Intelligence-Led Policing (ILP) as A Strategic Planning Resource in the Fight against Transnational Organized Crime (TOC)

Dr. Peter Bell & Mitchell Congram

Faculty of Law,

School of Justice,

Queensland University of Technology

Phone: 617 3138 7105

Email: p6.bell@qut.edu.au

Abstract

With the advent of modern communication technologies and the global expansion of criminal enterprises across national and international borders, law enforcement agencies (LEAs) can no longer operate in an environment focused solely on addressing localised and 'minor' crime. The nature, complexity and volume of criminal challenges now faced by LEAs require a fundamental shift in their methodologies and approaches (Ratcliffe, 2003; 2008a; 2008b;Ratcliffe & Sheptycki, 2009)—one which recognises the importance of the use of intelligence not just as an evidentiary gathering tool but as a strategic planning resource, providing vital guidance for the deployment of enforcement strategies and resources. In the fight against transnational organized crime, where the communication between criminals and network associates presents itself as a key vulnerability, the ability of law enforcement agencies to utilise intelligence gathering tools such as communication interception technology is paramount. This paper explores the application of intelligence-led policing (ILP) as a strategic planning resource in the fight against transnational organized crime. It argues that through theimplementation of an intelligence-led policing model, law enforcement agencies can fully exploit the availability of tools such as communication interception technology. To do this, it considers the structure of transnational criminal enterprises and their vulnerability through communication, the role of intelligence-led policing, the limitations posed by legislative and operational restrictions placed on intelligence gathering and the need for a cultural shift in attitude towards the collection, analysis and use of intelligence. The paper contends that through an intelligence-led framework, law enforcement agencies will be able to capitalise on the use of intelligence to cause maximum disruption to criminal activities, for without it they will be unable to combat the growth of transnational organized crime.

Keywords: *intelligence, intelligence-led policing, communication interception technology, law enforcement agencies, transnational organized crime*

1. Introduction

The globalization and growth of transnational organized crime (TOC) is a cause for concern amongst society. Researching TOC and entrepreneurial criminals is an essential endeavour, as the expansion of

technology, dismantling of borders and connections across the globe means that all nations have the potential to be negatively impacted by TOC. Of all the policing methodologies available, intelligence-led policing (ILP) is uniquely positioned to effectively combat TOC

This study fills an important gap in the modern policing management theory by examining how TOC enterprises are structured, how they communicate and how this communication becomes a vulnerability that can be exploited by law enforcement agencies (LEAs) that adopt an ILP methodology. However, it also uncovers how the fight against TOC can be, or is currently, restricted by legislation, policing culture and privacy concerns. This study is important as the findings of the research can be used as a basis for more specific studies that examine exactly how intelligence-led policing and the subsequent use of intelligence as a strategic decision-making tool can be implemented appropriately into the law enforcement community.

1.1 Understanding TOC

To understand the role of ILP in the fight against TOC, it is first important to examine how TOC enterprises are structured, how they communicate and how this is a vulnerability that can be exploited by LEAs.

Whilst TOC can be viewed as a broad spectrum of activity, LEAs note a range of specific 'organized' activities. There has been substantial disagreement over the ability to succinctly define such an adaptable assortment of crimes and groups. Conklin (2009, p. 73) shares similar definitional notions of rules and codes and organisational characteristics put forward by Abadinsky (1994, 2007), and Grennan and Britz (2006, p. 12), and as such his definition is used within this study:

> 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)

1.2 Structure of TOC Groups

In line with Conklin's (2009, p. 73) notion of the criminal's self preservation, 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 organization". It is this complexity and sophistication of crime groups that impacts on policing, and further supports the need for specialized operations and international cooperation to address the full dimensions of international criminal organizations (Shelley 1998, p. 79). Understanding the structure of criminal groups is integral to the development and recognition of potential weaknesses.

