Briefing paper

CEPS ARC Centre of Excellence in Policing and Security

January 2012
>issue 9

Forensic intelligence represents a unique and exciting policing capability. The integration and linking of data from various forensic science sources – DNA, fingerprints, shoe-prints and biometrics – into a comprehensive searchable database would seem to offer a major advance in the pre-emption and identification of criminal activity by law enforcement. However, the potential of forensic intelligence is yet to be fully realized.

This Briefing Paper outlines the concept, and potential and actual applications, of forensic intelligence. The paper summarizes the current use of forensic intelligence in the international and Australian context, identifying the issues contributing to a limited uptake of this promising approach towards data capture and analysis. The authors highlight the potential for forensic intelligence by reviewing current military application of this methodology in counteracting the growing use of improvised explosive devices. This Briefing Paper concludes by noting the future directions for forensic intelligence and emphasizing its potential for transforming police practice.

This Briefing Paper highlights the work of CEPS researchers in the Effective Practice Program, one element of the Intelligence Methods Project. The authors are Dr Timothy Legrand, a CEPS Research Fellow, and Ms Lauren Vogel, a PhD candidate with CEPS.

R. Delaforce

Dr Ruth Delaforce
Editor
CEPS Research Fellow

Forensic Intelligence

Dr Tim Legrand and Ms Lauren Vogel

Overview

The purpose of this paper is to provide policy officials and practitioners with an introduction to the concept and application of 'forensic intelligence' in modern policing and security.

Forensic intelligence refers to the use of different forensic data to cross-reference and link together crime scenes, materials, and suspects. As a concept, it is gaining traction within policing and security communities due to the increasing quantities of data being generated by forensic technologies and, at the same time, becoming more affordable. Forensic intelligence provides a methodology for rigorous data analysis and offers the prospect of robust, evidence-based, approaches to policing and security at both operational and strategic levels.

What is Forensic Intelligence?

As it is currently understood, forensic intelligence refers to several 'treatments' of data. As a concept, it refers to the structured assimilation of forensic data (i.e. crime scene evidence such as DNA, fingerprint, ballistics, and trace evidence) within a cross-referenced and indexed dataset. This dataset may be subjected to rigorous qualitative and quantitative analysis to identify meaningful patterns of criminal enterprise. Such data analysis is held to be strategic insofar as it informs several elements of policing, including: (i) intelligence-led operations, (ii) preventative policing, and (iii) resource allocation.

While Birkett (1989) first raised the notion of using indexed data from multiple crime scenes, Ribeaux and Margot's work (1999) is regarded as the progenitor of the concept of forensic intelligence. Ribaux and Margot (1999, p 193) aimed 'to show that the study of inferences drawn by investigators during problem solving is a useful approach to analyse how forensic science data should be integrated into criminal intelligence.' Since then, the possibilities of forensic intelligence have been well elucidated: case studies include fingerprint analysis (Anthonioz *et al*, 2002), DNA analysis (Ribaux and Girod, 2003) and drug analysis (Esseiva *et al*, 2007).

Use in contemporary policing

While there has been a strong case made for the value of forensic intelligence, it nevertheless maintains a relatively benign status in policing. In a recent paper, Ribuax et al (2010) found that forensic intelligence needs to be underpinned by a framework connecting forensic science to intelligence-led policing. To derive useful and actionable intelligence, Ribuax et al (2010, p. 15) argue that forensic intelligence should 'result mostly from complex reasoning patterns that globally integrate all sources of relevant information available, including forensic case data, across separate organizations.'

Implementation of Forensic Intelligence

International Context

While the potential contributions of forensic intelligence to police investigations has been identified and expanded upon in the literature, its implementation has been somewhat limited. The most common example of forensic intelligence in practice is the use of DNA and fingerprint databases, which have been implemented in many countries including the United States, New Zealand, Australia, and European Union member states. Although not without controversy, the use of these databases has been arguably successful – in the United Kingdom, for instance, it is estimated that DNA matches link suspects to 15 murders, 45 rapes and 2500 volume crimes in a typical month (Mennell & Shaw, 2006). The concept of forensic intelligence, however, goes well beyond the utility of DNA databases. There appears to be a general lack of understanding on how to move beyond the traditional use of forensic data in individual cases of investigation, and the exploitation of forensic science in a more holistic approach to crime investigation and analysis; as such, forensic data remains, on the whole, poorly integrated within the investigative and crime analysis process (Ribaux *et al*, 2003).

