
Journal of Policing, Intelligence and Counter Terrorism
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rpic20

# Laying the Groundwork for the Successful Deployment of Communication Interception Technology (CIT) in Modern Policing

Mitchell Congram [a] & Peter Bell [b]

[a] Faculty of Law, School of Justice, Queensland University of Technology

[b] Faculty of Law, School of Justice, Queensland University of Technology

Published online: 03 Aug 2011.

To cite this article: Mitchell Congram & Peter Bell (2010) Laying the Groundwork for the Successful Deployment of Communication Interception Technology (CIT) in Modern Policing, Journal of Policing, Intelligence and Counter Terrorism, 5:1, 9-27, DOI: 10.1080/18335300.2010.9686938

To link to this article: http://dx.doi.org/10.1080/18335300.2010.9686938

# Laying the Groundwork for the Successful Deployment of Communication Interception Technology (CIT) in Modern Policing

MITCHELL CONGRAM

Faculty of Law, School of Justice, Queensland University of Technology

PETER BELL

Faculty of Law, School of Justice, Queensland University of Technology

## ABSTRACT

With the growth and development of communication technology there is an increasing need for the use of interception technologies in modern policing. Law enforcement agencies are faced with increasingly sophisticated and complex criminal networks that utilise modern communication technology as a basis for their criminal success. In particular, transnational organised crime (TOC) is a diverse and complicated arena, costing global society in excess of $3 trillion annually, a figure that continues to grow (Borger, 2007) as crime groups take advantage of disappearing borders and greater profit markets. However, whilst communication can be a critical success factor for criminal enterprise it is also a key vulnerability. It is this vulnerability that the use of CIT, such as phone taps or email interception, can exploit. As such, law enforcement agencies now need a method and framework that allows them to utilise CIT to combat these crimes efficiently and successfully. This paper provides a review of current literature with the specific purpose of considering the effectiveness of CIT in the fight against TOC and the groundwork that must be laid in order for it to be fully exploited. In doing so, it fills an important gap in current research, focusing on the practical implementation of CIT as opposed to the traditional area of privacy concerns that arise with intrusive methods of investigation. The findings support the notion that CIT is an essential intelligence gathering tool that has a strong place within the modern policing arena. It identifies that the most effective use of CIT is grounded within a proactive, intelligence-led framework

and concludes that in order for this to happen Australian authorities and law enforcement agencies must re-evaluate and address the current legislative and operational constraints placed on the use of CIT and the culture that surrounds intelligence in policing.

## Introduction

While an assortment of literature exists on communication interception technology (CIT) and transnational organised crime (TOC), the two bodies of knowledge rarely intersect to examine the effective and practical use that CIT can have against TOC. However, as evident in current literature, with the consistent development of communication technology and its subsequent use by criminal enterprises to advance their own illicit goals, there is a growing need to understand how CIT can be used effectively by law enforcement agencies (LEAs) to cause maximum disruption to criminal activities.

In reviewing and analysing the available literature, this paper seeks to create a better understanding of how CIT can be effective in modern policing and identify what direction needs to be taken in order to fully utilise this powerful tool in the fight against TOC. To do this it considers the structure and vulnerabilities of TOC groups, issues and concerns surrounding the practical implementation of CIT and the model of best practice for its use – namely the intelligence-led policing methodology. In doing so, it is hoped that this paper will provide law enforcement professionals and authorities with an integrated picture of the use of CIT within a modern policing context in the fight against TOC.

## Understanding TOC

In order to understand how CIT can be used as an effective weapon in this arena and identify the grounding needed for its effective deployment against TOC, it is first important to understand the nature, structure and vulnerability of TOC that lead to its appropriateness in this context.

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. These include 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; Davies, 2007; Lyman & Potter, 2007; Borger, 2007; Australian Crime Commission, 2009; Abadinsky, 2009).

