The Landscape Of Forensic Intelligence Research

Abstract: Criminology, forensic science and policing scholars have a significant role to play in exploring new developments and directions in modern policing. Yet while the concept of forensic intelligence has caught the attention of a number of policing agencies around the world, it has yet to become a mainstream undertaking. In part this is an artifact of a pragmatic policing culture that only institutes new practices based on demonstrable, research and practice-based effectiveness. Here we seek to draw attention to efforts in the scholarly community to accumulate a body of evidence on the efficacy of forensic intelligence. The article describes the international landscape of research pertaining to the development of forensic intelligence. We outline the key use of digitized, triangulated data on biometrics, scene of crime and illicit substances. In doing so, we draw attention to the challenges remaining for scholars and professionals to further understand and advance the use of forensic intelligence in mainstream policing.

Tim Legrand, The National Security College, The Australian National University: tim.legrand@anu.edu.au

Lauren Vogel, The ARC Centre of Excellence in Policing and Security, Griffith University: l.vogel@griffith.edu.au

Introduction

For a long time now, modern police agencies have dedicated resources to the development and exploitation of intelligence to help better allocate resources and target crime. At its outset, the model of 'intelligence-led policing' was predicated on the ‘soft’ intelligence gained from tip-offs, undercover operations and contacts in the criminal underworld. Yet, in recent years, the ‘hard’ intelligence emanating from forensic science has come of age to offer some powerful prospects for policing strategy. The reward on offer, outlined in more detail below, is that the forensic traces of crime -DNA, fingermarks, ballistics and so on- can be captured, digitized and analysed in sufficient detail to identify, prevent and/or intercept criminal behaviour. For some, forensic intelligence represents a metaphysical exercise asking fundamental questions of the truth and nature of crime[1]. At a more substantive level, Ribaux *et al*[2] describe it as the timely, accurate and usable product of logically processed forensic case data. In any case, wide-reaching transformations in policing, such as that offered by the forensic intelligence model, must satisfy two rather different masters with competing concerns: policing agencies and the public. There are two challenges to address; the demonstration to policing agencies that the model will genuinely tackle crime and an assurance to the public that the privacy rights will remain safeguarded and policing effectiveness enhanced. Research, both scholarly and professional, has a significant role to play in overcoming these challenges. On the first of these, Carole McCartney's article in this special issue addresses the concerns around safeguarding the public interest. In this article, however, we turn our attention to demonstrating the efficacy of the forensic intelligence approach to policing agencies via the scholarly and professional body of evidence-based research. Over the past fifteen years, public sector scholars and professionals have been animated by the notion of evidence-based practice. Popularised in 1997 by the New Labour government in the United Kingdom, the term and its companion injunction on public agencies to pursue a policy model of 'what works' has permeated across modern states, particularly Australia. For policing agencies, the 'what works' approach is manifested in the collaboration between academics and practitioners to generate research-based policing. In this article we present an overview of how this approach has shaped the landscape of forensic intelligence research. Here, our purpose is to draw attention to the diverse benefits offered by the forensic intelligence model.

Here we offer some considerations of research that is pushing forensic frontiers forward as explained by Ribaux et al. presented in this special issue. As this is a field populated by practitioners and academics, we give equal consideration to the theory and practice of forensic intelligence. We begin with a review of the basic building blocks of forensic intelligence; data collection and analysis. The article then provides a brief review of how forensic intelligence has been operationalised here in Australia and overseas. We then offer our view on the trajectory of and challenges for research in forensic intelligence. For the sake of brevity, we limit our scope here to those researchers operating explicitly within the scope of forensic intelligence.

Forensic data in a digital era

Fundamentally, the forensic intelligence model involves the exploitation of two or more linked pieces of forensic information in order to generate a new insight on a crime, pattern of crime or protagonist of crime. While the conceptual elements of the model are furnished in more detail in this special issue by Alastair Ross, here we emphasise two critical components of the model: data completeness and data compounding. Fundamentally, the added value of forensic ‘intelligence’ element is represented by the linkage and triangulation of forensic data and trends enabling the better understanding of phenomena relevant to policing and security. For example, the patterns of the production and consumption of illicit drugs can be estimated through forensic examination of disparate data sources. This might be achieved by combing detailed chemical profiling of seizures of illicit drugs; analysis of precursor substances on the internet; and analysis of wastewater in urban areas. By combining the findings of these analyses, we can enhance our knowledge of the patterns of drug sales and consumption in given areas. Of course, this belies the complexity of what can be achieved by analysis of much larger linked datasets, which can use an array of demographic, temporal, geographic and criminological variables to develop insights into crime patterns, trends and profiles.

