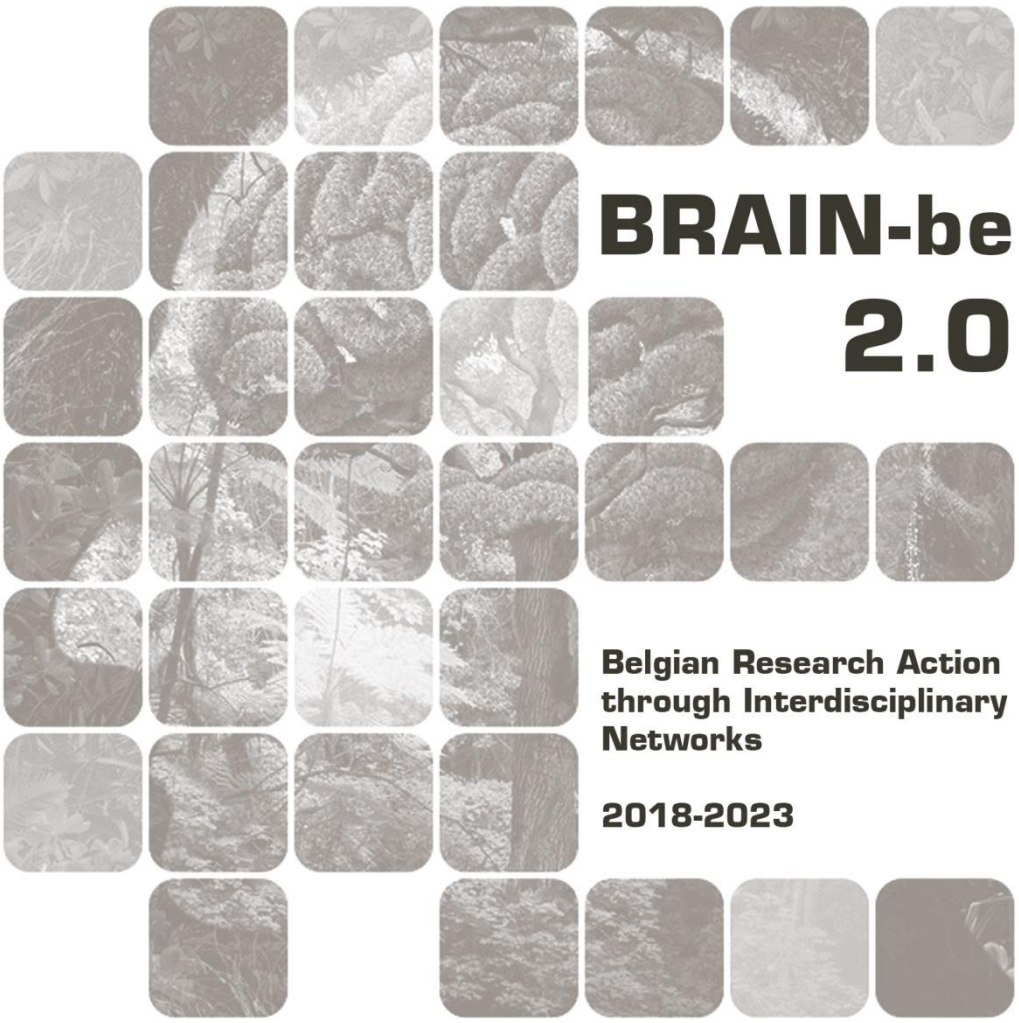


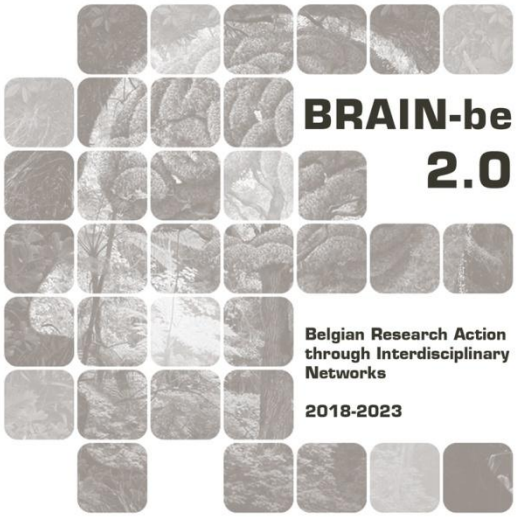
Be-ForIntel

Building the foundations of a Forensic Intelligence tool in Belgium

BERTRAND RENARD (NICC) - CAROLINE STAPPERS (NICC) - MAXIME MAUQUOY (NICC)- CHRISTOPHE VANDEVIVER (UGENT) - TOM VANDERBEKEN (UGENT) - DAYLE HARVEY (UGENT) - FABRICE GASON (NICC) - OLIVIER RIBAUX (UNIL) - NATHAN BALLÈVRE (UNIL)

Pillar 3: Federal societal challenges

belspo .be



NETWORK PROJECT

Be-ForIntel

Building the foundations of a Forensic Intelligence tool in Belgium

Contract - B2/223/P3/BeForIntel

FINAL REPORT

PROMOTORS: BERTRAND RENARD (NICC)
CHRISTOPHE VANDEVIVER (UGENT)
TOM VANDERBEKEN (UGENT)
FABRICE GASON (NICC)
OLIVIER RIBAUX (UNIL)

AUTHORS: CAROLINE STAPPERS (NICC)
MAXIME MAUQUOY (NICC)
DAYLE HARVEY (UGENT)
NATHAN BALLÈVRE (UNIL)


Published in 2026 by the Belgian Science Policy Office
WTCIII
Simon Bolivarlaan 30 bus 7
Boulevard Simon Bolivar 30 bte 7
B-1000 Brussels
Belgium
Tel: +32 (0)2 238 34 11
http://www.belspo.be
http://www.belspo.be/brain-be

Contact person: Emmanuèle Bourgeois
Tel: +32 (0)2 238 34 94

Stappers, C., Mauquoy, M., Harvey D., Ballèvre N., Vandeviver, C., Vanderbeken, T., Gason, F., Ribaux, O. & Renard, B. ***Be-ForIntel: Building the foundations of a Forensic Intelligence tool in Belgium.*** Final Report. Brussels: Belgian Science Policy Office 2026 – 113p. (BRAIN-be 2.0 - (Belgian Research Action through Interdisciplinary Networks))

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The Be-ForIntel project examined how forensic data in Belgium, covering DNA, ballistics, drugs, fingerprints, and more, could be systematically exploited for intelligence purposes beyond its current case-by-case judicial use. Organized around three work packages, the project mapped forensic data across the NICC and Federal Police (WP1), empirically assessed the added analytical value of integrating police and forensic DNA data through network analysis (WP2), and developed a comprehensive implementation roadmap with 21 structured recommendations (WP3). Key findings show that six implicit forensic intelligence practices already exist in Belgium, all operating at the tactical level and none integrated with each other. WP2 demonstrated that forensic DNA linkage data extends the relational visibility of criminal networks beyond what police data alone can reveal, and changes how network vulnerability and disruption effectiveness are assessed. The central obstacles to development are not technical but cultural, organizational, and legal: institutional silos, a dogmatic interpretation of GDPR, insufficient resources, and a structural misunderstanding between forensic scientists, investigators, and the judiciary. Notably, the Federal Police's refusal to grant access to national crime data—despite formal authorization—severely constrained the research and itself constitutes a significant finding. The project concludes that a phased, federated, and evidence-led implementation of forensic intelligence is both feasible and desirable in Belgium, provided a clear legal framework is established, institutional leadership secured, and analytical capacity built sustainably.

1. INTRODUCTION

The BE-FORINTEL project examines how forensic intelligence can be used beyond case-by-case evidentiary use of forensic traces. More specifically, it explores how forensic information can support crime analysis, case linkage, and intelligence-led policing. The project is organized around three main objectives that move from data identification and integration to analytical network comparison, to feasibility assessment and operational recommendations. Although forensic science is well established in Belgium for evidentiary purposes, an important gap remains between its tactical use in individual cases and its broader strategic use for intelligence. This introduction summarizes the current state of knowledge and situates the project's analytical and feasibility tasks within that context.

Various forms of forensic data are widely used in Belgian criminal investigations. They have contributed to solving and preventing crimes and other serious incidents. Forensic science lies at the intersection of science and law (Lopez et al., 2020). It applies scientific principles to the examination and interpretation of traces, typically on a case-by-case basis (Lopez et al., 2020; Roux et al., 2022).

Today, forensic data is still used primarily on a case-by-case basis as evidence in court. At the same time, it is well established that forensic data contains valuable information that can support investigations in their early stages (principle 1, Roux et al., 2022), and help identify links across highly repetitive and concentrated forms of crime (principle 6, Roux et al., 2022). It has also long been recognized that many investigative failures stem from "linkage blindness", that is, "the almost total absence of sharing or coordination of investigative information and the lack of adequate networking by law enforcement agencies"(Egger & Doney, 1990). Forensic intelligence offers a way to address this problem by extending the use of forensic information beyond individual cases.

The adoption of a forensic intelligence approach by law enforcement has proven effective in reducing linkage blindness in many investigations and has strong potential to improve crime analysis more broadly (Lopez et al., 2020). Forensic intelligence processes can support the analysis of many forms of repetitive crime, including high-volume crime (Ribaux et al., 2006), arsons (Bruenisholz et al., 2019), the use of false identity documents (Baechler & Margot, 2016), firearms (Braga, 2008),), and various

forms of online fraud (Rossy & Ribaux, 2020). Such an approach can also generate knowledge about co-offending patterns, modus operandi, and the spatial and temporal organization of crime series.

Realizing the full potential of forensic intelligence requires the aggregation of a wide range of forensic data across individual cases, their cross-referencing, and their integration into an overarching forensic intelligence database that can also be linked to police-recorded crime data (Kelty et al., 2013; Rossy et al., 2013; Lopez et al., 2020; Delgado et al., 2021). Ideally, such a database should be searchable and usable both reactively by law enforcement officers during criminal investigations, and proactively by crime analysts for strategic crime analysis. Interpreting forensic data in this way raises several challenges. Processes must therefore be clearly formalized considering investigative objectives and the monitoring of serial crime. The required interpretive skills must also be defined. The aim is not to build entirely new forensic databases, but rather to ensure that comparison results, such as identifications and links between cases, are properly exploited in broader analyses and investigations at appropriate levels.

However, in Belgium as in many other countries, several structural limitations currently prevent law enforcement agencies from fully exploiting the potential of forensic intelligence in crime analysis (Lopez et al., 2020; Ribaux et al., 2006). Forensic data is generally collected, analyzed, and reported on a case-by-case basis, with limited collaboration across partners. In addition, forensic data is drawn from multiple sources and stored in databases that are usually not connected to one another, creating "information silos" (Kelty et al., 2013; Lopez et al., 2020). As a result, relevant forensic data is difficult to identify, access, and use collectively. To realize the full potential of forensic intelligence for crime analysis, forensic data must be linked and aggregated across individual cases and investigations, and it must be stored and indexed in ways that allow cross-referencing and strategic analysis of data from specific investigations (Baechler et al., 2020). The integration of police and forensic data would further strengthen the potential of forensic intelligence for crime analysis (De Moor et al., 2018; Ribaux et al., 2006).

Even so, the potential benefits of integrating forensic intelligence into criminal analysis are clear and potentially substantial for law enforcement. These benefits include more effective use of crime scene evidence across the criminal justice system and a better understanding of offending patterns (Bruenisholz et al., 2016). Ultimately, integrating forensic intelligence into criminal analysis can help law enforcement allocate resources more effectively, refine strategies, and strengthen strategic and situational awareness of criminal activity (De Moor, 2018; De Moor et al., 2018; Lopez et al., 2020; Malsh et al., 2018). In turn, this can improve the disruption and prevention of crime, especially serial offending and co-offending (De Moor et al., 2020; Lopez et al., 2020).

Against this background, the BE-FORINTEL project pursues three main objectives that guide the work of the research team: (1) mapping current forensic intelligence practices in Belgium and identifying obstacles and enabling conditions for integration, (2) evaluating the analytical added value of forensic intelligence through data integration and network analysis, and (3) translating the findings into legal, technical, and operational recommendations. To operationalize these objectives, the project is organized into three work packages (WP1-WP3), each with specific tasks. WP1 focuses on mapping organizations and the forensic data generated across Belgium (Task 1.1: theory of forensic intelligence; Task 1.2: identification of relevant forensic information; Task 1.3: assessment of potential exploitation for forensic intelligence). WP2 examines the feasibility and added value of forensic intelligence integration through empirical network-based analysis (Task 2.1: data pre-processing; Task 2.2: network analysis; Task 2.3: statistical analysis; Task 2.4: identification of the legal, practical, and technical conditions for embedding forensic intelligence in crime analysis). WP3 focuses on translation into practice and future implementation (Task 3.1: development of guidelines for practitioners; Task 3.2: recommendations for political and judicial authorities regarding feasibility and added value). The aims and scope of each task are outlined in the sections that follow.

Implementation of the BE-ForIntel project requires access to police recorded crime data and forensic trace data. Access to the data required for this project proved to be a major challenge and significantly constrained the scope and ultimate impact of the work. Prior to the start of the project, we had received initial support from the SPF Justice (The Be-ForIntel project is the first BELSPO project co-funded by the Department of Justice), and from the Federal Police for access to and use of national-level police-recorded crime data (Our research team has received written assurances of access to both DRI, DJSOC and DJT data).

Once the project got underway, these various forms of support were confirmed and formalized through an authorization granted by the College of Prosecutors General. Extensive discussions were then held with the Federal Police, including DRI and DJSOC, to determine the practical modalities for data access. However, despite these efforts and the formal authorization in place, access was ultimately not implemented by the Federal Police for a range of reasons that lay beyond the responsibility and influence of the project team. Nevertheless, our team made numerous efforts, both with the national federal police authorities and with the College of Prosecutors General (and the matter was regularly discussed within the college's "police" expert network). In a protectionist reflex, the federal police considered that Belgian law does not provide a sufficient legal basis for access to police data for research purposes, even though the research results could have benefited the police. Discussions held over the past three years have not clarified this position in a favorable way to the research. This observation already constitutes important research finding.

As a result, we were unable to access national-level police-recorded crime data and were therefore limited in our ability to demonstrate the full potential of a forensic intelligence system in Belgium. As a mitigation strategy, a local police zone in Belgium expressed its willingness to support the project and provided access to police-recorded crime data in line with the conditions set out by the College of Prosecutors General. We would like to express our explicit gratitude to the Local Police of Bruges for their willingness to support this project and facilitate access to these data. Similar difficulties were encountered in relation to forensic trace data collected and stored within the Federal Police, which ultimately also remained inaccessible. The National Institute of Criminalistics and Criminology, however, provided forensic trace data under the conditions specified in the authorization of the College of Prosecutors General. We would like to express our sincere gratitude to the Criminalistics Department of the NICC for making these data available. Overall, it should be emphasized explicitly that, due to reasons outside the control of the project team, the scope and impact of this project were severely limited.

These difficulties also caused a significant delay in the completion of certain research tasks and yet did not result in BELSPO granting our request for an extension of the completion deadlines (without additional funding). It was only after filing an appeal against the Finance Inspectorate's decision that this extension was granted, and the delay in the decision and the hesitation involved once again did not create optimal conditions for conducting the research. Despite all these difficulties, the research team was able to complete nearly all tasks as scheduled.

2. WP 1: MAPPING THE ORGANISATIONS AND THE FORENSIC DATA GENERATED BY THEM

2.1 The theory of forensic intelligence

The first objective of WP1 was the identification and critical reading of the literature on forensic Intelligence, to provide a state-of-the-art picture of forensic intelligence. Task 1.1. forms the first analytical component of a broader effort to map forensic data and practices in Belgium. Before examining the Belgian landscape, it is essential to clarify conceptual foundations that underpin the notion of forensic intelligence and to situate them within existing international models. This objective was pursued through the production of two international literature reviews: one focusing on the definition of forensic intelligence, and the other on international forensic intelligence models.

The first aimed to clarify **the concept of forensic intelligence** and to establish a clear and coherent framework for the current project and, more broadly, for the development of forensic intelligence in Belgium. The second sought to provide an **analysis of existing forensic intelligence models** at the international level and to draw useful conclusions that can be applied to the Belgian context, considering technical, social, structural, organizational, and political dimensions. This conceptual grounding is necessary to ensure that the subsequent mapping of Belgian forensic data can be interpreted within a coherent and well-defined analytical structure. These literature reviews were carried out according to an elaborate methodology, including the definition of clear search criteria, the selection of relevant bibliographic databases and a structured analysis.

2.1.1 The definition of the “forensic intelligence” concept

2.1.1.1 Methodology

The first literature review focused on defining the concept of forensic intelligence. Initially, exploratory readings were conducted to identify a simple and explicit definition. These readings revealed the existence of ambiguity surrounding the concept of forensic intelligence, confirming the need for an in-depth effort to adopt a clear definition and establish a common foundation for the development of forensic intelligence in Belgium.

On this basis, a research strategy was developed starting with two initial questions:

- What are the underlying logics of forensic intelligence?
- What philosophies are expressed and defended through the notion of forensic intelligence?

These questions were designed to orient the analysis beyond the mere formulation of a definition, towards the identification of the foundational components of forensic intelligence.

The databases and keywords used were then defined. Since they best reflected the research objective, the keywords "forensic intelligence” and “renseignement forensique” were tested a priori. Based on obtaining a manageable number of results across several tested databases, these terms were retained as the final keywords. The decision to include both English and French keywords was justified by the fact that several research works written in French originate from the School of Criminal Sciences (ESC) in Lausanne, a key and active player in the field of forensic intelligence.

The bibliographic databases Scopus, PubMed, and Cairn were consulted. This choice was guided by the recognized quality of these databases, their accessibility, our research domain, and the relevance of the results obtained with respect to the keywords used. Several inclusion and exclusion criteria were defined. Among the inclusion criteria was the relevance of the source to our research object,

verified through an initial reading of the title and abstract of each source and a search for the previously determined keywords within the source. Sources presenting an explicit definition of forensic intelligence, a description of its objectives, origin, perspectives, and/or underlying philosophical conceptions were included in the corpus. Other criteria concerned the type of source (empirical or theoretical; review article, research report, doctoral thesis, book or book chapter, institutional report), accessibility, and language.

The relevant sources were recorded using the bibliographic reference management software Zotero (version 7.0.15) and then analyzed using the analysis software NVivo.12 Pro. “Nodes" were created based on an in-depth reading of the publications, corresponding to categories that allowed the structure and content of the literature review to emerge. For example, all the paragraphs dealing with a function of forensic intelligence were grouped together in a "FORINT functions" node. This categorization is therefore based on the content of the sources and does not result from a prior definition, following an inductive process.

2.1.1.2 Scientific results and recommendations

Clarifying the definition of forensic intelligence is a necessary preliminary step for the Be-ForIntel project. The concept is widely discussed in the literature but remains difficult to operationalize due to its conceptual ambiguity. This subsection therefore examines existing definitions and literature to identify the conceptual foundations and key elements necessary for a practical definition of forensic intelligence in the Belgian context.