Research by the United Nations (2002) of 40 organized crime groups in 16 countries led to the development of five organizational structures for TOC groups. These included standard hierarchy; regional hierarchy; clustered hierarchy; core group; and criminal network(United Nations 2002). While Lyman and Potter (2007) note that not all TOC groups fit specifically within these five structures it is argued that the basic typologies provide an important understanding of how organizations can vary in

structure, highlight difficulties that can be had in disrupting organizations using core group or criminal network typologies (Malkin 2007).

Of the five structure, core groups and criminal networks are the "fluid, dynamic and loosely structured networks" described by Cressey(1997, p. 3) and Williams (2001, p. 70). 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, used to carry out business (see Figure 1). The group exists solely for the profit motivation and will shift business activities to generate the greatest profit. This structure is argued as one of the most readily emerging forms of organized 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 (Lyman & Potter, 2007, pp. 13-14; United Nations, 2002, pp. 39-41).

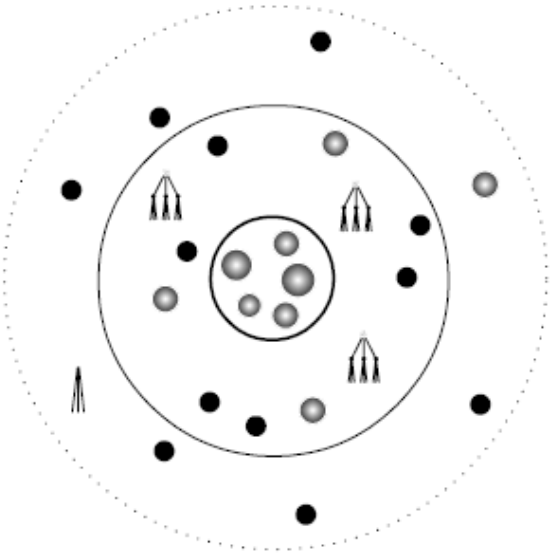

Figure 1 - Core Group (United Nations, 2002, p. 39)

The criminal network is the clearest example of the globalization of TOC(Cressey, 1997; Malkin, 2007). Criminal networks are the loosely organized, highly adaptable, fluid networks of individuals that engage themselves in illicit activities with regularly shifting alliances (Lyman & Potter 2007, p. 14; United Nations, 2002, p. 41; Cressey, 1997, p. 3; Williams, 2001, p.70) (see Figure 2). The networks are created and re-formed in line with continuing criminal projects. The lack of predefined identity and maintained structure ensures difficultly for LEAs to infiltrate or dismantle the network. While key individuals exist their association with each other is usually distanced, ensuring that even if LEAs successfully target and prosecute one key individual the network will still remain connected and operational(United Nations, 2002, pp. 41-43; Lyman & Potter 2007, pp. 14-15). Lyman and Porter (2007) identify that this form of criminal network is emerging as the new forefront of TOC structures.

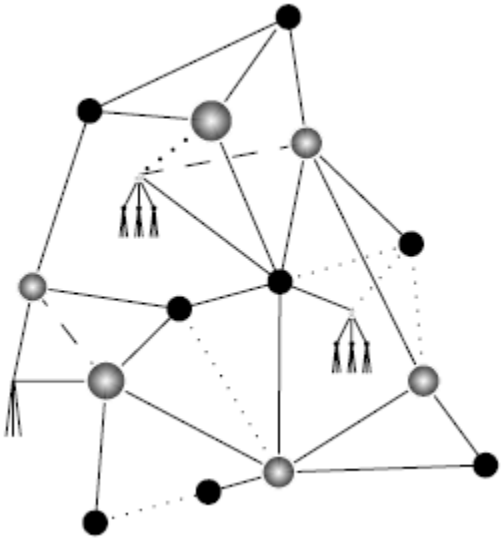

Figure 2 - Criminal Network (United Nations 2002, 41)

1.3 Vulnerabilities of TOC

Although there is minimal research on the weaknesses and vulnerabilities of TOC groups with current literature focusing on the vulnerabilities of victims, through an understanding of the structure of criminal enterprises it is possible to identify a core vulnerability that will only intensify as groups expand their areas of operation over greater distances and move towards more unstructured networks (Malkin, 2007)—the need to communicate quickly, easily and effectively (Grabosky & Smith, 1998).