Yet the efficacy and utility of forensic intelligence remains beholden to the completeness of data collected and processed by front-line officers and technicians. Of course, forensic information in the policing domain comes in all shapes and sizes, from fingerprints and shoemarks to forensic ballistics, palynology (pollen analysis) and DNA profiling. These represent a diverse range of vectors which –along with broader geographic and demographic information, for example- may be linked between different crimes and, in so doing, build up better knowledge of the crimes/patterns at hand. Thus forensic intelligence is also a compounding analysis. Each additional vector of analysis simultaneously increases both complexity and the clarity of the overall patterns of crime. Linking disparate pieces of forensic information allows analysts to bridge between crime scenes, suspects, modus operandi and time periods. Previously, sufficient data about crimes has been collected, but not properly combined. Indeed, as Ribaux *et al*[2] note, 'it is recurrently discovered retrospectively, that all the information needed was previously in the files and could have been proactively used in order to solve the case earlier' (p.171). In a compounding analysis, every additional unit has the potential to increase the 'reconstruction' of the overall picture, even though there remains the possibility that some data might not be used by the forensic analyst. Suspects can be identified at a much earlier opportunity, allowing for the rapid interdiction –and easier prosecution- of crimes that might otherwise go unchecked.

To acquire complete and compounded data, however, is far from a straightforward task. Bringing together and comparing data provides potentially infinite variables that must be organised to make meaningful sense. Until very recently, this was a task performed manually and the numerous forensic traces gathered at a crime scene would often be analysed just in the context of the crime at hand. The labour-intensive nature of this work meant that crimes tended to be addressed independently of one another. Yet in recent years forensic analysis has been strengthened by two crucial developments: first, the emergence of a range of technologies, from rapid DNA analysis to more sophisticated trace tests; and, second, the era of digitization, which has allowed cross-referencing, rapid storage, search, manipulation and indexing of vast quantities of forensic data. Together, these advances mark a watershed moment in forensic data capture and analysis. It is our view that forensic intelligence, which has existed for some time now, is potentially the natural beneficiary of this watershed.

The systematization and computerization of forensic data

The systematization and computerization of forensic data, as a fundamental pillar of forensic intelligence, constitutes the primary research stream in this area. Broadly, current research is focused on formalizing the forensic intelligence process, with an emerging interest in this body of work aimed towards databases containing biometric data. In an era where television shows depict forensic sciences as a convenient panacea to the most complex of crimes, it would probably come as a surprise to the public at large that forensic analysis is actually a time-consuming and complex process. This is a result of the necessity to ensure that laboratory processes are designed to cater for the evidentiary demands of criminal court cases. Yet processing a crime scene appropriately is a demanding task for police officers and technicians at the best of times and forensic traces might easily be overlooked or go uncollected. Robertson[3], for example, draws attention to the inherent problems of collecting and drawing inferences from DNA and trace evidence at a crime scene. In this context, correctly-collected and processed forensic data is invaluable. In the pre-digital era of policing, forensic data –on fingerprints for example- would be stored and searched manually. The onerous task of associating forensic data with a particular suspect could take weeks, if it occurred at all.

However, in the 1980s the arrival of affordable desktop computing and, crucially, digitized databases, revolutionised data management in policing. For the first time, police agencies could electronically record, store and search details of crimes and criminals. Although crime data collection and analysis has continued to grow in sophistication and complexity, until recently the *scale* of data management has been hindered by the cost of data storage. In recent years, however, data storage costs have dropped dramatically. Since the 1980s, technological development has greatly advanced the size of digital storage while reducing costs. Villasenor[4] calculates that storage costs over the past thirty years has declined by a factor of 10 every decade. Adjusted for inflation, the cost per gigabyte in 1984 was US$85,000, whereas today the per-gigabyte cost stands at around 5 cents (and even that tiny cost is continuing to decline). As these storage barriers have diminished, the opportunities for the 'digitised' forensic intelligence approach have widened to something now approaching a critical mass with the costs of recording and storing data at an almost negligible level.