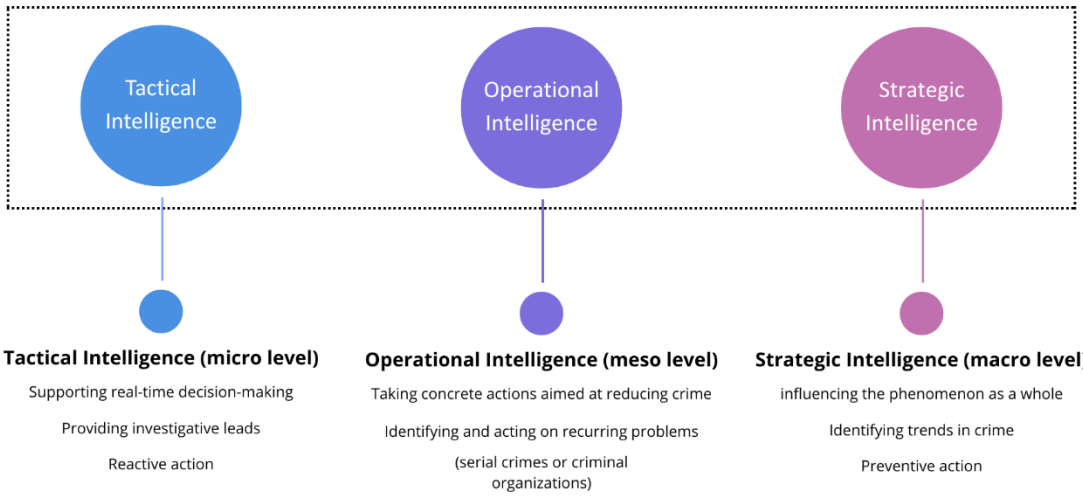
First exploratory readings revealed several proposed definitions of forensic intelligence. Despite these proposals, forensic intelligence remains a complex concept, leaving room for divergent interpretations and making its practical implementation challenging. Indeed, the notions of “intelligence” and “forensics” refer to wide-ranging fields of action, providing a “metatheoretical framework” that lacks clarity by its very nature (Legrand & Vogel, 2015). This conceptual breadth leads to differing interpretations, both between organizations and within the same structure, with a role that is often poorly understood beyond forensic units (Taylor et al., 2024). A poor understanding of forensic intelligence by police services is still evident, influenced by a managerial vision shaped by the traditional judicial view of forensic science as being primarily dedicated to courts and tribunals (Crispino et al., 2015). In addition, the proposed definitions themselves often rely on general or abstract notions requiring further clarification and exhibit notable differences.

To reduce this conceptual ambiguity, we chose to begin by examining the functions of forensic intelligence. Clarifying these functions provides a structured entry point into the concept and helps articulate what forensic intelligence is expected to achieve in practice.

2.1.1.2.1 The functions of forensic intelligence

The literature consistently describes forensic intelligence as serving three complementary functions: tactical, operational and strategic intelligence (Ioset et al., 2007; Ribaux et al., 2010; Roux et al., 2012; Morelato et al., 2013; Marclay, 2014; Baechler, 2015; Taylor et al., 2024). These different functions form a continuum, ranging from real-time investigative support to the broader understanding and prevention of crime phenomena.

Figure 1: The functions of forensic intelligence



From a *tactical perspective* (micro level), forensic intelligence is described as a tool designed to guide investigations by suggesting hypotheses or confirming or disproving investigative leads (Baechler, 2015). Several authors associate this function with a reactive approach, as it provides targeted information on specific cases and supports real-time decision-making by frontline police officers (Marclay et al., 2013; Marclay, 2014; Hachem et al., 2023). Ratcliffe (2008, as cited in Bruenisholz et al., 2016) emphasizes this investigative focus by considering tactical intelligence as a decision-making tool directly linked to actions within an individual case. Forensic intelligence therefore makes it possible, through the logical analysis of traces, to provide accurate, timely and usable information for the detection of offences, the identification, location and arrest of potential offenders, as well as for the collection of evidence for prosecution (Ribaux et al. 2006). Overall, tactical intelligence enhances investigative responsiveness by transforming trace information into direct and usable guidance.

Beyond real-time support to investigations, forensic intelligence can also be mobilized at a broader level to address recurring patterns and criminal problems. From this *operational perspective* (meso level), it supports decision-makers within geographic areas in their efforts to prevent and reduce crime (Morelato et al., 2013; Hachem et al., 2023). Indeed, numerous authors underline its ability to contribute to crime disruption (Marclay et al., 2013; De Alcaraz-Fossoul & Roberts, 2017; Spaulding & Morris, 2019; Morelato et al., 2023; Taylor et al., 2024). This function is oriented towards the identification and resolution of recurring issues – such as serial crimes or criminal organizations, through the systematic analysis of traces (Marclay et al., 2013; Marclay, 2014). At this level, forensic intelligence is particularly valuable because the links established between forensic entities allow investigators to distinguish serial and organized criminals, but also to define the characteristics of a specific criminal problem or sub-problem (Baechler, 2015). For instance, Morelato et al. (2013) describe how similarities between illicit drug samples can reveal relationships between separate seizures or cases. Such information may help identify vulnerabilities along a supply chain that can subsequently be targeted (Taylor et al. 2024). Operational intelligence therefore acts as a bridge between individual investigations and broader strategic insights by addressing patterned forms of criminal activity.

While operational intelligence targets specific issues, *strategic intelligence* (macro level) adopts an even broader perspective aimed at understanding and influencing crime phenomena over the long term. In this framework, it contributes to identifying trends and improving the understanding of different types of criminality (Marclay et al., 2013; Morelato et al., 2013; Baechler, Boivin, et al., 2015;

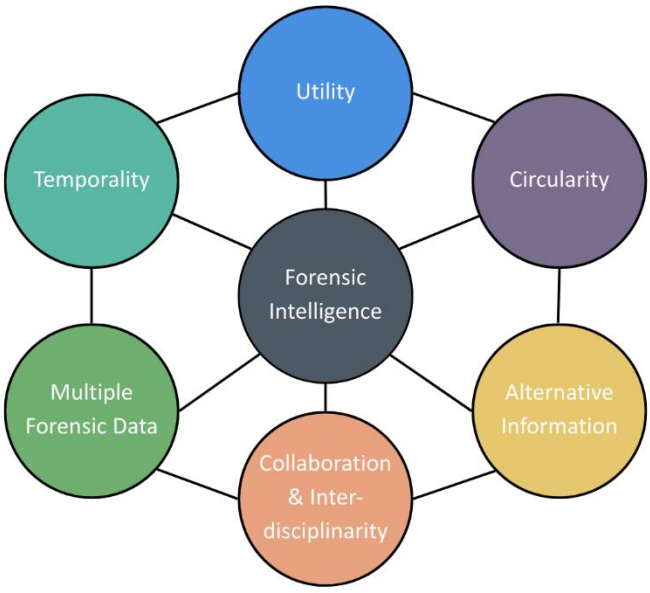
Hachem et al., 2023; Taylor et al., 2024). (Morelato et al., 2014) define a trend as the association of a set of forensic entities sharing similar characteristics that indicate a break, deviation, or shift in data along four typical dimensions: time, space, relationships, and quantity/quality. (Esseiva et al., 2007) show how forensic intelligence can help reveal the extent and size of a drug market, assess the risks associated with drug consumption within a consumer population and identify the logistical and material requirements underlying trafficking activities. In this context, several authors highlight the potential of forensic science to contribute to crime prevention (Ribaux & Talbot Wright, 2014; Baechler, 2015; De Alcaraz-Fossoul & Roberts, 2017) and to support decision-making for stakeholders such as police executives, public health services and policymakers (Morelato et al., 2013; Taylor et al., 2024). Strategic intelligence is therefore strongly proactive and aims to influence the phenomenon as a whole rather than specific criminal activities (Marclay, 2014). Strategic intelligence thus provides a high-level understanding of crime dynamics and informs long-term planning, prevention strategies and policy development.

Taken together, these three functions outline the purposes and levels of action of forensic intelligence. The following section examines the key elements that constitute its conceptual foundations.

2.1.1.2.2 The key elements of forensic intelligence

Beyond its functions, the literature also allows us to identify several constitutive elements that define what forensic intelligence encompasses in practice. These elements collectively clarify the constituents of the concept and specify what is expected behind the notion “forensic intelligence”, thereby providing a clearer understanding of its scope and meaning. Six elements emerge consistently from literature: utility, circularity, temporality, integration of multiple forensic data, integration of alternative information, and collaboration.

Figure 2: The six key elements of forensic intelligence



As the objectives of forensic intelligence have already been highlighted, the notion of *utility* is obviously the first essential point. The idea of utility is at the heart of forensic intelligence. It partly emerges in response to concerns regarding the added value of forensic science, prompting a return to its fundamental constituents to express its full potential within both judicial and security frameworks.

As Ribaux et al. (2015) point out, the contribution of forensic science is little understood, formalized and largely diluted when the focus is placed solely on crime detection. In this sense, forensic intelligence constitutes a means of maximizing the operational value of forensic science in policing (Taylor et al., 2024). The intelligence process therefore aims to add value to the information collected and to produce an intelligence product capable of supporting decision-making (Morelato et al., 2013; Hachem et al., 2023; Taylor et al., 2024).

A second key point concerns the *cyclical nature* of the intelligence process. Authors dealing with forensic intelligence consistently refer to an information processing process (Ross, 2015; Baechler, Boivin, et al., 2015; De Alcaraz-Fossoul & Roberts, 2017; Ribaux et al., 2006). As Hachem et al. (2023) point out, the general principles of intelligence, which are applied in many fields, also apply to forensic science: intelligence is based on a cyclical process in which raw information is collected, evaluated, collated, analyzed, disseminated and continuously re-evaluated to guide decision-making. This framework – widely described in the model proposed by Morelato et al. (2014) for forensic intelligence – implies opportunities for systematization, formalization, transparency and control at every stage. It also requires careful considerations at each of these stages, whether it is about the collection of data, their organisation, the conclusions drawn or even the selected communication channels (Ribaux et al., 2006). Because new information can reshape existing interpretations, the cycle is inherently adaptative: changes in offender behavior, for example, can inform crime-scene practices, which in turn influence the information circulating in the system (Ibid).

A third fundamental element relates to *temporality*. Forensic intelligence relies on the continuous integration of new data into a structured memory capable of linking past and new information to develop or update hypotheses regarding criminal structures, behaviors or seriality (Talbot-Wright et al., 2016). This constant updating of the memory is directly linked to time: the usefulness of the intelligence product depends on its timely availability for decision makers (Baechler, Boivin, et al., 2015). Processing delays can considerably reduce the value of intelligence. For example, identifying links between drug seizures months after an operation significantly limits investigative opportunities, whereas early detection may reduce the action of criminals (Morelato et al., 2013). Temporality therefore requires dynamic data management and adequate processing speed throughout the cycle (Ribaux et al., 2010; Morelato et al., 2014).

The fourth element is the *integration of multiple types of forensic data*. Many authors highlight that the crossing of data from different forensic disciplines opens up new analytical possibilities. Indeed, cross-fertilization between fields broadens the scope of logical inferences and reduces the fragmentation that leads to linkage blindness when traces are considered in isolation (Ribaux et al., 2006). To sum-up, the results of different disciplines taken collectively through informed analysis can give rise to links and identifications that would not otherwise have been possible (Ross, 2015).

Beyond the cross-referencing of forensic data, a fifth key dimension concerns the *integration of alternative information*, which is crucial to the intelligence product (Ross, 2015; Talbot-Wright et al., 2016). The alternative information should be understood here as any information other than forensic science-based, gathered by the police or available to the police, such as spatiotemporal information, interviews, observations, electronic surveillance, financial transactions, travel and customs information, statistics, criminology and open source information (Morelato et al., 2014). This consideration is essential since the consideration of these data allows for contextualizing and strengthening forensic results which alone could present limited added value (Ibid.). For example, a fingerprint comparison may not provide a direct match but may well provide information indicative of a person of interest which, combined with other relevant information available, can be used by the investigator as part of the overall investigation process (Ross, 2015).

Finally, this cross-aggregation of information implies a sixth constitutive element: *collaboration and interdisciplinarity*. An integrated process of forensic intelligence relies on shared understanding of actors from different disciplines, such as analysts, forensic scientists, crime-scene officers and policymakers (Morelato et al., 2014, 2023). The existence of committed partners and trust-based partnerships contributes to break down existing silos and enables cross-case and cross-domain analysis (Ross, 2015; Taylor et al., 2024; Bruenisholz et al., 2016). Collaboration is therefore not an optional addition but a structural requirement for a functional forensic intelligence process.

Together, these elements provide the conceptual foundations required to adopt a clear and operational definition of forensic intelligence for the purpose of this project.

2.1.1.2.3 Conclusion: the definition of forensic intelligence for the Be-ForIntel Project

A literature review was conducted around the concept of forensic intelligence. This work highlighted the essential components of the concept and led to the adoption of a clear and precise definition for the purposes of this project. Rather than attempting to develop a new proposal, the decision was made to adopt an existing definition, that of Ribaux et al. (2006, p. 172), identified as the most adequate and in line with the elements emerging from the literature: "Forensic intelligence is the accurate, timely, and useful product of the logical processing (analysis of) forensic case data (information) for investigation and/or intelligence purposes." To avoid falling into the pitfalls of an abstract definition, the adopted definition was complemented by explanatory elements drawn from the literature review.

Consequently, logical processing can be likened to the cyclical intelligence process, including the stages of collection, evaluation, collation, analysis, dissemination, and re-evaluation of information. This cyclical structure reflects the dynamic and adaptative nature of forensic intelligence, in which new information continuously reshapes existing hypotheses.

The notions of accuracy, timeliness, and usefulness relate to two major characteristics emerging from the literature specific to forensic intelligence: utility and temporality. They reflect that the forensic intelligence process aims to add value to the information and guide decision-making at different levels of action. This objective can only be achieved if the information is processed within a certain time frame since the cyclical process involves a framework dependent on the evolution of criminal activity. The information produced by the model must therefore be usable by decision-makers in a timely manner; otherwise, it loses its usefulness. The intelligence product itself represents this informational added value derived from the processing of forensic data.

The investigative and intelligence purposes can finally be linked to three main functions: tactical (direct investigations, suggest or confirm/deny hypotheses or investigation leads), operational (supporting crime reduction, identifying and solving repetitive problems) and strategic intelligence (to identify criminal trends and prevent crime). The objective is to guide decision-making at these different levels of action. Taken together, these functions situate forensic intelligence within a continuum ranging from immediate investigative support to long-term crime prevention and understanding.

Finally, another element to consider is the integration of non-forensic data into the process, requiring collaboration between different stakeholders (forensic laboratories, magistrates, police, policymakers). This integration reinforces the multidimensional nature of forensic intelligence and underscores the importance of cooperation across organizational boundaries.

These elements provide a conceptual and operational framework for developing forensic intelligence practices in Belgium, ensuring that the approach is theoretically sound and practically applicable. With this conceptual foundation in place, the next section examines how forensic intelligence has been operationalized in different national contexts.

2.1.2 Forensic intelligence: existing models and practices internationally

2.1.2.1 Methodology

The second literature review focused on the analysis of existing models and processes of forensic intelligence at the international level. While this theoretical work quickly proved essential, its importance was further reinforced by discussions during the Guidance Committee meetings, where several participants shared their experiences with concrete projects in their respective countries, notably Switzerland and the United States. These exchanges revealed that the implementation of forensic intelligence occurs within diverse contexts and that numerous technical and social dimensions must be considered. Accordingly, this work was conducted using a methodology comparable to that employed in the first literature review.

Five categories of search criteria were defined: content of the source; type of source; language; methodology; accessibility. Based on these criteria, sources addressing a forensic intelligence model or practice, as well as sources discussing its implementation (processes, obstacles, recommendations, feedback) were deemed relevant. Given the objectives of the project, no restrictive methodological criteria were applied, allowing theoretical, descriptive and empirical sources to be considered. Similarly, journal articles, books, book chapters, doctoral theses and organizational reports were included. The language of the sources selected was limited to English and French, the latter justified by the prominence of scientific works on forensic intelligence emanating from the University of Lausanne. Finally, accessibility was also considered, as some sources proved difficult to obtain.

Several bibliographic databases were selected for the research, guided by their recognized scientific quality, diversity and relevance to our research subject: ScienceDirect, Scopus, Pubmed, Erudit and Swisscovery. Using multiple databases strengthened the research corpus by minimizing gaps and ensuring the inclusion of highly relevant sources. The following keywords were then tested: "Forensic Intelligence" AND "Model". The results were stored in the bibliographic reference management software Zotero (version 7.0.15). Each source was then scanned a first time based on a reading of the title and abstract and annotated "included" or "rejected" based on the previously established search criteria (except for accessibility). After removing duplicates, sources marked "included" were read in their entirety and annotated as "included +" or "included -" according to the same criteria (including accessibility).

In a second phase, a snow-balling technique was applied by examining the references cited in the selected sources, enabling the identification of additional relevant publications. Furthermore, publications available on the websites of several organizations (ANZPAA, NIJ) were also searched. The same inclusion/exclusion process was applied.

Simultaneously, a structured analysis was carried out. All the sources of the corpus were integrated into analysis software NVivo.12 Pro. “Nodes" were created based on an in-depth reading of the publications, corresponding to categories that allowed the structure and content of the literature review to emerge. For example, all the paragraphs dealing with an implemented FORINT model were grouped together in an "Existing FORINT models" node. Sub-categories were then created for each node to facilitate analysis. This categorization is therefore based on the content of the sources and does not result from a prior definition, following an inductive process.

2.1.2.2 Scientific results and recommendations

This chapter maps international forensic intelligence practices and implementation models. It identifies the fundamental elements that appear consistently in the countries concerned and draws lessons that can credibly inform a Belgian pathway. To better understand how forensic intelligence is implemented abroad, the following section first examines documented practices and the associated models.

2.1.2.2.1 International forensic intelligence practices: what traces, what model

This section summarizes the main internationally documented practice areas and highlights integrated configurations that target high-volume crime and serial problems.

The first clearly identifiable domain concerns the profiling and comparative analysis of forged identity documents. Initiated in Switzerland by Baechler et al. (2012, 2013), this approach demonstrated the value of linking documents based on visual and technical features, such as printing methods, to identify common sources. The method involves profiling selected documents, storing them in a database, and comparing them using a scoring system to detect links and trends, for example suggesting the activity of prolific offenders or a manufacturing method. A concrete model has been implemented in Switzerland (Moulin et al., 2022, 2024) and progressively evolved, leading today to a European project named ProFID including 16 participating countries (Baechler, 2024). Similar practices have also been implemented or tested in Australia (Devlin et al., 2023) and in Québec (Tapps et al., 2024).

The second domain concerns the profiling and comparative analysis of illegal drugs. In the same vein as the profiling of false identity documents, the objective is to link cases and highlight trends in order, for example, to detect a distribution network. Concrete models are referenced in Australia through the AIDIP program and the ENIPID project (Collins et al., 2007; Collins, 2017; Popovic et al., 2022), in Switzerland (Marclay et al., 2013; Broséus et al., 2016; Meola & Esseiva, 2022) or even in Finland (Broséus et al., 2015; Meola et al., 2021). In addition, a method has also been proposed as part of the fight against doping, which presents both criminal and health issues (Marclay et al., 2013).

Another domain in which forensic intelligence has been operationalized relates to illicit firearms. In Australia, the Australian Federal Police (AFP) has adopted forensic intelligence methods to combat illicit firearms, incorporating a proactive approach to uncover unknown threats (Taylor, Turbett, et al., 2024). In an integrated approach combining ballistics data with other forensic information, technical indicators are created and integrated with crime scripts to detect abstract traces that reveal vulnerabilities (Ibid.). These vulnerabilities are then proactively targeted to identify unknown threat entities within the community. These entities are assessed as being involved in illegal firearms crime. Similar strategies can be found in the United States, through Crime Gun Intelligence Centers (CGICs). These are inter-agency platforms focused on the timely collection and analysis of firearm-related evidence (CGIC, 2017, 2022; Flippin et al., 2022). They integrate forensic and police intelligence to link crime scenes, materials, and suspects (Delgado et al., 2021).

