5

Forensic Intelligence and Traceology in Digitalised Environments: The Detection and Analysis of Crime Patterns to Inform Practice

Olivier Ribaux, Simon Baechler, and Quentin Rossy

Abstract Different data processing methods can support the detection and analysis of various forms of crime patterns. The authors document the influence and role of forensic science and how this has been transformed by digitalization. Forensic intelligence is key and they illustrate their argument of its potential by discussing two new forensic intelligence systems and their underlying digital infrastructure, one facilitating the forensic comparison of fraudulent ID documents (ProFID) and the other the monitoring of online frauds (PICSEL).

Introduction: Forensic Science and Security

Since the 1970s a range of innovative policing practices have been developed under the umbrella of different proactive policing models which have been defined as, *All policing strategies that have as one of their goals the prevention or reduction of crime and disorder and that are not reactive in terms of focussing primarily on uncovering ongoing crime or on investigating or responding to crimes once they have occurred* (Weisburd and Majmundar 2018, p. 1).

O. Ribaux (✉) • S. Baechler • Q. Rossy
Ecole des Sciences Criminelles, University of Lausanne, Lausanne, Switzerland
e-mail: olivier.ribaux@unil.ch; simon.baechler@unil.ch; quentin.rossy@unil.ch

M. Gill (ed.), *The Handbook of Security*, https://doi.org/10.1007/978-3-030-91735-7_5

This definition provides a useful framework for situating forensic science. At first glance, forensic science clearly positions itself outside proactive models, by limiting its contribution to responding to crimes once they have occurred. It focusses on providing services to the criminal justice system and assisting in the management of scientific information in investigative processes and court proceedings. It is implemented through forensic science laboratories, borrows methods and techniques from the natural and physical sciences (e.g. chemistry, biology, biochemistry, physics), and translates the analytical results obtained in a way that makes sense to a court of law.

Biased scientific expertise provided in specific high-profile cases has given rise to the general idea that the way forensic science is implemented contributes to miscarriages of justice (NAS 2009). The forensic science community has been urged by the legal profession to focus on the scientific substance of the results it provides to assist courts in making better decisions.

Currently, the process of digitalisation has added a layer of complexity to forensic science and the way it is used (Pollitt 2010). The extended traceability of human behaviour in the digital world has gradually brought digital forensic scientists to the centre of many investigations, at the expense of traditional crime investigators.

Others within the criminological movement have questioned the value of forensic science (Doleac 2016; Julian et al. 2011; Wilson et al. 2011), but such evaluations have been partial in their coverage, typically measuring only specific elements of processes that are inherently multidisciplinary and intertwined.

For example, some have focussed on the direct value of DNA processes and databases, which are often considered the flagships of the discipline. These studies have mainly assessed a number of detections: in how many cases has a DNA profile extracted from a biological trace at a crime scene have been linked to a person's DNA profile by the DNA database, possibly leading to prosecution (Brown and Ross 2012; Brown et al. 2014). The findings from these evaluations dampened the initial enthusiasm for DNA and associated databases because they appeared to contribute to solving a very small percentage of both serious crimes (Brodeur 2008) and high volume crimes (Amankwaa and McCartney 2019; Brown and Ross 2012).

Studies to measure the effectiveness of databases in aiding policing are much more difficult to design than those which focus solely on crime detection (e.g. crime reduction). It is even questionable whether such evaluations make sense in the absence of a framework that would allow a broader set of contributions to be clearly expressed and isolated (Amankwaa and McCartney 2019; Doleac 2016; Ribaux et al. 2017; Wilson et al. 2011). This observation

extends to other areas of forensic science as it is difficult to accurately measure the added value of each forensic process and technology implemented independent of the other factors that may contribute to an outcome (De Ceuster et al. 2012).

Therefore, it makes sense to step back from the standard reactive model used to express the value of forensic science in policing (Ribaux et al. 2017). While early research recognised significant potential for forensic science to contribute to solving repetitive and high volume crimes (Tilley and Ford 1996), it has emerged that most organisations fail to effectively integrate different elements of forensic science into emerging proactive policing processes.

The concept of forensic intelligence (Ribaux et al. 2006) assumes that, beyond the basic function of explaining a single event from the past, forensic information also contributes to detecting crime patterns and generally supports a more comprehensive analysis of crime for supporting proactive policing.

Furthermore, in the age of digitalisation, we argue that a trace-based (forensic) crime analysis model, which we discuss in this chapter, can take a central role in proactive policing. This model takes into account the strong interactions between criminal (or unusual) activities and the substrate (physical, IT infrastructures) on which they take place. The resulting traceability changes the nature of crime analysis. In particular, it exponentially increases the volume and variety of traces available indicating human behaviours, and, consequently, demand more focus on the protection of fundamental freedoms and privacy.

