Knowledge-Managed Policing Framework for Communication Interception Technologies (CIT) in Criminal Justice System

Geoff Dean, Peter Bell &
Mitchell Congram

Abstract

This is a conceptual paper on Communication Interception Technologies (CIT) within the criminal justice system because little substantive research exits, outside of the military/defence and national security domains, on several methodological issues surrounding the use of CIT particularly in a policing context. The paper proposes the adoption of an organising framework based on a Knowledge-Managed Policing (KMP) approach to the use of CIT to effectively address methodological concerns. The paper initially overviews what is characteristically involved in a Knowledge-Managed Policing perspective. It concentrates of three key dimensions that of police practitioners' knowledge as the basis of a KMP system; the technological processes which support a KMP system; and the organisational context of police work from a KMP perspective. Then the conceptual dimensions of CIT are briefly outlined and discussed with reference to adopting a KMP framework. The paper concludes with some speculative comments on the suitability of KMP as a regulatory framework for CIT.

Keywords

Police Knowledge, Communication Interception Technologies, Knowledge Management, Knowledge-Managed Policing, Human Rights, Regulatory Frameworks, and Criminal Justice System

Introduction

Criminal justice systems and the police organisations that serve them don't have a choice about the environment they operate in. Like the rest of society we are all locked into a globally-wired world where if one country's economy falters we all stumble and get our toes kicked. The global financial crisis (GFC) of recent times is a clear example of the massive ripple effects of a networked world. Globalization has collapsed boundaries and borders of nations and countries, big and small. Yet many societal institutions, and in particular, policing, law enforcement and the courts remain, often stubbornly, out-of-sync in terms of their knowledge base with the changes and challenges wrought on them by the rapid technological and societal drivers of late modernity (Beck, 1992; Ericson and Haggerty, 1997).

In so far as the criminal world is concerned it has been transformed before the eyes of the police into a global village where instantaneous communication is the cyberspace norm. The distinction often made between 'local' policing and 'global' policing has been rendered obsolete by the growth in criminal entrepreneurialism, global terror and its nexus with transnational crime. Peter Neyroud, current Chief Constable and Chief Executive of the National Policing Improvement Agency (NPIA) in the UK, made the salient point that: "Policing has become an intensely knowledge-based profession, whose investigative practice has been transformed by science and technology."(Neyroud, 2008:xix). However, policing organisations, like all bureaucratic-bound institutions, are slow in responding to such challenges.

Hence, this paper focuses on the use of Communication Interception Technologies (CIT) within the criminal justice system generally and by the police in particular. CIT provides a clear example of where there is an urgent need for instituting a Knowledge-Managed Policing (KMP) framework in the fight against global crime and terrorism.

'Knowledge-Based' to 'Knowledge-Managed' Policing

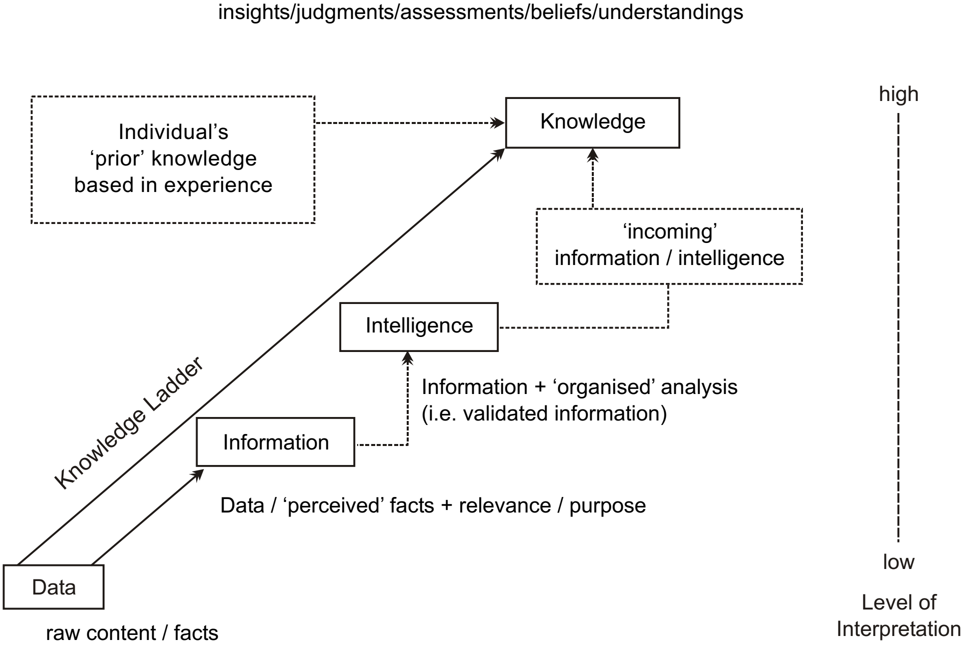
The notion of Knowledge-Based Policing (KBP) is gaining currency in the scholarly literature. But like most new concepts is it slippery to define. Williamson (2008: 6) attempts to capture it as follows, "Knowledge-based policing is envisaged as responding to technological and social drivers that are leading to an emerging new policing paradigm whose purpose is the management of risk." Hence, for Williamson (ibid.) "The primary object of knowledge-based policing is the management of risk".

