Forensic Science International 250 (2015) 44–52

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

Forensic intelligence framework. Part II: Study of the main generic building blocks and challenges through the examples of illicit drugs and false identity documents monitoring

Simon Baechler [a,b], Marie Morelato [c,*], Olivier Ribaux [a], Alison Beavis [c], Mark Tahtouh [d], K. Paul Kirkbride [c,e], Pierre Esseiva [a], Pierre Margot [a], Claude Roux [c]

[a] Ecole des Sciences Criminelles, Université de Lausanne, 1015 Lausanne, Switzerland
[b] Service forensique, Police neuchâteloise, Rue des poudrières 14, 2006 Neuchâtel, Switzerland
[c] Centre for Forensic Science, University of Technology Sydney, Broadway, NSW, Australia
[d] Forensics, Australian Federal Police, Sydney, NSW, Australia
[e] School of Chemistry and Physics, Flinders University, Bedford Park, South Australia, Australia

ARTICLE INFO

Article history:
Received 1 October 2014
Received in revised form 30 January 2015
Accepted 22 February 2015
Available online 28 February 2015

Keywords:
Forensic science
Comparison process
Organisation and decisions
Model
Integration

ABSTRACT

The development of forensic intelligence relies on the expression of suitable models that better represent the contribution of forensic intelligence in relation to the criminal justice system, policing and security. Such models assist in comparing and evaluating methods and new technologies, provide transparency and foster the development of new applications. Interestingly, strong similarities between two separate projects focusing on specific forensic science areas were recently observed. These observations have led to the induction of a general model (Part I) that could guide the use of any forensic science case data in an intelligence perspective. The present article builds upon this general approach by focusing on decisional and organisational issues. The article investigates the comparison process and evaluation system that lay at the heart of the forensic intelligence framework, advocating scientific decision criteria and a structured but flexible and dynamic architecture. These building blocks are crucial and clearly lay within the expertise of forensic scientists. However, it is only part of the problem. Forensic intelligence includes other blocks with their respective interactions, decision points and tensions (e.g. regarding how to guide detection and how to integrate forensic information with other information). Formalising these blocks identifies many questions and potential answers. Addressing these questions is essential for the progress of the discipline. Such a process requires clarifying the role and place of the forensic scientist within the whole process and their relationship to other stakeholders.

1. Introduction

The fundamental principle of forensic intelligence is that, instead of treating each case individually with the aim of assisting the court (i.e. evidential focus), a multi-case focus and more holistic approach based on the study of crime phenomena should be followed [1,2]. The structured and systematic exploitation of crime traces is essential to produce knowledge that will guide strategic, operational and tactical decisions, in particular in models such as intelligence-led policing [3]. The main objective of such models is to monitor repetitive crimes that are evolving and complex due to their underlying organised nature. However, such clues do not represent the whole crime picture and a collaborative approach is required to provide actionable intelligence to decision makers.

In a previous paper [4], we described the induction process that led to the proposition of a forensic intelligence framework. Not only will the implementation of a general model break barriers between specific fields of study in forensic science and intelligence, but it will also help solve issues that are common across crime and trace types (hence the name 'transversal'). Indeed, a transversal model has the potential to offer a common vocabulary and an integrated framework, and will also assist in defining cross-discipline difficulties. It was observed that fundamental issues were treated in a similar way in two apparently different areas (i.e. illicit drugs and false identity documents). The general framework

* Corresponding author. Tel.: +61 40 535 55 49.
E-mail address: Marie.Morelato@uts.edu.au (M. Morelato).

http://dx.doi.org/10.1016/j.forsciint.2015.02.021
0379-0738/

proposed in Part I [4] is a first significant step towards defining forensic intelligence, situating its role in policing, and exposing the potential opportunities and limitations.

The framework serves as a support for the development, implementation and evaluation of specific intelligence processes. It helps in the making of good and objective decisions about the way to elaborate and implement its particular components (or building blocks) and defining its relations with other information processes in order to maximise its overall efficiency. Part II further develops the general framework by exploring the main generic building blocks presented in Part I. The objective here is to further develop the modelling and generalisation efforts initiated in Part I and to provide illustrations of the potential use and limitations of the transversal model through two independent fields of application, i.e. illicit drugs and false identity documents. This contribution also aims to highlight the outcome of these formalisation efforts, which is to bring together in a common framework a qualitative approach (used to build the framework), quantitative approaches (i.e. metrics, scores, threshold values, error rates) and a Bayesian approach.

