & Lichtblau, 2005).

In 2007, the US Attorney General informed Congress that the Foreign Intelligence Surveillance Court (FISC) had issued orders authorising the collection of international communications into and out of the United States when the government had probable cause to believe that the communications belonged to a terrorist organisation. As a result of the FISC order the President would discontinue his authorisation of TSP and conduct all electronic surveillance under FISA. Some saw the updating of FISA in 2007/08 as a way to facilitate additional backdoor intelligence gathering practices, such as large-scale data mining and represented a weakening of civil liberties in the United States (Lowenthal, 2009).

As with many democracies, the challenge surrounding the interception of communications will remain balancing the rights of the individuals and the needs of the public interest.

5.2 Open Source Intelligence

Another form of intelligence gathering used in the fight against transnational crime is open source intelligence (OSINT). Although having been in existence for as long as SIGINT, it has been increasingly relied upon since the explosion of the internet and the increasing availability of information in subsequent years.

OSINT is defined in a similar fashion throughout the literature, with Gibson (2004, p. 17) defining it as "...the analytical exploitation of information that is legally available and in the public domain". OSNIT can be obtained from various sources including traditional media broadcast, commercial 'on-line' premium, specialist technical/tactical, 'grey literature', overt human observers, commercial imagery and mapping specialists. Specific examples include the use of newspapers, the Internet, phone books, scientific journals, textbooks, periodicals, books, pamphlets, and radio and television broadcasts (Umphress, 2005, p. 84; Best, 2006, p. 5).

In terms of the practical application of OSINT in the public sector, it has great potential in the areas of defence and security, which are becoming increasingly complex as new communication technologies aid in the emergence of transnational criminal networks (Gibson, 2004, p. 20). As Shelley (2002, p. 4) maintains, terrorist and transnational criminal groups use "cellular and satellite phones, the Internet, email and chat rooms" to communicate. "They code their messages through encryption and steganography (hiding messages within other messages)" (Shelley, 2002, p. 4). Moreover, Stohl (2006, p. 231) acknowledges the use of the Internet by transnational crime groups in order to spread propaganda and/or to recruit members. Since these public forms of communication are being exploited by criminal networks, OSINT is indispensable in the fight against transnational crime. As

Gibson (2004, p. 19) stated, OSINT has emerged as a result of "…changing aspects of contemporary society as both a product of it and a tool to deal with it".

The use of OSINT in a law enforcement context is not without its problems, particularly in relation information overload, quality control, misinformation and/or legal issues. However, the utility of the Internet in creating OSINT cannot be ignored. In this respect, some authors call for greater public funding and focus upon OSINT protocols, especially within the public sector, in order to combat global issues such as transnational crime. As Gibson (2004, p. 19) recognized, OSINT is both a product of the 'changing aspects of contemporary society' as well as a tool to deal with it. However, more focused efforts at integrating OSINT into the broader Intelligence Community are required, especially at a public sector level. Indeed, "…in an age characterised by instantaneous, distributed, publicly available, open source information, uninformed decision-making arising from an inability to understand, harness and exploit the potential of this new breed of information becomes a significant security weakness (Gibson, 2004, p. 20). Not only is it a security weakness, but it is an unforgivable security threat. As Hulnick (cited in Mercado, 2004) stated, "Neither glamorous nor adventurous, open sources are nonetheless the basic building block for secret intelligence". In this regard, OSINT is merely one form of intelligence and is intended as one thread in a complex web of intelligence sources that can be used be LEAs in areas such as the fight against TOC.

5.3 Issues Surrounding CIT

Whilst SIGINT has been used extensively and effectively in military environments for over a century, it is difficult to comprehend why CIT continues to remain so severely limited in its use. In much of the literature, there are two primary issues surrounding the use of CIT—legislation (governing usage) and privacy. These issues directly correlate with concerns regarding the infringement of privacy rights influencing the controls and limitations placed on the use of CIT within the legislation. Despite this, there is a distinct lack of research examining these issues in context of the practice application of CIT.

Starey (2005) analyses the Australian legal framework governing CIT comparing it with the United States' (US) framework. It is argued that whilst Australia cannot directly adopt the same legislation applied in the US, we can learn from their errors and debates to improve our own laws and increase their clarity (Starey, 2005, p. 55). A common feature evident in both countries is the narrow restrictions on, and subsequent difficulty in, being issued a warrant for lawful interception under the TIA Act. Starey (2005) demonstrates that the current legislation caters for CIT only as a last resort and serves a primary purpose as an evidence gathering tool, rather than a forefront intelligence collection method. In contrast, stored communications are significantly easier to access under the Amendment Act.