The structure of organised crime networks, domestic or transnational, have long since been viewed as highly organised hierarchical structures, however research shows that 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". It is this complexity and sophistication of crime groups that impacts on policing and further supports the need for specialised operations and international cooperation to address the full dimensions of international criminal organisations (Shelley, 1998, p. 79).

## Vulnerabilities of TOC

A review of the current research shows there is limited research on the vulnerabilities of TOC, with literature focusing predominantly on the vulnerabilities of victims. However, 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) – in one of which CIT has the capacity to be a significant weapon: communication.

The need to communicate quickly, easily and effectively is a basic requirement for any business operating across large distances, either domestically or internationally. As such, for criminal enterprises – businesses unto themselves, albeit illegitimate ones, – the need to communicate their activities is just as important (Grabosky & Smith, 1998). Through the identification of contact and communication points by LEAs, vital information can be acquired and subsequent intelligence developed to facilitate operational response strategies.

Research shows that criminal enterprises currently use a range of communication methods and strategies aimed at reducing detection and interception by LEAs. These include utilising mobile phones programmed to send or receive from specific phone numbers; exploiting the easy availability and poor identity checks of prepaid mobile phone SIM (Subscriber Identity Module) cards along with access to cheap handsets; accessing free and temporary email accounts that require no identification and allow messages to be transmitted with relative anonymity; and utilising encryption devices to either encode whole messages, or messages within a particular attachment such as an image, document or link (Bakier, 2007; Jackson *et al*, 2007; Waters, Ball & Dudgeon, 2008).

Criminals require instantaneous communication that spans the globe amongst their networks of contacts – their suppliers, conspirators and other members of the network. However, the very sophistication and complexity that dictates their business activities also makes it highly susceptible to high quality intelligence attack by tools such as CIT.

## Defining CIT

In line with the development and growth of communication technology – and its exploitation by TOC groups – there is 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 [EFA], 2006). The decision to develop and use the term 'communication interception technology' (CIT) is as a result of the preconceived notions attached to the definition of 'telecommunications' which can be seen to represent solely traditional telecommunication methods such as telephone calls. Conversely, the use of the term CIT can be said to imply a broader scope for all forms and methods of communication and subsequently is used to reference the interception methods and related technology. Interception can occur with both stored and live communication. The distinction being that live communications concern messages communicated in "real time" (Starey, 2005; Ahmed, 2007) and stored communications which cover communication that is stored – albeit at the very least for an instant – on one or more pieces of equipment belonging to a service provider or carrier before being retrieved by a recipient (Starey, 2005; Ahmed, 2007).

### SIGNALS INTELLIGENCE

Signals intelligence (SIGINT) has a long history of use by military forces around the world. Richelson (1999, p. 167) claims that traditionally, signals intelligence is considered one of the most important and sensitive forms of intelligence providing a vast amount of information. Whilst traditionally signals intercepted and analysed were from 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. 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.

### 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, 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). 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 essence, OSINT is intended as one thread in a complex web of intelligence sources.

## Issues surrounding CIT

Whilst SIGINT and OSINT have been used extensively and effectively in military environments, CIT continues to remain severely limited in its use. In much of the literature, two primary issues arise surrounding the use of CIT: legislation (governing usage) and privacy. Whilst seemingly separate, these issues are directly correlated. The concerns regarding the infringement of privacy rights have subsequently influenced the controls and limitations placed on the use of CIT within the legislation. In particular, despite the increasing use of communication technologies by TOCs, under current legislation CIT can still only be used once all other avenues of inquiry have been investigated. These include OSINT, surveillance resources, interrogation, interviews of witnesses, deployment of undercover operatives and collection of physical evidence. In addition, despite the coverage of both privacy and legislative issues, there is a distinct lack of research that examines both these issues in context of the practice application of CIT.