Whilst, this view has merit is drawing attention to the need for risk management by police it also, rather unfortunately, reduces the notion of 'knowledge' in policing to little more than using it for 'risk aversion' purposes. This is unfortunately because it is also rather commonly known that police agencies are very good at 'risk aversion' already (Stephenson, 2008; Ratcliffe, 2008c).

A more enhanced understanding of 'knowledge' is provided in the literature. Knowledge is generally defined as the most valuable form of content in a hierarchical continuum starting at data, encompassing information, and ending in knowledge (Gottschalk, 2005). Dean and Gottschalk (2007) have written extensively about this hierarchy of knowledge as it applies in a policing context and therefore include police 'intelligence' as a specific form of content on a knowledge ladder[1] as shown below.

[1] Sometimes wisdom is included beyond knowledge in this 'data-information-knowledge-wisdom (DIKW) hierarchy as the ultimate end goal (Rowley, 2007; Davenport and Prusak, 1998; Spiegler, 2000). This DIKW hierarchy is part of the canon of information science and management however it is nonetheless a contested notion by some academics (see Frické, 2009).

Figure 1.1: 'Knowledge Ladder' in Policing


insights/judgments/assessments/beliefs/understandings
Individual's 'prior' knowledge based in experience
Knowledge
high
'incoming' information / intelligence
Intelligence
Information + 'organised' analysis (i.e. validated information)
Knowledge Ladder
Information
Data / 'perceived' facts + relevance / purpose
Data
raw content / facts
low
Level of Interpretation

A police practitioner acquires knowledge and accumulates expertise over time as indicated on the knowledge ladder. Policing knowledge consists of *information* (including data and intelligence-based information for simplicity of discussion) which when combined with an individual officer's *experience* forms the basis of the understandings, insights, and judgments that constitute *police knowledge*.

Therefore, the concept of Knowledge-Managed Policing (KMP) proposed by Dean[2] (2010) offers a much broader and holistic use of 'knowledge' in policing than simply risk management. Whilst policing is 'based' on knowledge it is the 'management' of knowledge which gives policing its cutting edge. In other words, where KBP is about the management of risk in contrast KMP is about managing the application of knowledge for enhancing policing effectiveness. Hence, KMP provides a useful framework for managing the challenges Communication Interception Technologies (CIT) present to policing in particular and more generally to the criminal justice system.

[2] For further information on 'Knowledge-Managed Policing' readers are referred to Dean's latest book where he introduces the term (Chapter 7) in *Organised Crime: Policing Illegal Business Entrepreneurialism* to be published by Oxford University Press in UK in Sept 2010.

Dimensions of Knowledge-Managed Policing

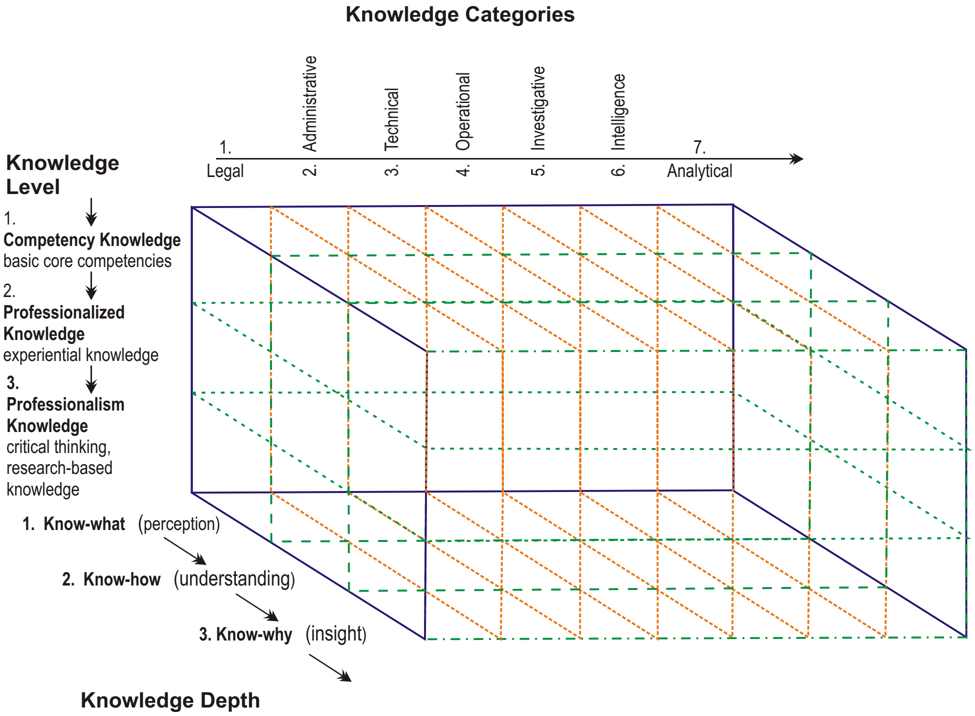
In essence, Knowledge-Managed Policing (KMP) entails the harnessing of practitioner-based knowledge and technological support systems in order to manage, systematically the application of policing knowledge in all its forms, levels and depth to serious and complex policing problems. To achieve this KMP has three interrelated dimensions to manage. They are: police practitioners, policing technologies, and police organisations themselves.