The digital era has resulted in the mass systematization and computerization of forensic science data. Notwithstanding the controversy of this development, it has undoubtedly led to positive advances in the identification of offenders and, in line with the forensic intelligence model, links within the data and trends in the broader crime milieu. However, it remains important to note that this is merely one tool by which to achieve the aim of forensic intelligence; "the use of forensic case data in an intelligence-led perspective"[12]. The net result of digitisation has been the creation of large national databases containing biometric data on portions of the population. Many countries, including Australia, the United Kingdom, New Zealand and the United States now have such databases. Although not without controversy (see McCartney, this issue) legislative powers relating to the collection and storage of this information has continued to evolve and resulted in the expansion of many of the databases in existence reflecting a confidence in the ability of biometric data to reliably identify offenders and aid in their prosecution. The United Kingdom National DNA database contains data on 7% of the population, the New Zealand National DNA database represents 2.1% of the population, the United States 1.7%[5], and Australia 2.2%. Aside from definitional issues regarding the measurement of database performance and effectiveness[5], when measured purely in terms of hit rates databases generally perform well. Mennell and Shaw[6], for example, report that a typical month in the UK sees suspects matched to 15 murders, 45 rapes and 2500 volume crimes. Gunn[7] reported that in the first seven years of the UK DNA database's existence, the total number of hits was 178,828, including 164,200 person-to-scene and 14,628 scene-to-scene matches.

However, some research indicates that not all databases are equally effective or perform equally as well[8] and the traditional performance measure of hit rates tell us nothing about the key factors that determine either effectiveness or optimal database performance. Empirical research conducted by Simon Walsh and colleagues[5,9] has begun to address this gap in research on database effectiveness and performance. Walsh et al[5] proposed that database performance (or the return index) can be estimated by way of a model incorporating the number of crime-to-person hits and the number of person and crime samples in the database, where a high estimate indicates a high return (maximum number of hits per person and crime sample tested). This model facilitates comparisons of database performance across jurisdictions as it is data independent. Interestingly, it was found that larger sampling regimes generated redundancy in the database over time resulting in a plateauing of returns or outcomes. Thus, this program of research has provided some specific measures that are important when measuring database performance and considering factors that drive optimal database performance, for instance targeted sampling seems to be key in considering optimal database performance.

Databases containing information aside from biometric have also been created in various countries, including those containing earmark, glovemark and toolmark data and ballistics and firearms information. The systematic integration of forensic data such as these with the view to performing link or trend analysis is a fundamental pillar of forensic intelligence and can be facilitated by the use of databases in which this type of forensic information is digitized, stored, and automatically analysed. The use of forensic data in this manner has been elucidated and implemented most extensively in Switzerland where it has been applied to serial volume crime (e.g. burglary, vehicle theft, arson, counterfeit watch manufacture and distribution) as well as serious and organised crime (e.g. illicit drug manufacture and distribution). Since 2008, intelligence units in six states of Switzerland have been involved in the implementation of a common crime intelligence database that integrates forensic case data across these jurisdictions in order to identify links and interpret the crime environment[10]. Data included in the database are DNA, shoemarks, images, fingerprints, earmarks, glovemarks and toolmarks. Rossy et al[10] demonstrated that 37.8% of all series identified within this common crime intelligence database were initially detected by forensic data, primarily DNA, shoemarks and images. In many cases, situational information commonly relied upon in police investigations was unable to identify these links.