Other forensic intelligence practices can still be identified, particularly in relation to counterfeits (Dégardin et al., 2015; Hochholdinger et al., 2019; Mireault et al., 2025), arson (Bruenisholz et al., 2015, 2017, 2019), handwritings (Agius et al., 2017, 2018; Devlin et al., 2024) and digital forensic intelligence (Bollé & Casey, 2018; Quick & Choo, 2018; Rossy & Ribaux, 2020; Ribaux et al., 2022; Ngo & Le-Khac, 2023). Finally, as specified by Morelato et al. (2014), any type of trace can be exploited in a forensic intelligence framework. The areas mentioned have, however, been the subject of special attention in scientific literature.

Beyond trace-specific applications, several countries also rely on integrated models that combine multiple forensic and non-forensic data sources. These models generally rely on DNA traces, fingerprints, shoeprints, drugs, or tool marks. Such processes typically target recurring crime-related issues, specifically high-volume crime. This is the case of the PICAR database managed by the CICOP in Switzerland (Rossy et al., 2013; Grossrieder, 2017), the "Fusion Centers" in the United States (Garvey et al., 2023) or the AFP's FORINT unit in Australia, which notably focuses on serial offenders in the context of property crime (Taylor et al., 2024). Another example, specific to intelligence related to drugs, is the centralized forensic laboratory attached to the National Bureau of Investigation (NBI) in Finland (Meola et al., 2021). Together, these models illustrate how profiling applied to DNA, fingerprints, drugs, shoeprints and tool marks forms the backbone of integrated forensic intelligence systems.

2.1.2.2.2 What international forensic intelligence models tell us

Beyond these operational practices, it is equally important to examine how countries' structure and govern their forensic intelligence systems. The next section therefore focuses on implementation models and the factors that shape them.

2.1.2.2.2.1 Emergence of forensic intelligence practices: implementation and structure

The previous section revealed a great diversity of models. While the objectives pursued are widely shared, it appeared that the implementation methods vary according to political, organizational, and cultural contexts. Indeed, the various cases illustrated in the literature enable us to differentiate between a *bottom-up vs top-down* and *centralized vs decentralized* implementation. This two-axis classification provides a useful framework to situate existing models.

Australia illustrates a top-down and centralized configuration, presenting a culture of forensic intelligence driven by bodies (NIFS) at a national level. In this context, the implementation strategy involves the development of a precise framework (national directives, common lexicon) and a general action plan. This direction is being driven in particular by the AFP via an intelligence unit and a real transformation of the forensic division's intelligence-led operational model.

In a top down but decentralized configuration, the United States is pursuing a national initiative aimed at supporting and harmonizing forensic intelligence initiatives across the country. However, these initiatives are scattered and carried out by laboratories or law enforcement agencies at different levels (local, state, federal), reflecting the decentralized federal structure. Existing structures, such as the Fusion Centers and the Crime Gun Intelligence Centers (CGIC) are therefore supported by national tools but attached to a more local governance.

Finally, in a bottom up and decentralized configuration, we can situate the Swiss and Canadian models. In Switzerland, initiatives have emerged at a regional level, particularly in the western part of the country, notably through CICOP and the PICAR database, the profiling of false identity documents or even the profiling of illegal drugs. These initiatives often involve several states, but the lack of a dedicated federal structure limits national coordination. In Canada, documented forensic intelligence practices are mainly concentrated in the province of Quebec, through the initiatives of the Laboratoire de Sciences Judiciaires et de Médecine Légale (LSJML). Although there is functional centralization at provincial level, no federal structure coordinating or harmonizing these practices is identified.

These different conformations illustrate that the development of forensic intelligence can follow different paths that are rooted in a particular national and institutional context. This diversity confirms that there is no single model but rather adaptable principles. In this context, the challenge for Belgium

is to identify a realistic configuration compatible with its institutional landscape, while drawing inspiration from existing international practices.

2.1.2.2.2.2.2 Difficulties related to the development of forensic intelligence practices

While implementation logics help situate national configurations, understanding the obstacles that constrain these systems is essential for assessing feasibility in other contexts. This section therefore examines the main difficulties identified across countries.

The first one is linked to *cultural aspects*. Indeed, one of the major obstacles to forensic intelligence lies in the deeply rooted perception of forensic science as serving purely judicial purposes, where priorities are dictated by magistrates and oriented toward prosecution and conviction (Morelato et al., 2013; Delgado et al., 2021). This concept is deeply ingrained and has multiple consequences. Firstly, the current justice-oriented model creates an asymmetry between forensic service providers and dominant actors (e.g. police, prosecutors), limiting their autonomy and capacity for evolution (Houck, 2020). Secondly, the judicial objective demands certainty and precision, fostering a "zero-error" culture that is incompatible with the forensic intelligence vision, which accepts a higher degree of risk and uncertainty (Ribaux et al., 2010; Morelato et al., 2013; Garvey et al., 2023). In this framework, uncertainty is inherent due to abductive reasoning, where multiple hypotheses may explain the same observation (Baechler et al., 2013, cited by Morelato et al., 2014).

This justice-oriented culture also shapes *education and training*, which remain largely focused on judicial procedures and insufficiently toward intelligence-based approaches (Ribaux et al., 2010; Delémont et al., 2018). Indeed, there is an abstract understanding of the approach among the actors expected to be involved in the process (Ribaux et al., 2006). Analysis in a forensic intelligence framework is complex and requires going beyond a single training in intelligence or forensic science (Taylor et al., 2024).

Thirdly, *structural and organizational* aspects must be noted. The development of a culture and practices of forensic intelligence is strongly hindered by disciplinary, inter-organizational, and functional fragmentation. At the disciplinary level, forensic sub-disciplines often operate independently, involving the isolated consideration of traces (Ribaux et al., 2006; Devlin et al., 2024). At an organizational level, capabilities required to support forensic intelligence models may be dispersed across multiple organizations, resulting in fragmented information and responsibilities, as well as incompatible systems (Morelato et al., 2014; Taylor et al., 2024). Finally, functional fragmentation arises when actors involved in forensic intelligence processes do not share the same missions, constraints or priorities, hindering the implementation of a coordinated framework (Baechler, Morelato, et al., 2015).

Arising from fragmentation, *access and processing of information* represent another difficulty. Indeed, the "silo effect" involves differentiated processing of forensic data, sub-disciplinary specialization and difficulties in communication and coordination. Added to this are political, jurisdictional or logistical restrictions that may affect data access (Garvey et al., 2023), as well as legal aspects, as highlighted in the context of anti-doping (Marclay et al., 2013). More fundamentally, existing information management systems are not always suited to forensic intelligence objectives. This is due to the technical design of these systems, which are primarily built for judicial purposes (Garvey et al., 2023). Finally, the increasing number of cases and potential links can become complex to manage, requiring adapted operational models and prioritization frameworks (Meola & Esseiva, 2022; Taylor et al., 2024).

Finally, *resources constraints*, human, financial and temporal, are a persistent limiting factor. These constraints hinder or prevent the use of the intelligence product, create delays and limit profiling

activities (Meola et al., 2021; Meola & Esseiva, 2022). The need to reallocate resources can also generate a negative perception of forensic intelligence initiatives (Taylor et al., 2024). Moreover, time represents a major issue in a context where judicial priorities dominate, particularly in backlog situations (Ross, 2015).

All these obstacles show that the development of forensic intelligence is not only linked to technical and organizational choices but that it fits well into a complex cultural, institutional and operational framework. These difficulties highlight that long-term implementation requires much more than simply adjusting existing processes. For Belgium, this analysis invites to consider a progressive approach adapted to its institutional realities and structural conditions allowing to anchor a culture and practices of forensic intelligence.

2.1.2.2.3 A conceptual framework for forensic intelligence

To guide the analysis of the Belgian context, the next section sets out a conceptual framework that synthesizes the common process and key variations found internationally.

2.1.2.2.3.1 A transversal forensic intelligence process with contextual differences

The literature identifies a multitude of forensic intelligence practices based on different types of trace. Despite this diversity, the experiences documented internationally highlight a common procedural logic, made possible by the gradual spread of methods between countries – that it involves scientific publications, institutional exchanges or inter-laboratory collaborations. This transversality has moreover been theorized by Morelato et al. (2014) and Baechler et al. (2015), establishing a model of forensic intelligence applicable to any type of trace and following key steps: detection of an object; establishment of profiles; definition of a meta-metric model of the object; definition of metrics and comparison scores; evaluation and interpretation of the scores; integration and organization of data in a memory; analysis of information; integration of alternative (non-forensic) information; communication of the intelligence product to decision-makers.

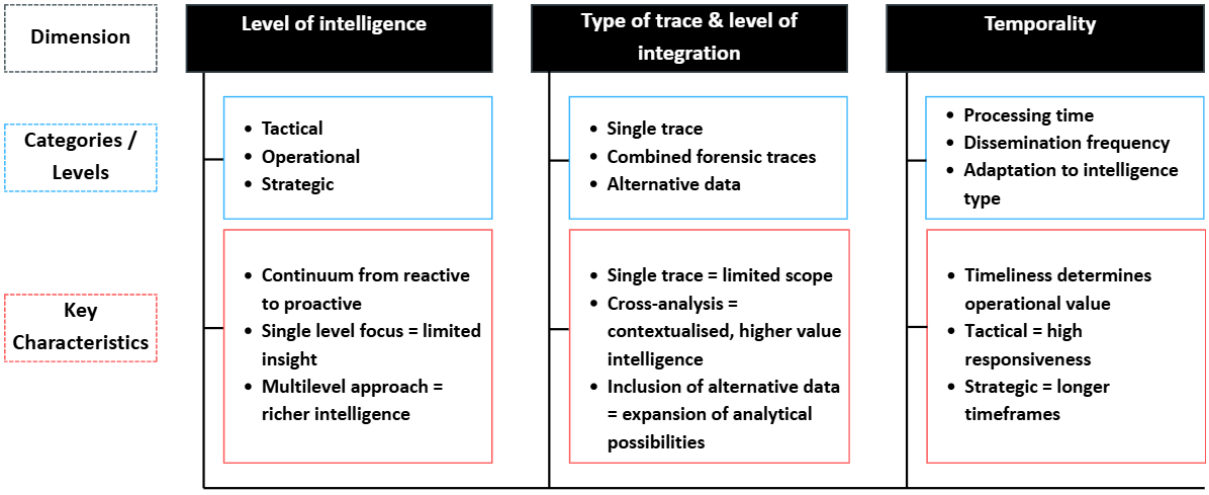
We indeed observe a similar logic followed in the different models observed. However, a number of contextual differences exist at different stages of the process. Indeed, the implementation of these models varies according to the technical, organizational and strategic choices specific to each context. These variations appear as early as the phase of detection or inclusion of traces in the process, which depends on national priorities, legal frameworks or even available analytical capacities. The characteristics used to establish profiles, the storage methods, the nature of the integrated alternative information or even the dissemination formats may also differ. These choices often reflect the mode of implementation of the forensic intelligence – more or less centralized, managed in a top-down manner or carried locally – as well as the political, operational or technical constraints specific to the country concerned.

To sum up, the clear definition of the process therefore involves choices that are highly dependent on the context and possibilities in terms of forensic intelligence implementation: type of trace, available data, organizations involved, data sharing, coordination, human and technical resources, means of dissemination. Understanding this process also requires identifying the key dimensions that structure its practical application. The next subsection details three recurring dimensions highlighted across the literature.

2.1.2.2.3.2 Three structuring dimensions of forensic intelligence

The analysis of the scientific literature allows identifying three major structuring dimensions of forensic intelligence.

Figure 3: The three structuring dimensions of forensic intelligence



The first relates to tactical, operational and strategic levels of intelligence. As highlighted earlier, these different purposes should be seen as part of a continuum, ranging from the most reactive (tactical) to the most proactive (strategic). However, certain practices tend naturally more towards one end of the spectrum or the other, depending in particular on the type of trace and the criminal phenomenon involved. Thus, drug profiling tends to produce primarily operational and strategic intelligence – for example to identify distribution networks – while DNA analysis is traditionally mobilized for essentially tactical purposes, notably to guide the investigation through the identification of a suspect.

The second dimension concerns the extent of data considered in the process. Two categories of data can be distinguished: forensic data, from trace analysis, and alternative data, from other police or informational sources. Among the models encountered, some rely on a single type of trace, while others combine several forensic data. Similarly, alternative data is not systematically integrated, limiting the added value of product information and accentuating the linkage blindness. The integration of various data therefore appears as an essential lever to enrich the analysis and reveal elements that would otherwise remain invisible. This dimension needs to be considered from the design of a forensic intelligence process, as it conditions the scope and quality of the final product.

Finally, a third dimension concerns temporality, a key element of any forensic intelligence process. The value of intelligence depends on how quickly it is processed and disseminated. If the analysis is carried out too late, the product may become obsolete and lose its practical use. However, this requirement tends to vary depending on the level of information sought. Tactical intelligence often requires a high degree of responsiveness, whereas more strategic intelligence relies on trend analysis built over broader time horizons. Temporality is also conditioned by the level of integration of data and technical and organizational capabilities involved. Defining clear and realistic temporal criteria for the production and dissemination of forensic intelligence is therefore essential.

Beyond these structuring dimensions, the nature of the data mobilized and the way it is organized analytically also play a decisive role. The next subsection therefore focuses on trace types and the production models used to exploit them.

2.1.2.2.3.3 Type of data and production models for forensic intelligence

A third consideration concerns the nature of the data mobilized and the associated operating model. The literature highlights that many types of traces can be mobilized in a forensic intelligence process, whether they are drugs, DNA, false documents, fingerprints, handwritten documents or digital traces. However, any type of trace can in principle be valued, as long as it can be compared, approximated or contextualized.

Beyond purely forensic data, some models also integrate alternative data, such as spatio-temporal information, elements related to the modus operandi or other police sources or open data. This information plays an important role in the contextualization of traces and the enrichment of established hypotheses.

Based on the literature, two major models of forensic intelligence production can be distinguished

- The first is a *specialized model (mono-trace)*, in which each type of trace is treated separately within distinct databases or processes. It allows a thorough exploitation of a type of data but limits the possibilities for cross-referencing and can reinforce a fragmented vision.

- The second one is an *integrated model (multi-traces)*, which combines several types of forensic (and sometimes non-forensic) data within a single analysis system. This integration makes it possible to enrich the links between cases, produce more contextualized information and identify more complex criminal phenomena.

The transition from a specialized to an integrated model must, however, be considered as a methodological progression, requiring beforehand that each type of trace is subject to rigorous, harmonized and systematic treatment. Integration thus implies centralization of data, compatibility of formats and a clear analytical framework.

2.1.2.2.4 Conclusion: What the international landscape implies for Belgium

The analysis of the international literature highlights a set of elements that can be used to examine the Belgian forensic landscape and its possibilities in terms of intelligence. The practices identified reflect a great diversity of models, each shaped by their own institutional contexts and distinct implementation logics. This diversity confirms that there is no directly transposable model of forensic intelligence but rather a number of principles which need to be adapted to national realities.

In general, several points of attention can be identified. The first concerns governance: international initiatives testify to the importance of considering an adapted implementation mode – centralized or decentralized, top down or bottom up – closely linked to institutional realities, coordination capacities, information sharing and standardization. In this regard, the mapping of forensic data constitutes a decisive insight. The second point refers to the cultural, structural, organizational and technical constraints and obstacles identified. These elements should also be considered in any reflection on the development of forensic intelligence in Belgium.

Finally, a conceptual framework was developed based on the literature, identifying a transversal forensic intelligence process, three structuring dimensions (level of intelligence, data integration, temporality) and two operating models (mono-trace and multi-traces). This framework offers a relevant reading grid to examine Belgian practices, evaluate the possibilities of evolution and determine the conditions necessary for the development of a functional forensic intelligence model.

2.2 The potential relevant forensic information in Belgium

In contrast to studies related to forensic intelligence in other countries, which start from a particular phenomenon, e.g. burglaries, and link certain forms of forensic data, we want to map all available forensic data independently of certain phenomena.

The starting point is practical and bottom-up, identifying the available information and the implicit forms of forensic intelligence that may already exist in Belgium. Indeed, several databases are operational (e.g. DNA, fingerprints, ballistics, etc.). It is therefore conceivable that implicit forms of comparison between these databases could exist within some smaller organizations, such as a local police area or a technical and scientific police laboratory (e.g. shoe marks or toolmarks).

The ultimate goal of mapping is not to link all forensic data, but rather to identify opportunities and challenges. The success of developing a forensic intelligence tool does not lie in the ambition to link all identified data, but rather in structuring the progressive integration of different types of forensic data into a planned and realistic process.

Based on a literature review and exploratory interviews, we mapped out the actors that hold data relevant to research on forensic intelligence. Given the vast number of potential sources, we opted to focus primarily on the Federal Police and the National Institute of Criminalistics and Criminology (NICC).

2.2.1 Methodology

2.2.1.1 National Institute of Criminalistics and Criminology

The work of mapping forensic data within the NICC began with an analysis of internal documentation addressing various aspects related to the structure and organization of the Operational Directorate of Criminalistics, which encompasses the different forensic services and laboratories within the NICC. Documents concerning quality assurance and GDPR compliance were also examined. This preliminary analysis provided an overview of the work processes of each forensic laboratory and service, as well as an initial insight into forensic and administrative data, databases, and systems in use.

Subsequently, semi-structured interviews were conducted with various stakeholders from the laboratories and services of the Criminalistics Department, including heads of services, forensic experts, and forensic advisors. These individuals were selected based on their experience and knowledge of ongoing forensic processes. The interviews aimed to clarify the existing forensic data and to understand how these data are collected, produced, stored, analyzed, and ultimately used within the judicial system. An interview guide was developed and divided into two sections: one dedicated to mapping forensic data and another focused on perceptions and possibilities of forensic intelligence.

The “mapping” section included questions on work processes, data production, structuring, and purposes, as well as on the systems employed. Beyond strict forensic data, attention was also given to administrative data, as the use of such data constitutes a key element of forensic intelligence. The “perception” section comprised questions regarding the actors’ views on the potential of forensic intelligence, their understanding of the concept, identified challenges and opportunities, and their ideal scenarios. These considerations aimed, on the one hand, to explore how current processes and data could be leveraged within a forensic intelligence framework and, on the other hand, to ensure that no formal or informal practices of forensic intelligence already existed within the NICC.

Participants were invited to take part in the interviews via email, and the interviews were conducted in person at their workplace. Each interview was recorded with the participant's consent and after explaining the project's objectives and the interview framework. Transcriptions were produced using noScribe software and subsequently reviewed and corrected manually. During this process, participants' names were anonymized. The data were then analyzed using NVivo 12 Pro to identify, first, the different databases and types of data produced and, second, the potential practices, perceptions, and perspectives of the stakeholders. A second wave of non-recorded interviews was conducted with certain participants to clarify more technical aspects related to forensic data production.

2.2.1.2 Federal Police

Although Belgium has an integrated police system with a common ANG (National General Database), the Federal and Local Police operate with a high degree of autonomy. This autonomy is also evident within each level, where operations are organized geographically—by judicial districts or local zones.

Mapping all zones and services was therefore not feasible. Consequently, this study focused on the Federal Judicial Police (DGJ) due to the specificity of its mandate. DGJ consists of 14 decentralized directorates (FGPs) across judicial districts and four central directorates in Brussels.

Within DGJ, two central directorates were selected: DJT and DJSOC.