### LEGAL RESPONSES TO CIT WITHIN AUSTRALIA

The work of Starey (2005) analyses the legal framework that CIT operates under in Australia making comparisons with applicable United States' (US) legislation. She argues that whilst Australia cannot directly adopt the same legislation applied in the US, we should be able to 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 Telecommunications (Interception and

Access) Act 1979 (TIA Act), live communication interception warrants may only be issued for serious offences (matters of national security or offences punishable by a maximum period of at least seven years imprisonment), must be accompanied by strong evidence to support reasonable grounds for the suspects involvement, must take into regard the level of privacy to be interfered with, how useful the intercept will be and what other investigative methods have been used (Starey, 2005; EFA, 2006). Further, interception warrants can only be authorised by select Federal Judges or Administrative Appeals Tribunal members to authorised LEAs (Starey, 2005; EFA, 2006). Starey (2005) demonstrates that the current legislation caters for CIT only as a last resort and as an evidence gathering tool, rather than a forefront intelligence collection method. Stored communications however, are significantly easier to access under the Amendment Act in which requirements are for either serious offences or serious contraventions (penalty of at least maximum three years imprisonment), may be issued to all enforcement agencies, including criminal law, civil penalty and public revenue agencies and can be issued by any Commonwealth, State or Territory Judge or Magistrate.

## PRIVACY RESPONSES TO CIT WITHIN AUSTRALIA

The main issues surrounding privacy and the use of CIT as identified in current literature include the sole focus on the right to privacy by advocacy groups, the call for a regulatory model advocating human rights and due process as central components and concerns surrounding the increased use of CIT by states and territories as opposed to the traditional use only by federal agencies.

As argued by privacy advocate Electronic Frontier Australia (EFA) (2006), the legal responses seemingly position stored communications as a "less important" communicative method, despite its increased adoption and preference 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 does still provide 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 outweigh the cost of individual privacy. It is here that EFA (2006) lacks the ability to recognise the careful balance of proportionality between privacy and enforcement. As power shifts in favour of increased privacy, it greatly limits vital enforcement technique and technology. Sir Robert Megarry VC explains in the case of *Malone v Metropolitan Police Commissioner* (1979), Ch 344 at 377D;

> "One has to approach these matters with some measure of balance and common sense. The rights and liberties of a telephone subscriber are indeed important; but so also are the desires of the great bulk of the population not to be the victims of assault, theft or other crimes. The detection and prosecution of criminals, and the discovery of project crimes, are important

> weapons in protecting the public ... The question is not whether there is certainty that the conversation tapped will be iniquitous, but whether there is just cause or excuse for the tapping and for the use made of the material obtained by tapping".

EFA's (2006) sentiments 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". Bronitt and Stellios (2005; 2006) also 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 organised and transnational criminals do not limit themselves 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; Ratcliffe, 2008b; Flood & Gasper, 2009).

## POLICY RESPONSES TO TOC WITHIN AUSTRALIA

In addition to the legal and privacy responses surrounding CIT, 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. Consequently, 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, pp. 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 occurring within Australian borders. These legislative measures have not only introduced definitions and offences for transnational criminal activities, based off the UN Convention against TOC, but further assist in 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 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 & 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. 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.

### OPERATIONAL RESPONSES TO TOC WITHIN AUSTRALIA

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. This is achieved through the construction of trust based relationships through assistance provided by Federal Agents and Diplomats (Cornall, 2005, p. 62). 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, and consequently, the response of a single nation is less than effective.

As illustrated, TOC and CIT are diverse and complicated arenas. While legal and operational responses can assist LEAs in combating transnational crime, they also need a method and framework that allows them to effectively utilise technology to identify and intercept criminal communications to cause maximum disruption.