Problematically, the current focus on digital data capture would seem to indicate that the creation of databases is the key aim of forensic intelligence or that implementing databases will automatically result in increased capacity to detect and solve crime; however, this is not the case. Firstly, the implementation of large cross-jurisdictional databases is not a blanket solution for all crime problems. De Ceuster et al[8], for example, argue strongly against the implementation of a shared ballistics database within Europe. By contrast, Gagliardi[11] calls for the international sharing of forensic data regarding firearms through the INTERPOL Ballistic Information Network (IBIN) and within the framework of intelligence-led policing. Consistent with other research[5,9,10] De Ceuster et al maintain that the accumulation of samples in the database over time decreases the probability of obtaining true hits or matches. They also argue that most laboratories would not be able to cope with the additional workload necessitated by the analysis and maintenance of the database. In 40% of cases at present, qualified comparison between a gun and bullets or cartridge cases requires manual inspection of either the original sample or copies of it, adding to the workload of laboratory staff as well as generating logistical difficulties. Finally, De Ceuster et al found a limited need or justification for a shared European database. Current shared ballistics databases produced extremely low hits, with the current IBIN system having produced no targeted cross-border hits as of May 2011. Based on statistics from Germany and the Netherlands, it appears that the majority of guns travel less than 100kms before they are either re-used or confiscated. De Ceuster et al concluded that in only 1 out of 20,000 cases would a link be made between crime scenes more than 500 kilometers apart. The extrapolation of these criticisms raised by De Ceuster et al to other databases is unclear; however, it illustrates the need for more research into the effectiveness, applicability and feasibility of databases (particularly those that are cross-jurisdictional) prior to implementation. Furthermore, it highlights the issue raised by Morelato et al[12] with regard to the operationalization of forensic intelligence; that any digital depository of forensic data must be "flexible and continuously updated in order to collectively, truly and timely reflect the criminal activity that is dynamic in nature: (p. 10).

Beyond digitization: Forensic intelligence in a broader context

Whilst computerization and systematization of forensic data are crucial for supporting the inferential reasoning necessary when dealing with a crime environment, the forensic intelligence model is not restricted to these processes.[12]. Essentially the forensic intelligence model, when implemented in practice, involves significant changes and indeed challenges to traditional policing and forensic science paradigms. The forensic intelligence framework is a more holistic approach to crime (including crime prevention, detection, and investigation) in a process that is on-going and not necessarily predicated by a specific crime event. Thus, it is a proactive, rather than reactive, approach to crime management. Inherent within the model of forensic intelligence is the integration or fusion of multiple sources and types of forensic data and investigative intelligence, generally within a digital database but supplemented and augmented by human knowledge and digital analysis.

While digitization offers forensic sciences vastly strengthened analytical capabilities, we should not forget that the forensic intelligence process is constituted by and reliant upon a host of prior decisions made by human operators within the forensic sciences and beyond. Each stage of the forensic intelligence process is shaped by the decisions and actions of individuals, which may strengthen or weaken the intelligence produced by a human-driven forensic analysis. For the sake of practicality, it is not possible to capture all the data that might be relevant to criminological analysis: the analyst must make a host of decisions of relevance, which will inevitably influence the sort of analyses that can occur. For example, human operators must answer the questions such as: What is ‘relevant’ data? What, for practical purposes, can be captured for use in forensic intelligence? What data can be converted into a digital format, and what can be used to contextualize or qualify digital data? The analysis of trends found in datasets is determined by human operators who must interpret and evaluate the significance of any findings. This requires careful qualitative determination about the usefulness of quantitative patterns uncovered in any dataset.

It therefore follows that we should be wary of treating digitised datasets as an end in and of themselves: since all data is selected or ‘filtered’ by operators who have an imperfect knowledge of the world, we might expect, and be wary of, analysis stemming from digital databases to suffer from the same issues that have plagued crime trend data for decades. This is illustrated by some well-understood examples: the empirical focus on *reported* crime might easily overlook patterns of crime in deprived areas that frequently go unreported. Equally, a sudden surge of arrests pertaining to car theft might be the result of a local police crack-down, rather than an upsurge in criminal activity. This has important implications: first, forensic intelligence analysts must maintain a strong awareness of contextual information in assessing crime patterns and trends, and, second, forensic intelligence must therefore accommodate both qualitative and quantitative analysis. Any quest for *objective* forensic intelligence is probably futile, especially since any analytical endeavour is undertaken by individuals who interpret data according to their own understanding of their institutional role, policing objectives, their own experiences of crime, and so on. The qualitative and social components of forensic intelligence are thus embedded in the analysis of data, irrespective of its depth or complexity[12].