As argued by privacy advocate Electronic Frontier Australia (EFA) (2006), these responses seemingly position stored communications as a "less important" communicative method, despite the increasing adoption and preference of these methods over live communication by individuals and business. Their position however is degraded due to their failure to recognise the advantages attached to CIT in law enforcement and sole focus on rights to privacy. Whilst

it is undeniable that privacy is an important aspect of life, it also provides additional protection to criminals and criminal enterprises. Grabosky and Smith (1998, p. 29) argue that the respect for an individual's privacy is not an absolute interest and is conversely subject to other competing interests of importance within society. The use of interception technology is justified when the social benefits of its use outweighs the cost of individual privacy. It is here that EFA (2006) lacks the ability to recognise the careful balance between privacy and enforcement—as power shifts in favour of increased privacy it greatly limits vital enforcement technique and technology.

The sentiments of Electronic Frontier Australia (2006) are also shared by Bronitt and Stellios (2005, p. 887), whose evaluation of the regulatory framework for CIT in Australia results in the rejection of the 'balancing' model and proposes the development of a regulatory model advocating human rights and due process as a "paramount consideration". Despite these claims however, they fail to detail the proposed model. Bronitt and Stellios (2005; 2006) also consistently raise concerns regarding the increasing use of interception technology by states and territories, rather than sole use by Federal agencies. What Bronitt and Stellios (2005; 2006) fail to acknowledge is that the growth of TOC is not limited to breaching only federal or state laws, indeed they are well known to exploit proposed restrictions (Irwin 2001). Providing all agencies with access to these methods is an integral part of the unification of Australian LEAs, a factor which is stressed as an essential requirement throughout the literature (Irwin, 2001; Glenn, Gordon & Florescu, 2008; Flood & Ratcliffe, 2008b; Gasper, 2009).

The primary debate surrounding the use of CIT is the individual's right to privacy and the public interest will continue for decades. What is apparent is the need for ongoing attention being applied to the laws (and oversight authorities) governing the use of CIT in the targeting of TOC.

6. Implications for Further Research

This paper highlights significant gaps in CIT, TOC and ILP literature, and in doing so provides the basis for future research in two key areas: the effectiveness and deployment of CIT by interviewing law enforcement investigators and analysts and closely examining national and international case studies; and the communicative methods, strategies and structures of TOC groups—in particular the 'what', 'where', 'when', 'how' and to a limited extent, 'why', of criminal communication.

Whilst the use of CIT is seemingly essential in the fight against TOC, without a strong foundational knowledge of how it's targeted and deployed, there will continue to be limits on the production of high quality intelligence. This second research need is noted also by Malkin (2007) and Grabosky and Smith (1998; 1999).

7. Conclusion

The globalization and growth of transnational organized crime (TOC) is a cause for great concern amongst society. While advancements in communication technologies have changed the communication landscape, they have also created opportunities for organized criminals to

use the available technology for their own illegal gains. Organized crime can no longer be considered in relation to strict geographic boundaries – it now extends globally across a spectrum of activities including money laundering, drug trafficking, sex/human trafficking, people smuggling, arms trafficking, endangered species trafficking, cybercrime and, most notably over the last decade, terrorism (Abadinsky, 2009; Davies, 2007; Lyman and Potter, 2007; Australian Crime Commission, 2009; Borger, 2007; Grennan and Britz, 2006).

However, while the increased availability of communication technologies and their usage presents opportunities for criminals and corrupt networks, it also presents opportunities for the law enforcement agencies (LEAs) tasked with fighting such crime and corruption. The need for two or more criminal or corrupt entities to exchange information regarding their planned activities is a critical point at which LEAs can disrupt those activities. As such, communication interception technology (CIT) presents itself as a crucial weapon to be harnessed by LEAs. However, despite its possibilities CIT remains drastically underutilized as an investigative tool and, while literature exists on TOC and CIT, very few if any studies intersect to examine the theoretical or practical use of CIT as a tool to fight crime.

Recognising the need to better understand how CIT is currently used, and could be used, to fight organized crime, this research builds on existing literature on organized crime and CIT, drawing them together to provide a clearer overview of CIT's use in an enforcement and intelligence capacity. This was achieved by asking the following questions:

1) How effective is CIT in the fight against TOC? and;
2) How should the issues surrounding CIT be best managed within a practical law enforcement framework by English-speaking Commonwealth countries such as Australia that share comparable legislative platforms?

In addition to addressing several gaps in the current literature the research identifies the most appropriate policing methodology – intelligence-led policing (ILP) – to underpin the use of CIT and how it can be, or is currently being, restricted by the policing culture and privacy concerns present in various English-speaking Commonwealth countries such as Australia. In doing so this research makes a valid contribution to the body knowledge in developing greater efficacy for law enforcement strategies and the disruption of the serious threat posed by TOC to society.