Criminals require instantaneous communication capabilities that span the globe amongst their networks of contacts and 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 categorized into four basic methods: coordinating and planning criminal activities; marketing and distribution of illicit services or products; sustaining the organizational structure; and used to obstruct 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.

Grabosky and Smith (1998) note a variety of communication strategies used by various criminal enterprises through the brief review of law enforcement operations and case studies, these include: UHF radios, video phones, scrambling devices for internet connections and pagers. However, since Grabosky and Smith's work, 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 identified through enforcement operations to utilize mobile phones that are programmed to send or receive from specific phone numbers only, reducing the identification and thus interception of a phone by law enforcement and are known to exploit the easy availability and poor identity checks of prepaid SIM (Subscriber Identity Module) cards for mobile phones, along with access to cheap handsets. This allows them to frequently change both SIM and phone and again reduce the

chances of detection, interception and limit their links to other criminal counterparts (Waters, Ball & Dudgeon, 2008; Jackson et al., 2007). Through the use of the internet, criminals have access to a growing multitude of free and temporary email accounts that require no identification and can allow messages to be transmitted with relative anonymity (Waters, Ball and Dudgeon, 2008). The growing availability of encryption devices also allow criminals to encode whole messages, or encode messages within a particular attachment such as an image, document or link(Bakier, 2007). Known as steganography, this is designed to ensure the message content itself can appear otherwise innocent if intercepted.

2. Role of ILP in the Fight against TOC

Whilst crime groups are vulnerable to detection and disruption because of their communications, LEAs need a method and framework that allows them to combat these crimes efficiently and successfully. Ratcliffe (2008a, 2008b) and Weisburd and Eck (2004) contend that the primary methodologies of LEAs can be broken into five models traditional policing, community-orientated policing, problem-orientated policing, computer statistics and intelligence-led policing. While each of these five models have their own differing concepts of strategic goals and possess their own strengths and weaknesses, a common factor and subsequently a negative consequence presented in the first four methodologies is their specific focus only on the local area. Rapid and significant changes on a global scale have changed the criminal environment as such these methodologies fail to possess the qualities required to address the more serious threat of TOC. As such ILP is the only method uniquely positioned to effectively combat TOC.

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).

Flood and Gasper (2009, p. 57) note that the primary difficulty 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 allows the development of a clearer understanding of what once appeared complex and haphazard to reveal 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. As such ILP characterizes itself as the most suitable methodology for combating TOC(Flood & Gasper, 2009, p. 57).

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. Among the literature there is a clear acknowledgement regarding 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 (Ratcliffe, 2002; 2008a). This is in part due to the difficulty to effectively evaluate a business model, and as stated by Keelty(2004, p. 11), the impact of intelligence is “notoriously difficult to measure”. Within Australia, the use and slow integration of ILP has been used with limited, and in some cases, flawed evaluation of its effectiveness.

2.1 Managing our Knowledge of CIT, TOC and ILP

In line with the development and growth of communication technology and its subsequent use by TOC, there has been an increasing requirement for the use of communication interception technologies by LEAs. However, there is an obvious disconnect in the literature between the use of CIT and ILP as a whole. Gaps also exist in the discussion of intelligence collection and knowledge management in this area.

2.2. Defining CIT

As is the case in Australia, for example, 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 and concerns the fact the recipient instantly receives the message being communicated in 'real time' (Starey, 2005; Ahmed, 2007). *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. As a result, Starey (2005) and Ahmed (2007) argue that this information can be intercepted prior to the intended recipient actually receiving the message.