Two examples of forensic intelligence in practice

Illicit substance interdiction

Several strands of forensic science-related research demonstrate the increasing capacity of forensic science to meet the practical needs of an intelligence-led policing paradigm. One of these areas of development is in relation to the use of physical or chemical profiling of illicit drugs in an intelligence perspective. In this case, forensic science has moved beyond simply identifying the type of illicit drug to profiling its chemical, organic and physical properties, thus allowing drug networks and trends in manufacture, importation and distribution to be mapped. For instance, drug profiling of organically-based drugs can indicate where the plant was grown and how and where it was processed into usable form whilst examination of manufacturing by-products in synthetic drugs can indicate the synthetic route and precursor chemicals[13]. Research in the area of drug profiling has expanded rapidly in the last decade and includes, for example, applications of drug profiling to intelligence-led policing[14], various methods of profiling drugs including organic and physical characteristics of different types of illicit drugs[15-19], optimal methodologies for comparing and linking different batches of seized illicit drugs[20-22], and the application of organic drug profiling to mapping cultivation patterns and geographic origin[23].

Within the Australian context drug profiling has developed with promise. In 2003, the Australian Illicit Drug Intelligence Program (AIDIP) was initiated, based on the National Heroin Signature Program (NHSP). The AIDIP produces forensic drug intelligence on both chemical and physical characteristics of seized illicit drugs. A database was constructed that allowed the monitoring of trends in relation to: manufacture, importation, and geographical distribution; unusual features of the packaging, and; chemical identity, purity and profile of the illicit drugs – thus facilitating the linkage of seized batches of drugs[13]. Whilst facilitating the monitoring of trends and mapping of networks, the AIDIP also produces actionable information aside from that useful to criminal investigations, for example identification of legitimate industrial chemicals utilised in illicit drug manufacture assists the Australian government in the regulation of these legal chemicals[13]. The AIDIP is the only routine drug profiling program in Australia; however it communicates with similar initiatives in jurisdictions overseas in order to track and compare trends[24]. The AIDIP also facilitates the provision of technical assistance to Australian Federal Police Crime Scene Scientists as well as responses to drug related issues raised by external agencies[24]. The AIDIP primarily analyses samples from Australian Federal Police seizures that, owing to the nature of its responsibilities and casework, are generally seizures at the Australian border and thus the data primarily relates to drugs smuggled into the country. However, in 2009 the Enhanced National Intelligence Picture – Illicit Drugs Project was initiated that, in partnership with state and territory jurisdictions, obtains illicit drug samples from seizures within Australia.

Countering improvised explosive devices (IEDs)

This article has primarily focused on forensic intelligence in the context of modern policing; however developments within the military, although not implemented under the banner of forensic intelligence, are nonetheless noteworthy. For instance, coalition forces, including Australia, the United States, the United Kingdom, and Canada, have implemented similar and complementary initiatives to counter IED use in Afghanistan and Iraq. The Australian Defence Force has formed a counter-IED task force, that 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[25]. 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[25]. Similarly, the US has implemented the 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, enabling the identification and disruption of networks that employ these devices. According to JIEDDO publications and resources[26], the program has been successful in improving the detection and neutralisation of IEDs and in reducing US causalities as a result; however the program remains controversial due to large expenditure, mismanagement, duplication of efforts, a lack of practical effective technology to counter IEDs on the ground, and the lack of an evidence-base for best practice or effective technology as data is not retained that would allow an assessment of what works and what does not. Clearly addressing these concerns is an avenue for future research and practice.

The future of forensic intelligence

Several avenues of research in relation to new technologies and forensic analysis are developing with promise. New and/or improved forensic techniques and capabilities in relation to drug profiling is one such area that has already been outlined in this article. A second example of a promising avenue of research that increases the capacity of forensic science is a program of research conducted by Susan Walsh and colleagues[27-29]. They have developed the IrisPlex system designed to predict blue/brown eye colour based on DNA samples. An accuracy rate of between 91% and 98% was established based on a broad European sample[29]. This work has expanded into the HIrisPlex system that is capable of predicting both hair and eye colour with an accuracy ranging from 69.5% to 87.5% for hair colour in a European sample[28]. The implications of this type of research are significant, whereby forensic science can assist in identifying key characteristics of potential suspects based on biometric data collected from crime scenes. This is illustrative of the advances in forensic technologies, techniques and ability to store digital data that increasingly facilitate the reliable matching of samples, whether it is person to crime scene or crime scene to crime scene[30]. However, new technologies such as this require further evaluation in relation to the utility and effectiveness for policing investigations in order to provide an evidence-base for the most efficient incorporation into policing and forensic science paradigms.