## Intelligence-led policing and CIT

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 (COP), problem-orientated policing (POP), computer statistics (COMPSTAT) and intelligence-led policing (ILP). However, of these five, only ILP is equipped to utilise CIT in the fight against 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). Ratcliffe (2002; 2003; 2008a; 2008b; 2008c), a leading authority in the area of ILP, has developed a range of criteria allowing for an appropriate definition (Ratcliffe, 2002; 2003; 2008a; 2008b; 2008c; Ratcliffe & Guidetti, 2008, p. 112):

> "Intelligence-Led Policing is a business model and managerial centred philosophy where data analysis and crime intelligence are pivotal to an

> objective, top-down decision-making framework that facilitates crime and problem reduction. It is proactive and informant and surveillance-focused with heightened attention directed toward recidivists and serious crime offenders, and it provides a central crime intelligence mechanism to facilitate objective decision-making and disrupt and prevent crime".

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 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 it characterises itself as the most suitable methodology for combating transnational organised crime (Flood & Gasper, 2009, p. 57).

## Laying the groundwork for the successful deployment of CIT

This research paper reveals a number of themes that illustrate the required direction of CIT if it is to be an effective tool in combating TOC. In particular, the successful deployment of CIT is influenced by intelligence direction, the adoption of an ILP methodology and the practical application and effectiveness of CIT.

### INTELLIGENCE DIRECTION

A theme consistent throughout communication interception literature is the requirement for policing agencies to move from the traditional role of reactive policing, or 'local' policing, to a more proactive manner that utilises intelligence as their foremost weapon in addressing the growth of TOC. Heldon (2009, p. 125) highlights this concept by stating: "Unfortunately, in the current law enforcement environment where policing agencies are at the forefront of combating terrorism, transnational crime as well as more 'traditional' community-level offences, understanding and information are critical. Intelligence must be able to support decision-makers to negotiate this environment".

The first section of this statement can be seen to identify that currently, policing agencies lack a clear understanding of the nature of the criminal enterprises in organised crime and terrorism. This is taken further to imply this standard of understanding goes so far to apply to the more minor of crimes found within a specific locality, which one can assume includes vandalism, property crime such as burglary, robbery and car theft, assaults and the like. The second statement requires little explanation – the use of intelligence, which can be derived from CIT, is an integral aspect for combating and identifying transnational crime. As such, its use must be strategic.

Resultant from the demonstrated need to utilise intelligence in a manner that provides ultimate direction to policing objectives and targets, it is further recognised 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 confirm the importance of intelligence and CIT as a vital component, with intelligence placed at the centre of law enforcement doctrine rather than simply used as an investigation support tool. This is an important aspect as it identifies the current flaws of many policing agencies, particularly in Australia.

It goes further to recognise that where there is a need for intelligence to be placed 'at the heart', then there is a requirement to introduce a policing framework or methodology that does not simply encourage this change to happen, but forces it to occur in recognition of the obstinate nature of LEAs within Australia. Intelligence activity is therefore recognised as an essential part of policing practice. It is this theme that reinforces the purpose of CIT – without an established means and flow of data collection there can be no analysis and thus no intelligence product.

## THE PRACTICAL APPLICATION OF CIT

The literature is scant on information relating directly to the specific use of CIT. Research shows that rather than being recognised as an individual investigative tool, CIT is more frequently incorporated into the 'surveillance' arena of practical methodologies. Christopher and Cope (2009, pp. 238-239) discuss the importance of the use of surveillance techniques that result from the inability to utilise "traditional" methods of investigation stating that "targeted policing ultimately depends upon the capability to infiltrate 'difficult to access' criminal milieu in order to gather information. The capacity to penetrate inimical environments and subcultures is afforded by covert policing".

This statement can apply to multiple covert collection methods, such as undercover policing, interception technology, CCTV, physical surveillance, GPS and electronic tracking systems, however its importance to CIT is still relevant. The pervasive nature of TOC is ensuring that intelligence collection is an increasingly problematic situation. It has been recognised that more invasive and intrusive measures, such as CIT, are becoming essential to LEAs. These views are supported by Ratcliffe (2003; 2008a; 2008b) who notes that the use of covert information gathering techniques, such as CIT, is an important aspect of ILP.