- **DJT**, the Central Directorate of Technical and Scientific Police, is a specialized unit within the Federal Police that provides forensic support and expertise. Its services extend to the integrated police, judicial and administrative authorities, and other external partners. DJT manages extensive forensic data with nationwide coverage. Although not formally part of DJT, the **Laboratories of Technical and Scientific Police (LTWP)**which fall under the decentralized judicial directorates—were also included, as they operate under DJT's supervision.
- **DJSOC**, the Directorate for Combating Serious and Organized Crime, was selected because of its mandate and the types of criminal phenomena it addresses. These cases could greatly benefit from a forensic intelligence approach and likely involve significant forensic data. DJSOC provides specialized support to integrated police services and external national and international partners (e.g., fire brigade, customs, Europol). Its core tasks include:
    - Combating corruption, organized economic and financial crime, and cybercrime.
    - Monitoring priority crime phenomena identified in the National Security Plan
    - Executing judicial missions in military environments Additionally, DJSOC offers expertise in areas such as online child pornography, vehicle identification, dismantling drug production laboratories, organized theft, firearms, and public health. Here too, the decentralized judicial directorates (FGPs) were considered.

To collect detailed information on the structure, data sources, and operational context of these services, semi-structured interviews were conducted with representatives of the selected directorates. This qualitative approach allowed for systematic yet flexible exploration of their practices and resources, ensuring both comparability and depth of insight.

2.2.2 Scientific results and recommendations

2.2.2.1 National Institute of Criminalistics and Criminology

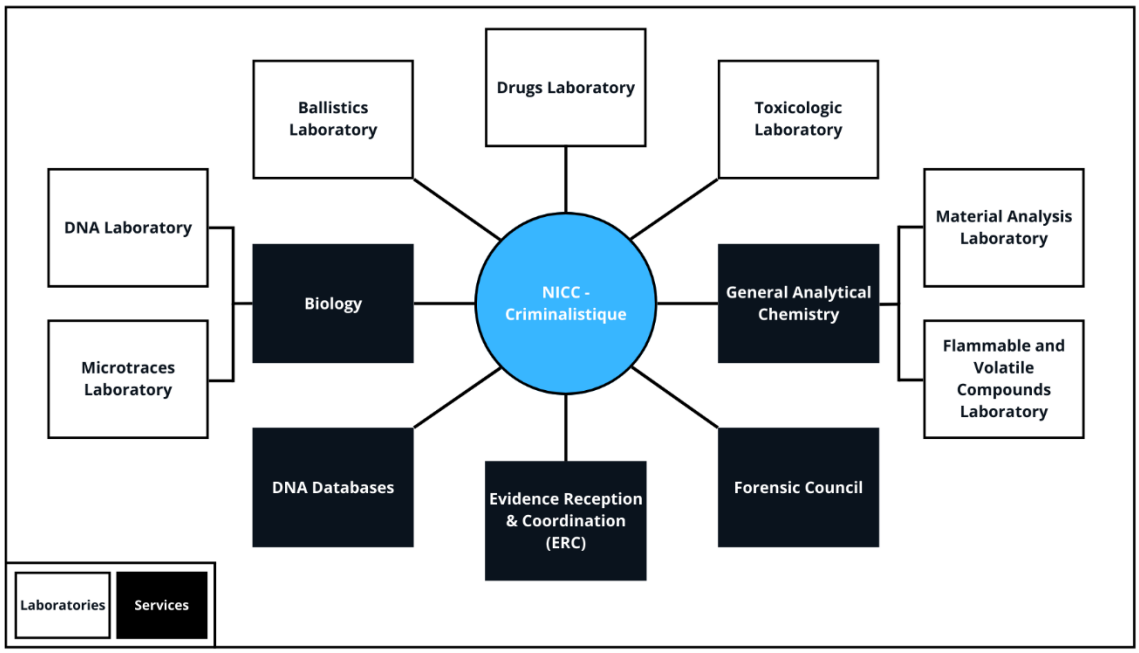
2.2.2.1.1 Organizational Description

The National Institute of Criminalistics and Criminology (NICC) is a scientific institution within the FPS Justice. It conducts independent investigations at the request of judicial authorities.

- The operational directorate of Criminalistics identifies and analyses traces from suspects and the modus operandi, thereby helping to find the perpetrators of crimes and establish the burden of proof.
- The operational directorate of Criminology examines the functioning of the penal system and how it can be improved.

The operational directorate of Criminalistics consists of several services and laboratories (see scheme 2):

Figure 4: The services and laboratories of the NICC's operational criminalistic directorate.



Except for the forensic council and the ERC, these various services produce and record forensic data.

2.2.2.1.2 Systems and tools used by the NICC

Different types of systems and tools related to information processing have been identified within the services and laboratories of the NICC. First, a common system called **DECK** acts as a central program containing all incoming information: requisition, evidence, and SIN (Single Identification Numbering), requisition number, name of the magistrate, date, judicial district, sample numbers. This system also includes the expert reports produced.

Each laboratory also has its own **Laboratory Management System (LIMS)**, except for the micro-traces laboratory and certain laboratories within the General Analytical Chemistry service. LIMS is a program that manages the complete analytical process of the laboratories as well as case tracking. It generally includes the requisition data (internal file number, evidence and associated requisition), information regarding the type of analysis requested, and certain specific details unique to each laboratory. The DNA service uses **BsLIMS**, which records, for example, the quantities of DNA obtained for each sample analyzed. The Ballistics laboratory uses **BALWARE**, which contains administrative information as well as forensic elements such as detailed records related to weapons and ammunition components, along with a list of matches established between weapons and ammunition components. The General Analytical Chemistry service uses **LIMSTex**, which also acts as a database for analyzed textile fibers, helping to understand the prevalence of certain types of fibers encountered in cases. Finally, the Drugs and Toxicology laboratories use **DRUWARE** and **TOXWARE** respectively, which include administrative information as well as certain forensic data (identification and quantification of drugs or psychoactive substances). The DIS Service, which manages the DNA databases, do not have a LIMS, as it is not a laboratory.

Next, we find the **databases**, created with sometimes very different objectives. Some were built for comparisons between established profiles for judicial purposes: these include the three **DNA databases** (criminalistic DNA database, convicted persons DNA database, and missing persons DNA database) and the **National Ballistics Data Bank (BNDB)**. The other identified databases act more like libraries and are not designed for comparisons, but rather to establish the prevalence of certain types of traces encountered. This is the case for internal GAC databases created for tool paints, spray paints, gunshot residues and fires and flammable volatile compounds. In a way, LIMS also constitute databases since they contain forensic information for each case. However, they are not used to making comparisons, and the forensic data they contain are not chemical or physical profiles that allow comparison for intelligence purposes. They are not built for that purpose, but rather for management purposes.

A multitude of tools are still used by each service and laboratory to conduct analyses that produce forensic data. These are systems that allow the creation of profiles, the execution of comparisons, the identification and quantification of certain substances, or the extraction and recovery of specific data.

2.2.2.1.3 Forensic data produced by the NICC

2.2.2.1.3.1 The DNA laboratory

The NICC DNA laboratory is one of the five existing laboratories in Belgium. The laboratory performs DNA analyses on exhibits and swabs collected from crime scenes. Experts establish trace profiles and reference profiles (from a suspect). Based on the results, the profiles and/or matches identified are transmitted to the national DNA databases.

2.2.2.1.3.2 The DNA Databases

The DNA databases are managed by the DIS (DNA Index System) service at the NICC. There are three DNA databases:

- **The criminalistic database**: the various DNA Belgian Laboratories conduct DNA analyses on exhibits and swabs taken from crime scene. There are 5 laboratories: NICC (Brussels), IML (Liège), UZA (Antwerp), UZL (Leuven), Eurofins (Brugge, Genk, Hasselt). These laboratories

establish traces profiles and reference profiles (from a suspect). Regarding trace profiles, only the profiles of one or two individuals are transmitted to the NICC's DIS (DNA Index System) service, except for exceptions. As for reference profiles, they are all transmitted to DIS, but not systematically registered. A reference profile is registered in two situations: (1) if it gives a match with the profile of a trace from the same case (2) if it gives a match with a profile already registered in the DNA databases. The database in which these profiles (trace and reference) are stored is the criminalistic database;

- **The convicted offender database**, which records the reference profiles of people convicted of a number of offences. The reference swabs of convicted offenders in Belgium are taken in the various prisons, arrive at the national DNA cell at the Federal Public Prosecutor's Office and are then collected by the Eurofins Germany laboratory, which establishes the DNA profiles and then transfers the data to DIS service, which registers them in the database;

- **The missing person's database**, that records DNA profiles of family members of the missing person, objects that belonged to a missing person and profiles of unidentified bodies or body parts, with the aim of finding missing persons or identifying bodies (not for criminal purposes here).

With the CODIS system, the DNA profiles from the three databases are compared at both national and international levels (via Prüm, for comparison with all European countries). The links between profiles are therefore also recorded. For certain files where there are no suspect and mixed traces from 3 individuals (e.g. the victim and the rest are complete enough to find the author in it), another program is used: Smart Rank. The reference profiles (suspects and convicted offenders) are extracted from databases and Smart Rank will look for matches with other criteria, by proposing a list of potential candidates based on a LR (Likelihood Ratio). It can also be used for partial profile of two individuals.

2.2.2.1.3.3 The Ballistic Laboratory

The ballistics laboratory has several tasks:

- **The examination of ballistic evidence**: firearms, ammunition (cartridges), and ammunition components (shell, casing, and bullet).
- **The comparison of these different pieces** with the ballistic database that contains ammunition components (casings and bullets). This is done semi-automatically.

The ballistics laboratory also manages the National Bank of Ballistic Data (BNDB). The characteristics of each Weapon (brand, model, caliber, dimensions ; presence or absence of a serial number, serial number, presence or absence of a magazine, ammunition capacity, safeties and security of the weapon, sighting, proof marks[1] and associated information (year, country where it is approved, etc.), possible accessories, modifications made, condition of the weapon) are recorded in the BNDB. Bullets and cartridges cases found at crime scenes are also registered.

Reference shootings are carried out with the discovered weapons. The purpose of this trace collection is to compare it with the ammunition elements found on crime scene and recorded in the BNDB. Using the BALWARE LIMS and the Evofinder program, comparisons are then performed. With BALWARE, comparisons are made between ammunition elements from reference shootings and those from crime scenes, producing a list of cases with similar characteristics. Matches are then manually examined. In cases where no weapon is available, Evofinder can be used to compare ammunition elements found

[1] Firearms produced must go through a proof house, which is a control organisation to ensure that each weapon meets defined criteria and is functionally safe. In Belgium, the proof house is located in Liège.

at different crime scenes with each other. A list ranked by similarity (score between 0 and 1) is then generated, followed by manual comparison if necessary.

2.2.2.1.3.4 The General Analytical Chemistry Service

Within the general analytical chemistry service, there are 5 main types of evidence: **gunshot residue** evidence, **fiber** evidence, **paint** evidence, **security ink** evidence (Material analysis laboratory), and **flammable product** evidence (Fires and volatile compounds laboratory). For these different types of evidence, the process is quite similar and generally involves analyzing the spectrum of the different elements. This is the case for paints, fibers and textiles, as well as flammable products. Regarding Gunshot Residue, the objective is to answer the magistrate's specific questions. (e.g., is the question whether the individual was in the shooting environment, if the individual fired, if the person brought a firearm, etc.). An analysis can be carried out to search for particles of interest and quantify them, in order to obtain an accurate picture of the dispersion of gunshot residues according to the context. Regarding security inks, the analysis focuses on the tracers they contain, allowing for subsequent comparison with international databases.

2.2.2.1.3.5 The Drug Laboratory

The role of the drug laboratory is to conduct analyses to identify and quantify drugs, cutting agents, precursors, and medications. To achieve this objective, screenings and spectral analyses are carried out. All analysis results (screening, identification, quantification) are recorded in the LIMS DRUWARE.

The drug laboratory also collaborates with the Clan Lab Response Unit[2] (CRU), which intervenes when clandestine drug laboratories, storage sites, or chemical waste dumps are discovered. Therefore, the drug laboratory lists clandestine laboratories in an Excel file (since around 2015) transmitted at the European level (Europol), including all the elements of the case.

Finally, in 2024, a forensic expertise center was also established within the laboratory, with three main objectives**:**

1. Ensure correct and safe sampling of drugs by the police and customs
2. Develop forensic methods to establish specific drug profiles
3. Create and manage a drug-related database: the goal is to identify trends, produce evaluation reports, and provide additional information to the police and justice system

2.2.2.1.3.6 The Toxicology Laboratory

The role of the toxicology laboratory is to perform toxicological analyses to identify the presence and quantity of certain psychotropic substances (drugs, alcohol, medication) in various natural matrices (saliva, blood, urine, hair). Two types of cases are distinguished: routine cases, which concern 'drugs and driving' (9,000 files per year), and non-routine cases (800 files per year), which include "driver license regranting" cases, general toxicology cases (which can include murder, rape, narcotics cases), and post-mortem cases (research in collaboration with a forensic pathologist). To achieve this objective, screenings and spectral analyses are carried out. All analysis results (screening, identification, quantification) are recorded in the LIMS TOXWARE.

[2] Unit of the Central Directorate for the Fight Against Major Organized Crime (Federal police)

2.2.2.1.3.7 The IT Laboratory

The IT laboratory does not yet conduct routine expertise (for the year 2024, there are no IT files at the time of the interview[3]) but engages in an ISF[4] project aimed at developing two areas of expertise:

- The recovery of photo and video data from various media
- The identification of photos: each camera has a variation in the process used to create pixels (sensors). This information is used to link certain photos or to link multiple photos (from the same source) to the source in question (cameras: smartphone, professional, video, etc.). For this, the service takes photos with the cameras to have references and determine their specific print. Then, it tries to determine if a certain photo is compatible with this print.

The IT department will soon have its own system for storing input data as well as all data extracted during the analysis. The stored data will mainly be photos (JPEG format) and videos (MP4).

2.2.2.1.3.8 Conclusion

The various laboratories and services of the NICC offer a wide range of expertise and enable the production and recording of numerous forensic data, as well as alternative data that could be used in a forensic intelligence context. The following table illustrates and summarizes this diversity of data currently produced by the NICC.

Figure 5: The forensic and administrative data produced or recorded by the NICC.

Service or Laboratory	Forensic Data	Administrative Data
DNA Laboratory	• Quantity of DNA • Trace profiles • Reference Profiles	Requisition Type of analysis requested Notice number Case file date Judicial District related to the case Exhibits and their SIN Number Samples and their number Expert report including results and interpretation Communication that have been carried out Regarding DNA Databases : DNA-be code Regarding Toxicology Laboratory : collector number (related to trace matrice) Regarding Drug laboratory : data on clandestine labs (lab or dumping, type of lab, location, environment Eventual descriptions or photos
DNA Databases	• DNA Profiles (trace; reference from suspect; reference from convinced; reference from familiy members of missings persons • Matchs between profiles and clusters information	
Ballistics Laboratory	• Profiles of bullets and casings from crime scene • Reference profiles of bullets and casings • Matchs between profiles • Physical information on weapons and ammunition components	
General Analytical Chemistry	• Spectrum of analysed fibers • Spectrum of analysed tools, spray and automative paints • Spectrum of security inks • Gunshot residues	
Drugs Laboratory	• Identity and quantity of drugs, medicines, precursors and cuttings agents • Spectrum of drugs (raw data generated during analyses)	
Toxicologic Laboratory	• Trace matrice (saliva, blood, urine, hair) • Identity and quantity of psychotropic substances (drug, alcohol, medication, NPS) • Spectrum of substances (raw data generated during analyses)	

[3] Due to a period of research project development (ISF Project).

[4] Internal Security Fund (Internal Security Fund (2021-2027) - European Commission)

2.2.2.2 Federal Police

2.2.2.2.1 DJT

The Central Directorate of Technical and Scientific Police (DJT) is a specialized entity within the Federal Police that provides technical and forensic expertise to support criminal investigations. Its structure ensures centralized coordination and decentralized execution of forensic tasks across Belgium.

At the top level, DJT consists of three main divisions:

- Management Division – Responsible for budgets, personnel, logistics, ICT, and welfare.
- Strategy and Policy Division – Oversees strategic projects, quality assurance, and innovation.
- Operational Coordination Division (Ops) – Exercises functional authority over specialized operational services that collect and process forensic data.

Under Operational Coordination, five operational services are organized:

1. Biometric Identification Service (BIS) – Handles biometric data such as fingerprints and facial recognition.
2. Disaster Victim Identification (DVI) – Specializes in identifying victims in mass casualty events.
3. Behavioral Sciences (GWS) – Provides psychological profiling, behavioral analysis, and forensic expertise in complex cases.
4. Central Office for Combating Forgeries (OCRF) – Focuses on document fraud and counterfeiting.
5. Expertise Service (Expertise) – Offers technical and scientific expertise in various forensic domains, supporting investigations with specialized knowledge and advanced methodologies.

Additionally, DJT supervises the Laboratories of Technical and Scientific Police (LTWP), which operate at a decentralized level within judicial districts but follow DJT's standards and protocols. These laboratories perform technical and scientific analyses of forensic evidence, ensuring nationwide consistency.

For this research DVI is not considered given the fact they only conduct investigations on a case-by-case basis without collecting data that might be useful for a forensic intelligence tool.

This chapter examines the functioning of the Laboratories of Technical and Scientific Police (LTWP), which operate at a decentralized level but are directed by the Central Directorate of Technical and Scientific Police (DJT). Subsequently, it provides an in-depth analysis of the specific operational services under DJT.

2.2.2.2.1.1 The Laboratory of Technical and Scientific Police (LTWP)

The LTWP performs forensic tasks upon request from both the Federal and Local Police. Their intervention may be required for a wide range of criminal cases, including residential or commercial burglaries, vehicle theft, sexual offenses, assault and battery, arson, as well as suspicious deaths or homicide.
Importantly, the LTWP is also deployed in situations where a crime is not immediately evident, such as in cases of fire or suicide, to rule out the possibility of criminal activity. This proactive approach ensures that forensic expertise is applied consistently, even in ambiguous circumstances, thereby safeguarding the integrity of investigations.

LTWP is composed of two units: CSI and FPL.

A. CSI

Crime Scene Investigation (CSI) units play a crucial role in the forensic process managed by the Laboratories of Technical and Scientific Police (LTWP). Their primary responsibility is to secure and document crime scenes, collect physical evidence, and ensure the integrity of all traces for subsequent forensic analysis.
CSI teams perform on-site interventions for a wide range of incidents, including burglaries, vehicle theft, sexual offenses, assaults, arson, suspicious deaths, and homicides. They also intervene in cases where criminal involvement is uncertain—such as fires or suicides—to rule out foul play.
The tasks conducted by CSI include:

- Scene Documentation: Photography, video recording, sketches, and 3D scanning of the crime scene.
- Evidence Collection: Gathering biological samples, fingerprints, footwear impressions, trace materials, and other physical evidence.
- Preservation and Packaging: Ensuring proper labelling, sealing, and chain-of-custody compliance for all collected items.
- Data Entry in LIMS: Registering collected traces and administrative details in the Laboratory Information Management System (LIMS), which structures cases based on the initial police report number (PV-number).

Through these activities, CSI provides the foundational data for forensic laboratories, enabling accurate analysis and supporting judicial investigations. Their work ensures that evidence is collected systematically, documented thoroughly, and integrated into national forensic databases for further processing.

The traces collected by CSI are recorded in a Laboratory Information Management System (LIMS). Currently, the Federal Police Laboratory (FPL) still uses the previous system, namely LIS2, but the transition to LIMS is expected soon.