This chapter begins with a definition of forensic science based on the concept of the *trace* (Margot 2014) providing the foundation of the model we outline. Then, we use three concrete operational systems to demonstrate how the information conveyed by the trace can merge with other pieces of information to improve crime analysis in proactive models. All three systems have been previously implemented in different Swiss jurisdictions. They result from multiple forensic intelligence research projects initiated at the School of Criminal Justice of the University of Lausanne involving close collaboration between academia and the professional field. All the systems presented are integrated and managed by the police organisations involved. The first system covers high volume crimes. The second focusses on a new forensic methodology that processes physical and digital features of fraudulent identity and travel documents to reveal the activity of serial forgers and criminal networks. The third is a recently initiated crime analysis system for online fraud that highlights the progress being made by digital techniques in informing crime analysis.

Forensic Science, Traceology and Crime Analysis

Forensic science consists of detecting, observing, measuring and interpreting *traces* resulting from unusual events. In this context, 'unusual' denotes harmful disruptions to the regular course of events and primarily involves human activities that violate a law or rule. In terms of security, socially deviant behaviours, as well as natural and technical phenomena that cause damage and destabilise a community, are also part of the events of interest. For example, explaining the cause of a fire (natural, technical or human) from debris is a central forensic activity.

The forensic *trace* is the result of an analogue or digital change in a physical or virtual environment caused by these kinds of events. It can be material (e.g. a shoeprint, an object, a sound) or immaterial (e.g. a change produced by inappropriate use of a computer program) (Pollitt et al. 2018).

According to (Margot 2014), important characteristics of the forensic trace include the following: (1) its existence is independent of an observer; (2) it comes from a singular event in the past that can neither be reproduced nor reconstructed with certainty; (3) when caused by human activity, it has generally been unintentionally created or transferred; (4) it is imperfect in nature (fragmentary, degraded), and the imprecision of its measurement depends on the reliability and accuracy of the instruments and the quality of observations made; (5) the representativeness of the traces detected among the traces actually created by the event is unknown; (6) it is a sign of a presence of an object/a person or a sign of an activity/event.

The term 'trace evidence', which is often used to refer to the treatment of minute amounts of fibre, glass or paint chips, is particularly misleading. The association of minute quantities of materials with trace evidence is based on chemical definitions that are not adequate for forensic purposes. In our definition, a trace is a physical or digital remnant of an unusual event, regardless of its size or shape. In addition, most of the traces recovered from crime scenes are never interpreted as evidence in the context of a court trial. The information traces conveyed are typically used in other investigative processes or for providing knowledge about the mechanisms underlying events of interest (e.g. modus operandi, chronologies or links between events and crimes).

The totality of traces linked to an event help to provide answers to quintilian questions of who, when, where, what, how, with what, and can occasionally explain why. Deciphering these traces therefore belongs to a logical process of reconstruction to find the best possible explanations for the traces collected (see Fig. 5.1).

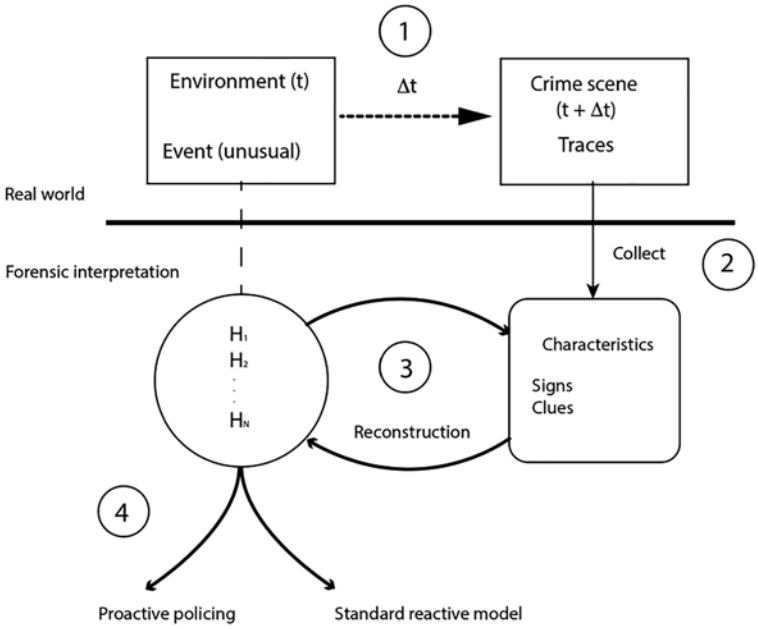

Fig. 5.1 (1) unusual events cause traces. (2) Resulting traces are collected when the crime scene is investigated. (3) Explanations are sought (reconstruction). (4) Conclusions feed the standard process (legal characterisation of an activity) or proactive policing models (actionable knowledge about the unusual event)

This process of interpretation is at the heart of forensic methodology. It works in cycles by imagining possible explanations (hypotheses) for the traces collected and then testing them through experimentation or further observation (hypothetico-deductive).