What is not highlighted, and thus frequently misunderstood about the ILP framework, is that although it encourages the use of surveillance techniques, the

purpose of the data and subsequent intelligence is for strategic direction (Ratcliffe, 2008a, p. 280; 2008b). This is a 'make or break' issue that concerns the acceptance of ILP by law enforcement and the public. Regarding the practical use of CIT and its effectiveness as a law enforcement tool, the Attorney General's Department (2008, p. 15) reports that:

> "There remains a constant view among agencies that telecommunications interception continues to be an extremely valuable investigative tool. Agencies have again noted that evidence gathered through the execution of a telecommunications interception warrant can lead to the successful conclusion of an investigation in circumstances where alternative evidence is uncorroborated, unavailable or insubstantial".

The understanding of this statement is twofold. The apparent view stemming from this statement is that Australian LEAs who utilise CIT believe that it is an effective tool in the fight against crime. Whilst this is positive for the reinforcement of CIT's use, the statement exposes the flaw in current use by Australian agencies. It is clear that the use of information collected is specifically directed to individual cases or investigations, with CIT working as an evidence-gathering tool, rather than an intelligence-gathering tool. The important distinction, as highlighted by Ratcliffe (2008a; 2008b), is that when employing CIT under the ILP business model, intelligence collection is used for operational targeting as well as strategic decision making. This combination ensures that the law enforcement role is continually maintained by LEAs – rather than intelligence simply informing against possible threats it provides vital guidance for the deployment of enforcement strategies on either persons or areas of interest.

### THE EFFECTIVENESS OF CIT

There are limitations on the availability of examples and evidence concerning CIT's effectiveness. An initial review of figures supplied by the Attorney General's Department (2008) suggest that CIT, even in its current state of use as an evidentiary gathering tool, is an effective technology. Approximately 63 per cent of warrants issued resulted in arrests based on lawfully intercepted information, which would indicate effectiveness and compliance with the requirements of the TIA Act. This information does not, however, illustrate the overall effectiveness of CIT on crime rates, nor does it provide any measure for the level of disruption caused by arrests, prosecutions and convictions from lawfully intercepted communication on criminal enterprises. While the use of case studies would provide a more valuable means of examining CIT effectiveness limited evidence is available.

## Adopting an intelligence-led model

The findings illustrate that the use of intelligence is an essential prerequisite for effective modern policing. As such, an appropriate framework must be adopted to manage intelligence use. ILP is the only framework that utilises intelligence as a

primary asset. The business/philosophy model that employs crime intelligence to objectively direct decisions for police resourcing and targeting was further identified through the content analysis as a frequent theme emerging in literature.

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 recognised as an appropriate model for policing within the 21st century as globalisation continues to grow.

Ratcliffe (2008a) in his evaluation of ILP, recognises the importance of information collection using CIT. He notes that within law enforcement, the technologies such as CIT have been used as evidentiary gathering tools for reactive investigations and whilst useful for prosecutions, as a manner of crime prevention their efficacy is limited (Ratcliffe, 2008a, p. 267).

It has been shown that the use of CIT in a proactive intelligence-led model can play a vital role in the disruption and prevention of TOC. However, literature also shows that the use of CIT is constrained by a number of factors including a lack of evidence to support its use, privacy debates and the prevailing culture of scepticism surrounding intelligence.

## Barriers to successful CIT deployment

The centrality of crime intelligence and data analysis in the ILP model has been identified as a crucial link to developing a model of best practice for the use of CIT. Currently CIT must only be deployed as a last resort and as such tends to be used as a resource for developing case-specific evidence, arguably due to the legislative restrictions. As Ratcliffe (2008b, p. 269) states, the use of intelligence derived from covert information and techniques is essential for strategic planning and strategic planning has a greater proactive and preventative nature than its traditional reactive counterpart does. However, with CIT forming a critical part of ILP and the use of strategic planning and assessment, a complete picture of the criminal environment can be developed and actions instigated to disrupt these activities (Ratcliffe, 2008a; 2008b).