2.3 Signals Intelligence

Signals intelligence (SIGNIT), while used predominantly in military settings has seen a slow expansion into criminal groups. Communication Intelligence (COMINT) and Electronics Intelligence (ELINT) form the majority of CIT relevant to law enforcement. COMINT, the interception of signals between people, broadly corresponds to live communications such as telephone calls and ELINT, the interception of signals between machines, corresponds to stored communication mediums such as email or SMS. In Australia the intelligence collection and analysis within the Australian Intelligence Community (AIC) is largely undertaken by the Australian Defence Signals Directorate (DSD) in a national security oriented position, rather than a crime-fighting agency.

2.4 Open Source Intelligence

Another form of intelligence gathering used in the fight against transnational crime is open source intelligence (OSINT). OSINT exists in addition to SIGINT and imagery intelligence (not discussed in this paper). 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.

3. Legal Responses to TOC within Australia

Over the past decade, Australia has introduced a variety of reforms to assist in the combat of TOC activities occurring on and off shore (Hughes, 1999, p. 10). 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). Legislative changes introduced since 2001 have introduced definitions and offences for transnational criminal activities based off the UN Convention against TOCand further assisted in combating 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 of 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 and 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 oflaw enforcement and intelligence agencies.

In Australia this has included the creation of the Australian Crime Commission, National Threat Assessment Centre and Transnational Crime Coordination Centre, along with the identification of 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. In addition to the policy responses, operational responses have been important in the fight against TOC. The extent of international deployment and operations occurring through the AFP has enhanced not only intelligence gathering, but also diplomatic ties between nations, namely Indonesia, Papua New Guinea and those in the Pacific Islands. However, Glenn, Gordon and Florescu (2008) argue that whilst Australia has instigated significant changes to recognize the growth of TOC, where 'transnational' underscores organized crime, the need for a comprehensive, integrated global counter-strategy is required, and consequently, the response of a single nation is less than effective.

3.1 Moving towards an Intelligence-led Model

The comparative analysis of the documents collated during the course of this research revealed two key themes that impact on the successful adoption of an ILP grounded model: intelligence direction and the ILP model. Analysis also identified that current limitations exist not only in terms of legislative restriction, but also in cultural attitudes towards the collection, analysis and use of intelligence.

3.2 Intelligence Direction

A theme consistent throughout the literature of communication interception relates to the concept revealing the requirement for policing agencies to move forward from the traditional role of reactive policing, or 'local' policing, to a more proactive manner that utilised intelligence as their foremost weapon in addressing the growth of TOC. Heldon(2009, p. 125) highlights that currently, policing agencies lack a clear understanding of the nature of the criminal enterprises in organized crime and terrorism that they are fighting and that the use of intelligence is an integral aspect for combating and identifying transnational crime. As such, its use must be strategic. It is important here to reiterate that intelligence is not information butvalue-added data which has an attached relevance and purpose, and has been subject to an organized analysis by an intelligence officer or analyst (Dean & Gottschalk, 2007b, p. 5).

This is further supported by Williams (1980) following the Australian Royal Commission of Inquiry into Drugs, who also promotes intelligence use by stating:

> "Intelligence is the most important single weapon in the armoury of law enforcement generally and of drug law enforcement in particular. Evidence received by this commission left no doubt that good intelligence is an essential prerequisite to effective law enforcement" (1980, p. 35).

This can reveal that even during the raft of Royal Commissions that occurred during the 1970s and 1980s into the Australian law enforcement and intelligence community, the concept of underpinning intelligence use as a primary strategic resource in law enforcement methodologies was integral to the growing sphere of organized and transnational crime. The specific use of terminology is also important in this statement. The terms 'good' and 'effective' emphasize that only information, data with clear relevance and purpose, subjected to analysis, not simply raw data misinterpreted as 'intelligence' (Ratcliffe, 2008b, p. 87; Oakensen, Mockford & Pascoe, 2002, p. 57) will ensure the efficacy of law enforcement activity.