The volume and diversity of these traces increase dramatically when the traceability of human activities in the physical world is added to the traceability resulting from the use of information and communication infrastructures. This radically changes the relative importance of the data to be processed in criminal investigations but also impacts all forms of understanding of crime, behaviour and the events that cause harm.

Traceology is forensic science that focusses on traces. As such, it belongs to the family of historical sciences which help to explain singular past events (Cleland 2011). However, it also feeds more inductive processes (generalisation) that generate knowledge and models that enable proactivity. The use of the term 'traceology' carves a new space for forensic science beyond its legal conception, that could become the cornerstone that underpins many

processes in criminal investigation, crime analysis, law enforcement and various fields of criminology more generally.

To illustrate this perspective, three different concrete systems of trace-based crime analysis integrating new digital aspects are presented. Their architecture is generic, but the framework on which they were developed, the Swiss police system, was of great importance in determining their current state.

These example systems are implemented in a police environment, but this approach based on traceability goes far beyond the police. The approach can provide a basis for dealing with a wide variety of security-related problems in many other areas covered by private or public actors (Rossy et al. 2018).

Context of the Three Projects: Decentralised Forensic Activities

Switzerland is a small federal country in the centre of Europe that is not easy to manage in terms of security. It is composed of more than 30 police organisations of different sizes, each with a high degree of autonomy in policing. Citizens speak four different official languages, as well as numerous dialects. Most forensic activities are integrated into the 26 states' police organisations (Ribaux 2019).

This high degree of decentralisation has methodological consequences and means that relatively small, non-specialised units covering both crime scene investigations and basic laboratory functions have a major influence on police work; this contrasts with the more centralised forensic laboratory models implemented in many other countries that offer more specialised services and radically changes the way traces are used in the daily work of the police. On the one hand, this approach offers more flexibility in the use of traces. On the other hand, such a structure makes it more difficult to harmonise the processing and exchange of information between jurisdictions. This becomes relevant when considering the following three trace-based crime analysis systems.

System 1: Physical Traces and the Analysis of High Volume Crimes

In the early 1990s, the police felt that the collapse of the Berlin Wall had changed something in the structure of crime in Central Europe (Gerber and Killias 2003). More transnational crimes were emerging, and victimisation

surveys clearly showed that, slightly out of step with other Western countries than Switzerland, house burglaries and other thefts had doubled in less than a decade (Killias et al. 2007).

Due to the fragmented nature of the police crime recording system, it was difficult to obtain an accurate picture of these developments. This difficulty was the catalyst for six police forces in Western Switzerland, covering a population of 2.5 million people, to regionalise their crime analysis system. Traditional crime analysis models (Clarke and Eck 2005) were progressively integrated with forensic intelligence practices borrowed from the UK (Birkett 1989).

As with early versions of intelligence-led policing (Ratcliffe 2016), the original idea was to target prolific offenders and coordinate investigations of them, such as by detecting and analysing the activity of a single offender or group of offenders and avoiding separate investigations where cases could be linked. This approach has led to many investigative leads that have ultimately resulted in the identification, location and arrest of multiple offenders.

This crime analysis and forensic intelligence service quickly went far beyond simply providing investigative support. It currently operates a shared database named PICAR,[1] which has gradually become a hub covering many forms of repetitive crime, such as violent and sexual offences, arsons and computer-based serial crimes. These approaches enable the crime analysis and forensic intelligence service to play a broader role in proactive strategies, for example, by orienting police patrols or proposing other types of measures (crime disruption and prevention).

Many local incidents are detected quickly due to the numerous opportunities for exchanging information between forensic scientists themselves or investigators (e.g. various meetings or more informal exchanges). Series of offences that cross jurisdictions, or which present less common modus operandi characteristics, were found to be more likely to be discovered through systematic comparisons of the traces collected. Similarities between these characteristics sometimes indicate repeat activity by the same offender(s), without necessarily indicating who the offenders are. Initially, the traces used were mainly shoe, tool, glove and ear marks (Ribaux et al. 2003), although this has been extended over time to include DNA profiles (through a national database), CCTV images from various contexts and other digital traces.

Trace analysis informs the crime analysis process by systematically linking crimes and interpreting modus operandi. Conversely, crime analysis informs crime scene interventions by providing a consolidated view of the crime environment, patterns, situational elements and modus operandi (Ressnikoff et al. 2015).

Case Study

Links provided by the Swiss centralised DNA databases led to the detection of a particularly interesting pattern. The same DNA profile coming from biological traces collected from separate burglaries indicated that the same offender was present in two periods separated by two years. A very simple geographical analysis of those cases showed a common characteristic: they were aligned but dispersed all along the Swiss border with France and Germany. The existence of this previously unknown pattern was confirmed by other sources of data (e.g. shoe marks, other DNA profiles, comparison of modus operandi, etc.). The analysis of the available information was further examined along two different axes. Firstly, the analysis of the immediate physical and social environment of the dwellings and factories led to many prevention initiatives being started and better coordinated. Secondly, from an investigative perspective, these collective approaches led to the discovery that a group of international criminals specialising in this type of burglary were responsible.