Data in LIMS are structured based on the initial police report number (PV-number). When creating a case, each case also receives a specific number at the LTWP level (case number). Subsequently, various types of information can be added to a case: involved persons, legal entities, vehicles, objects, traces, memos, documents, photos, and operators.

CSI creates a case in LIMS based on the initial PV-number. Control mechanisms have been implemented to avoid errors in this process. This entity contains all administrative data about the case, such as the responsible CSI officer, the initial PV-number, the client, file numbers in other databases such as GES and PACOS, a description of the fact based on the crime code, the magistrate involved, the status (investigative or judicial inquiry), the case number of the investigating judge, the modus operandi, the address of the fact and any characteristics of the location, the date of the fact, and the type of damage. Most of these variables can be filled in via pre-programmed drop-down menus.
Next, the case can also include the intervention. This indicates which task was performed (e.g., photography, video, sketch, 3D scans, …), as well as administrative information such as the date and time of the intervention or the number of a subsequent PV.

In addition to the fact entity, there is the person's entity. This stores all data related to the persons in the file (name, date of birth, gender, etc.), both suspects and non-suspects. This is done through a link with the National Register. Suspects can only be added if an APFIS number is known. This information is also linked to the SDB trace database, to which new suspects are automatically added. If a suspect is already known in SDB, all known data are transferred.

The third entity in LIMS is legal entities. This contains all data on legal entities in the file, without distinguishing between suspects and non-suspects. There is a link with the KBO (Business Register).

Next is the vehicles entity. All vehicles involved in this fact are included here. This includes administrative data such as license plate, color, make, SIN numbers, country of registration, and forensic observations made by the laboratory, such as signs of forced entry, condition of the vehicle, the read license plate, and chassis number. This entity is linked to DIV and EUCARIS.

In the Objects entity, the objects collected in a case are recorded. This entity is linked to PACOS based on live data. Information changed in PACOS is also updated in LIMS. This includes, for example, the officer responsible, the unit, the status, storage location, etc. This entity also indicates which tasks need to be performed by FPL if the object is located within its unit. It can also specify whether the object is intended for DNA analysis (DNA coding). The tasks that can be assigned to FPL include fingerprinting, DNA sampling, blood detection, photography, footwear impressions, erased numbers, and others to be described. Each object is described, and its location and packaging method are recorded.

In addition to Objects, there is also a Traces entity, which aims to provide an overview of fingerprints, ear prints, and footwear impressions. CSI receives the overview, while FPL can track the development of traces (LIMS-FPL).
There is also a memo entity for adding general information. This is an open field without length restrictions, and each memo can be linked to other entities (e.g., vehicle, person, etc.).

In the Documents entity, all documents related to the case are collected. Documents can be created using templates or uploaded (e.g., PDF, Excel, …). The FPL report is also made available here.

Photos can also be stored in the Photo File entity. These can be linked to documents. Multiple photo files can be created, each containing several photos.

Finally, there is the operator's entity. Its purpose is to track who worked on the case. It also allows modification of access rights within a case, with options for read-only or written permissions. CSI can only view cases within its own unit and modify its own (personally created) cases. They can also see that colleagues in another unit have created a case in the same file. For example, if a carjacking occurs in Brussels and the Brussels laboratory performs an intervention, they create a case under the initial PV-number. If the vehicle is later found in Antwerp and the Antwerp laboratory performs an intervention, they create a new case under the same initial PV-number from Brussels. They can see that a case already exists within this file number, but they cannot view details or make changes. The Brussels laboratory can grant rights to colleagues in Antwerp.

Thus, there is a national database, but no complete overview or unrestricted access to all data.

In addition to the fact entity, LIMS also includes bindings. These provide an overview of all cases that, based on the initial PV-number, are linked to each other. For example, in the context of one case, multiple interventions may be conducted by CSI. These have different case numbers but share the same initial PV-number and therefore belong to the same fact.

B. FPL

The Forensic Police Laboratory (FPL) receives physical evidence and traces collected by Crime Scene Investigation (CSI) units. It performs specialized forensic examinations, such as fingerprint analysis, footwear and ear print comparison.

FPL currently still works with LIS2, the predecessor of LIMS, but will switch to LIMS in the near future. In addition, they mainly use SDB to enable comparisons between traces.

CSI collects traces and delivers them to FPL. These may include traces collected on gelatine foils or objects that FPL needs to examine for traces (e.g., fingerprints).

FPL processes the traces, enters them into LIS2, and then into SDB. SDB stands for "*Sporendatabank"* (Trace Database). All collected traces and reference traces are stored in this system. Currently, only footwear, ear, and fingerprint traces are included in SDB, although technically it is possible to add other types of traces.

The traces entered into SDB must be validated. They are checked to ensure they meet certain requirements. For example, the resolution of a shoeprint must be 800 ppi. These traces are then oriented correctly, mirrored, if necessary, etc. Once the quality of the traces is confirmed, their status is changed to "accepted."

Administrative information is recorded for each trace (from LIS2, soon LIMS), such as the date of the incident, the file number, the type of trace (E(ar), E(ar)R(eference), S(hoe), S(hoe)R(eference), Finger), the case number, trace number, initials of the responsible CSI officer, and initials of the responsible FPL officer.

Each FPL is responsible for multiple CSI units. For example, Ghent is responsible for East and West Flanders, Antwerp for Antwerp and Limburg, etc.

The method of comparison is determined by each FPL unit individually. In Antwerp, for example, it was decided that traces from CSI Antwerp are only compared with other traces from CSI Antwerp. The same applies to Limburg. For shoeprints, searches are also time-limited (2 months and a maximum of 6 months), as shoes are constantly subject to change. Other judicial districts, however, compare traces across all of Belgium.

The results are then forwarded to CSI, which includes them in their official report (PV) and delivers them to the investigating unit.

The analysis of crime scene evidence and the subsequent transmission of data to the Federal Police Laboratory (FPL) is a time-intensive process. After CSI units collect and document traces, these must be transported to FPL, registered in the laboratory information systems, validated, and analyzed before results can be communicated back to the investigating authorities. This multi-step workflow inherently introduces delays, meaning that forensic results often reach investigators only after a considerable period.
The duration of this process is strongly influenced by two critical factors: budgetary limitations and personnel availability. Current staffing levels within both CSI and FPL are insufficient to meet the growing demand for forensic services, resulting in backlogs and extended turnaround times. Budget constraints further restrict the ability to invest in advanced technologies, additional personnel, and streamlined processes. Consequently, while forensic analysis remains a cornerstone of modern investigations, its operational efficiency is highly dependent on resource allocation.

2.2.2.2.2 BIS

The Biometric Identification Service (BIS) constitutes an essential component of the Belgian forensic landscape, where fingerprints and other biometric data are processed for the purposes of criminal investigations. The service has evolved from a traditional "store everything" system to a more refined approach that considers privacy regulations and operational efficiency.

The original paradigm of the service was based on the principle that more fingerprints automatically led to more identification possibilities. This resulted in a policy in which all data, both from suspects and from innocents, were permanently stored without systematic cleansing of the database. Although attempts are now being made to apply statutes of limitations, the practice remains complex due to the nature of criminal procedures, in which new facts often lead to the extension of retention periods.

A. Organization and structure

The BIS historically operated according to a cumulative model in which all biometric data were stored under the motto *"whatever we can have, we take."* This paradigm was aimed at maximizing identification possibilities by creating the most extensive database possible. The consequence of this approach was that both suspects and innocent individuals remained permanently in the system, without systematic cleansing.
Over time, the service has taken steps to revise this policy. Attempts are now being made to respect statutes of limitations and to conduct periodic cleansing of the database. However, this evolution is complicated by the realities of criminal procedures, in which individuals are often involved in multiple cases over different periods. This regularly leads to statutes of limitations being reset, meaning that individuals effectively remain in the system for long periods.

An important operational distinction within BIS concerns the different treatment of data from suspects versus victims. For suspects, comparisons are conducted against the entire database, consulting all available reference data. This broad comparison process is aimed at identifying connections with previous cases or known individuals in the system.
By contrast, victim data are only compared within the context of their specific case file. No comparison is made with the broader database, even if potential matches might exist with other cases. This approach respects the privacy of victims and prevents unwanted links that are not relevant to the specific investigation.

A notable difference between the fingerprint database and the DNA database concerns the anonymization of data. While DNA data can be anonymized, fingerprint data remain linked to identifiable personal information. This choice is operationally motivated, since full anonymization would undermine the practical usability of the system. The need to connect biometric data to specific identities requires that this link be preserved somewhere within the system.

B. Data processing procedures

The BIS applies to two main categories of biometric data, each undergoing a specific processing workflow. The first category concerns fingerprints with known identity, originating from individuals who have been arrested or otherwise come into contact with the justice system. The second category consists of traces of unknown origin, generally collected during crime scene investigations.

Fingerprints with known identity are collected within the framework of the so-called *"judicial triptych"*, a standard procedure that includes three elements: descriptive data (name, first name, date of birth, physical characteristics), photographic documentation (face, profile), and biometric data (fingerprint and palm prints). For each person, 24 prints are systematically taken, consisting of rolled and flat fingerprints plus palm prints.
The system operates according to a *"lights out"* principle for standard processing, meaning automatic comparisons are performed without human intervention. Within eight minutes of receiving new fingerprints, the police district receives an automatic report stating either *"hit"* or *"no hit"*, depending on whether the person is already known in the system.

When a person is not known, they are added to the database with a unique identification number. For individuals already known, the information is added to the existing profile, including historical data and any aliases. This rapid response time is crucial, as police officers are legally required to establish the identity of an arrested person within 12 hours.
The automatic system is supported by a quality control mechanism. When prints are of insufficient quality or inconsistencies are detected (for example, swapped fingers), the process is paused and forwarded to human operators for manual verification and correction.

Traces collected from crime scene investigations follow a more complex processing workflow. These traces are analyzed by the Forensic Police Laboratory (FPL) and transmitted in digital format to BIS via specialized stations. The traces are grouped per case file and assigned to fingerprint experts based on urgency and workload.
Urgency is determined by the magistrate: urgent cases are processed within D0 (same day), while regular cases are processed within D2 (two days). This phasing allows the service to distribute workload evenly among available staff, considering the complexity of different case files.
The analysis of crime scene traces begins with a preliminary automatic comparison against the database. This first step usually produces candidates of limited quality, as raw traces often contain artifacts or ambiguities. The fingerprint expert then refines the search by selecting specific areas for analysis.
The system generates candidates with associated characteristic points, which are manually evaluated by the expert. This evaluation involves adding, removing, or modifying these points based on professional expertise. For a positive identification, at least 12 points are required, although fragmentary traces may also be used if sufficient reliable features are present.

C. International cooperation

The BIS maintains extensive international connections for cross-border identification. The system is directly linked with nine European countries and has access to databases in the United States. For other countries, cooperation takes place via CGI (Interpol) networks, which provide worldwide comparison possibilities.
This international cooperation, however, faces practical limitations, including daily quotas for international comparisons. A maximum of five international comparison requests can be submitted per day, forcing the service to strategically prioritize cases.
The service operates within various European cooperation frameworks, each with specific characteristics and applications. The Prüm system facilitates direct comparisons between member states according to a *“touch and go”* principle, whereby comparisons are conducted, and results are immediately returned without permanent data storage.
The SIS Recast system, by contrast, offers persistent search functionality, with data remaining active for three years and automatically compared with new entries. This system is particularly valuable for complex, long-term investigations where identification may only become possible after some time.
A recent development concerns the implementation of “Article 40 procedures”, which allow traces to be placed in international systems for three years. This procedure, however, has strict limitations regarding the nature of crimes (only serious criminality) and requires proof that traces are *“with high probability”* from the perpetrator.
This requirement has led to the development of new procedures in which crime scene investigators (CSI) assess the likely origin of traces during collection. This assessment categories traces as probably originating from the victim, the perpetrator, or as undetermined.

D. Future vision

The BIS is preparing for a significant technological upgrade with the implementation of the **Automated Biometric Identification System (ABIS)**, replacing the current AFIS (Automated Fingerprint Identification System). This transition, planned for the end of 2026, introduces a modular, multimodal approach to biometric identification.
The new system will begin with two modules: fingerprint analysis and facial recognition, with plans to expand to voice comparison in the future. This modularity enables the service to gradually integrate new identification technologies without requiring full system replacement.

Currently, BIS conducts facial comparisons on a one-to-one basis, where photos of suspects are compared with reference material from specific case files. These comparisons require that investigating judges explicitly designate a suspect and provide reference material from official sources such as the ANG (General Database) or the National Register.
The new ABIS system will enable one-to-many comparisons through the integration of a photo library, allowing photos of unknown individuals to be compared against the entire database of known people within the judicial system. This expansion of capabilities does, however, require human specialists to evaluate the candidates generated by the system using 19 comparison criteria.

2.2.2.2.1.3 GWS

The Behavioral Sciences Service consists of four separate departments. Three of these services operate on a case-by-case basis and are therefore only briefly discussed in this report. Within the framework of this project, emphasis is placed on the ZAM-VICLAS department, a database developed in Canada that is designed to identify patterns and connections between violent crimes, particularly sexual offenses and murders with a sexual motive.

A. Behavioral analysis (GAC)

The Behavioral Analysis Department employs four psychologists and one sociologist who provide specialized psychological expertise for complex criminal investigations. Their main tasks include assisting in the interrogation of difficult individuals, such as those with psychopathic tendencies, and preparing detailed profiles of suspects in unsolved murder cases where the perpetrator’s identity is unknown.
In addition, this department analyses various forms of threats, including letters and text messages, to assess the credibility and urgency of potential dangers. The team examines behavioral indicators and communication patterns to aid in the identification of individuals and in risk assessment.
The GAC operates on a case-by-case basis, without maintaining a central database of its work.

B. Polygraphy (POLY)

The Polygraph Department consists of seven police officers who conduct polygraph tests as an investigative tool. This department also operates on a case-by-case basis, without systematic integration into a database, and responds to specific requests from investigative units when polygraph tests are deemed necessary for the progress of a case. The officers in this department have received specialized training in administering and interpreting polygraph tests, enabling them to provide technical expertise in investigations where the assessment of truthfulness is of crucial importance.

C. Technique of Audiovisual Interviewing of Minors, Victims, or Witnesses of crime (TAM)

The Audiovisual Interviewing of Minors Department (TAM) consists of two French-speaking specialists and one Dutch-speaking specialist who focus specifically on the specialized field of interviewing minor victims and witnesses. The main task of this department is to train police officers throughout Belgium who conduct interviews with minor victims and witnesses, ensuring that these sensitive interactions follow established protocols designed to minimize trauma and maximize the quality of the information obtained.
The TAM department also maintains statistical databases related to its requests, recording key data such as the frequency of interviews, the age of the children interviewed, the types of crimes, and the judicial districts and magistrates that most frequently call upon TAM's services. At present, the department is developing, in collaboration with IT services, a centralized data system based on SharePoint to modernize methods of data collection and storage.

D. Sexual Offenses Analysis (ZAM-ViCLAS)

The Sexual Offenses Analysis Unit (ZAM-ViCLAS) consists of a total of seven staff members, including two operational officers and five CALOG employees. The linguistic composition includes three Dutch-speaking and four French-speaking analysts who together cover the entire Belgian territory. The main task of this unit is the management of the ViCLAS database and conducting crime linkage analyses for violent rapes and sexually motivated murders, although the system can, in principle, also be used for other types of criminal offenses.

a) Structure and data processing

The ViCLAS system currently used in Belgium is version 5 of the crime linkage analysis system developed in Canada. Belgium is the first country outside Canada to implement this latest version, following the strategic decision to adopt the system without modifications to maintain full compatibility with the original Canadian framework. This decision was made to ensure rapid implementation and preserve consistency with international standards, although it has led to some adaptation challenges within the Belgian context.

The ViCLAS system uses a comprehensive questionnaire structure consisting of 153 variables designed to capture detailed information about criminal acts and offender behavior patterns. These questions are divided into two main categories: multiple-choice questions with checkboxes for standardized answers and open-ended questions that allow for detailed descriptions of incidents and additional contextual information.
The multiple-choice questions cover a wide range of behavioral and situational factors, including offender behavior patterns, methods of approaching victims such as deception, violence, or manipulation, detailed characteristics and physical descriptions of offenders, geographic and temporal factors related to the crime, specific sexual and violent behavior during the offense, and verbal communication or threats by the offender. The open-ended questions mainly focus on chronological descriptions of incidents, providing a comprehensive account of the criminal events, with space for additional information that does not fit into the structured question format.

The process of coding information into the ViCLAS system involves several stages that require significant manual intervention and expertise.
The initial assessment phase consists of reviewing police reports (PV's) to determine whether they meet the ViCLAS criteria and contain sufficient behavioral information to be included in the database. For this assessment, analysts must evaluate the quality and completeness of the information in the police reports.

After the initial review, qualified analysts conduct the data entry process, manually inputting behavioral elements and incident details into the framework of 153 questions. This process requires careful interpretation of the descriptions in the police reports and victim statements to identify relevant behavioral indicators and situational factors. Analysts must have sufficient expertise to recognize significant behavioral patterns and translate descriptions into the structured format required for the database.
Following the initial data entry, quality control procedures are applied to check the completeness and accuracy of the entered data. At this stage, it is verified whether the information has been correctly interpreted and entered, and whether all relevant behavioral indicators have been captured. Finally, the verified data is integrated into the searchable database structure, making it available for future analytical queries and linkage analyses.
The time required for this coding process varies significantly depending on the complexity of individual cases. Simple cases with clear descriptions typically take about two hours, while complex cases involving extensive victim statements, multiple incidents, or detailed behavioral descriptions may require several hours or even days. The subsequent analysis phase, in which analysts search for possible links to existing cases, can take anywhere from one day to a week, depending on the number of identified potential connections and the complexity of the behavioral patterns.

The ViCLAS system enables advanced multi-parameter searches, allowing different types of information to be combined to identify possible links between criminal incidents. Analysts can construct queries based on offender demographics—such as age, race, and physical characteristics—geographic parameters, including location and proximity relationships—behavioral patterns, including approach methods and verbal communication, levels of violence and specific sexual behavior—and victim characteristics and relationship dynamics.
The linkage analysis method requires analysts to manually construct searches that strike a balance between stable behavioral elements and more variable characteristics. Stable elements may include consistent behavior patterns or distinctive physical features, while variable elements may include clothing descriptions or vehicle information that can change over time. The system relies on human interpretation and expertise to:

- assess potential links between cases,
- evaluate the geographic feasibility of links, taking offender mobility patterns into account,
- analyses temporal factors and their significance for potential connections, and
- weigh the need for specificity against the need for broad pattern-recognition capabilities.

b) Operational workflow

The official procedure for processing ViCLAS cases is outlined in COL 04/2020, which establishes the theoretical framework for how cases should progress from initial police reports to analysis by ViCLAS. According to these regulations, investigators must prepare comprehensive police reports (PV) that capture relevant behavioral and situational information about criminal incidents. These reports should then be processed by AIK (Arrondissemental Information Crossroads), where staff review and categorize them according to established criteria.
The regulations stipulate that reports of sexual offenses and murders with a sexual component must automatically be forwarded to the ViCLAS-ZAM unit for potential inclusion in the database. Upon receipt, ViCLAS analysts code relevant behavioral data into the database system, after which a systematic comparison with existing database entries is conducted to identify possible links. This workflow is designed to create a streamlined, largely automated process that ensures comprehensive coverage of eligible cases while minimizing the need for manual intervention.