Police Practitioners

The first KMP dimension is a people system, that is, practitioner knowledge. The simple fact is that all knowledge originates in the human brain. Knowledge results from the combination of experience and context and is subject to interpretation, reflection, intuition and creativity by human beings. Hence, 'knowledge', itself, cannot be stored in a computer. Only some form of representation of knowledge can be stored in a computer as data or information like text, or a diagram, a picture, audio and video files or some other representational system. Thus, a general distinction is made in the literature to refer to knowledge which resides in people's heads as 'tacit' knowledge and knowledge that can be captured and stored in some representational system as 'explicit' knowledge.

Moreover, the diverse forms a police practitioner's knowledge covers include *legal, operational, administrative, technical, investigative, intelligence,* and *analytical* aspects. Also, such policing knowledge categories involve knowledge levels to do with *competency* knowledge, *experiential* knowledge, and *critical thinking evidence-based* knowledge. Whilst the depth of a practitioner's policing knowledge entails *'know-what' {perception} knowledge, 'know-how' {understanding} knowledge and 'know-why' {insight}* knowledge. These police knowledge forms, levels and depth are conceptually integrated as a 'knowledge cube' which is diagrammatically represented in the following 3-D graphic in Figure 1.2 below.

Figure 1.2: Police Practitioner's 'Knowledge Cube'


Knowledge Categories
1. Legal
2. Administrative
3. Technical
4. Operational
5. Investigative
6. Intelligence
7. Analytical
Knowledge Level
1. Competency Knowledge basic core competencies
2. Professionalized Knowledge experiential knowledge
3. Professionalism Knowledge critical thinking, research-based knowledge
1. Know-what (perception)
2. Know-how (understanding)
3. Know-why (insight)
Knowledge Depth

Taken together the two figures presented so far (1.1-knowledge ladder and 1.2-knowledge cube) graphically highlight in their own way the essential point about KMP that effective policing in the final analysis is utterly dependent of the quality of the multi-faceted knowledge a practitioner possesses and how they choose to use it. This is why KMP is first and foremost all about harnessing practitioner knowledge. Once such practitioner-based knowledge exits then it can be managed, technologically and organisationally. The next sections make it clear capturing and managing practitioner-based knowledge is not an easy task.

Police Technologies

The second KMP dimension involves the technological systems. Although knowledge cannot originate outside the heads of individuals, explicit knowledge can be *represented* in and often embedded in technologically processes, routines, and networks, and sometimes in document repositories. However, such explicit representations of knowledge are seldom complete outside of the tacit knowledge of individuals because they often lack depth and quality unless the creativity and adaptability of people and processes (higher-order learning) is built into the institutional mechanisms themselves.

In this regard the tacit/explicit distinction referred to previously is useful to bear in mind for it highlights the fact that capturing a person's, and in this case a police practitioner's, *tacit* knowledge is not a simple matter. It is about capturing the depth of their experientially-based knowledge, which they themselves may only be partially aware of the extent and degree of such knowledge, as well as the 'interpretation' they place of their own knowledge that surfaces in such an in-depth dialogue of knowledge sharing. Moreover, all knowledge is subject to interpretation as it results from human reasoning which itself is a representational system devised by human beings to aid understanding. Therefore, knowledge capture is far more than merely sitting someone down and doing an After Action Review (AAR) and thinking you have their knowledge in a nutshell. What you have is the nutshell and the degree of quality knowledge in it is a matter of conjecture. This is why it is important to understand that Knowledge Management (KM) involves both a 'philosophy' and a 'practice'.

There are two distinctly different philosophical orientations, mechanistic and dynamic, to KM. The mechanistic view equates KM with IT and adopts a 'platforms & programs' approach where the emphasis is on getting the right platform and software applications to harvest an organisation's knowledge. The dynamic perspective takes a 'context & culture' approach to KM and asserts that the only thing that can really be 'managed' about knowledge is the context and culture in which it occurs (Dean and Gottschalk, 2007). Given these divergent perspectives, competition and conflict are inevitable byproducts in the world of KM.

'IT-aligned' KM experts favour selling more platforms and programs to police to the point where the inoperability of technological systems is the norm rather than the exception. Jan Berry, a police technology expert at the National Policing Improvement Agency (NPIA) was reported as stating that 'Police and criminal justice work is being slowed by a lack of interoperability and integration between IT systems". Berry argues that "One of the biggest problems is the vested interests of Chief Information Officers (CIOs). Forces agree on national standards, then go away and do their own thing" (ZDNet UK, 11/6/2010). Furthermore, the cost of misaligned systems is staggering. For instance, in the UK there are 43 police forces and each uses its own 'different system' as Nick Gargan, Deputy Chief Executive of the NPIA was reported as saying, " IT is frankly too expensive. It's wrong that we have 4,500 to 5,000 people in police IT roles. It's wrong that they are supporting 2,000 business applications and rely on 6,000 suppliers" (Computer Weekly.Com, 10/6/2010).

KM experts who are more 'culture and context-aligned' are more discerning about technology and what it can do for them. They favour systems which support 'communities of practice' and knowledge sharing applications (Van den Hooff and

Huysman, 2009). Since these activities are more likely to produce, create and capture the 'deep' knowledge locked inside the heads of experienced practitioners which can then be harnessed for organisational purposes.

Hence, KM as a technological 'practice' looks like a simple recipe to follow since it involves a set of distinct yet complementary IT processes for *creating, capturing, storing, retrieving, transferring, sharing, applying* and *integrating* the work practices of police organisations. However, like most cookbook approaches there is no guarantee of a good cake or in the policing context a quality Knowledge Management Technology (KMT) system.