Results in Numbers

It is inherently difficult—if not impossible—to measure the effects of such a system on crime reduction or its benefits to public perception of security (Boba Santos 2014). The whole methodology, as well as its associated computerised system (PICAR), have developed and evolved over time. The structure of crime has also changed during the same period.

Rossy et al. (2013) undertook a statistical overview of different crime activities supposed to be perpetrated by a single offender or multiple co-offenders from 2009 to 2011. At that time, half of the series detected (i.e. two or more linked cases) were cross-jurisdictional; this confirmed the high degree of mobility of thieves and fraudsters, which contrasted somewhat with the common notion that offenders were more local. One third of the crime series were detected by traces (i.e. traces constituted the first link detected), mainly shoe marks, DNA profiles and images (e.g. extracted from CCTV). These series ranged from two related cases to over 100 cases. The number of crime series detected was relatively high (e.g. 22% of robberies were considered to be part of a series). However, the crime analysis and forensic intelligence system did not allow the detection of all crimes in the series and probably yielded much lower figures than the actual concentration of these crimes.

More recent research indicates some positive evolutions of this trace-based crime analysis system.[2] The six states that joined forces, like many countries, are experiencing a marked decrease in high volume crime, undergoing an approximately 60% drop in dwelling and shop burglaries since 2011, with about 10,000 cases recorded in the region by 2019. Approximately 2500 crime series (from two cases linked up to several hundred cases linked) were detected in 2019, with 30% of the repeats detected through the use of traces (314 by shoe marks, 221 by images, 120 by DNA and 13 by various traces). Half of the crime repetitions or series detected covered more than one jurisdiction. Interestingly, traces can provide links even to extremely temporally and spatially distant cases. The progression over the last 10 years is striking, especially when looking at CCTV images, which help detect more repeats than the comparison of DNA profiles extracted from biological traces, identifying four times more repetitions than nine years ago even while the number of cases has more than halved. This efficiency can be interpreted as a consequence of a much more systematic use of the methodology, relevant collection and processing of information from the crime scene to the crime analysis department, and the effects of digitalisation through the increasing use of CCTV and other images.

System 2: Forensic Document Examination and the Analysis of Identity Frauds

A totally different type of concentration of crime can be deciphered using a similar trace-based approach, namely the manufacture, distribution and use of fraudulent identity and travel documents (Baechler and Margot 2016). A false identity can be a powerful crime enabler, used in contexts ranging from petty crimes (e.g. obtaining a service) to the most organised and threatening offences (e.g. human trafficking, serious fraud or terrorism; Europol, 2017). Fraudulent documents can be used to deceive various stakeholders in many situations both in the public sector (i.e. to cross a border, identify yourself during a police check, register with an administration to access welfare) and the private sector (i.e. to board a plane, open a bank account, rent a vehicle).

In a standard law enforcement model, when a fraudulent identity document is found, it is confiscated and the holder is charged with a specific crime. The false document is then destroyed or archived with the offender's file. Each fraudulent document, however, has another use in that it conveys information about its manufacturing process. Compared systematically with other seized

documents using forensic methods, one can detect the repetition of a modus operandi, revealing the 'trademark' of a forger or of a criminal network (e.g. a combination of repeated printing defects or spelling errors in the texts). Such information has significant value in terms of intelligence from strategic to operational levels (Baechler and Margot 2016).

Given the value of analysing documents, a trace-based method was developed to process, manage and systematically compare features of fraudulent identity documents and is now implemented in the same region within the same legal framework as PICAR (system 1 described in the section above).

The development of the trace-based method started in 2007 and rapidly became a PhD research project (Baechler 2015). Beyond the methodology itself, a prototype, in the form of a basic database named ProFID (standing for Profiling Fraudulent ID documents) was quickly developed. Gradually, new functionalities and improvements made it possible to focus on the most promising characteristics of the documents. The database saves time on tasks such as data entry or comparisons of documents (e.g. automatic image processing) and facilitates the use of a computer vision-based classification algorithm. Profiling digital images of documents has enabled the transition from processing physical traces only (observations of documents themselves) to combining physical and digitised traces. The detected repetitions, also called series, provide insights regarding how forgers and criminal networks operate.

Beyond assisting investigations and crime analysis efforts, the transversal analysis of series and their associated patterns provides guidance to (1) law enforcement agencies and private sector stakeholders in targeting the search for fraudulent documents in the field (e.g. at the border, during police checks, at the counter of a bank, at the gate of an airport), (2) the security document industry on how to design more secure documents.

The full integration of the methodology and the ProFID system into an appropriate, intelligence-led process remains a challenge. One of the reasons for this difficulty is that document fraud is an enabler of multiple forms of crimes and deviant behaviours that may fall within the competence of separated units, agencies and organisations, both public and private. It is therefore technically as well as administratively challenging to create a sufficiently fluid process that crosses these organisational barriers. This is a characteristic example of (1) the tension between the traditional law enforcement model imposing a siloed organisational structure and proactive policing models that require a more transversal and multidisciplinary approach, and (2) the lack of workable models for partnerships between the state and private sectors.