However, there have been attempts to integrate forensic science data with the investigative process, in a manner which is consistent with the concept of forensic intelligence. Ribaux and Margot (2003), for example, have developed a framework for crime analysis in which forensic case data are fully incorporated in the form of a computerised system designed to analyse serial crime. The practical utility of this framework is demonstrated on several cases of volume serial crime, including the identification of a highly probable linked series of radio thefts from vehicles occurring across two jurisdictions in Switzerland, resulting in the solving of over 250 cases. It is in Switzerland where the concept of forensic intelligence has been most successfully implemented and integrated with police investigations involving volume, serial and organised crime such as burglary, vehicle theft, arson, counterfeit watch manufacture and distribution, and illicit drug manufacture and distribution. The United Kingdom has also developed several initiatives, including coded databases of burglary and robbery shoe-marks, and improved retrieval and recording of forensic data from crime scenes; these are initiatives which increase forensic intelligence capabilities.

Australian Context

Within the Australian context, forensic intelligence is not as developed as overseas, nor has its potential been explicitly articulated. However, various databases currently in operation, including the Australian Illicit Drug Data Centre and the Australian Bomb Data Centre - both situated within the Australian Federal Police - indicate that there is the potential and capability to expand both military and policing investigative and crime analysis processes. Furthermore there are several, albeit isolated, indicators of a paradigm shift within investigative approaches. For example, the *Commonwealth Organised Crime Strategic Framework Overview* (2009) states that 'forensic intelligence is vital in order to strengthen the understanding, investigation and responses to organised crime in Australia.' Similarly, the Western Australia *Scientific Investigation Strategy* (2009-2010, p. 6) states that an overarching aim is to 'integrate forensic evidence with crime information and intelligence to link offences and offenders and raise forensic practitioner awareness of the ways forensic evidence contributes to intelligence-driven policing.'

With the shift towards evidence-based practice and intelligence-led policing, these isolated examples seem to indicate a stronger potential role for forensic science, and its integration and utilization that is consistent with the concept of forensic intelligence. Within the Australian context, however, there is a long way to go in terms of theory and practice development.

Issues in Forensic Intelligence

Forensic intelligence offers the prospect of objective, timely and consolidated data on crime. Yet Ribaux *et al* (2010) argue that forensic intelligence needs to be underpinned by a framework that connects forensic science to intelligence-led policing. In the United Kingdom, the use of shared and collaborative databases, such as the Police National Database, augurs a new era of technological sophistication in policing. Indeed, there are calls for 'the need to change the paradigm of forensic evidence as a pure probative exercise to a powerful investigative science' (Esseiva, 2007, p.254). Yet, forensic intelligence poses a number of conceptual and operational challenges. Overcoming these challenges is crucial for its operational utility, and it is here that academia can play a central role, since '[m]anaging the relationship with forensic users and providers, together with academia, will be critical for optimal success' (Mennell and Shaw, 2006, p.12). Ribaux, Walsh and Margot (2005) set out this relationship in the following objective, where the:

> *Forensic science community should seek to find, 'a desirable synergy between forensic science, crime analysis, investigation and other fields related to the study of crime'* (Ribeaux, Walsh, Margot, 2005, p.172).

Below, we summarise the challenges and critiques of forensic intelligence identified in the literature.

1. The concept of forensic intelligence is ambiguous

By their nature, meta-theroretical schemas tend to lack a clear remit, and forensic intelligence shares this weakness. While the concepts of 'forensics' and 'intelligence' separately describe two far-reaching fields of policing, their combination does not bring much more into focus. As the notion remains 'fuzzy' (Ribaux, et al, 2005), it is unlikely to be brought into standard police practice or training.

2. Forensic sciences are seen as a separate culture to investigations

The use of forensics in policing tends to be reactive; that is, forensics are used in response to a crime or crime scene and then used in 'case-building' (Mennell and Shaw, 2006, s9). Whilst there is a clear capacity for forensic intelligence to become a proactive component of policing - such as identifying likely suspects or risk factors - there remains a divide between the forensic and front-line policing cultures. This is partly due to the relatively new use and development of forensic science in resolving cases and it is possible that, over time, forensic data will be used increasingly at a strategic level. Yet, as Esseiva (2007, p. 253) notes, the forensic intelligence approach

'is neither natural to (the) traditional forensic scientist and to law enforcement investigators.' Moreover, the integration of forensic and investigatory fields will generate legal opposition, 'since some in the legal profession insist on a complete independence of science from the investigative process' (Esseiva, 2007, p.253).