TOC is a diverse and complex area costing global society in excesses of US$3 trillion annually – a figure which is set to grow (Borger, 2007). This paper has highlighted that while new communication technologies provide new opportunities for criminal and corrupt networks to expand their operations they also provide a unique opportunity for LEAs and corruption investigators to disrupt these activities. By using CIT, investigators can garner timely and valuable information, better understand the structure and nature of the criminal entities they are targeting and uncover larger networks of criminal or corrupt operations. While the effectiveness of CIT is still difficult to determine based on current literature, what is apparent is that it presents as a powerful tool to combat the new and evolving criminal structures of today's global environment. Its limited use in an investigative capacity is largely

due to the legal complexities and privacy concerns surrounding its use, as well as the cultural issues which mean that intelligence often fails to truly take centre stage in an investigation. However, there is a way forward. While there are barriers to the effective use of CIT in investigations this paper identifies how CIT can be embedded in an ILP framework while still supporting the underlying philosophy of the right to privacy and its balance with the public interest. Taking a common sense approach the paper seeks to balance the privacy rights of individuals – by ensuring legal thresholds are met – with the public interest, enabling investigators to access the necessary powers to utilize CIT in the effective investigation of TOC.

As stated by Williams (1980, p. 35), 'Intelligence is the most important single weapon in the armoury of law enforcement generally …'; as this paper attests, if embedded in a proactive ILP framework, CIT has the power to secure that intelligence, presenting as a powerful weapon in the fight against TOC and official corruption.

References

Abadinsky, H. (1994). *Organized Crime* (3rd ed.). Chicago: Nelson Hall.

Abadinsky, H. (2009). *Organized Crime* (9th ed.). Belmont, CA: Wadsworth Publishing.

Adams, R. E., Rohe, W. M., & Arcury, T. A. (2002). Implementing Community-Oriented Policing: Organizational Change and Street Officer Attitudes. *Crime Delinquency, 48*(3), 399-430. http://dx.doi.org/10.1177/0011128702048003003

Ahmed, S. (2007). B-Party Intercepts and the Telecommunications (Interception) Amendment Act 2006 (Cth). *Internet Law Bulletin, 10*(1).

Andreas, P., & Nadelmann, E. (2006). *Policing the Globe: Criminalization and Crime Control in International Relations*. New York: Oxford University Press.

Australian Crime Commission. (2009). *Organised Crime in Australia*. Canberra: Australian Crime Commission.

Bakier, A. H. (2007). The New Issue of Technical Mujahid: A Training Manual for Jihadis. *Terrorism Monitor, 5*(6).

Bazan, E. B. (2009), The Foreign Intelligence Surveillance Act: Comparison of the Senate Amendment to HR 3773 and the House Amendment to the Senate Amendment to HR 3773, 12 June 2008, in Confrontation or Collaboration: Congress and the Intelligence Community, Belfer Centre, Harvard Kennedy School of Government, 2009, p. 1.

Bhaskar, R., & Zhang, Y. (2007). Knowledge Sharing in Law Enforcement: A Case Study. *Journal of Information Privacy & Security, 3*(3), 45-68.

Borger, J. (2007). *Organised Crime: The $2 trillion threat to the world's security. The Guardian*. Retrieved from http://www.guardian.co.uk/world/2007/sep/12/topstories3.mainsection

Brady, H. (2008). Europol and the European Criminal Intelligence Model: A Non-State

Response to Organised Crime. *Policing, 2*(1), 103-109. http://dx.doi.org/10.1093/police/pan014

Braga, A. A., & Weisburd, D. (2006). Problem-Oriented Policing: The Disconnect between Principles and Practice. In A. A. Braga & D. Weisburd (Ed.). *Police Innovation: Contrasting Perspectives* (pp. 133-152). New York: Cambridge University Press.

Branch, P. A. (2003). Lawful Interception of the Internet. *The Australian Journal of Emerging Technologies and Society, 1*(1), 1-7.

Bronitt, S. and Stellios, J. (2005). Telecommunications Interception in Australia: Recent trends and regulatory prospects. *Telecommunications Policy, 29*(11), 875-888. http://dx.doi.org/10.1016/j.telpol.2005.06.010

Bronitt, S. and Stellios, J. (2006). Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution? *Prometheus, 24*(4), 413-428. http://dx.doi.org/10.1080/08109020601030001

Cahill, L. and Marshall, P. (2004). T*he Worldwide Fight Against Transnational Organised Crime: Australia*. Canberra: Australian Institute of Criminology.