The implementation of this intended workflow varies significantly across different regions of Belgium, resulting in considerable inconsistencies in case handling and database coverage. In Flanders, SICAD

functions relatively well, with regular forwarding of police reports to the ViCLAS-ZAM unit. However, even in this better-functioning region, occasional issues arise with excessive inclusion, where cases that do not meet ViCLAS criteria are forwarded, requiring additional filtering and triage by ViCLAS analysts.
The situation in the Walloon Region, particularly in areas such as Hainaut, is much more challenging. In these regions, cases are rarely forwarded automatically to ViCLAS, forcing analysts to manually retrieve cases. This means that ViCLAS staff must review crime bulletins daily to identify potential cases and then contact local police zones directly to request specific reports. This process is highly inefficient and consumes time that could be better spent on data entry and analysis.
Due to reliance on individual relationships rather than systematic processes, some experienced ViCLAS analysts have built personal networks with investigators and police zones in their assigned regions. While this has helped maintain a certain level of functionality, it raises concerns about sustainability in the event of staff turnover and deviates from the intended systematic approach.

One of the main operational constraints faced by the ViCLAS unit is the lack of direct access to ISLP (the police reporting system where PVs are created) for ViCLAS analysts. This limitation forces the unit to rely on the transfer of PV documents via email instead of integrated systems that would allow direct access to relevant reports. The inability to access ISLP directly results in multiple layers of inefficiency and dependence on external staff for access to basic information.
Although management acknowledges this issue, attempts to resolve it have been unsuccessful. Requests to IT services to implement direct ISLP access for ViCLAS personnel have been denied or postponed, citing technical complexity and integration challenges. The absence of a dedicated ViCLAS destination code within the ISLP system exacerbates the problem, as there is no systematic way to automatically flag and forward relevant cases to ViCLAS staff.

The implementation of ViCLAS procedures is hindered by inconsistent application across the various SICAD centers in Belgium. Some centers actively identify and forward relevant cases, while others lack the staff or training to effectively execute the procedures. Many SICAD centers do not have dedicated ViCLAS contact personnel, and where such roles exist, they are often filled by individuals with numerous other responsibilities, making it difficult for them to focus on ViCLAS tasks.
The lack of systematic training and awareness among frontline police further exacerbates these challenges. While officers specializing in sexual offense investigations have received some ViCLAS awareness training and generally pay more attention to relevant behavioral details, general patrol and investigative units often lack insight into which information is crucial for ViCLAS analysis. This results in police reports that may omit detailed behavioral observations necessary for effective database analysis.

c) System limitations and adaptation challenges

The decision to implement ViCLAS version 5 without modifications has created several adaptation challenges within the Belgian operational context. The system was specifically designed for the Canadian legal and cultural environment, and some elements cannot be directly transferred to the European criminal justice context. For example, the demographic classification system includes categories such as “Aboriginal,” which are of limited relevance in Belgium, while categories that better reflect Belgium’s demographic composition—such as specific classifications for North African populations—are missing.
To address these limitations, Belgian ViCLAS personnel have developed internal adaptation strategies that preserve the integrity of the database while meeting local needs. These include repurposing existing categories to reflect Belgium’s demographic reality, such as using the “Indigenous” classification for North African suspects and maintaining internal documentation on category reinterpretations to ensure consistency among analysts. While these adaptations allow the system to

function within the Belgian context, they represent compromises that may limit analytical accuracy and comparability with other national ViCLAS implementations.

The ViCLAS system currently operates as a standalone database with limited connectivity to other law enforcement information systems. This isolation results in significant inefficiencies and reduces the system's analytical potential. Analysts must perform time-consuming manual cross-references when accessing information from other databases, and the fragmented information landscape diminishes overall analytical effectiveness.
Database modifications pose a particular challenge due to the large volume of historical data stored in the system. With more than 11,000 cases coded using the current classification systems, changes to variable definitions or category structures would require extensive data migration and validation processes. There is legitimate concern about the risk of data corruption or loss of analytical consistency if changes are implemented retroactively. This concern has contributed to resistance to system modifications, even when such changes could improve operational effectiveness.
The standalone nature of the ViCLAS system also limits the ability to perform automated cross-references with other forensic databases. Currently, all links between ViCLAS behavioral analyses and physical evidence—such as DNA profiles—must be identified through manual processes initiated by investigators, rather than through systematic database integration that could automatically detect potential connections.

2.2.2.2.1.4 Central Office for combating Forgery OCRF

The Central Office for Combating Forgery (OCRF) has been streamlined into two divisions. The Documents Division is located in the Federal Police buildings, while the Counterfeit Currency Division is physically housed within the National Bank. This organizational separation stems from a European Commission requirement mandating that each member state address counterfeiting in accordance with established directives.
Belgium occupies a unique position within Europe, as it is one of only two member states—alongside Spain—where police officers are physically stationed inside the National Bank. Belgium further distinguishes itself by having these officers not only present in the bank but also working on the same platform as the National Analysis Centre (NAC). The Counterfeit Currency team consists of four members, while the Documents Division has twelve staff members.
The phenomenon of document control is divided between administrative police and judicial police. The DJT-Documents service falls under the judicial police, which represents a fundamental difference compared to border controls, which belong to the administrative police and fall under the NALB (National Agency for Aviation and Inland Navigation). This division implies different working methods and responsibilities.

A. Documents

The primary responsibility of the OCRF- Documents service is to determine the authenticity of identity documents. Unlike border controls, where documents are compared to the person presenting them, this service mainly works with documents without the accompanying individual. Most often, they receive a document or, at best, a scan whose quality is not always optimal.

A particular challenge faced by the service involves "impostors." These are individuals who use genuine passports that have been lost or stolen. This method is frequently employed by people attempting to enter Europe via Greece. Criminal organizations maintain libraries of original documents and select documents based on physical resemblance to the user. After use, these documents are often returned to the criminals via the same means of transport.

The service distinguishes three primary categories of document forgery:

1. Completely fake documents manufactured from scratch.
2. Altered documents, where original documents are modified or tampered with.
3. Original documents issued based on false source documents—the most complex category.

An illustrative example of the third category involves a case in a municipality where officials issued driver's licenses during their lunch breaks to individuals who could not provide valid documents. These licenses were sold for amounts ranging from €3,000 to €10,000, depending on the type of license. Approximately 400 licenses were created in this manner before the fraud was uncovered.

One of the largest information streams comes via Project Europe, which involves EU nationals who must register with a municipal or city administration after a certain period. According to guidelines, these administrations must scan identity documents and forward them to the DJT-Documents service. Each year, the service receives approximately 56,000 scans of residence permits, identity cards, and passports.
Working with scans, however, presents significant limitations, as certain security features, such as UV and infrared detection, cannot be verified on scanned documents. This greatly restricts authentication capabilities, and sometimes the service must conclude that a document cannot be authenticated based on the available scan.
When a document is assessed as authentic, the municipality is generally not notified due to capacity constraints. For suspicious or forged documents, the local police are informed, who then initiate an investigation and question the individual. If necessary, the physical document is sent to the DJT-Documents service for further authentication.

The second major processing channel involves foreign driver's licenses that must be exchanged for Belgian licenses. Individuals who stay in Belgium for more than 180 days or are registered must exchange their foreign license. Each year, approximately 13,000 licenses are physically examined by the service.
These licenses come directly from municipal administrations or via local police acting as intermediaries. Each license is accompanied by an inventory sheet. When a license is deemed authentic, it is returned to the municipal administration. For suspicious documents, the license is sent to the local police for further investigation.

In addition to regular document processing, the service also provides operational support. This can range from roadside checks by traffic police to joint actions with the National Social Security Office (RSZ) or raids by the Social Inspection. The service has also assisted in bicycle checks in Liège and collaborates with various Federal Judicial Police (FGP) units that submit documents for verification.

The main system for document management is BrainGate, currently operating in version 2. The original BrainGate 1 was developed by an internal staff member and featured advanced functionalities such as facial recognition and automatic verification of Machine Readable Zones (MRZ). This system could automatically check whether names were already present in the database and offered extensive control features.
When the original developer retired, the system was taken over by DRI (Directorate of Investigative Information). However, BrainGate 2, developed under DRI's management, has become a "flat database" without the advanced features of its predecessor. Facial recognition, automatic MRZ checks, and other intelligent tools have been removed, significantly complicating the work.

In addition to BrainGate, the service uses the FADO system, a database maintained by the Council of Europe, which is currently in a transition phase and will be taken over by Frontex. FADO contains

descriptions of identity documents from all EU member states, complete with images of security features.
The system has three access levels:

- FADO Perl: Accessible to only a few individuals per member state (in Belgium, this is limited to two people).
- eFADO: Less detailed but available to staff trained in document expertise, such as border control officers.
- PRADO: Publicly available online but includes only security features visible to the naked eye.

Access to FADO is strictly controlled. The two Belgian administrators work in a separate locked room. Only they have access to the key, and visitors must register. Recently, an audit was conducted by twelve representatives from the Council of Europe, verifying all security measures, including the requirement that computer screens face inward to prevent outside viewing.

A major practical issue faced by the service concerns the management of the large volume of documents received via email. Mailboxes cannot manage the storage capacity required for all incoming scans. Documents assessed as authentic eventually disappear from the mailbox to make room for new messages. There is no systematic archiving or database that tracks which documents have previously been verified.
This approach leads to inefficiencies, as the same person may be checked multiple times when moving to a different municipality. There is no mechanism to prevent duplicate work or to consult historical verifications.

A significant problem involves the varying quality of scans provided by municipal administrations. A survey by DVZ revealed that only half of the municipalities responded to questions about Project Europe. Among respondents, some did not follow procedures correctly, resulting in poor-quality scans or complete failure to send documents.
Some municipalities send emails from “no-reply” addresses, making communication impossible. Contact people frequently change roles, causing communication lines to break down.

The normal processing time for documents is two to three weeks from receipt. However, some documents are already six weeks old by the time they reach the service, indicating delays at municipalities or local police. The service attempts to work chronologically according to the “first in, first out” principle, but capacity constraints and staff shortages can lead to longer waiting times.

B. Money

Counterfeit banknotes are primarily detected within the banking sector during quality control checks. Banks are required to perform at least one quality check per banknote before recirculating it. During this process, counterfeit notes are identified and forwarded to the National Analysis Centre (NAC).
Each counterfeit note receives a codification assigned by the European Central Bank (ECB) in Frankfurt. This coding system enables linking notes from the same counterfeit series, even across national borders. For example, if Belgium finds fourteen banknotes with the same codification in different locations, and the same code also appears in Germany and the Netherlands, an operational meeting can be organized to trace the source.
The NAC prepares case files for counterfeit currency and forwards them to the DJT service. These cases usually involve complaints against unknown people, as the identity of the individual who deposited the counterfeit money cannot be established. The service drafts a police report (PV) and sends it to the public prosecutor’s office, where it is typically dismissed due to the inability to identify the perpetrator.

Although this procedure rarely produces concrete results, it is important for intelligence and statistical purposes. The files help identify counterfeiting patterns, particularly in the Brussels metropolitan area, where most issues occur.
DJT does not manage its own database on counterfeit currency.

2.2.2.2.2 DJSOC

DJSOC possesses specialized expertise and conducts strategic and operational analyses of criminal phenomena. These analyses are shared via the Centrex platform and contribute to the policy-making capacity of police services. In addition, DJSOC coordinates the implementation of the so-called Intel strategy, which focuses on an intelligence-led approach to crime.

2.2.2.2.2.1 GES

The primary platform used by DJSOC for data collection is GES, but it is not used uniformly across all units. There is flexibility in how information is entered, which leads to inconsistencies in data storage.

GES serves as the central case management system for investigations within the Belgian police and fulfills three essential functions:

1. Information Aggregation
   It collects all information from one or multiple files within an investigation. A file acts as a container with a title that can include various elements. An investigation may focus on a single case, a single note number, or multiple files involving different phenomena or individuals—ranging from sexual offenses to theft. All information is gathered under the supervision of an investigation director, either the examining magistrate or the public prosecutor during the initial phase.
2. Cross-Referencing and Analysis
   GES facilitates data matching and analysis, enabling investigators to trace investigative leads. The investigation director can decide to explore different directions, such as fiscal aspects, suspect identification, tracing stolen goods, or mapping multiple victims.
3. Task Management
   GES manages assignments within an investigation team. The investigation leader can organize the case by dividing it into tasks, which are then assigned to specific investigators, ensuring efficient distribution of workload within the team.

GES is connected to several external systems essential for police work:

- Itinera: Facilitates information exchange between police and judiciary, specifically with the MAG at the Ministry of Public Prosecution. Through this tool, police can obtain information about the status of cases, whether they are still under investigation, if individuals are being prosecuted, or if the case is going to court. It also allows sending mandatory documents such as margin notes.
- National Bank Link: A relatively new development, operational for two to three years. This connection enables sending requests to a central service to identify which banks and financial institutions a suspect has accounts with. The system provides near-complete visibility of all institutions active in Belgium—a significant improvement compared to the old process, which required sending over 250 faxes to different institutions.
- Mercure: While not a database, Mercure plays a key role in investigations. Based on data obtained from telecom operators via subpoenas, Mercure can cross-reference information, generate statistics, and establish links between different elements. It can correlate phones,

group related data, and visualize this information on a map. Data from Mercure is then entered into GES, becoming part of the case file.

All police tools are systematically linked to authentic sources such as the National Register and DIV (Vehicle Registration Service). These connections form a baseline standard, enabling reliable identification data collection during investigations.

One of the key functions of GES is the designation of targets, a term in police terminology referring to individuals for whom coordination is requested. This information is transmitted to the General National Database (ANG) via a DOS, which stands for “dossier.” A DOS acts as an information carrier containing various elements of the investigation, such as identification details, responsible parties, and, most importantly, all individuals for whom coordination must be organized.

How the System Works
When an investigation identifies two potential suspects, these individuals are entered into the ANG through the DOS. This means that anyone in Belgium can see that these two individuals are under investigation. For example, if an officer in Arlon conducts a query during an investigation, they can see that a colleague in Knokke has also investigated the same person. This enables coordination between different teams.
It is important to understand that this system operates under the consultation purpose, which is focused on investigations, and not under the control purpose, which is used to check whether someone is subject to a measure or needs to be arrested. The DOS and the flow from GES to ANG are specifically intended for investigation coordination.
This system was introduced following the Dutroux case investigation and has been active since 2006. Its goal is to improve national coordination and prevent different police units from working independently on the same cases.

Operational analysts make little use of GES because they do not draft police reports (PV). Their information mainly enters GES through PVs prepared by others or via investigative actions. However, this process involves significant delays, as PVs are often completed and entered days or even weeks after an investigation begins.

An important system for operational analysts is Mercure, which supports much of their daily work. This system consolidates telephony data, retrospective analyses, cell tower queries, wiretaps, ANPR (Automatic Number Plate Recognition) data, beacon data, and extracted phone contents. For about a year now, extracted phone data has been automatically entered into Mercure from the RCCU, reducing dependence on the speed and willingness of investigators.

A fundamental issue is that access to various systems is geographically restricted. For example, Mercure and GES in Antwerp are only accessible for Antwerp-specific data. Although, in theory, links to other regions are possible, this rarely happens in practice. Local police zones use their own Mercure systems, but these are not connected to the federal system.
There is, however, a possibility for certain entities to consult all GES data, presumably at a central level for statistical purposes. The system is designed to allow a centralized overview, but this is not accessible to individual investigation teams.

A striking feature of the current workflow is that information exchange largely occurs on a case-by-case basis. Intelligence analysts typically work upon requests from investigation teams and depend on what these teams choose to share. There is no systematic process that automatically consolidates all relevant information.

Data is stored in multiple locations: in physical files held by investigators, in shared OneDrive folders, on SharePoint sites, and in Teams channels. Operational analysts must actively search for this information and only have access to SharePoint sites to which they are explicitly added. This results in fragmented information flows where critical data can easily be missed.

To establish connections between different data sources, services rely on common variables. For the laboratory, the note number is the primary identifier. For operational analysts, everything begins with a case name, which is linked to the initial note number. This case name serves as a "hook" for all related information and is used in Mercure, on SharePoint sites, and in other systems.
The laboratory retroactively integrates this case name into its LIMS system once it becomes known. Although one case name can include multiple note numbers, Mercure only registers the initial note number. Links to other note numbers must be found manually and stored elsewhere.

A major technical limitation is that many systems do not communicate automatically with each other. While the infrastructure often allows for integration, there is a lack of standardization and mandatory procedures. As a result, information must be transferred manually between systems, which is time-consuming and prone to errors.

2.3 Mapping of the potential exploitation for forensic intelligence

In this part of the project, particular attention is paid to the potential links between the different data to identify the different possible levels at which a forensic intelligence model can be made. This approach is grounded in a rigorous analysis informed by the literature review and mapping work conducted in the preceding stages. The literature-based analysis seeks, more specifically, to provide a conceptual framework for understanding the modalities of forensic intelligence production, thereby enabling a clear and concrete distinction of development opportunities within the Belgian context. The mapping analysis, in turn, will serve to identify existing intelligence practices and to formulate a set of realistic perspectives, drawing upon the theoretical foundations previously established.

2.3.1 Existing Forensic intelligence practices in Belgium

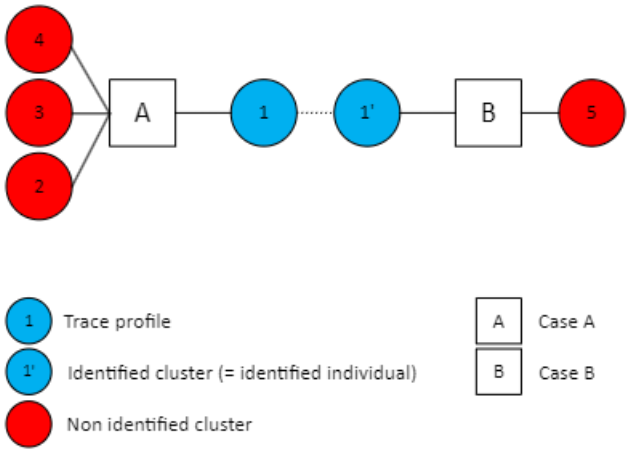
2.3.1.1 Forensic intelligence practices at the National Institute of Criminalistics and Criminology

Three operational forensic intelligence practices have been identified at the NICC level:

- The first is related to **DNA databases**. The service receives DNA profiles (trace and reference) from various DNA laboratories in Belgium and compares them with DNA databases that also include trace and reference profiles. As a result, links can be established between different cases, which opens up various possibilities for investigations, particularly for identifying a suspect in a case. In this regard, the primary purpose is **tactical**. In *Example 1*, a trace profile from case A is compared to the DNA databases and matches a recorded identified cluster[5] from case B, allowing a link to be made between an individual and the trace left at the crime scene. Thus, this seems to indicate that the individual involved in the events in case B also participated in the events in the new case (A). Another example is that two trace DNA profiles can also match. While this may not identify a suspect, it can provide valuable information by linking two judicial cases and potentially opening new investigative leads. The advantage of the DIS service is also that matches are tested at a European level.

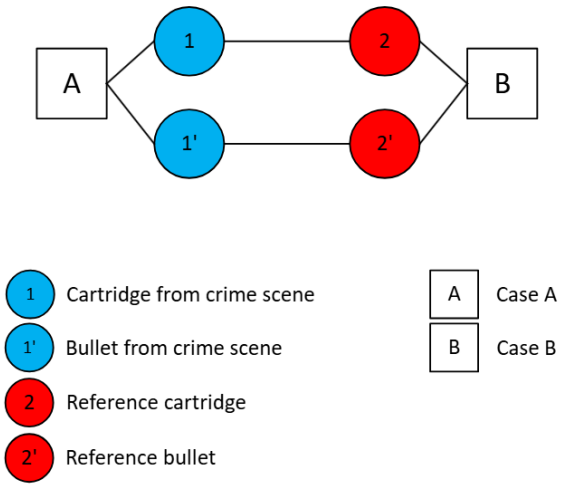
[5] An identified cluster means that in a case, a trace profile has been linked to a reference DNA profile.