3. Forensic data is difficult to standardize and combine

Forensic techniques can elicit swathes of separate scientific data from crime scenes, from DNA, fingerprints, shoeprints, fibers, CCTV analysis, and so on. Although the digitization of data is becoming cheaper and faster, there is a clear imperative to ensure that data collection and collation occurs in a systematic and coordinated manner, 'to ensure the capacity is in place to deliver the changing service needed, and that information and databases are managed to ensure compatibility, consistency and access, through a regulatory framework that sets standards' (Mennell and Shaw 2006, p.12). The concept of forensic intelligence requires that all such data is (a) accessible, (b) standardized, and (c) able to be indexed and cross-referenced. The introduction of the UK's Police National Database is a step towards achieving this end.

4. Forensic science itself is not well-suited to delivering timely intelligence

One of the technical limitations of many forensic processes is the time taken to process and develop concrete forensic data. Although this is changing (with the introduction of rapid mobile DNA testing suites, for example), improvements must be made across a swathe of forensic techniques to improve the timeliness - and utility - of data. Mennell and Shaw (2006, p 10) recommend four key changes to improve forensic data relevance to the investigatory process:

I. More forensic science – largely through changes in the use of forensic science;
II. Much faster forensic science;
III. 'Better' forensic science – that is, extending both the capability of forensic science, and its effectiveness and reliability; and
IV. Cheaper forensic science – in terms of unit costs rather than overall costs.

Case Study: The Use of Forensic Intelligence in Countering Improvised Explosive Devices

The following case study discusses the current employment, and future potential, of forensic intelligence by the military to counter a growing use of improvised explosive devices (IEDs). This case study demonstrates the potential effectiveness of forensic intelligence in countering IED use, as well as highlighting fundamental issues and potential challenges in implementation. IEDs offer many advantages to an insurgent group which is not as technologically advanced or as highly resourced as the force that they are opposing. IEDs are cheap, relatively quick and easy to construct and deploy, and highly amenable to innovation. As such, they are becoming the weapon of choice for insurgent, extremist, and revolutionary groups globally.

In an average month in 2010 - excluding Afghanistan and Iraq 260 IEDs were employed worldwide, whilst in Afghanistan alone, 9 137 IEDs were deployed throughout the entire year; these statistics represent a 19 per cent increase from 2009 (Joint Improvised Explosive Defeat Organisation, 2011). Faced with this increased use, as well as innovation of IEDs, many commentators and stakeholders argue that a revised perspective is required within the military to counter IED use in the long term – from a primary focus on developing methods to protect against IEDs, to an additional focus on identifying the networks and people that employ these devices. Forensic intelligence is uniquely positioned to address this need, and its gradual integration into coalition forces can be observed, although there is still some way to go before its full potential is realised in counteracting the use of IEDs.

Current military initiatives

Coalition forces - including Australia, the United States, the United Kingdom, and Canada - have implemented similar and complementary initiatives to counteract IED use in Afghanistan and Iraq. The Australian Defence Force has formed a counter-IED task force, which includes: weapons technical intelligence capabilities aimed at reporting accurate IED technical information; analysis of forensic evidence; device exploitation; analysis of insurgent tactics, techniques and procedures; and development of counter-measures (Winter, Meiliunas and Bliss, 2008). This process enables the identification of patterns in tactics, techniques and procedures, collection of biometric data, prediction of future IED activity, linking of groups or individuals to particular methods of construction or attack, and ultimately to the targeting of networks that employ IEDs (Winter et al, 2008). The underlying theory of this counter-IED task force is in line with the concept of forensic intelligence. However, the extent to which such a practical implementation is consistent with the principles of the concept is unclear.

Other members of the coalition force in Afghanistan have implemented comparable initiatives. The Canadian government has created a task force that aims to concentrate on the networks that finance, plan and build IEDs, rather than solely focusing on the device itself (Pugliese, 2008). The task force utilises forensic science to gather intelligence on the IED-construction process, with the preference being to disarm the IED rather than destroying it in place, and thereby allowing exploitation of the device for intelligence purposes (Pugliese, 2008). Similarly, the US has implemented a Weapons Technical Intelligence (WTI) program under the umbrella of the Joint Improvised Explosive Device Defeat Organisation (JIEDDO). This program focuses on the collection of forensic and technical intelligence regarding IEDs, facilitating the identification and disruption of networks that employ these devices. According to the JIEDDO Annual Report (2010), thousands of valuable latent fingerprints were recovered from IEDs, enabling biometric matches to people associated with IEDs (2011 Report Update).

Potentials and challenges in implementing forensic science

Winter *et al* (2008) state that the countries that make up the coalition force in the Middle East have similar and complementary weapons technical intelligence capabilities, although the communication capabilities between these separate military forces is not elucidated. Communication and sharing of valuable and useful information, whilst challenging in many instances, is a fundamental principle of forensic intelligence. Indeed, the need to ensure that military operations within

Afghanistan are coordinated and integrated between coalition forces has been identified (Defence Professionals 2010). Communication and information sharing could ensure that identification of networks is carried out in an effective and timely manner, for example, by linking databases to allow the identification of patterns in IED construction and deployment across Afghanistan, as well as linking IED incidents to particular bomb-makers or networks.