Case Study

Thanks to the trace-based ProFID system, a dozen counterfeit drivers' licenses from Country A were linked based on the detection of similar features, despite the fact that the cases were scattered across all the states of Western Switzerland and the documents seized under various circumstances. In some cases, people holding the fraudulent documents had caused car accidents with severe consequences. The trace-based profiling pointed first to a common manufacturing origin and then to the activity of an organised group of offenders. The counterfeit drivers' licenses were all held by nationals of Country B, a foreign country. The investigation revealed that they met the fraudulent documents providers during integration language classes.

This result was a surprise to law enforcement agencies as well as government departments since false documents from Country A had never appeared to be a problem before, and nationals from Country B were not regarded as likely offenders. Beyond a joint investigation aimed at dismantling the network, preventive measures have been proposed. They aim to both deter nationals of Country B from resorting to document fraud as well as to enable police and administrative personnel to further improve the detection of fraudulent documents. Quickly, the series was stopped. Thus, the trace-based crime analysis approach had an impact not only on crime detection but also on road safety. It also might have helped to deter other potential offenders.

Results in Numbers

From April 2017 to February 2021, 2400 fraudulent documents were entered into the ProFID database by police forces from eight different Swiss states as well as the federal police. Of these, 50% of the documents were linked and grouped into 178 series. The largest series consists of 160 documents. Interestingly, even based on this limited dataset and region, these results indicate a high concentration of fraudulent document production. The use of the methodology resulted in the initiation of several international investigations of high-profile forms of crime, shedding light on transnational organised groups the presence and scope of which were not previously recognised. An exploratory study on the use of the ProFID system at the international level revealed promising results, with links detected for about 20% of fraudulent documents seized by law enforcement agencies from two different countries. Based on those results, several organisations are now considering deploying the ProFID system at the European and international levels.

System 3: Internet Traces and the Analysis of High Volume Online Crimes

The size, extent and evolution of online fraud have recently been made visible through higher victimisation rates across countries (Reep-van den Bergh and Junger 2018). Some may argue that the police should not conduct a crime analysis project in this digital area. Rather, the task might be left to actors in online private security such as e-commerce platforms or other online service providers.

The hypothesis that private companies are supposed to analyse online crime is supported by at least three arguments. (1) Online crime analysis is supposedly carried out through publicly available reporting infrastructures, such as Action Fraud in the UK (Levi et al. 2017). These platforms are generally not operated by the police, which results in the increased fragmentation of relevant data. (2) Cybercrimes are global; local or regional police thus have a limited role to play. (3) These offences are closely related to cybersecurity issues and cyber-risks. Countries have put comprehensive models in place and built new structures to address these risks focussing on protecting their infrastructure, increasing their resilience and responding to incidents (CMM 2016). The police seem to have only a subsidiary role to play in this new landscape.

Nevertheless, these arguments present valid reasons for greater police involvement. Firstly, the police cannot be uninformed regarding what accounts for approximately half of the crimes committed. They must more fully understand their own data, even if it is only representative of what is reported to the police. A virtuous circle can result given that better recording and analysis increases knowledge about the harm caused and improves contact with the public, which will be more inclined to report crimes. Crime analysis can then indicate new proactive ways to disrupt certain crime mechanisms, reduce harm, orient priorities in investigations, develop new forms of prevention and open channels of communication with institutional and private partners as well as the public. Secondly, online frauds can take advantage of vulnerabilities specific to local systems or routine activities (Leukfeldt et al. 2019). Online crime analysis must thus be performed at all geographical levels covered by the different police. Thirdly, early cybersecurity models incorporated forensic and investigative considerations (Kent et al. 2006), but in an incidental way that failed to take full advantage of police and forensic experience on conducting investigations and the knowledge gained through in-depth and detailed analysis of individual cases (Casey and Nikkel 2020).

Finally, private companies can only monitor threats to their own or their customers' assets, which prevents them from seeing the full extent of the problems. The police force is in the best position to fill this gap.

The third system of trace-based crime analysis was developed in the same geographical territory using the same agreement and legal basis between the state police forces as the systems presented above (Rossy and Ribaux 2020). The need to establish an adequate intelligence process to handle online fraud involves the entire organisation in all levels, from the field officer, who may have difficulty recognising the problems when registering complaints, to management, which needs an overall vision to define adequate strategies. A process has therefore been put in place to train field officers to identify the main online crime phenomena that even victims sometimes barely understand. Current processes and most existing classification systems are inadequate for this purpose. Thus, a very simplified classification system has been developed that makes it possible to recognise the main types of online fraud. Experience has shown that a complaint report must be quick to compile and easy to understand to initiate a virtuous circle aimed at gradually increasing knowledge of the types of frauds.