The applicability of forensic intelligence to different types of crime and the most effective methods to implement forensic intelligence in practice are important avenues for future research. Initial research indicates that the forensic intelligence model may be more effective at addressing certain types of criminal behaviour. For instance, it appears that forensic intelligence is particularly useful when applied to serial volume crime where there are identifiable links between crime scenes and to offenders, or organised crime where networks and patterns are able to be mapped and tracked over time, such as in illicit drug manufacture and distribution or even terrorism. Furthermore, the most effective means by which to implement the forensic intelligence model in practice has received less attention in the scholarship. The concept of forensic intelligence, when implemented in practice, often involves a change in traditional understandings of forensic science and in approaches to investigation. Factors such as how to train the personnel responsible for the input of data and the end-user as well as how to ensure efficient and effective means of communication and assessment are important elements of forensic intelligence that have received little research attention. Educational challenges and opportunities in forensic intelligence are discussed in the paper by Crispino et al. in this issue.

As highlighted throughout this article, the concept of forensic intelligence is holistic and multifaceted and clearly goes beyond the implementation of databases. In relation to digitisation and databases, several important observations can be taken from this research. Implementation of a database will not automatically ensure effective use of the data contained within it; this is dependent upon the nature of the database itself, including the information contained within it, and the personnel who maintain it and retrieve data. To this end, bigger databases do not necessarily equate to better databases. As demonstrated in research[5,10] irrelevant samples multiple over time at the same time as the usefulness of relevant samples diminishes. One implication of this is that more research is needed into factors that drive optimal performance of databases, for example Walsh and colleagues[5] have demonstrated that additional measures to hit rates are important in assessing performance of DNA databases; however the applicability of these findings to other types of databases is unknown.

Conclusion

The benefits of digitized, indexed and cross-referenced forensic data offers a transformative approach to, in particular, volume crime and resource allocation and policing strategy. Yet while the organisational rewards are alluring, it is not fully apparent –especially to policing communities- how such benefits will accrue or what kind of organisational change will be required. The forensic intelligence model requires a shift -perhaps a radical one- in the business model of (policing) agencies, which have traditionally evolved incrementally rather than precipitately. It is therefore clear that those engaged in the theory and practice of forensic intelligence must direct their efforts in two directions: first, towards operationalizing an effective framework for the development and use of forensic intelligence and, second, towards spotlighting the successes of the framework to the wider community of policing and forensic practitioners.

1. Chan KW, Tan GH, Wong RC. Looking at forensic intelligence from the metaphysical perspective: Citing illicit heroin profiling as an example. Australian Journal of Forensic Sciences 2012 44(3):227-242.
2. Ribaux O, Walsh SJ, Margot P. The contribution of forensic science to crime analysis and investigation: Forensic intelligence. Forensic Science International 2006;156 171-181.
3. Robertson J. Should forensic science services be independent of policing?: A critical reflection. Current Issues in Criminal Justice 2012;24(1):131-137.
4. Villasenor J. Recording everything: Digital storage as an enabler of authoritarian governments. Centre for Technology Innovation at Brookings; 2011.
5. Walsh SJ, Curran JM, Buckleton JS. Modeling forensic DNA database performance. Journal of Forensic Sciences 2010;55(5):1174-1183.
6. Mennell J, Shaw I. The future of forensic and crime scene science. Part I. A UK forensic science user and provider perspective. Forensic Science International 2006;157:S7-S12.