### LACK OF EMPIRICAL EVIDENCE ON CIT EFFECTIVENESS

The primary issue underpinning the effectiveness of CIT is the lack of evidence available to support its use. This is primarily due to the fact that the necessary data is protected by Commonwealth legislation – and without access to this data it is impossible to truly measure just how successful the use of CIT is within the ILP model. As established in the findings of this study, the available figures – supplied annually by LEAs in Australia in the annual TIA Act report – only substantiate the grounds of impact of warrants on individuals. They do not ascertain the overall effectiveness of CIT's use on overall crime rates, nor provide any measure for the level of disruption

caused. It cannot be denied that there is a clear lack of empirical research that provides solid evidence for this cause. Whilst Grabosky and Smith (1998; 1999) provide an examination of case studies utilising CIT, they are neither recent nor in-depth. It can be theorised that this is partially caused by the classified nature of law enforcement and restrictive disclosure provisions that exist in the legislation controlling the use of CIT. However, when placed in a policing framework such as ILP, the effectiveness can be interpreted by the level of relevant and reliable information collected from interception sources. As such, with communication technologies increasing in its availability to, and adoption by, general society, it is an area that requires continued monitoring and use.



## PRIVACY

It is not surprising that the process of focussing policing tactics and the implementation of a proactive approach in which a majority of policing work is not publicly visible, is perceived by some as a threat to civil liberties, irrespective of the accuracy of their perceptions (Ratcliffe, 2008b, p. 220). As is noted by Innes (2004, p. 156), 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 regarding the issue of privacy must be addressed. As highlighted earlier, Bronitt and Stellios (2005; 2006) and privacy advocates such as EFA (2006) raise concerns regarding the legislative framework that governs CIT within Australia, arguing either that the model of 'balancing' law enforcement and privacy is fatally flawed or for greater restrictions to be imposed on the use of CIT. Even though Australia's legal protections for privacy rights are 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. Irrespective, it would be illogical to make recommendations that ignore privacy on a whole. Porter (in Radcliffe, 2008b) highlights this concept by noting:

> "Intelligence-led policing also brings with it special challenges ... information-gathering activities associated with intelligence-led policing may also infringe on the privacy and civil liberties of individuals. This type of information gathering requires the police to use more intrusive procedures, such as informants, undercover operations, electronic surveillance, and sophisticated intelligence analysis. Such intrusive procedures pose threats to civil liberties, privacy, and other rights".

It is therefore important for police organisations to put the protection of privacy and civil liberties 'up front' when implementing an ILP approach. Whilst it is understandable for 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.

## Intelligence and culture

As shown in the findings, for the most effective law enforcement practice, intelligence must be recognised by LEAs as substantially more than just data or information collected using the stereotypical means of 'intelligence collection' relating to covert information gathering. 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; 2008; 2008a; 2008b; 2008c), Oakensen, Mockford and Pascoe (2002) and Osborne (2006), for true ILP to be implemented there is 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, and that "intelligence reports collated centrally were said to disappear into an intelligence 'black-hole' – a space where all information is swallowed-up but from where no light emerges" (Ratcliffe & Sheptycki, 2009, p. 249).

Intelligence sharing is also a key aspect of not just ILP but of the combat of TOC. Agencies both domestically and internationally need to shift from the model of informal networks to a more defined arena that promotes effective intelligence sharing (Bhaskar & Zhang, 2007; Dean & Gottschalk, 2007a; 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 the slightest hint of a violation of rights and privacy 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).