Reports are then monitored by crime analysts to detect and analyse series and trends. They provide relevant and timely intelligence for different levels of the organisation as well as establish a dialogue with partners. Indeed, the process not only aims to identify suspects but may also lead to proactive measures in collaboration with private companies, as illustrated in the case study below.

The translation of this methodology into a computerised system is still in the early stages. A very simple database named PICSEL[3] was developed to gather and codify this information, most of which is based on Internet traces. Many difficulties still need to be overcome, but encouraging results thus far include increased awareness and knowledge throughout the organisation, better communication with the public and with other relevant communities, a shift towards a more proactive attitude, and changes in priorities.

The detection of crime repetitions in the database has various objectives. For example, targeted public information campaigns can be established when an emerging problem is detected. Strategies to disrupt crime by shutting down illegal websites or accounts operated on online platforms are increasingly being used. Crime analysis also provides guidance in more traditional police investigations. Moreover, the detection of cross-jurisdictional series helps to regroup cases, concentrate efforts and limit parallel (and occasionally contradictory) initiatives between the state's different police bodies in dealing with the same problem.

Case Study

The centralisation of cases at the regional level led to the detection of a significant number of cases of online shopping frauds (coupled with well-known advance fees schemes) from the same e-commerce platform. Contacts were made between the police and the platform's anti-fraud department in order to alert them to cases that had passed through their existing detection filters. A global analysis of the cases allowed the police to reconstruct the simple but surprisingly clever modus operandi deployed by the fraudsters. The offenders initially created ads with legitimate content that passed through the automatic filter. In a second step, they modified the ads to match their fraud scenario (e.g. a hot-product sold at a discounted price). When the ad was modified, the fraud filter did not check again, thereby allowing the ads to reach their target. Once the modus operandi was reconstructed, the filtering process was updated, and suspicious ads and accounts were deleted. The impact was immediate. The number of cases reported to the police about the platform was reduced by three quarters, without observing any obvious displacement to another online platform. In this example, police strategies were not oriented towards case detection but towards disrupting the offenders via a hardening of the environment to reduce opportunities.

Results in Numbers

A preliminary study based on the cases registered by one state police service was conducted in 2018 (Rossy and Ribaux 2020). In 2020, the PICSEL database was still in a pilot phase, but used by eight police organisations. From January 2019 to September 2020, approximately 7500 cases were registered by analysts. More than 85% were frauds, two thirds of which were related to e-commerce. Basic digital traces such as emails, accounts and ads from e-commerce platforms, social media profiles and other suspicious website URLs are systematically collected. Although the process is in its early stages, many links have been found by analysing information indicating identities extracted from these Internet traces. Globally, around 6000 pseudonyms, 4100 email addresses, 2700 phone numbers, 2700 bank accounts, 900 IP addresses, 700 URLs and 200 cryptocurrency wallets were registered. Of these, 360 clusters of cases (from two to more than 1000 linked cases), that is 62% of the total, were detected. Two thirds of the crime repetitions detected covered more than one jurisdiction. Around 100 series were registered by the analysts based on the detected links, and at least one fifth led to a criminal

investigation. Moreover, multiple crime prevention messages were disseminated to online platforms, targeted companies.

Conclusion

Forensic science has much to offer proactive policing, and much of the potential benefit has yet to be capitalised on. Traceology, as defined in this chapter, feeds inductive processes that create knowledge and models about numerous crime mechanisms and their environments. Digital transformations of crime and the related expansion of human traceability should make this approach much more central in policing. It could even become the cornerstone that underpins many processes in proactive policing models as well as creates a clear link between crime analysis and the investigation of serial crimes. To illustrate these perspectives, three different concrete systems of trace-based crime analysis model were presented.

These systems and their underlying methodology and deployment environments are oriented towards the transition to proactive policing models. It is evident that policing in a digital age goes far beyond the development of computerised systems. A whole methodology must be elaborated to gather and analyse information in a transversal way to ensure the translation of analysis results into a rational set of measures and to monitor their effectiveness. Traceology can foster cross-sectional crime analysis that overcomes the fragmentation implied by the standard model of policing and its organisational structures. In this increasingly digital landscape, the police remain a central actor with practical experience that is still not captured well in the cybersecurity models used by many stakeholders. Efforts to better express traceology and its potential in proactive policing models aim to facilitate such an integration.

Recommended Readings

To expand the debate around criticism of forensic science in the standard model, the report of the National Academy of Sciences in the US (NAS 2009) and the President's Council of Advisors on Science and Technology's report (PCAST 2016) are basic texts. Comments placing traceology at the forefront of the debate can be found in Margot (2011) or Roux et al. (2012).

A working group within the US Organization of Scientific Area Committees for Forensic Science (OSAC) has published a report that proposes an

integration of digital forensics with forensic science on the basis of the concept of trace (Pollitt et al. 2018). This report lays the groundwork for a new framework in which human digital traceability can be integrated with policing issues (Casey and Nikkel 2020; Casey et al. 2018).