Centre for Problem Oriented Policing. (2009). *Centre for Problem Oriented Policing*. Retrieved August 27, 2009, from http://www.popcenter.org

Chalk, P., & Rosenau, W. (2004). *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*. Santa Monica: RAND Corporation.

Chalk, P., Warnes, R., Clutterbuck, L., & Kirby, A. (2009). *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom.* Santa Monica: RAND Corporation.

Chan, J. B. L. (1997). *Changing Police Culture*. Melbourne: Cambridge University Press. http://dx.doi.org/10.1017/CBO9780511518195

Conklin, J. E. (2009). *Criminology* (10th ed.). Boston: Pearson.

Conser, J. A., Russell, G. D., Paynich, R., & Gingerich, T. E. (2005). *Law Enforcement in the United States* (2nd ed.). Sudbury, MA: Jones and Bartlett Publishers.

Cornall, R. (2005). Australia's Responses to Transnational Crime in the Region. *Public Administration Today, 4*(1), 61-65.

Cressey, D. R. (1997). The Functions and Structure of Criminal Syndicates. In P. J. Ryan & G. E. Rush (Ed.). *Understanding Organized Crime in Global Perspective* (pp. 3-15). London: Sage Publications.

Davies, S. (2007). JSB982 *Transnational Organised Crime: Statistics/Typologies of Transnational Organised Crime*. Queensland University of Technology.

Eck, J. E., & Rosenbaum, D. (1994). The new police order: Effectiveness, equity and efficiency in community policing. In D. Rosenbaum (Ed.). *The Challenge of Community*

Policing: Testing the Promises (pp. 3-26). Thousand Oaks, CA: Sage Publishing.

Electronic Frontier Australia. (2006). Telecommunications Interception & Access Laws. Retrieved April 14, 2009, from http://www.efa.org.au/Issues/Privacy/tia.html

Flood, B. (2004). Strategic aspects of the UK National Intelligence Model. In J. H. Ratcliffe (Ed.). *Strategic Thinking in Criminal Intelligence* (pp. 37-52). Sydney: The Federation Press.

Flood, B. and Gasper, R. (2009). Strategic aspects of the UK National Intelligence Model. In J. H. Ratcliffe (Ed.), *Strategic Thinking in Criminal Intelligence* (2nd ed., pp. 47-65). Sydney: The Federation Press.

Gibson, S. (2004). Open Source Intelligence: An Intelligence Lifeline. *Royal United Services Institute Journal, 149*(1), 16-22.

Glenn, J. C., Gordon, T. J., & Florescu, E. (2008). *2008 State of Future*. Washington DC: World Federation of UN Associations.

Goldstein, H. (1987). Toward Community-Oriented Policing: Potential, basic requirements and threshold questions. *Crime and Delinquency, 33*(1), 6-30. http://dx.doi.org/10.1177/0011128787033001002

Goldstein, H. (1990). *Problem Oriented Policing*. Ohio: McGraw-Hill.

Grabosky, P., & Smith, R. (1998). *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. Sydney: The Federation Press.

Grabosky, P., & Smith, R. (1999). Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities. *The FBI Law Enforcement Bulletin*, July.

Grennan, S., & Britz, M. T. (2006). *Organized Crime: A Worldwide Perspective Upper Saddle River*. NJ: Pearson Prentice Hall.

Heldon, C. (2009). Exploratory Analysis Tools. In J. H. Ratcliffe (Ed.), *Strategic Thinking in Criminal Intelligence* (2nd ed., pp. 124-146). Sydney: The Federation Press.

Hughes, A. (1999). Liaison Officers play a major role in Australia's fight against transnational crime. *AFP News, 86*(1), 10-12.

Irwin, M. P. (2001). Policing Organised Crime. In *4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses*. Canberra: Australian Institute of Criminology.

Jackson, B. A., Chalk, P., Cragin, R. K., Newsome, B., Parachini, J. V., Rosenau, W., … Temple, M. (2007), *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*. Santa Monica: RAND Corporation.

John, T., & Maguire, M. (2003). Rolling Out the National Intelligence Model: Key Challenges. In T. Newburn, T. Williamson & A. Wright (Ed.) *Crime Reduction and Problem-Oriented Policing* (pp. 38-68). Cullompton: Willan Publishing.

Lowenthal, M. (2009). *Intelligence: From Secrets to Policy* (4th ed.). Washington DC.: CQ Press, in in Confrontation or Collaboration: Congress and the Intelligence Community, Belfer Centre, Harvard Kennedy School of Government, 2009, pp. 4-5.