## Conclusion

This paper has served as a preliminary attempt to develop a practical framework for the use of CIT. The findings indicate that CIT can be an effective tool for LEAs,

but its effectiveness is best controlled through its placement within a proactive environment. This can be addressed by adopting an ILP methodology that utilises collated information as a form of intelligence, rather than the current reactive manner of evidence gathering. This study has employed a systematic methodology of document analysis to analyse CIT in fighting TOC within Australia. It explored the vulnerability of TOC groups to communication interception, the practice of this interception and the modern policing methodologies. The study has attempted to move beyond the criticisms and concerns that underpin the majority of research regarding privacy and has sought to address these issues in part with an intelligence-led model. In doing so it fills an important gap in current literature.

Transnational organised crime is a diverse and complicated arena, costing global society in excess of $3 trillion annually – a figure that continues to grow (Borger, 2007). It is hoped that this paper will contribute to the body of knowledge that currently exists on CIT, TOC and ILP and provides the basis for future research into the efficacy of CIT, particularly in the Australian context.

## References


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

Ahmed, S. (2007). B-Party intercepts and the telecommunications (interception) amendment act 2006 (Cth). *Internet Law Bulletin*, 10(1).

Attorney General's Department. (2008). *Telecommunications (interception and access) act 1979: Reporting for the year ending 30 June 2008*. Canberra: Public Affairs Unit, Attorney General's Department.

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).

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.

Borger, J. (2007, September). Organised crime: The $2 trillion threat to the world's security. *The Guardian*. Retrieved (no date) from http://www.guardian.co.uk/world/2007/sep/12/topstories3.mainsection

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

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

Bronitt, S. & 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. & Marshall, P. (2004). *The 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.

Christopher, S. & N. Cope. (2009). A practitioner's perspective of UK strategic intelligence. In J. H. Ratcliffe (Ed.). *Strategic thinking in criminal intelligence*, 2nd ed, (pp. 235-247). Sydney: The Federation Press.

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.

Davies, S. (2007). *Transnational organised crime: Statistics/typologies of transnational organised crime.* Queensland University of Technology.

Dean, G. & Gottschalk, P. (2007a). *Knowledge management in policing and law enforcement*. Oxford: Oxford University Press.

Dean, G. & Gottschalk, P. (2007b). *Knowledge management in policing and law enforcement: Foundations, structures, applications.* Oxford: Oxford University Press.

Denzin, N. & Lincoln, Y. (2005). *The sage handbook of qualitative research*. 3rd ed. Thousand Oaks, CA: Sage Publications.

Department of Justice. (2005). *Fusion centre guidelines*. Washington DC: Department of Justice.

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 (EFA). (2006). Telecommunications interception & access laws. Retrieved April 14, 2009 from http://www.efa.org.au/Issues/Privacy/tia.html.

Flood, B. & 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.

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.* New Jersey: 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 organised crime. *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., & Temple, M. (2007). Breaching the fortress wall: Understanding terrorist efforts to overcome defensive technologies. Santa Monica: RAND Corporation.

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.

Mason, J. 2002. *Qualitative researching*. 2nd ed. Thousand Oaks: Sage Publications.

McFarlane, J. (2001). Transnational crime and Asia-Pacific security. In S. W. Simon (Ed.). *The many faces of Asian security,* (pp. 197-230). Lanham: Rowman & Littlefield.

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

Monk, P. (2002, November 1). Silly, Mr. Downer? Keep thinking. *The Australian Financial Review*.

Oakensen, D., Mockford, R., & 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. 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.

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., & Guidetti, R. (2008). State police investigative structure and the adoption of intelligence-led policing. *Policing: An International Journal of Police Strategies & Management*, 31(1), 109-128.

Ratcliffe, J. H., & 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.

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

Shelley, L. I. (1998). Transnational organized crime in the United States: Defining the problem. *Kobe University Law Review*, 32(1), 77-91.

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.

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. (2000). *United Nations covenant against transnational organised crime*. Geneva: United Nations General Assembly.

Wardlaw, G., & 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.

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.