Resultant from the demonstrated need to utilize intelligence in a manner that provides ultimate direction to policing objectives and targets, it is further recognized that the use of a methodological framework, which correctly controls and harnesses the use of intelligence is imperative. This is reinforced by Wardlaw and Boughton(2006, p. 142) who assert importance of intelligence and CIT as a vital component. In particular they state that intelligence must be placed at the centre of law enforcement doctrine, rather than simply used as a support tool for investigations. This is an important aspect as it identifies the current flaws in the system of many policing agencies, particularly in Australia.

4. Intelligence-led Policing (ILP) Model

In finding that the use of intelligence is an essential prerequisite for effective policing, the need to adopt an appropriate model or framework to manage intelligence is paramount. As found earlier, ILP is the only policing methodology that utilizes intelligence as a primary asset.

The business/philosophy model that employs crime intelligence to objectively direct decisions for police resourcing and targeting was also a frequent theme emerging in the documents. As an information-organization model, it is apparent that there is a focus on being proactive by nature. Through an increase in clarity of the issue at hand, responses can be tailored in an effective manner.

As with any form of competition or game, law enforcement is no different in that the ability to maintain a strategic advantage will ultimately increase their ability to 'play' effectively, which should aid their ability to disrupt and dissolve criminal enterprises. It is for these reasons that the espousal of ILP to manage the use of intelligence information is recognized as an appropriate model for policing within the 21st century as globalization continues to grow.

In his evaluation of ILP, Ratcliffe (2008a) identifies that within law enforcement the use of technologies such as CIT has been as an evidentiary gathering tool for reactive investigations. Whilst useful for prosecutions, as a manner of crime prevention, its efficacy is limited. Chalk and Rosenau(2004, p. 2) describe this form of intelligence collection as a reactive-proactive hybrid, and it is evident that the introduction of an intelligence-led framework would assist in the amelioration of this hybrid that currently confounds law enforcement intelligence. This again highlights the importance of the use of intelligence for strategic planning and decision making, whilst observing that in combination with these methods of information collection that analysis is essential for intelligence development.

It has been shown that the use of CIT in a proactive intelligence-led can play a vital role in the disruption and prevention of TOC. Through the grounding in an intelligence-led model, CIT can be used in an effective, strategic manner that takes LEAs into the future, rather than reacting to the past. The next section will discuss these findings and the limitations that exist on the adoption of an intelligence-led framework within an Australian context.

4.1 Limitations for Advancement

It is not surprising that the process of focusing policing tactics and the implementation of a proactive approach in which a majority of policing work is not observable by the public is seen as a threat to perceived civil liberties by some, irrespective of the accuracy of their perceptions (Ratcliffe 2008b, p. 220). As is noted by Innes (2004, p. 156), these changes in policing methodology have been seen to increase the gap between those who are policing, and those who are being policed. Subsequently, this apprehension of society and advocates alike regarding the issue of privacy must be addressed. Bronitt and

Stellios(2005; 2006) raise concerns regarding the legislative framework that governs CIT within Australia, arguing that the model of 'balancing' law enforcement and privacy is fatally flawed. Similar views are held by privacy advocate groups such as Electronic Frontier Australia (EFA)(2006), who argue that greater restrictions should be imposed on the use of CIT and privacy should be placed at the forefront of all decision making. Even though Australia's legal protections for privacy rights is limited, protection is still afforded under Article 17 of the International Covenant on Civil and Political Rights and Article 12 of the Universal Declaration of Human Rights.Regardless of this it would be illogical to make recommendations that ignore privacy on a whole.

The concept of placing privacy 'up front' is clearly an important aspect to note. Whilst it is understandable for apparent reasons of operational security that transparent intelligence collection is unrealistic, options for building public trust and acceptance exist. Limiting unnecessary discretion and guiding necessary discretion within the decision making process, introducing tests of proportionality and/or the use of an independent oversight role, such as Queensland's Public Interest Monitor, reinforce the notion of civil liberties as the highest priority, whilst still ensuring the intelligence-led methodology can continue.