The various contributions in Fraser's and William's *Handbook of Forensic Science* (Fraser and Williams 2009) express the complexity of the use of traces in investigations. This complexity is also reflected in the series of works that emerged from an ambitious project in Australia led by Julian et al. (2011) on the effectiveness of forensic science.

By putting forensic science and proactive policing into perspective, Williams' contribution (Williams 2007) complements Tilley and Ford's initial study (Tilley and Ford 1996). Frameworks for the integration of forensic science with crime analysis were outlined in a series of papers from the late 1990s (Ribaux and Margot 1999). A summary of current discourse is proposed in *The Routledge International Handbook of Forensic Intelligence and Criminology* (Rossy et al. 2018).

The US National Institute of Justice has published a report on integrating forensic case data in intelligence processes that is largely based on studies cited in this chapter (Lopez et al. 2020).

Notes

1. PICAR is an acronym in French: Plateforme d'Information du CICOP pour l'Analyse et le Renseignement
2. Annual activity report of the regional analysis centre, 2019, not published, personal communication.
3. PICSEL is an acronym in French: Plateforme d'Information de la Criminalité Sérielle en Ligne

References

Amankwaa, A. O., & McCartney, C. (2019). The effectiveness of the UK national DNA database. *Forensic Science International: Synergy, 1*, 45-55. https://doi.org/10.1016/j.fsisyn.2019.03.004.

Baechler, S. (2015). *Des faux documents d'identité au renseignement forensique : développement d'une approche systématique et transversale du traitement de la donnée forensique à des fins de renseignement criminel.* (PhD). University of Lausanne, Lausanne.

Baechler, S., & Margot, P. (2016). Understanding crime and fostering security using forensic science: The example of turning false identity documents into forensic intelligence. *Security Journal, 29*(4), 618–639.

Birkett, J. (1989). Scientific Scene Linking. *Journal of the Forensic Science Society, 29*, 271–284.

Boba Santos, R. (2014). The Effectiveness of Crime Analysis for Crime Reduction: Cure or Diagnosis? *Journal of Contemporary Criminal Justice, 30*(2), 147–168.

Brodeur, J.-P. (2008). Scientific Policing and Criminal Investigation. In S. Leman-Langlois (Ed.), *Technocrime: Technology, Crime and Social Control* (pp. 169–193). Londres: Willan.

Brown, C., & Ross, A. (2012). *End-To-End Forensic Identification Process Project. Volume Crime*. Australia New Zealand Policing Advisory Agency—National Institute of Forensic Science.

Brown, C., Ross, A., & Attewell, R. G. (2014). Benchmarking Forensic Performance in Australia–Volume Crime. *Forensic Science Policy & Management: An International Journal of Police Science and Management, 5*(3–4), 91–98. doi:https://doi.org/10.1080/19409044.2014.981347.

Casey, E., & Nikkel, B. (2020). Forensic analysis as iterative learning. In M. M. Keupp (Ed.), *The Security of Critical Infrastructures*. International Series in Operations Research & Management Science; 288. Cham: Springer.

Casey, E., Ribaux, O., & Roux, C. (2018). The Kodak syndrome: risks and opportunities created by decentralization of forensic capabilities. *Journal of Forensic Sciences, 64*(1), 127–136. doi:https://doi.org/10.1111/1556-4029.13849.

Clarke, R. V., & Eck, J. (2005). *Crime Analysis for Problem Solver in 60 Small Steps*. Washington: U.S. Department of Justice, COPS.

Cleland, C. E. (2011). Prediction and Explanation in Historical Natural Science. *British Journal for the Philosophy of Science, 62*(3), 1–32.

CMM. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM). Global Cyber Security Capacity Centre*. University of Oxford, Oxford.

De Ceuster, J., Hermsen, R., Mastaglio, M., & Nennstiel, R. (2012). A discussion on the usefulness of a shared European ballistic image database. *Science & Justice, 52*(4), 237–242. doi:https://doi.org/10.1016/j.scijus.2011.12.003.

Doleac, J. L. (2016). *The Effect of DNA Databases on Crime* Social Science Research Network. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2556948.

Fraser, J., & Williams, R. (2009). *Handbook of Forensic Science*. Cullompton: Willan.

Gerber, J., & Killias, M. (2003). The transnationalization of historically local crime: Auto theft in Western Europe and Russia markets. *European Journal of Crime, Criminal Law and Criminal Justice, 11*(215–226).

Julian, R. D., Kelty, S. F., Roux, C., Woodman, P., Robertson, J., & Margot, P. (2011). 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, 43*(4), 217–229.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology,* (Special Publication—800-86). National Institute of Standards and Technology (NIST). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (accessed the 1rst of April, 2020).

Killias, M., Haymoz, S., & Lamon, P. (2007). *La criminalité en Suisse et son évolution à la lumière des sondages de victimisation de 1984 à 2005*. Bern: Staempli.