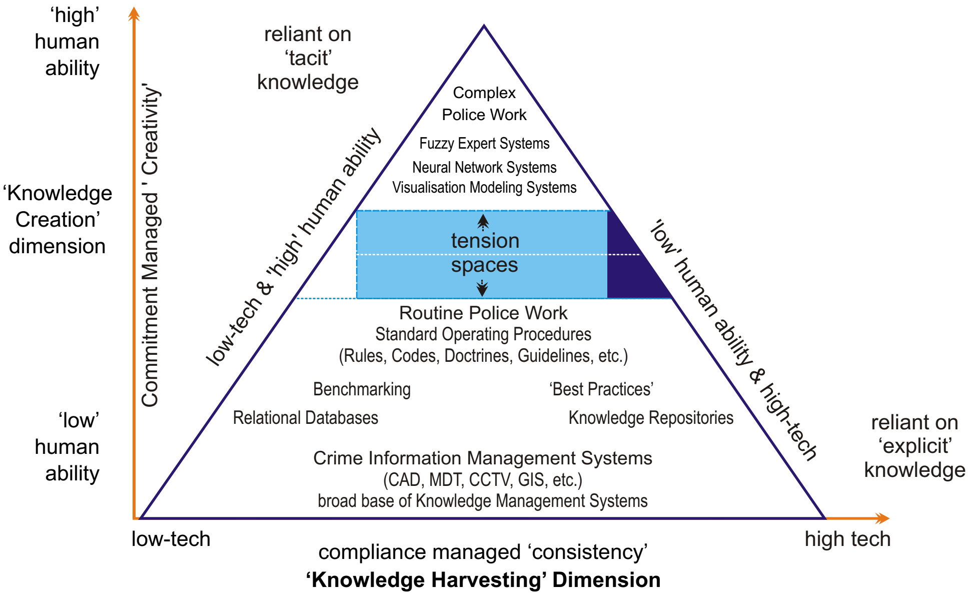
Police Organisations

The third KMP dimension is the police organisation itself. It is clear that even in an organisational context, all new knowledge stems from people. Thus, practitioner knowledge is a value-adding organisational resource. This is because practitioner knowledge has the greatest relevance to decisions and actions. But, it also has the greatest dependence on a specific situation or context. Hence, practitioner knowledge is also the most difficult type of knowledge to manage, since it originates and is applied in the minds of human beings.

People who are knowledgeable not only have information, but also have the ability to integrate and frame the information within the context of their experience, expertise, and judgment. In doing so, they can create new information that expands the state of possibilities, and in turn allows for further interaction with experience, expertise and judgment. However, they cannot be commanded to share their knowledge and acquired expertise. Therefore it is essential for the executive management of an organisation to take very seriously the dynamic 'context & culture' philosophical orientation to KM if they really want to harness the creative energy within their organisational context.

This leads to a crucial decision point for policing organisations for harnessing policing knowledge. The following figure 1.3 provides graphically overview of the key issues involved and the consequent decisions required from management.

Figure 1.3: Organisational 'Knowledge Pyramid' to harness Police Knowledge


'high' human ability
'Knowledge Creation' dimension
'low' human ability
Commitment Managed ' Creativity'
reliant on 'tacit' knowledge
low-tech & 'high' human ability
Complex Police Work
Fuzzy Expert Systems
Neural Network Systems
Visualisation Modeling Systems
tension spaces
'low' human ability & high-tech
Routine Police Work
Standard Operating Procedures
(Rules, Codes, Doctrines, Guidelines, etc.)
Benchmarking
'Best Practices'
Relational Databases
Knowledge Repositories
reliant on 'explicit' knowledge
Crime Information Management Systems
(CAD, MDT, CCTV, GIS, etc.)
broad base of Knowledge Management Systems
low-tech
high tech
compliance managed 'consistency'
'Knowledge Harvesting' Dimension

The central focus of the above diagram is the 'knowledge pyramid' and how it intersects two dimensions of knowledge a horizontal axis of knowledge harvesting and a vertical axis of knowledge creation. 'Knowledge harvesting' is where existing knowledge captured in an organisation's databases, information systems, knowledge repositories, best practices, 'lessons learnt' packages , and so forth is re-used and replicated to achieve pre-specified organisational goals and targets.

According to Malhotra (2004) knowledge harvesting is what passes for much of 'Knowledge Management' in most organisations. This knowledge harvesting approach to KM is easy to do for work that is routine and structured. It fits very comfortably with organisations that depend on rules and institutionalised procedures and work in predicable and stable environments.

On the other hand, knowledge creation is a much more active and dynamic concept that results from multi-level interactions between data, information, and intelligence combined with rules, procedures, best practices, lessons learnt and so forth by individuals and groups. Such people and groups show motivation, commitment and persistence to think innovatively in coming up with new ideas and ways to improve processes and/or solve problems. The critical point about knowledge creation is that its wellspring is in the mind of individuals not technology. Hence, a knowledge creation approach is most suitable for work that is predominately non-routine and largely unstructured and where an organisation operates in unpredictable and dynamic environments as shown on the diagram.

The essential difference between these two dimensions is that knowledge harvesting depends on technology for processing routine, structured work in stable environments. Whereas knowledge creation does not depend on technology but rather an individual's innovative thinking but uses technology to process non-routine, unstructured work in dynamic environments.