Example 1: Representation of a link established between a trace profile from Case 1 and an identified cluster from Case B.



- **The ballistics laboratory** also offers interesting possibilities in terms of forensic intelligence. Indeed, the presence of a national ballistics database listing weapons, bullets, and casings from crime scenes as well as reference samples allows for **the establishment of links between weapons and ammunition elements (bullets and casings) and, therefore, between different cases**. In *Example 2*, case A containing casings and bullets whose characteristics have been analyzed can be linked to a weapon found in case B through reference shots carried out in the laboratory (showing that the reference casings and bullets match the casings and bullets found in case A). This may mean that the weapon used in case B was previously used in case A, which provides additional informational value for the investigation. These comparisons are already carried out.

Example 2:. Representation of a link established between reference ammunition elements and crime scene ammunition elements



Finally, a last forensic intelligence practice exists within the drugs laboratory. For several years, chemical profiling of all amphetamine samples seized in Belgium has been carried out. The established profiles are recorded and compared in and through a European amphetamine database to identify

potential links. The aim is to control the international trade in amphetamine. The NICC represents Belgium as a partner within the European Drugs Profiling System (EDPS).

2.3.1.2 Forensic intelligence practices at the Federal Police

Within the federal police, the structured application of forensic intelligence remains limited. Although operational and strategic analysts engage in intelligence activities, there is no systematic use of integrated databases. Nevertheless, three existing systems can be identified that already embody limited forms of forensic intelligence.

- The first example is the **'Sporendatabank' (SDB).** This database collects and compares ear and shoe prints, thereby enabling the establishment of links between individuals and traces, as well as between different crimes, even when the donor of the trace remains unknown. The SDB thus represents a tactical application of forensic intelligence, primarily aimed at supporting ongoing investigations. Its value is constrained though by the inconsistent comparison policies across FPL units.

- A second example can be found in the **Biometric Identification Service (BIS)**. Here, forensic intelligence is also applied mainly from a tactical perspective. Fingerprints that are added to the database are automatically compared with all unidentified traces stored in the system. This continuous comparison can lead to breakthroughs in cold cases where identification was previously impossible. It is important to emphasize, however, that each match constitutes only a suggestion. Human verification remains indispensable, as the results must be manually checked, contextualized within the relevant case file, and validated by expert assessment.

- Finally, the **Violent Crime Linkage Analysis System (VICLAS)** also operates at a tactical level of forensic intelligence. By collecting the characteristics of different cases in a database, dossiers can be linked and patterns identified. At present, however, VICLAS functions as a standalone database with limited connectivity to other law enforcement information systems. This isolation generates significant inefficiencies and reduces the analytical potential of the system.

In summary, while the federal police already employ databases that support tactical forms of forensic intelligence such as SDB, BIS, and VICLAS, a structured and integrated approach is lacking. The current fragmentation and limited interoperability diminish the strategic value of these systems and restrict their contribution to the broader intelligence cycle.

2.3.2 Existing Forensic Intelligence perspectives in Belgium

Various concrete forensic intelligence practices are already in place in Belgium. However, these practices are primarily reactive, with the intelligence product serving a tactical intelligence objective. This is the case with DNA of SDB, where profiles of DNA, shoes, etc., comparisons with databases allow, for example, the identification of a suspect. The ballistic laboratory follows a similar logic with the comparison of ammunition elements, offering, for example, the possibility of linking ammunition found at a crime scene to a weapon found in another case, via reference shots. However, other forensic intelligence perspectives with a more proactive logic exist, such as cluster network analysis (DNA) or the analysis of links between modified weapon characteristics (ballistics). These analyses would serve both tactical and operational intelligence objectives by identifying criminal networks and thus providing valuable information to address a specific problem within a certain area of action. However, these practices are not yet implemented. Notably, an exception is the creation of the forensic expertise center within the drug laboratory, which aims to establish a national drug database

and conduct drug profiling, with the stated objective of detecting and combating drug trafficking networks as well as obtaining information on trafficking trends and type of drugs used. This concrete example indeed indicates an understanding of the possibilities related to operational and strategic forensic intelligence and a willingness to act more proactively in addressing a particular problem.

Besides a general limitation of forensic intelligence to a traditional reactive model, this type of intelligence does not include the integration of different types of forensic data, which is a fundamental element of forensic intelligence. This also illustrates the siloed functioning of the different 'sub-disciplines' of forensic science, leading to specific processing systems and databases for each laboratory or police service. However, the linking of different forensic data and their cross-analysis would offer greater possibilities in terms of intelligence at all levels (tactical, operational, strategic).

3. WP 2: ASSESING THE FEASIBILITY AND ADDED VALUE OF A FORENSIC INTELLIGENCE SYSTEM IN BELGIUM

3.1 Data pre-processing and integration of police and forensic data (Task 2.1)

3.1.1 Objective of Task 2.1

Task 2.1 focuses on preparing and integrating police-recorded crime data and forensic DNA linkage data for use in Work Package 2. The purpose of this task is to determine whether police and forensic datasets can be brought together in a structured, legally compliant manner. We also aim to understand whether this integration can produce a usable basis for FI analysis in Belgium.

The task is essential for understanding the workflows of institutions in Belgium and the conditions that shape the merging of data sources. Through our work, we examine the players and tools required to build an FI tool using data that are already available within the legal environment. Our task includes identifying common case-level identifiers, resolving inconsistencies, identifying analytically relevant variables, and preparing the data so that police, forensic, and combined relational structures can be constructed.

The objective of Task 2.1 is both practical and technical. It does not yet assess the full analytical added value of FI. That assessment is developed in Task 2.2. Task 2.1 instead creates the necessary data foundation by producing three structured datasets: a police-only dataset, a forensic DNA dataset, and a combined dataset. These outputs make it possible to compare the relationships visible in police data, explore the analyses that may be possible with forensic DNA data, and examine the relationships that become visible once both sources are integrated.

Within Work Package 2, Task 2.1 is guided by the following operational question:

> *To what extent can police-recorded crime data and forensic DNA linkage data be cleaned, harmonized, and integrated into a combined case-level dataset suitable for FI analysis in Belgium?*

This task also supports the broader Work Package 2 research question by establishing the empirical basis for assessing the feasibility and added value of a FI tool in Belgium.

3.1.2 Data sources

Task 2.1 relies on two administrative data sources: police-recorded crime data and forensic DNA linkage data. These sources were selected because they represent two distinct information layers that are available within the Belgian criminal justice and forensic environment.

The police data captures recorded crime information. This data reflects cases, known or anonymized individuals, and investigative links derived from a recorded involvement with the law. The forensic DNA data, on the other hand, captures trace-based case linkages. This dataset identifies relationships between cases in which the same biological profile appears across multiple case records, including cases where no suspect is known.

The two datasets, therefore, capture different relational planes. Police data provides a suspect-based and administratively recorded view of case relationships. Forensic DNA data provides a trace-based view of case relationships. Bringing these sources together enables examination of how FI can expand the relational field available for crime analysis. This reflects the broader premise of Work Package 2: police-based networks provide operational visibility, while FI can introduce trace-based visibility independent of investigative awareness.

3.1.2.1 Police-recorded crime data

Police-recorded crime data were provided by a local police zone under a data-sharing agreement specifying the scope of use, storage conditions, and reporting limitations. The dataset covers cases registered between 2016 and 2021 and initially contained 177,787 case-level records linked to anonymized person identifiers, consistent with administrative and network-based crime research practices (Bright et al., 2014; Morselli, 2009).

For Task 2.1, only the variables necessary for case-level integration and relational network construction were retained. These included the case identifier and an anonymized individual identifier. The anonymized individual identifier indicates that a specific individual was involved in one or more cases. When two cases shared the same anonymized individual identifier, this was treated as an observable investigative link between those cases.

The police dataset, therefore, provides the baseline relational structure for Work Package 2. It reflects the relationships that are visible through recorded police information, including shared individuals and case-level co-involvement. This makes it suitable for constructing a police-only relational dataset and, later in Task 2.2, a police-only case network.

At the same time, the police data must be interpreted as a recorded information layer. They reflect cases and relationships that have been reported, detected, processed, and recorded. They do not represent the full underlying structure of criminal activity. This is a central reason why police data are appropriate for Task 2.1: they provide the current reference point against which the contribution of FI can be assessed.

3.1.2.2 Forensic DNA linkage data

Forensic DNA linkage data were provided through collaboration with the National Institute of Criminalistics and Criminology (NICC), subject to comparable access and reporting restrictions. The data were derived from Belgium's national forensic DNA system and were limited to case-linkage information. No genetic profiles, biological trace data, or laboratory-level analytical metadata were provided.

The forensic dataset identifies relationships between cases through shared DNA cluster numbers. A cluster indicates that the same biological profile was detected in multiple cases. This means that cases can be forensically linked even where no suspect has been identified or formally linked in police records. In this way, forensic DNA linkage data provide a relational source that is independent of known offender identity. Cases lacking a cluster assignment were retained in the forensic dataset and appeared as isolated cases in the resulting relational structure. This decision preserved the structure of the forensic dataset and avoided excluding cases solely because they did not link to another case at the time of analysis. This is important because FI analysis must account for both linked and unlinked cases to reflect the actual information environment available to investigators.

For Task 2.1, the forensic DNA dataset provides the basis for constructing a forensic-only relational dataset. This dataset is then integrated with the police dataset to create a combined case-level dataset. The integration allows Work Package 2 to assess whether forensic DNA linkages introduce additional case relationships beyond those visible in police-recorded data.

3.1.2.3 Data access, anonymization, and storage conditions

All processing complied with Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR). The police and forensic datasets were pseudonymized by a trusted third party before transfer

to the researcher. This allowed linkage between sources while preventing direct identification of individuals. The datasets were processed and stored on secure, access-restricted university systems.

The primary unit of analysis is the criminal case, represented through a harmonized case identifier. The case was selected as the primary unit because it provides a common unit of comparison across police and forensic sources. It also allows forensic linkages to be integrated without requiring direct person-level identity resolution across systems. Individuals are represented through anonymized identifier codes that enable relational linkage. DNA cluster identifiers function as relational attributes that connect cases. This approach ensures that Task 2.1 can examine data integration without transferring or processing directly identifiable personal data. It also ensures that the resulting datasets are suitable for case-based FI analysis rather than person-level identification. No personal data was transferred or used in the analytical work carried out for Work Package 2. No genetic profile data, biological trace data, or laboratory metadata were provided. The forensic data were limited to case-linkage information, meaning that the analysis examines whether cases are connected through forensic DNA clusters, not the scientific content of the DNA profiles themselves.

3.1.3 Limitations and usefulness of data sources

The police and forensic datasets used in Task 2.1 are shaped by structural constraints that both limit and enhance their analytical value. These constraints are not treated as isolated weaknesses. They are features of the institutional and operational environment in which FI would be implemented in Belgium and any other jurisdiction.

Police-recorded crime data reflect the observable surface of crime rather than its full underlying structure. The well-established “dark figure” of crime means that many offences remain unreported, undetected, or unrecorded (Sparrow, 1991). Even within recorded cases, not all actors are identified, and investigative attention is unevenly distributed across proactive activities and policing priorities. Police-derived relational structures are therefore shaped by both offender behavior and enforcement practice (Morselli, 2009). They capture relations among detected cases and recorded individuals, not the full structure of criminal activity.

This limitation also defines the usefulness of police data. Police-recorded information is the primary information environment in which law enforcement currently operates. It provides the practical baseline for assessing how FI changes what can be observed, linked, and analyzed. For Task 2.1, the police dataset is therefore not treated as a complete representation of crime. It is treated as the operational reference layer against which forensic data integration can be evaluated, and of which FI can potentially enhance.

Forensic DNA linkage data are shaped by a different form of selectivity. Not every offence produces recoverable biological material, and trace availability varies by crime type, environmental conditions, evidence preservation, and investigative practice. Decisions about collection, prioritization, and laboratory submission introduce additional selectivity shaped by available resources, legal thresholds, and operational priorities. Forensic clusters, therefore, reflect the interaction between offender behavior, material trace production, and institutional capacity (Ribaux et al., 2003; Rossy et al., 2013).

This means that forensic DNA data should not be interpreted as a complete or neutral map of criminal activity. Certain offence types are more likely to generate usable DNA evidence, while others rarely produce trace material suitable for database comparison. The resulting forensic dataset is therefore selective. However, this selectivity does not remove its analytical value. DNA-based cluster identifiers can reveal cross-case relationships that are structurally independent of suspect identification. They may connect cases involving unknown offenders and identify links that are not visible through police records alone (Moor et al., 2020; Ribaux & Wright, 2014).

The usefulness of Task 2.1 lies in making these two forms of visibility comparable. Police data provide a layer of suspect-based, operationally recorded data. Forensic DNA data provide a trace-based layer. The combined dataset enables Work Package 2 to examine whether these layers duplicate or complement one another, or reveal distinct relational structures. This is important because the added value of FI depends not only on the existence of additional data, but also on whether that data can be integrated in a form that supports analysis and decision-making.

3.1.4 Methodology

The analysis relied on two administrative datasets: police-recorded crime data covering all cases registered between 2016 and 2021, and forensic DNA data derived from a national forensic database over the same period. Before processing, the police dataset contained 177,787 cases, and the DNA dataset contained 6,551 cases. These datasets were harmonized through a shared case-level identifier for network construction.

Each case was assigned a unified identifier constructed from available administrative case fields. This step allowed the datasets to “speak to one another” while preserving the inherent asymmetry between police and forensic data. The purpose was to establish a common case-level unit that allowed comparison and integration. From the police dataset, only the case identifier and anonymized individual identifier were retained for relational construction. When two cases shared the same anonymized individual identifier, this indicated that the same person was involved in both cases and created an observable investigative link between them. From the forensic dataset, relations were identified through shared DNA cluster numbers. When two cases shared a cluster, this indicated that the same biological profile had been detected in both cases and created a forensic link between them.

The integration process then prepared the data for three separate relational outputs. First, a police-only dataset was created by grouping cases according to shared anonymized individual identifiers. Second, a forensic DNA dataset was created by grouping cases according to shared DNA cluster identifiers. Third, a combined dataset was created by combining police- and forensic-derived case relationships.

For the combined dataset, police-derived relationships were added first. Forensic-derived relationships were then incorporated. Where a connection existed in both datasets, the relationship was retained only once and annotated to reflect its dual origin. This preserved a single, consolidated structure while allowing each data source's contribution to remain visible. Following this, a cleaning step was applied where a connected component consisted solely of two nodes, with one appearing only in the police network and the other appearing only in the forensic dataset; we removed the pair. These pairs were interpreted as administrative overlaps rather than meaningful investigative relationships. Retaining them would have artificially inflated the presence of trivial links. Apart from this targeted cleaning step, the datasets were left structurally intact, including isolates, because fragmentation and unevenness are part of the real-world intelligence environment.

The final output of Task 2.1 is a set of harmonized and integrated datasets suitable for network construction and analysis in Task 2.2. The task, therefore, establishes the technical basis for comparing police-only, forensic DNA, and combined representations of case relationships. It also demonstrates the practical requirements for forensic data integration in Belgium, including the need for compatible identifiers, clear data governance, secure processing conditions, and careful interpretation of the different relational logics contained in police and forensic datasets.

3.1.4.1 Construction of police, forensic, and combined datasets

The output of the cleaning, harmonization, and integration process was the construction of three case-level relational datasets: a police-only dataset, a forensic DNA dataset, and a combined dataset. These datasets were prepared for the network analysis conducted in Task 2.2. The police-only dataset was

constructed by grouping cases according to shared anonymized individual identifiers. Where the same anonymized individual appeared in more than one case, a police-based relationship was created between those cases. This dataset, therefore, represents the relationships visible through recorded police information. The forensic DNA dataset was constructed using the same relational principle, with DNA cluster identifiers replacing person identifiers. Where cases shared the same DNA cluster, a forensic relationship was created between them. This dataset represents the relationships visible through trace-based linkage. The combined dataset incorporated both police-derived and forensic-derived relationships. Police-derived relationships were added first, followed by forensic-derived relationships. Shared relationships were retained once and annotated to show their source. This allowed the combined dataset to serve as a single analytical structure while preserving the ability to identify which relationships originated in police data, forensic data, or both.

All three datasets were prepared as undirected and unweighted relational structures. A link indicates that two cases are related according to the relevant linkage criterion. Directionality was not imposed because Task 2.1 focuses on whether cases can be linked, not on temporal order, command flow, or sequence of interaction. Edge weights were also not applied at this stage because the purpose was to establish relational visibility rather than measure the strength of evidence or intensity of interaction. The three datasets produced in Task 2.1 provide the basis for Task 2.2. They allow the Work Package 2 analysis to compare the police-only view, the forensic DNA view, and the combined forensic-enhanced view using a consistent case-level structure.

3.1.5 Scientific results and recommendations

Task 2.1 demonstrates that police-recorded crime data and forensic DNA linkage data can be prepared and integrated into a common case-level structure. The task also shows that successful integration depends on careful identifier harmonization, source-specific interpretation, and clear documentation of data provenance.

The main result is the creation of three usable datasets that support the next stage of Work Package 2. The police-only dataset provides the reference layer for currently visible police relationships. The forensic DNA dataset provides a trace-based linkage layer. The combined dataset provides an integrated view for assessing the added value of FI in Task 2.2. A key finding from Task 2.1 is that integration is technically feasible, though not automatic. It depends on the availability of common or harmonizable identifiers, clear rules for retaining and excluding records, and the ability to distinguish between meaningful relational links and administrative overlap. This has direct relevance for the development of a FI tool in Belgium.

Task 2.1 also confirms that forensic data should be treated as a distinct relational layer rather than as a simple supplement to police data. Police and forensic sources do not capture the same relationships in the same way. Their integration requires careful interpretation. A combined dataset is most useful when it preserves source information and allows analysts to determine whether a link comes from police records, forensic traces, or both.

3.1.5.1 Police-only dataset

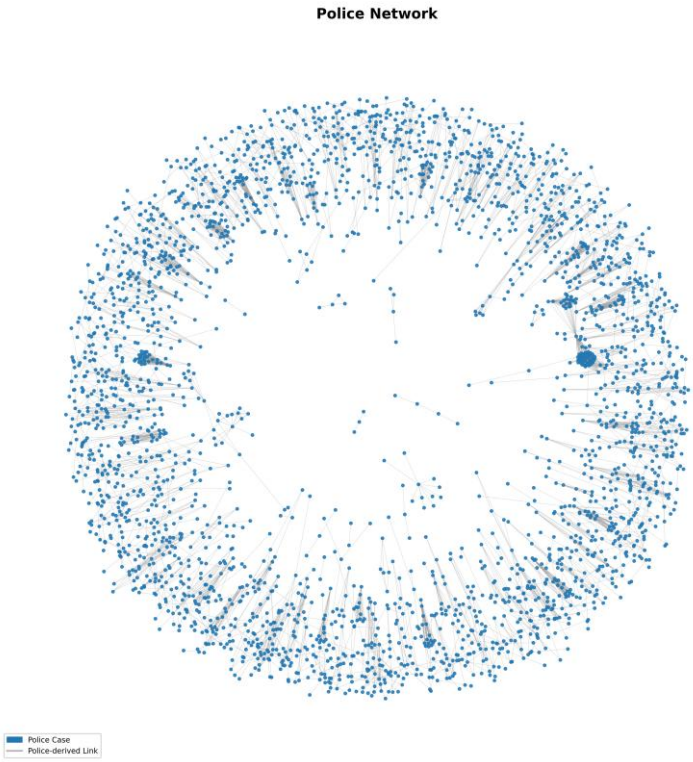
The police-only dataset provides the baseline relational layer for Work Package 2. Imagery of this dataset and its relational nature can be found in

6 below. It captures relationships between cases that are visible through shared anonymized individuals. In practical terms, this represents the type of case linkage that can be derived from recorded police information. The resulting structure reflects an operational intelligence view of crime. It is shaped by recorded cases, known or anonymized individuals, and investigative processes. This

makes it highly relevant as a reference point, as police-recorded data currently form the main basis for many crime and network analysis activities.