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime, 22*(3), 324–345. doi:https://doi.org/10.1007/s12117-019-09366-7

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law and Social Change, 67*(1), 77–96. doi:https://doi.org/10.1007/s10611-016-9648-0.

Lopez, B. E., McGrath, J. G., & Taylor, V. G. (2020). *Using Forensic Intelligence To Combat Serial and Organized Violent Crimes*. National Institute of Justice. Retrieved from https://nij.ojp.gov/topics/articles/using-forensic-intelligence-combat-serial-and-organized-violent-crimes.

Margot, P. (2011). Commentary on the Need for a Research Culture in the Forensic Sciences. *UCLA Law Review, 58*(3), 795–801.

Margot, P. (2014). Traçologie: la trace, vecteur fondamental de la police scientifique. *Revue internationale de criminologie et de police technique et scientifique, LXVII*(1), 72–97.

NAS. (2009). *Strengthening Forensic Science in the United States: a Path Forward*. National Research Council of the National Academies, Washington D.C.

PCAST. (2016). *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods*. Executive Office of the President President's Council of Advisors on Science and Technology Committee, Washington.

Pollitt, M. (2010, 2010//). *A History of Digital Forensics.* Paper presented at the Advances in Digital Forensics VI, Berlin, Heidelberg.

Pollitt, M., Casey, E., Jaquet-Chiffelle, D.-O., & Gladyshev, P. (2018). *A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence*. OSAC Task Group on Digital/Multimedia Science.

Ratcliffe, J. (2016). *Intelligence-Led Policing* (2nd edition ed.). Cullompton, UK: Willan.

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science, 7*(1), 5.

Ressnikoff, T., Ribaux, O., Baylon, A., Jendly, M., & Rossy, Q. (2015). The Polymorphism of Crime Scene Investigation: an Exploratory Analysis of the influence of Crime and Forensic Intelligence on decisions made by Crime Scene Examiners. *Forensic Science International 257*, 425–434. doi:https://doi.org/10.1016/j.forsciint.2015.10.022.

Ribaux, O. (2019). Federalism and Swiss police reforms. In J. Janssen, K. Lünnemann, W. D'haese & A. Groenen (Eds.), *Cahiers Politiestudies, Gompel & Svacina, 51*, 247–260.

Ribaux, O., Girod, A., Walsh, S., Margot, P., Mizrahi, S., & Clivaz, V. (2003). Forensic Intelligence and Crime Analysis. *Probability, Law and Risk, 2*(2), 47–60.

Ribaux, O., & Margot, P. (1999). Inference Structures for Crime Analysis and Intelligence Using Forensic Science Data: the Example of Burglary. *Forensic Science International, 100*, 193–210.

Ribaux, O., Roux, C., & Crispino, F. (2017). Expressing the value of forensic science in policing. *Australian Journal of Forensic Sciences, 49*(5), 489–501. doi:https://doi.org/10.1080/00450618.2016.1229816.

Ribaux, O., Walsh, S. J., & Margot, P. (2006). The Contribution of Forensic Science to Crime Analysis and Investigation: Forensic Intelligence. *Forensic science international, 156*, 171–181.

Rossy, Q., Décary-Hétu, D., Delémont, O., & Mulone, M. (Eds.). (2018). *The Routledge International Handbook of Forensic Intelligence and Criminology*. Abingdon UK: Routledge International.

Rossy, Q., Ioset, S., Dessimoz, D., & Ribaux, O. (2013). Integrating forensic information in a crime intelligence database. *Forensic science international, 230*, 137–146. doi:https://doi.org/10.1016/j.forsciint.2012.10.010.

Rossy, Q., & Ribaux, O. (2020). Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms. *European Journal on Criminal Policy and Research, 26*, 335–356. doi:https://doi.org/10.1007/s10610-020-09438-3.

Roux, C., Crispino, F., & Ribaux, O. (2012). From Forensics To Forensic Science. *Current Issues in Criminal Justice, 24*(1), 7–24.

Tilley, N., & Ford, A. (1996). *Forensic Science and Crime Investigation* (73). Police Research Group, Home office, London.

Weisburd, D., & Majmundar, M. K. (2018). *Proactive Policing. Effects on Crime and Communities (2018)*. National Academies of Sciences, Engineering, and Medicine, Division of Behavioral and Social Sciences and Education; Committee on Law and Justice; Committee on Proactive Policing: Effects on Crime, Communities, and Civil Liberties.

Williams, R. (2007). Policing and forensic science. In T. Newburn (Ed.), *Handbook of Policing* (pp. 760–793). Cullompton: Willan.

Wilson, D. B., Weisburd, D., & McClure, D. (2011). Use of DNA testing in police investigative work for increasing offender identification, arrest, conviction and case clearance. *Campbell Systematic Reviews, 7*(1). doi:https://doi.org/10.4073/csr.2011.7.