As shown the 'Knowledge Harvesting' dimension is most closely associated with a managerial focus that seeks 'compliance' in order to minimise variance and hence produce a consistent result that is often pre-specified and pre-determined by some type of performance outcome indicator, target or measurement. Organisational control is imperative for this type of compliance-based management. For routine police work this 'Command and Control' managerial style works up to a certain degree (the 'fuzziness' factor see tension spaces on Figure 1.3). However, beyond where that 'certain degree' may be drawn a 'command & control' compliance model becomes problematic for a KM policy.

Whereas, the 'Knowledge Creation' dimension requires a managerial focus on the creation of new knowledge, which by definition is tacit in origin (in someone's head), and hence must be willing to share it, so line management has to be 'commitment' based in order to harness an individual's willingness to share their knowledge.

Police executives need to ensure that their management models find the right balance between maintaining a 'command & control' compliance model of management for routine police work while at the same time facilitating the movement towards a more commitment-centered, mindfulness-based management model for some routine police work and for the majority of complex police work.

The crucial point derived from figure 1.3 is police organisations must strive to find and then sustain a correct balance between the dimensions of 'knowledge harvesting' and 'knowledge creation' if it seeks to benefit fully from adopting a KMP approach. How a Knowledge-Managed Policing framework can be applied to Communication Interception Technologies (CIT) is the subject of the rest of the paper. Before that discussion a brief outline of salient dimensions of CIT follows.

Dimensions of Communication Interception Technologies

The rapid growth of communication technology in the new millennium coupled with the rise of terrorism and the globalization of organised crime (Stohl, 2006; Gibson, 2004; Shelley, 2002) has also witnessed a corresponding need for increasing the use of interception technologies in policing. Such 'popularity' for CIT has spawned several concerns. Among the most prominent are definitional issues, the securitization of a surveillance society (Wood, 2006; Norris 2006) and privacy rights (Bronitt and Stellios, 2005).

There is debate in the literature regarding the most appropriate definition for CIT (Branch, 2003; Starey, 2005). The term 'communication interception technology' (CIT) resulted from the preconceived notions attached to the definition of 'telecommunications'largely associated with solely traditional telecommunication methods, such as telephone calls. Conversely, CIT implies a broader scope for all forms and methods of communication and is subsequently used to reference the interception methods and related technology. In Australia the legislation concerning CIT, divides 'communications' into two distinct categories: live communications and stored communications (Telecommunications (Interception) Amendment Act, 2006). Whilst, legislation in other parts of the world is drafted differently this distinction is generally adhered to in most countries (Starey, 2005).

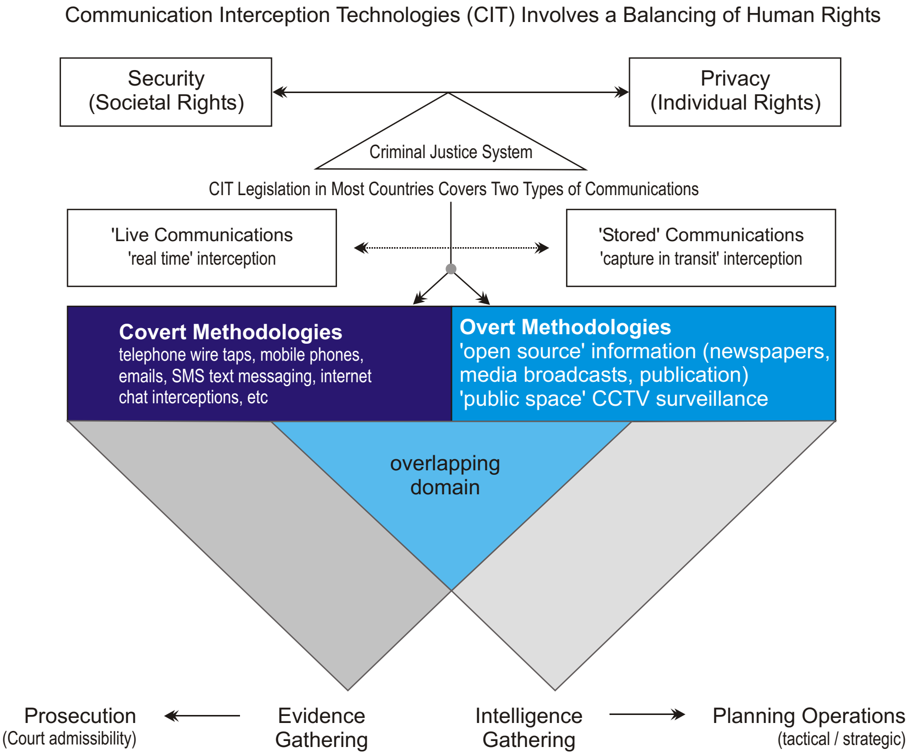
'Live communications' addresses the category of communication that passes over a telecommunication system, such as voice telephony. The 'live' aspect concerns the fact that during a telephone call, the recipient instantly receives the message being communicated in 'real time' (Starey, 2005; Ahmed, 2007).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

Conversely, stored communication or communication stored in transit covers communication that during the course of its transmission is stored on one or more pieces of equipment of a carrier or service provider before being retrieved and accessed by the recipient. Starey (2005) and Ahmed (2007) both state that the concept of stored communication applies to most forms of electronic communication. During the transmission of electronic communicationsuch as email, SMS text messaging, voice mail, internet chat or instant messaging software and VoIP telephonythe data packets transmitting this information are stored, at least momentarily, on various service provider servers and computer equipment. This information can therefore be intercepted prior to the intended recipient actually receiving the message (Starey, 2005; Ahmed, 2007).