4.2 Intelligence and Culture

As shown in the findings, for the most effective law enforcement practice, intelligence must be placed at the centre of the organization's ethos. There is an identified need to ensure that it is evident throughout an organisation that intelligence is analysed information. This recognition needs to be supported by a cultural shift promoting the importance of support staff, such as crime intelligence officers and analysts, to centre stage. As noted by the work by Heldon(2009), Dean and Gottschalk (2007b), Ratcliffe(2002;2008a;2008b; 2008c), Oakensen, Mockford and Pascoe (2002) and Osborne (2006) , for true ILP to be implemented, a methodology that relies on high-quality analysis, there would be a need to introduce education and training to all personnel, so that a greater understanding of intelligence reports provides an appropriate decision-making regime. Ratcliffe and Sheptycki(2009, p. 249) note that at current, intelligence officers and analysts often see few results from their work. This goes further with Ratcliffe(2003,p. 4; 2008b, p. 158) noting that whilst seemingly melodramatic, it would be impossible to identify the number of intelligence failures that have occurred across the world as a result of decision-makers failing to identify the importance of an intelligence product, or an agency or analyst failing to convince their clients of its importance.

Intelligence sharing is also a key aspect of not just ILP, but of the combat of organized crime on a transnational scale. Agencies both domestically and internationally need to shift from the model of informal networks to a more defined arena that promotes effective intelligence sharing (Dean & Gottschalk, 2007a; Bhaskar & Zhang, 2007; Ratcliffe, 2008b).

This extends through both law enforcement and security agencies. With TOC shifting and consorting in manners that pose threats to both crime control and national security, it is no surprise that intelligence overlaps occur. With dissemination forming the final stage of the intelligence cycle (dependent on the model used, here referring to direction, collection, collation, analysis, dissemination) it is vital that there is a shift out of the reinforced cultural stigma that underpins hording of information and refusal to volunteer intelligence for fear of losing their status of 'importance', which can be felt integral to continued funding (Bamford 2009). The efficacy of a new intelligence-led model is greatly reduced without the transformation out of a competitive mindset. In line with the continued privacy concerns, it is

also essential to ensure that appropriate privacy policies are in place for intelligence sharing systems. For only the slightest hint of a violation of rights and privacy of individuals will quickly see intelligence sharing, and in part, effective transnational policing, succumb to a significant setback (Department of Justice, 2005, p. 49; Ratcliffe, 2008b, p. 222).

5. Conclusion

This paper has explored the importance of an ILP as a strategic resource in the fight against TOC. In particular it has identified that a proactive environment, addressed through the adoption of the ILP methodology, will ensure that tools such as CIT can be utilized as effective weapons against TOC.

The study has discussed the gaps in current literature by providing an examination of the structure of TOC groups, how they communicate and how LEAs can effectively combat a key weakness by operating with an ILP framework. It moves beyond the criticisms and concerns that underpin the majority of CIT research regarding privacy and has sought to address these issues in part with an intelligence-led model. Furthermore, this study has offered a perspective that can help drive future research.

In particular, it is suggested that future research should allow law enforcement investigators and analysts to contribute their own opinions and experiences, such as their attitudes surrounding the switch in focus from reactive to proactive policing, thereby supporting the philosophy of knowledge-managed policing. This can be balanced with a closer examination of case studies from both law enforcement and intelligence agencies.

The application of this theoretical framework can also be aided by assessing its applicability to the Australian law enforcement environment. By assessing the similarities and differences in culture and dynamics experienced in international examples such as the UK's National Intelligence Model and the employment of ILP by the United States' New Jersey State Police there is an ability to 'learn from mistakes' and introduce an effective framework.

A third area importance, also noted by Malkin(2007) and Grabosky and Smith (1998; 1999), is the communicative methods, strategies and structures of TOC groups, and the 'what', 'where', 'when', 'how' and, to a limited extent, 'why', of criminal communication. Whilst the use of intelligence is seemingly essential, without a strong foundational knowledge of how tools such as CIT should be targeted and deployed, there will continue to be limits on the production of high quality intelligence.