Part II proposes scientific and rational criteria useful to properly conceive and operate a forensic intelligence system, and to compare and assess alternatives. Based on these criteria, the paper then explores the decision points that are crucial in defining the process architecture as well as in assisting in making objective decisions in real caseworks. Building blocks related to the comparison process and the evaluation systems are first presented. The development of these particular blocks is mainly driven by forensic science and those blocks work relatively independently from general intelligence and investigative data. This separation is however neither logical nor practical when other building blocks are considered as they concern the many people and organisations that are involved in the whole forensic intelligence process. The reflections regarding these other components or building blocks must thus be seen as shared by all participants collaborating in the overall process.

2. Relevant criteria in conceiving and operating a forensic intelligence system

Forensic intelligence ultimately serves different objectives in a wide variety of operating contexts where decisions are often of a different nature than evidence-based court decisions [5]. Systems implementing the forensic intelligence process must be pragmatic enough to sustain uncertain reasoning while remaining scientifically rigorous and controllable. To cope with these constraints and manage risks of reasoning and acting under potentially false hypotheses, it is argued that a balance must be struck between four general parameters: *credibility*, *integrity*, *timeliness and flexibility* [6–9]. The performance of any forensic intelligence system as well as its building blocks can be assessed using these four parameters regardless of the nature of the trace considered. The notions are defined hereafter:

- *Credibility* depends on the system ability to limit the erroneous positive information it provides. In other words, credibility is related to the reliability of the positive results provided by the system. Credibility is measured through the rate of type I errors (i.e. to consider true a hypothesis that is actually false).
- *Integrity* depends on the system ability to limit the erroneous negative information it provides. In other words, integrity is related to the completeness of the positive results provided by the system (or wholeness, entireness, referring to the Latin origin of the word *integrity*). Integrity is measured through the rate of type II errors (i.e. to consider false a hypothesis that is actually true).
- *Timeliness* is associated with the system ability to provide information that can be used by decision-makers in a timely fashion. Time is critical when analysing criminal activity. Ideally, in order to be useful, the analysis response should be compatible with the rapid evolution of the phenomenon of interest [10]. Indeed, relevant information obtained at the wrong time would not only be useless but might be detrimental to the efficiency of further actions [11].
- *Flexibility* is the ability of the system to adapt to and account for the different contexts in which forensic intelligence may be applied [12]. The crime environment is dynamic and evolves rapidly. As a consequence, there is no universal system configuration that is adequate in every situation and flexibility is a key parameter of any evaluation system.

Flexibility and timeliness should both be maximised to provide actionable intelligence. In contrast, credibility and integrity cannot be maximised simultaneously since they evolve in opposite directions. For instance, a system that achieves high credibility but low integrity provides truthful but incomplete results, while a system that achieves low credibility and high integrity provides comprehensive but unreliable results. When considering the ability of the system to detect links among forensic case data, integrity is connected to the well-known risk of *linkage blindness* [13] while credibility is connected to the risk of detecting links that are actually absent. It is hypothesised that the credibility and integrity of the system are the driving factors for decision-making in performing any forensic intelligence task. Any selection of a metric or of an evaluation system, any queries in a database or any risk assessment are based on these criteria to balance the decision in order to fit the results to the expectations of operators. Finding the optimal trade-off between these criteria and the operational needs is a constant challenge for forensic scientist and intelligence analysts.

The following sections present the integration and role of the above criteria in regards to the different building blocks of the forensic intelligence process.

3. Comparison process: iterative selection of the ‘best’ metric

Once the features to be profiled are selected and extracted from specimens collected (see Section 5.2), a process of comparing profiles and measuring their similarity must be selected [14]. Contrary to a common misconception, this choice, or decision point, is not only important when conceiving the system, but also arises each time the system is used. In fact, the choice of the best comparison process depends on the operator objectives and the kind of problem at stake, which may vary according to the context within which the forensic intelligence process is operated (see Section 6). Thus, the system must enable a flexible and dynamic selection of solutions to compare profiles and measure their similarity.

Metrics are the generic solution for the comparison process irrespective of the nature of the trace (i.e. visual, physical, chemical or even digital). A metric is defined as “*a transformation that adds a new layer of information since it starts with entities (*i.e. *profiles) and concludes with a measurement describing the degree of relationship between entities (*i.e. *scores)*” [4]. They are used to compare and measure the (dis)similarity between specimens. They have the critical advantage of relying on explicit, transparent and verifiable rules. They can be used with both quantitative and qualitative data, as demonstrated in previous work [15,16]. Furthermore, metrics can be seamlessly integrated with additional statistical methods commonly used to manage and process big datasets typically