This breakdown is especially important with regards to legislative definitions and subsequent abilities to intercept communications, where 'interception' is defined as the act of listening to, recording or reading through any means a communication without the knowledge of the person making the communication (Starey, 2005; Telecommunications (Interception) Amendment Act, 2006; Ahmed, 2007).

The following diagram in Figure 1.4 sketches out the dimensions of the 'balancing act' debate over security versus privacy with regard to CIT as well as defining the legislative framework.

Figure 1.4: CIT as Knowledge-Managed Investigative Tool


Communication Interception Technologies (CIT) Involves a Balancing of Human Rights
Security (Societal Rights)
Privacy (Individual Rights)
Criminal Justice System
CIT Legislation in Most Countries Covers Two Types of Communications
'Live Communications 'real time' interception
'Stored' Communications 'capture in transit' interception
Covert Methodologies telephone wire taps, mobile phones, emails, SMS text messaging, internet chat interceptions, etc
Overt Methodologies 'open source' information (newspapers, media broadcasts, publication) 'public space' CCTV surveillance
overlapping domain
Prosecution (Court admissibility)
Evidence Gathering
Intelligence Gathering
Planning Operations (tactical / strategic)

Also, it will be noted on Figure 1.4 that CIT from a Knowledge Management perspective is an investigative tool where two distinct methodologies (overt and convert) can be employed, usually together or in parallel. Furthermore, in practice these methodologies overlap each other and are used for two quite different directions or purposes (gathering evidence and/or intelligence). Starey (2005) argues that the current legislation in Australia caters for CIT only as a last resort and sees its primary purpose as an 'evidence gathering' investigative tool, rather than intelligence collection. This over-emphasis in legislation on CIT's evidential aim creates a bias in terms of its investigative potential. Clearly, as figure 1.5 shows evidence and intelligence gathering should be equally weighted in a Knowledge-Managed Policing (KMP) framework. This issue is taken up in more detail in the next section.

Discussion

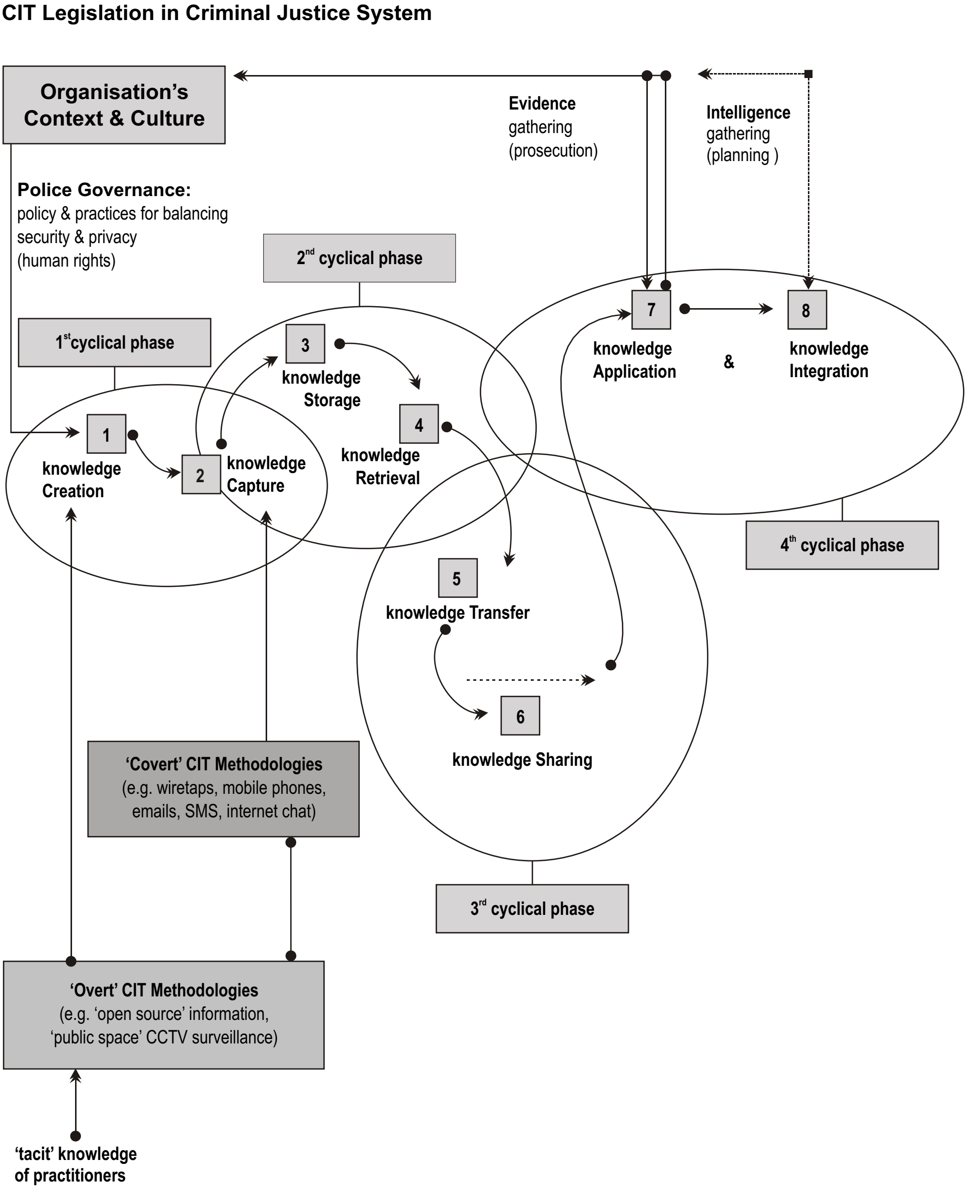
Any consideration of CIT within the criminal justice system must consider two points. Firstly CIT needs to be seen and understood as more than a 'surveillance' methodology, which is where it generally resides in the literature (Christopher and