This paper has employed a systematic methodology of document analysis studying the role of ILP as a strategic resource in combating TOC. It focuses on a proactive intelligence-led framework that can both be beneficial to law enforcement in their crime fighting agenda, whilst ensuring a balance of proportionality remains to satisfy the concerns of privacy advocates and legislation.

References

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

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

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

Bamford, J. (May 19, 2009). *The Spy Factory*[Television broadcast].Australia: SBS.

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

Bronitt, S. and Stellios, J. (2005). Telecommunications Interception in Australia: Recent trends and regulatory prospects. *Telecommunications Policy*, 29(11), 875-888.

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.

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

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

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

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 and G. E. Rush (Ed.). *Understanding Organized Crime in Global Perspective*.(pp. 3-15). London: Sage Publications.

Dean, G. andGottschalk, P. (2007a). *Knowledge Management in Policing and Law Enforcement*. Oxford: Oxford University Press.

Dean, G. and Gottschalk, P. (2007b). *Knowledge Management in Policing and Law Enforcement: Foundations, Structures, Applications.* Oxford: Oxford University Press.

Department of Justice. (2005). *Fusion Centre Guidelines*. Washington DC: Department of Justice.

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

Flood, B. and Gasper, R. (2009). Strategic aspects of the UK National Intelligence Model. In 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.and Florescu,E. (2008). *2008 State of Future*. Washington DC: World Federation of UN Associations.

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

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

Grennan, S. and 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.

Innes, M. (2004). Reinvesting Tradition? Reassurance, Neighbourhood Security and Policing. *Criminal Justice*, 4(2), 151-171.

Irwin, M. P. (2001). Policing Organized 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., Simpson, E. M., Sisson, M. and Temple, M. (2007). Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies. Santa Monica: RAND Corporation.

Keelty, M. (2004). Can Intelligence Always be Right? In *13th Annual Conference of the Australian Institute of Professional Intelligence Officers*. Melbourne: AIPIO.

Lyman, M. D. and 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.

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

Oakensen, D., Mockford, R. and Pascoe, C. (2002). Does There Have to be Blood on the Carpet? Integrating Partnership, Problem-Solving and the National Intelligence Model in Strategic and Tactical Police Decision-Making Processes. *Police Research and Management*, 5(4), 51-62.

Osborne, D. (2006). *Out of Bounds: Innovation and Change in Law Enforcement Intelligence Analysis*. Washington DC: Joint Military Intelligence College.

Ratcliffe, J. H. (2002). Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice. *Policing and Society*, 12(1), 53-66.

Ratcliffe, J. H. (2003). Intelligence-Led Policing. *Trends and Issues in Crime and Criminal Justice*, 248.

Ratcliffe, J. H. (2008a). Intelligence-Led Policing. InR. W. Wortley and 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.

Ratcliffe, J. H. (2008c). Knowledge management challenges in the development of intelligence-led policing. In T. Williamson (Ed.). *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions*(pp. 205-220). Chichester: John Wiley and Sons.

Ratcliffe, J. H. and Sheptycki,J. (2009). Setting the Strategic Agenda. In J. H. Ratcliffe (Ed.). *Strategic Thinking in Criminal Intelligence*, 2nd ed, (pp. 248-268). Sydney: The Federation Press.

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

Smith, R. (1997). *Controlling the Interception of Communications: Law or Technology?* Proceedings of the Communications Research Forum: Canberra.

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.

Strauss, A. and 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.* Winter, 82-91.

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.

Wardlaw, G. and Boughton, J. (2006). Intelligence-Led Policing: The AFP Approach. In J. Fleming and 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. and Dudgeon, I. (2008). A*ustralia and Cyber-Warfare, Canberra Papers on Strategy and Defence*(pp. 168). Canberra: Australian National University E Press.

Weisburd, D. and 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.

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

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