The implementation of forensic intelligence in many cases involves a change in perspective or understanding of the role of forensic science. Several stakeholders (e.g. Berg 2010; Moulton 2009) have identified the need to change the prevailing military perspective regarding IEDs. Moulton (2009) argues that current military leaders view IEDs from a conventional war perspective; that is, as impediments to effective maneuver. However, IEDs might be better regarded as a crime scene, and a valuable source of forensic and technical information. Moulton (2009) argues that viewing the IED as a source of forensic data would enable the identification of networks employing these devices, linking them to attacks and thereby ensuring a criminal conviction (which may have the added benefit of bolstering the local judicial system).

Berg (2010) presents a complementary argument, albeit one that is more in line with the concept of forensic intelligence as presented in the literature. Similar to Moulton (2009), Berg (2010) argues that changing the current military approach is crucial to countering IED use, and that collection of biometric and forensic intelligence should focus on threat identification, assessment and methods of neutralisation. Furthermore, Berg (2010) contends that prosecution is a by-product of this process. This is an important principle in forensic intelligence, whereby the collection of forensic intelligence in this context is focused on providing useful information, rather than evidence admissible in court proceedings. Hence Berg (2010) maintains that a shift in the military and legal mindset is crucial to countering IED use in the long term. However, whilst identifying networks should be at the forefront of the military's approach to countering IEDS (and prosecution goals in the background), the two aims are not mutually exclusive (Berg 2010). In fact, there have been more than 400 criminal prosecutions in Iraq based upon forensic intelligence.

In summary, a shift in military perspective is needed in order to effectively prevent IED use in the long term. This shift could involve a change in thinking about the IED as a hindrance to military operations (and therefore must be destroyed) to the idea that it is a valuable tool to be exploited in providing intelligence about the insurgent network. Focusing on the IED as a tool to be exploited will provide greater benefits in the long-term, for example, in neutralising the overarching networks that employ IEDs. This case study demonstrates that the concept of forensic intelligence is consistent with the contemporary goals of coalition forces in Afghanistan and Iraq. If it is implemented explicitly and according to its core principles, it can be a valuable framework within which to counteract IED use in the long-term.

This case study illustrates several important aspects of forensic intelligence, including:

1. The importance of communication and information sharing between personnel, agencies, and even countries;

2. The benefits of forensic intelligence are evident as a long-term strategy, providing viable solutions to military (and policing) problems;

3. The goal of forensic intelligence is to identify patterns in, and links between, data rather than evidence for prosecution (although this could be a by-product); and

4. The implementation of forensic intelligence involves a change in traditional understandings of forensic science (and often in approaches to the military or policing problem itself).

Future Directions in Forensic Intelligence

Quite simply, modern policing is more data rich than ever before and forensic scientists have access to more accurate and sophisticated scientific technology. Yet, it is by no means clear that policing agencies are capable of exploiting the data and technology at their fingertips. A CEPS workshop in October 2011, co-hosted at the Australian National University, with the Australia New Zealand Policing Advisory Agency and University of Technology Sydney, explored a number of the issues and challenges outlined in this briefing paper. Significantly, it was noted that forensic scientists and police agencies would need to undertake a cultural change to effectively integrate forensic intelligence in their day-to-day activities. Nevertheless, there are strong indications that policing agencies are becoming more adept at data analysis and integration. The Queensland Police Service (QPS) is an example of where such cultural change is occurring. QPS have initiated an integrated crime data system, Queensland Police Records and Information Management Exchange (QPRIME). QPRIME synthesizes crime records and data into a single portal that can automatically cross-reference and index crime data. Using the QPRIME system, QPS officers can identify crime trends and hotspots, and share information between agencies more efficiently. Such integrated data systems augur an era of rapid information analysis and sharing. As data analysis techniques become more sophisticated and, importantly, referenced against other forms of intelligence, forensic intelligence is poised to transform the way in which law enforcement agencies target and prevent crime.

References

Anthonioz, A., Aguzzi, A., Girod, A., Egli, N., & Ribaux, O. (2003). 'Potential use of fingerprint in forensic intelligence: Crime scene linking'. *Z Zagadnien Nauk Sadowych-Problems of Forensic Sciences*, *51*, 166–170.