Cope, 2009). Secondly, the prominence on evidence gathering within the CIT literature (Ratcliffe, 2002; 2003; 2008a) obscures its investigative potential for wider intelligence collection on terrorism and organised crime.

The growth of transnational organised crime (TOC) groups has little regard for the jurisdictional boundaries in which police work. In fact, TOC's exploit such jurisdictional restrictions (Irwin 2001). Hence, it is imperative for agencies within the criminal justice systems to be unified, locally and globally, to have anywhere near a level playing field against organised crime and terrorism (Glenn, Gordon & Florescu, 2008; Flood and Gasper, 2009; Ratcliffe, 2008b). Thus, any framework for CIT must be inclusive of these two essential points.

The following diagram in Figure 1.5 presents such an organising framework based on a KMP approach to CIT. This framework combines elements of KM technological processes and dimensions of CIT as an investigative tool. The KMP framework is presented as a flowchart involving a series of boxes numbered 1 to 8 corresponding to the eight processes of knowledge *creation, capture, storage, retrieval, transfer, sharing, application* and *integration* as shown. These 8 processes are paired up as four inter-linked cyclical phases. Each phase is cyclical in the sense that each of its paired processes can repeat themselves many times within their own phase before moving onto the next linked phase. For instance, captured knowledge is stored in databases and can be retrieved in several formats using a range of different programs. However, some but not all such stored data will be or should be retrieved. Thus a cycle of storage and retrieval occurs and at some point in time decisions to select data for retrieval is instigated then another phase of knowledge transfer and sharing occurs and the cycle continues.

Figure 1.5: Knowledge-Managed Policing Framework for CIT


CIT Legislation in Criminal Justice System
Organisation's Context & Culture
Evidence gathering (prosecution)
Intelligence gathering (planning)
Police Governance: policy & practices for balancing security & privacy (human rights)
2nd cyclical phase
1st cyclical phase
1 knowledge Creation
2 knowledge Capture
3 knowledge Storage
4 knowledge Retrieval
7 knowledge Application
&
8 knowledge Integration
4th cyclical phase
5 knowledge Transfer
6 knowledge Sharing
'Covert' CIT Methodologies (e.g. wiretaps, mobile phones, emails, SMS, internet chat)
3rd cyclical phase
'Overt' CIT Methodologies (e.g. 'open source' information, 'public space' CCTV surveillance)
'tacit' knowledge of practitioners

To navigate the flowchart follow the numbered KM processes (1 to 8) through each of the four cyclical phases. This is the logical sequence of how CIT can be integrated into a Knowledge Management Technological (KMT) system. At each KM process there are issues CIT are required to consider. Several of these issues have been touched on in this paper already. For instance, in relation to box 1- the *knowledge creation* process it is clear that the 'tacit' knowledge of police practitioners plays a central role in selecting and interpreting 'open source' information (a CIT overt methodology) as shown on figure 1.5. A practitioner's tacit knowledge is also involved in CIT covert methodologies to a lesser degree of interpretation. Because police governance requires a court order to be obtained before a 'person of interest' telephone, mobile, emails, internet chat and so forth can be intercepted, listened into and/or stored (box 2 - *knowledge capture* process).

In relation to the second cyclical phase which involves the KM processes of *knowledge storage* [box 3] and *knowledge retrieval* [box 4] it is evident that information overload is a major concern for database storage in terms of how much and what to store and for how long. The retrieval of stored knowledge represents enormous cost in terms of money and resources needed, especially if language translation is involved for hundreds of hours of taped conversations.

With regard to the third cyclical phase involving respectively boxes 5 and 6 *knowledge transfer* and *knowledge sharing* it will be noticed that there is a broken-dotted line between these two KM processes in figure 1.5. This is to signify a possible disjunction can occur at this phase between the *transferring* of knowledge and the *sharing* of it. In that, knowledge transfer is about distribution whereas knowledge sharing is about participation. Also, the issue of the interoperability and compatibility of technological platforms and programs can be a major roadblock at this phase as evidenced by the comments by NPIA noted previously.

Finally, there is another possible disjunction point between knowledge application [box 7] and knowledge integration [box 8] at the fourth cyclical phase as indicated on figure 1.5. This disjunction revolves around the issue of developing an integrated, united system of applied knowledge that is readily available organisation-wide when similar problems in the future may arise that have been effectively dealt with in the past rather than 're-inventing' the wheel each time a similar problem occurs. Investing in future knowledge-managed problem solving activities is often not considered a high priority in over-stretch and under-resourced police organisations.