7. Gunn B. An intelligence-led approach to policing in England and Wales and the impact of developments in forensic science. Australian Journal of Forensic Sciences 2003;35(1):149-160.
8. De Ceuster J, Hermsen R, Mastaglio M, Nennstiel R. A discussion on the usefulness of a shared European ballistic image database. Science and Justice 2012;52:237-242.
9. Walsh SJ, Buckleton JS, Ribaux O, Roux C, Raymond T. Comparing the growth and effectiveness of forensic DNA databases. Forensic Science International: Genetics Supplement Series 2008;1:667-668.
10. Rossy Q, Ioset S, Dessimoz D, Ribaux O. Integrating forensic information in a crime intelligence databases. Forensic Science International 2012.
11. Gagliardi P. Transnational organized crime and gun violence. A case for firearm forensic intelligence sharing. International Review of Law, Computers & Technology 2012;26(1):83-95.
12. Morelato M, Baechler S, Ribaux O, Beavis A, Tahtouh M, Kirkbride P, Roux C, Margot P. Forensic intelligence framework: Part I: Induction of a transversal model by comparing illicit drugs and false identity documents monitoring. Forensic Science International 2014 - in press.
13. Collins M, Huttunen J, Evans I, Robertson J. Illicit drug profiling: the Australian experience. Australian Journal of Forensic Sciences 2007;39(1):25-32.
14. Esseiva P, Ioset S, Anglada F, Gaste Lt, Ribaux O, Margot P, Gallusser A, Biedermann A, Specht Y, Ottinger E. Forensic drug Intelligence: An important tool in law enforcement. Forensic Science International 2007; 167:247-254.
15. Dufey V, Dujourdy L, Besacier F, Chaudron H. A quick and automated method for profiling heroin samples for tactical intelligence purposes. Forensic Science International 2007;169 108-117.
16. Dujourdy L, Besacier F. Headspace profiling of cocaine samples for intelligence purposes. Forensic Science International 2008;179 111-122.
17. Dujourdy L, Dufey V, Besacier F, Miano N, Marquis R, Lock E, Aalberg L, Dieckmann S, Zrcek F, Bozenko Jr JS. Drug intelligence based on organic impurities in illicit MA samples. Forensic Science International 2008;177:153-161.
18. Lociciro S, Hayoz P, Esseiva P, Dujourdy L, Besacier F, Margot P. Cocaine profiling for strategic intelligence purposes, a cross-border project between France and Switzerland. Part I. Optimisation and harmonisation of the profiling methods. Forensic Science International 2007;167:220-228.
19. Milliet Q, Weyermann Cl, Esseiva P. The profiling of MDMA tablets: A study of the combination of physical characteristics and organic impurities as sources of information. Forensic Science International 2009;187 58-65.
20. Bolck A, Weyermann C, Dujourdy L, Esseiva P, Berg Jvd. Different likelihood ratio approaches to evaluate the strength of evidence of MDMA tablet comparisons. Forensic Science International 2009;191 42-51.
21. Esseiva P, Gaste L, Alvarez D, Anglada F. Illicit drug profiling, reflection on statistical comparisons. Forensic Science International 2011;207 27-34.
22. Lociciro S, Esseiva P, Hayoz P, Dujourdy L, Besacier F, Margot P. Cocaine profiling for strategic intelligence, a cross-border project between France and Switzerland. Part II. Validation of the statistical methodology for the profiling of cocaine. Forensic Science International 2008;177 199-206.
23. Hurley JM, West JB, Ehleringer JR. Tracing retail cannabis in the United States: Geographic origin and cultivation patterns. International Journal of Drug Policy 2010;21 222-228.

24. Australian Federal Police. 2012 Australian Illicit Drug Data Centre. Commonwealth of Australia <http://www.afp.gov.au/what-we-do/operational-support/aiddc.aspx>. 20 February 2013.

25. Winter E, Meiliunas A, Bliss S. Countering the improvised explosive devices threat. United Service 2008;59(3):9-11.

26. Joint IED Defeat Organisation. n.d. JIEDDO Information Resources. Joint IED Defeat Organisation <https://www.jieddo.mil/resources.aspx>. 30 November 2012.

27. Walsh S, Lindenbergh A, Zuniga SB, Sijen T, Knijff Pd, Kayser M, Ballantyne KN. Developmental validation of the IrisPlex system: Determination of blue and brown iris colour for forensic intelligence. Forensic Science International: Genetics 2011; 5: 464-471.

28. Walsh S, Liu F, Wollstein A, Kovatsi L, Ralf A, Kosiniak-Kamysz A, Branicki W, Kayser M. The HIrisPlex system for simultaneous prediction of hair and eye colour from DNA. Forensic Science International: Genetics 2012, in press.

29. Walsh S, Wollstein A, Liu F, Chakravarthy U, Rahu M, Seland JH, Soubrane G, Tomazzoli L, Topouzis F, Vingerling JR and others. DNA-based eye colour prediction across Europe with the IrisPlex system. Forensic Science International: Genetics 2012;6:330-340.

30. Julian RD, Kelty SF, Roux C, Woodman P, Robertson J, Davey A, Hayes R, Margot P, Ross A, Sibly H and others. What is the value of forensic science? An overview of the effectiveness of forensic science in the Australian criminal justice system project. Australian Journal of Forensic Sciences 2011;43(4):217-229.