Australian Government. (2009). *Commonwealth Organised Crime Strategic Framework: Overview*. Retrieved from [http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_OrganisedCrime]

Birkett, J. (1989) 'Scientific scene linking.' *Journal of the Forensic Science Society*, 29(4), 271–284.

Berg, E. (2010) *Identifying, tracking and targeting asymmetric threats and their social networks*. Retrieved from [http://authentegrity.com/Library/library1.html]

Defence Professionals. (2010). *UK and US outline strategy for counter-IED operations*. Retrieved from [http://www.defpro.com/daily/details/481/.]

Esseiva, P., Ioset, S., Anglada, F., Gasté, L., Ribaux, O., Margot, P., Gallusser, A., et al. (2007). 'Forensic drug intelligence: an important tool in law enforcement' *Forensic science international*, 167(2-3), 247–254.
Joint Improvised Explosive Defeat Organisation. (2011). Joint Improvised Explosive Defeat Organisation Annual Report. Retrieved from [https://www.jieddo.dod.mil/resources.aspx.]

Mennell, J., & Shaw, I. (2006). 'The Future of Forensic and Crime Scene Science:: Part I. A UK forensic science user and provider perspective.' *Forensic science international*, 157, S7–S12.

Moulton, J. (2009). 'Rethinking IED strategies: From Iraq to Afghanistan.' *Military Review*, 89(4), 26 – 33.

Pugliese (2008) 'Canadians Launch Push Against IEDs in Afghanistan,' *Defence News*, Published: 18 Jun [http://www.defensenews.com/story.php?i=3587952]

Ribaux, O., & Margot, P. (1999). 'Inference structures for crime analysis and intelligence: The example of burglary using forensic science data.' *Forensic Science International*, 100(3), 193–210.

Ribaux, O., Girod, A., Walsh, S. J., Margot, P., Mizrahi, S., & Clivaz, V. (2003). 'Forensic intelligence and crime analysis.' *Law, Probability and Risk*, 2(1), 47.

Ribaux, O., Walsh, S. J., & Margot, P. (2006). 'The contribution of forensic science to crime analysis and investigation: Forensic intelligence.' *Forensic science international*, 156(2-3), 171–181

Ribaux, O., Baylon, A., Roux, C., Delémont, O., Lock, E., Zingg, C., & Margot, P. (2010). 'Intelligence-led crime scene processing. Part I: Forensic intelligence'. *Forensic science international*, 195(1-3), 10–16.

Ribaux, O., Baylon, A., Lock, E., Delémont, O., Roux, C., Zingg, C., & Margot, P. (2010). 'Intelligence-led crime scene processing. Part II: Intelligence and crime scene examination.' *Forensic science international*, 199(1-3), 63–71.

Western Australian Police. (2009) *Scientific Investigation Strategy 2009-2010*. Retrieved from [http://www.police.wa.gov.au/Aboutus/Strategyandplanning/Informingstrategies/tabid/1525/Default.aspx]

Winter, E., Meiliunas, A., & Bliss, S. (2008). 'Countering the improvised explosive devices threat.' *United Service*, 59(3), 9 – 11.

About the Authors

Dr Tim Legrand completed his PhD in Political Science at the University of Birmingham in 2008. His thesis, The Politics and Pathways of Policy Transfer, explored the processes by which policymakers learn from the experiences of their overseas counterparts. This research involved a series of interviews with policy officials in the UK, USA, Canada, and Australia. Tim is currently a Research Fellow of the Centre of Excellence in Policing and Security (CEPS) where he is engaged on an Australian Research Council project looking at Vulnerable Infrastructures and Government Coordination. He is the co-editor of a volume with Allan McConnell on International Perspectives in Emergency Policy (Ashgate, forthcoming).

Prior to joining Griffith University, Tim worked with the UK Home Office, Department of Children, Schools and Families, Ministry of Justice and Department of Health as a specialist policy advisor.

Ms Lauren Vogel graduated from Griffith University in 2009 with a Bachelor of Psychogy with Honours. She started her Doctor of Philosophy through the School of Psychology and CEPS in late 2010. Her Doctoral research is looking at how the perceptions and narratives of women involved in extremism serve to exclude them from political processes around conflict resolution and peacebuilding. She is also involved in a number of research projects at CEPS focusing on intelligence methods and risky people. Lauren has extensive experience working as a Research Assistant at several institutions. Her research interests include peace psychology, feminist international relations, political and revolutionary violence, and terrorism/extremism.

ARC Centre of Excellence in Policing and Security

M10_3.01
Mt Gravatt Campus
170 Kessels Road
NATHAN QLD 4122
Ph: 07 3735 6903
Fax: 07 3735 1033

www.ceps.edu.au

Australian Government
Australian Research Council