Conclusion

The significance of the proposed Knowledge-Managed Policing (KMP) framework for Communication Interception Technologies (CIT) is twofold. Firstly, KMP functions as an 'organising' framework for CIT by locating it within a wider conceptual perspective than simply a surveillance methodology. Secondly, KMP can act as police governance mechanism and 'regulatory' framework to ensure transparency, accountability and integrity in the use of CIT as an investigative tool by appropriate legislative bodies in the criminal justice system.

Inherent in this paper is the need for a police agency to base its use of CIT in a regulatory framework like the KMP approach advocated to ensure a proper balance is achieved in the criminal justice system and more importantly maintained between what a society expects in terms of security and individual privacy rights.

References

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

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: Sage.

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

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

Christopher, S. and N. Cope. (2009). A Practitioner's Perspective of UK Strategic Intelligence. In J. H. Ratcliffe (Ed.). *Strategic Thinking in Criminal Intelligence*. (2nd edition) Sydney: The Federation Press. Pp. 235-247.

Computer Weekly.Com. (2010) http://www.computerweekly, accessed on 10/6/2010.

Davenport, T.H. and L. Prusak (1998). *Working Knowledge*. Boston, MA: Harvard Business School Press.

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

Dean, G., Fahsing, I., and Gottschalk, P. (2010). *Organised Crime: Policing Illegal Business Entrepreneurialism,* London, UK: Oxford University Press (published in Sept 2010).

Ericson, R. V., and Haggerty, K. (1997). Policing the Risk Society. Toronto: University of Toronto Press.

Frické, M. (2009). The knowledge pyramid: a critique of the DIKW hierarchy. *Journal of Information Science*, 35 (2): 131-142.

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.

Gottschalk, P. (2005), *Strategic Knowledge Management Technology*, Hershey, PA, USA: Idea Group Publishing.

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

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

Malhotra, Y. (2004) Why Knowledge Management Systems Fail? Enablers and Constraints of Knowledge Management in Human Enterprises, in Michael E.D. Koenig & T. Kanti Srikantaiah (Eds.), *Knowledge Management Lessons Learned: What Works and What Doesn't,* Information Today Inc. (American Society for Information Science and Technology Monograph Series). 87-112.

Neyroud, P. (2008). Foreword. In T. Williamson (Ed.). *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions.* Chichester: John Wiley and Sons. P. xix.

Norris, C. (2006). *A report on the Surveillance Society: For the Information Commissioner. Expert Report: Criminal Justice*. Surveillance Studies Network. London: Information Commissioner.

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

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.* Chichester: John Wiley and Sons. Pp. 205-220.

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

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

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy, *Journal of Information Science*, 33 (2): 163-180.

Shelley, L.I. (2002). The nexus of organised international criminals and terrorism. *International Annals of Criminology*. http://pagesperso-orange.fr/societe.internationale.de.criminologie/pdf/Intervention%20Shelley.pdf., accessed on 28-2-2010.

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.

Stephenson, K. (2008). Rethinking Governance: Conceptualizing Networks and their Implications for New Mechanisms of Governance Based on Reciprocity. In T. Williamson (Ed.). *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions.* Chichester: John Wiley and Sons. Pp. 323-340.

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.

Spiegler, I. (2000) Knowledge Management: A New Idea or a Recycled Concept? *Communications of the Association for Information Systems*, 3 (14).

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

Van den Hooff. B., and Huysman, M. (2009). Managing knowledge sharing: Emergent and engineering approaches. *Information & Management*, 46, (1), pp.1-8.

Williamson. T. (2008). Introduction to the Handbook. In T. Williamson (Ed.). *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions.* Chichester: John Wiley and Sons. Pp. 1-8.

Wood, D.M. (2006). *A report on the Surveillance Society: For the Information Commissioner.* Surveillance Studies Network. London: Information Commissioner.

ZDNet UK. http://www.zdnet.co.uk/news/business-of-it/clunky-it-sytems-hamper-police-work, accessed on 11/6/2010.

The author Geoff Dean is Associate Professor in the School of Justice in the Faculty of Law. His areas of expertise, teaching specialisation and research are in police Knowledge Management, the cognitive psychology of investigative thinking, criminal and terrorism profiling, global organised crime and international policing. He is the principal author of Knowledge Management in Policing and Law Enforcement: Foundations, Structures, Applications published by Oxford University Press in the UK in 2007. Dr. Dean was principal Guest Editor of a Special Issue on 'Local Research Links to Global Policing' in Police Practice and Research: An International Journal, Vol 9, No.4 in 2008. His latest book, as principal author is Organised Crime: Policing Illegal Business Entrepreneurialism which is due for publication in late 2009 by Oxford University Press in the UK.

The author Peter Bell is a Senior Lecturer and the Director of Postgraduate Studies at the School of Justice in the Faculty of Law. He has wide and diverse experience in policing, law enforcement and security including senior analytical and operational positions with the Queensland Police Service, the Australian Bureau of Criminal Intelligence, the Australian Federal Police and the Organised Crime Agency of British Columbia- Canada (OCABC). Dr Bell has written extensively for police/security agencies on topics to do with official corruption, international drug trafficking, terrorism, critical infrastructure security and transnational organised crime.

And the author Congram is an Honours graduate of the Queensland University of Technology's School of Justice, with a Bachelor's degree majoring in both Policing and Criminology with a focus on transnational organised crime. He currently works as a Graduate for the Commonwealth of Australia