Lyman, M. D., & Potter, G. W. (2007). *Organized Crime* (4th ed.). New Jersey: Pearson Prentice Hall.

Malkin, S. (2007). *Social Networks of Organized Crime: Towards a Communication Approach*. Proceedings of the National Communication Association 93rd Annual Convention, November 15: Chicago.

Manning, P. K. (2005). Problem Solving? *Criminology and Public Policy*, 4(2), 149-154. http://dx.doi.org/10.1111/j.1745-9133.2005.00012.x

Mercado, S. C. (2004). Sailing the sea of OSINT in the information age: a venerable source in a new era. *Studies in Intelligence, 48*(3). Retrieved February 22, 2010, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html

Ratcliffe, J. H. (2002). Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice. *Policing and Society, 12*(1), 53-66. http://dx.doi.org/10.1080/10439460290006673

Ratcliffe, J. H. (2008a). Intelligence-Led Policing. In R. W. Wortley & L. Mazerolle (Ed.). *Environmental Criminology and Crime Analysis* (pp. 263-282). Cullompton, Devon: Willan Publishing.

Ratcliffe, J. H. (2008b). *Intelligence-Led Policing*. Cullompton, Devon: Willan Publishing.

Richelson, J. T. (1999). *The U.S. Intelligence Community* (4th ed.). Colorado: Westview Press.

Risen, J., & Lichtblau, E. (2005) Bush Lets US Spy on Callers Without Courts, New York Times, 16 December 2005, in Confrontation or Collaboration: Congress and the Intelligence Community, Belfer Centre, Harvard Kennedy School of Government, 2009 (pp. 2-3).

Robertson, S. (1997). Intelligence-Led Policing: A European Union View. In A. Smith (Ed.). *Intelligence-Led Policing - International Perspectives on Policing within the 21st Century* (pp. 21-23). New Jersey: International Association of Law Enforcement Intelligence Analysts Inc.

Scott, M. S. (2000). *Problem-Oriented Policing: Reflections on the First 20 Years*. Washington DC: COPS Office.

Shelley, L. I. (2002). The nexus of organised international criminals and terrorism. *International Annals of Criminology*. Retrieved February 28, 2010, from http://pagesperso-orange.fr/societe.internationale.de.criminologie/pdf/Intervention%20Shelley.pdf

Starey, T. (2005). Getting the Message - A Comparative Analysis of Laws Regulating Law Enforcement Agencies' access to stored communications in Australia and the US. *Media and*

Arts Law Review, 10(1), 23-55.

Stohl, M. (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law and Social Change, 46*, 223-238. http://dx.doi.org/10.1007/s10611-007-9061-9

Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage Publications.

Telecommunications (Interception) Amendment Act Cth. (2006). Australia.

Umphress, D. A. (2005). Diving the digital dumpster: the impact of the Internet on collecting open-source intelligence. *Air and Space Power Journal,* 82-91.

United Nations. (2000). *United Nations Covenant against Transnational Organised Crime*. Geneva: United Nations General Assembly.

United Nations. (2002). *Results of a Pilot Survey of Forty Selected Organized Criminal Groups in Sixteen Countries*. Geneva: United Nations Office on Drugs and Crime.

United Nations Office of Drugs and Crime. (2008). *World Drug Report*. United Nations Office of Drugs and Crime.

Wardlaw, G. and Boughton, J. (2006). Intelligence-Led Policing: The AFP Approach. In J. Fleming & J. Wood (Ed.). *Fighting Crime Together: The Challenges of Policing and Security Networks* (pp. 133-149). Sydney: University of New South Wales Press.

Waters, G., Ball, D., & Dudgeon, I. (2008). A*ustralia and Cyber-Warfare, Canberra Papers on Strategy and Defence* (pp. 168). Canberra: Australian National University E Press.

Weisburd, D., & Eck, J. E. (2004). What Can Police Do to Reduce Crime, Disorder, and Fear? *The Annals of the American Academy of Political and Social Science, 593*(1), 42-65. http://dx.doi.org/10.1177/0002716203262548

Weisburd, D., Mastrofski, S., McNally, A. M., Greenspan, R., & Willis, J. (2003). Reforming to preserve: COMPSTAT and strategic problem-solving in American policing. *Criminology and Public Policy, 2*(3), 421-456. http://dx.doi.org/10.1111/j.1745-9133.2003.tb00006.x

Williams, E. S. (1980). *Australian Royal Commission of Inquiry into Drugs*. Canberra: Royal Commission.

Williams, P. (2001). Transnational Criminal Networks. In J. Arquilla & D. Ronfeldt (Ed.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 61-97). Santa Monica, CA: Rand Corporation.