The police-only dataset is useful because it shows what can already be observed through police information. It also identifies the limits of that view. Relationships that depend on unknown offenders, trace-based similarities, or links not recognized through police records are unlikely to appear in this layer. For this reason, the police-only dataset provides the necessary baseline for evaluating whether FI adds new relational information. The main recommendation is that police datasets used for FI purposes should retain stable case identifiers and anonymized individual identifiers in a form that supports cross-case linkage. Without consistent identifiers, the analytical value of police data is reduced, even where relevant information exists.

Figure 6: Image of Police Recorded Dataset Network

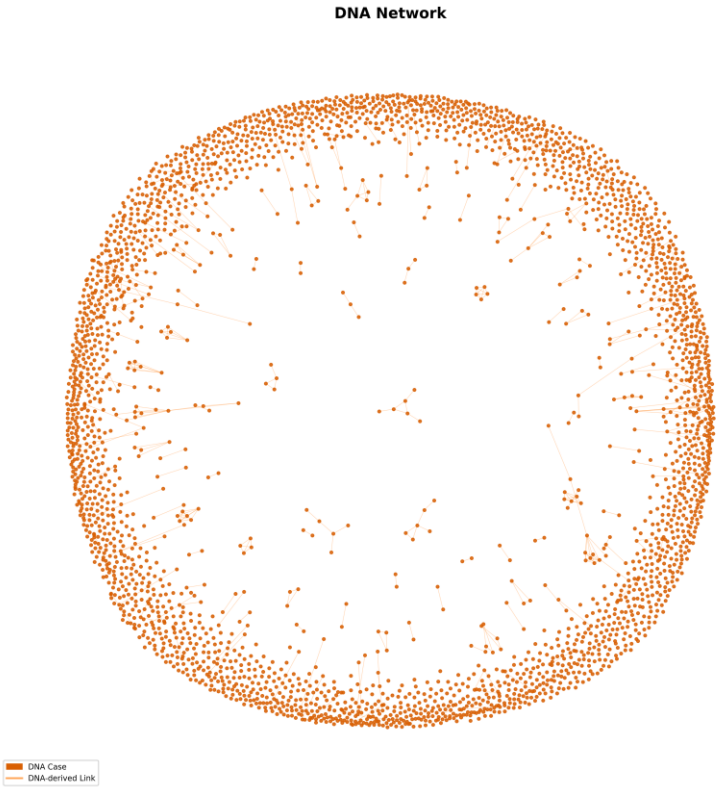


3.1.5.2 Forensic DNA dataset

The forensic DNA dataset provides the trace-based relational layer for Work Package 2. It captures relationships between cases through shared DNA cluster identifiers. Imagery of tis dataset and its relational nature can be found in Figure 7 below. These relationships can exist even where no suspect is known or where no police-based relationship has been recorded. This dataset is analytically useful because it represents a different form of visibility. It does not rely on shared suspects or recorded co-involvement. Instead, it identifies case relationships through forensic trace recurrence. This makes it especially relevant for detecting links that may remain invisible in police-recorded data. The forensic DNA dataset also has clear limitations. It reflects only those cases where traces were recovered, submitted, analyzed, and linked through the forensic system. It should therefore be interpreted as a selective linkage layer. This selectivity is not a reason to exclude the data. It is a condition that must be documented and considered when interpreting results.

The main recommendation is that forensic linkage data should be made available in a structured analytical format where legally and operationally appropriate. For FI purposes, the key requirement is not access to genetic profiles or laboratory detail. The essential requirement is access to validated case-linkage information that can be integrated with police-recorded case data.

Figure 7: Image of Forensic DNA Dataset Network

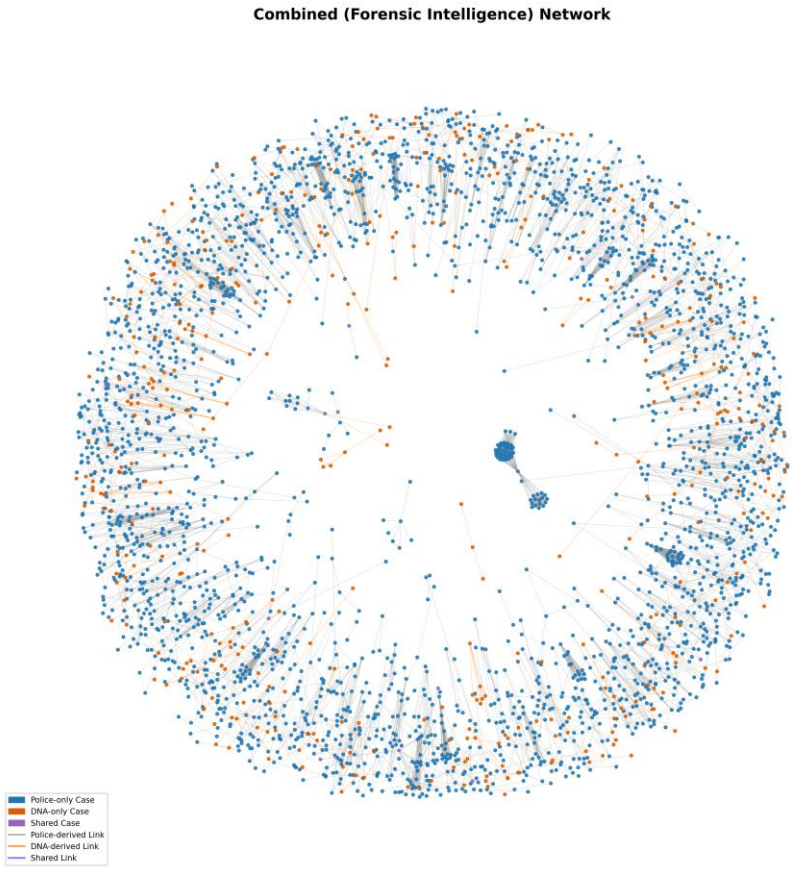


3.1.5.3 Combined dataset

The combined dataset is the main output of Task 2.1. It brings together police-based and forensic DNA-based case relationships in a single structure while preserving the origin of each link. Imagery of this dataset and its interconnected nature can be found in Figure 8 below. This dataset allows Work Package 2 to assess the added value of FI in a concrete way. It allows comparing the police-only view with the forensic-enhanced view and identifying which cases or relationships become visible only after integration. This provides the empirical basis for the network analysis carried out in Task 2.2. The combined dataset also shows that integration changes the analytical frame. It does not simply add more records. It creates a broader relational structure in which different forms of visibility can be compared. Police data show relationships based on recorded involvement. Forensic data show relationships based on trace recurrence. The combined dataset brings these layers together without removing their distinct meaning.

The main recommendation is that any future FI tool should preserve source provenance. Analysts must be able to identify whether a relationship is police-derived, forensic-derived, or present in both sources. This is necessary for interpretation, accountability, and operational usefulness.

Figure 8: Image of the Combined FI Dataset Network



3.1.5.4 Practical conditions for merging police and forensic data

Task 2.1 identifies several practical conditions for merging police and forensic data in Belgium.

- The first condition is the presence of a shared or harmonizable case identifier. Without such an identifier, police and forensic data remain separate information systems and cannot be reliably integrated for relational analysis.
- The second condition is data minimization. The analysis did not require access to genetic profiles, biological trace data, or directly identifiable personal data. Case-level linkage information was sufficient for FI analysis. This is important because it shows that added analytical value can be explored while limiting the sensitivity of the data being processed.
- The third condition is clear data provenance. Police-derived and forensic-derived links must remain distinguishable in the combined dataset. This allows analysts to understand what each source contributes and prevents the combined structure from being interpreted as a single undifferentiated information layer.
- The fourth condition is governance. Integration requires clear rules on access, storage, reporting, and interpretation. The technical ability to merge data is only one part of feasibility. A FI tool also requires institutional procedures that define who may access the data, for what purpose, under what safeguards, and with what reporting limitations.
- The final condition is interpretive caution. Forensic links are analytically valuable, although they do not automatically imply direct offender interaction or shared criminal organization. They identify trace-based case relationships that require contextual assessment. Any future tool should therefore support interpretation rather than replace expert analysis.

3.1.6 Conclusion: implications for forensic data integration in Belgium

The findings indicate that forensic data integration is feasible when case identifiers can be harmonized, data provenance is preserved, and linkage information is handled under appropriate governance conditions. The task also shows that useful FI analysis does not require access to genetic profiles or directly identifiable personal data. Validated case-linkage information can be sufficient to support relational analysis. For Belgium, the implication is that a FI tool should be developed around structured, case-level integration. Such a tool should support comparison between police and forensic information layers, retain clear source labels, and allow analysts to identify where forensic data adds new relational visibility. Task 2.1 establishes the practical data foundation for assessing the added value of FI in Task 2.2.

3.2 Network analysis of police, forensic, and combined data (Task 2.2)

3.2.1 Objective of Task 2.2

Task 2.2 assesses the added analytical value of FI by comparing the network structures produced from police-recorded crime data, forensic DNA linkage data, and the combined dataset prepared in Task 2.1. The purpose of this task is to determine whether forensic DNA linkages provide additional relational information beyond what is visible in police data alone, and whether these additional relationships are meaningful for crime analysis.

Task 2.1 established the data foundation by preparing three case-level relational datasets: a police-only dataset, a forensic DNA dataset, and a combined dataset. Task 2.2 uses these outputs to examine how each data layer represents criminal connectivity. The analysis focuses on whether forensic linkages change the observed structure of the network, where those changes occur, and what they contribute to investigative understanding.

The task addresses the following research question:

> *To what extent does the inclusion of FI enhance investigative insight at the case-linkage and ego-network levels?*

This task is also linked to the broader Work Package 2 objective of assessing the added value of a FI tool in Belgium. It does this by examining whether FI changes what becomes visible in network analysis and whether these changes support more informed interpretation of criminal relationships.

3.2.2 Analytical framework

Task 2.2 is based on the premise that criminal networks are data-dependent representations. They are shaped by the information sources used to construct them and by the criteria used to define relationships between cases. Police data and forensic DNA data capture different forms of visibility. Police data capture relationships based on known or recorded involvement. Forensic DNA data capture relationships based on trace recurrence across cases.

This distinction is central to the analysis. If different data sources produce different relational structures, then conclusions about connectivity, clustering, and investigative relevance depend on the data layer used. FI may reveal additional cases and links that extend the observable network, alter local structures, and reposition cases within the broader relational field. The analysis therefore treats FI as a relational data layer and evaluates its contribution through structural comparison, ego-network analysis, and offence-type profiling.

3.2.2.1 Case linkage and relational structures

Case linkage refers to the identification of connections between criminal events based on shared attributes, actors, or trace-based associations. In Task 2.2, a linkage exists when two or more cases are connected through a defined relational criterion. In the police network, this criterion is a shared anonymized individual identifier. In the forensic DNA network, this criterion is a shared DNA cluster identifier.

Relational structures emerge when multiple case linkages are analyzed together. These structures may appear as isolated pairs, small clusters, larger connected components, or local ego networks around a focal case. In this task, relational structure is treated as the minimum condition for network-based analysis. Cases that have no links remain analytically relevant because they show the limits of observed connectivity in each data layer.

The core analytical question is whether forensic DNA linkages identify relationships that are absent from police-recorded data. This is important because forensic traces can connect cases where no suspect is known, where no shared individual appears in police records, or where conventional investigative pathways have not recognized a relationship. The value of FI therefore lies in its capacity to reveal cross-case links that are structurally independent of suspect-based police information.

3.2.2.2 Network representation

A network representation is the graph model created from recorded or inferred relationships between cases. It does not claim to capture the full underlying criminal organization. It represents the relationships that become visible through a specific data source and a specific linkage rule.

In Task 2.2, three network representations are compared. The police-only network represents relationships visible through shared anonymized individuals. The forensic DNA network represents relationships visible through shared forensic clusters. The combined network integrates both forms of linkage in one case-level structure. These representations are analytically useful because they allow the same underlying crime environment to be viewed through different information layers. Police-based networks reflect operational visibility. FI-derived networks reflect trace-based visibility. The combined network shows what becomes visible when these information layers are brought together. This approach supports the Work Package 2 objective of assessing whether FI changes the observed structure of criminal networks in Belgium.

3.2.2.3 Nodes, edges, and network construction

In Task 2.2, nodes represent criminal cases. Edges represent relationships between cases. The construction logic is consistent across the three networks, while the source of the relationship differs. In the police-only network, an edge is created when two cases share the same anonymized individual identifier. In the forensic DNA network, an edge is created when two cases share the same DNA cluster identifier. In the combined network, both police-derived and forensic-derived edges are included. Where the same relationship appears in both sources, it is retained once and marked by source. All networks are treated as undirected and unweighted. An undirected edge indicates that two cases are connected without assigning direction. This is appropriate because the analysis focuses on the presence and structural effect of case relationships, rather than temporal sequence, command flow, or direction of interaction. An unweighted edge indicates that a relationship is present according to the relevant linkage criterion. Edge strength is not assessed in this task.

3.2.3 Methodology

Task 2.2 applies a comparative multi-layer network design. The analysis compares three case-based networks constructed from the outputs of Task 2.1: police-only, forensic DNA, and combined. This design allows FI's contribution to be isolated as a relational layer. Structural comparison is used to evaluate global network properties, while ego-network analysis and crime-type profiling are used to assess where FI contributes and whether those contributions are analytically meaningful.

The analysis proceeds in three stages. First, the police-only, forensic DNA, and combined networks are compared using standard network measures. Second, selected ego networks are examined to identify local changes produced by forensic integration. Third, forensic-introduced cases are profiled by crime category to identify offence domains where FI contributes most clearly.

3.2.3.1 Comparative network analysis

The first stage compares the three networks at the global structural level. This comparison assesses whether police and forensic data produce different network configurations and whether integration changes the overall structure of the observed network.

The analysis examines the number of nodes, number of edges, largest connected component, average degree, density, clustering coefficient, and Average Shortest Path Length (ASPL). These measures capture different dimensions of structure: network size, connectivity, local cohesion, and path-based efficiency. Since all three networks are built from the same case-level logic, differences between them can be interpreted as differences in information visibility rather than differences in analytical design.

The Largest Connected Component (LCC) (Equation 1) refers to the size (number of nodes) in the largest subset of mutually reachable cases. It captures the extent of structural cohesion within the network and indicates how many cases are embedded within the main relational field (Jiang et al., 2025; Musawi et al., 2023).

$$\boldsymbol{LCC} = | \boldsymbol{Cmax} | \tag{1}$$

Where:

- $\mathcal{C}$= set of connected components in the network
- $| C |$= number of nodes in component C

The average degree (Equation 2) represents the mean number of edges per node in an undirected network. It provides a summary measure of how many relational ties each case maintains on average (Porreca et al., 2025).

$$\bar{\mathbf{k}} = \frac{\boldsymbol{2E}}{\boldsymbol{N}} \tag{2}$$

Where:

- E= total number of edges
- N= total number of nodes

Network Density (3) expresses the proportion of observed edges relative to the total number of possible edges in an undirected network of the same size. It reflects overall connectivity relative to scale (Goswami et al., 2018).

$$\boldsymbol{D} = \frac{\boldsymbol{2E}}{\boldsymbol{N(N-1)}} \tag{3}$$

Where:

- E= number of observed edges
- N= number of nodes in the network

The clustering coefficient (Equation 4 and 5) measures the extent to which a node's neighbors are also connected to each other. The reported value corresponds to the global average clustering coefficient and captures the prevalence of locally cohesive triadic structures. (Yin et. al 2019) measure is computed by first calculating the clustering coefficient for each node C_i, and then averaging these values across all nodes in the network.

Global formula:

$$\boldsymbol{C = \frac{1}{N}\sum_{i=1}^{N} C_i} \tag{4}$$

Where the node-level clustering coefficient is defined as:

$$\boldsymbol{C_i = \frac{2e_i}{k_i(k_i - 1)}} \tag{5}$$

Where:

- C_i= clustering coefficient of node i
- e_i= number of edges between neighbors of node i
- k_i= degree of node i

The average shortest path length (ASPL) (Equation 6) represents the mean geodesic distance between all pairs of nodes in a network. When networks are disconnected, ASPL is computed on the largest connected component to ensure meaningful path comparison (Musawi et al., 2023).

$$\boldsymbol{ASPL = \frac{1}{N(N-1)}\sum_{i \neq j} d(i,j)} \tag{6}$$

Where:

- $d(i,j)$= shortest path distance between nodes $i$and j
- N= number of nodes in the component being evaluated (typically the LCC)

3.2.3.2 Ego-network analysis

The second stage examines micro-level changes through ego-network analysis. Ego networks focus on a selected case and its direct connections. They are useful for showing how forensic linkages change the immediate investigative context around specific cases. In police-forensic analysis, ego networks can show how DNA-based linkages transform isolated cases into connected cases, extend existing police clusters, or position a case as a bridge between separate investigative domains.

Candidate ego networks were selected by comparing the police-only and combined networks. Cases were identified where connectivity increased after forensic integration. This included cases that were isolated in the police network but connected in the combined network, as well as cases that gained new forensic-only neighbors. Three representative ego networks were selected to illustrate distinct forms of forensic contribution: isolation to connection, peripheral forensic extension, and multi-system case hub. These were selected by their unique qualities from each other, and the dataset.

3.2.3.3 Crime-type profiling

The third stage examines the offence categories represented among forensic-introduced cases. The purpose is to determine whether FI contributes evenly across offence types or whether its contribution is concentrated in particular domains. Forensic-only cases introduced into the combined network were assigned to crime categories using the available offence classification. These categories

were then used to assess where forensic DNA data added the most case-level information. A focused subgraph analysis was also conducted for organized crime and serious offences because this category represented one of the domains where forensic contributions were most pronounced.

3.2.3.4 Network measures and analysis strategy

The network measures used in Task 2.2 were selected to capture complementary aspects of network structure. The Largest Connected Component (LCC) measures the size of the largest subset of mutually reachable cases. Average degree measures the average number of links per case. Density measures the proportion of observed links relative to the number of possible links. The clustering coefficient measures the extent to which linked cases form locally cohesive groups. ASPL measures the average distance between cases within the largest connected component.

Jaccard similarity (Equation 7) was used to quantify structural overlaps between the police-only and combined networks. It measures the proportion of shared edges relative to the total number of unique edges across both representations. In this task, Jaccard similarity is used to assess how much of the combined network was already visible in the police-only network and how much can be attributed to forensic DNA integration.

The index is calculated as:

$$\boldsymbol{J(A,B)} = \frac{|\boldsymbol{E_A} \cap \boldsymbol{E_B}|}{|\boldsymbol{E_A} \cup \boldsymbol{E_B}|} \tag{7}$$

Where:

- E_A= edge set of network A(police network)
- E_B= edge set of network B(merged network)
- $| E_A \cap E_B |$= number of shared edges

$| E_A \cup E_B |$= total unique edges across both networks

The index reflects the proportion of links in the combined network that were already present in the police network, and therefore how much of the merged structure can be attributed to FI alone. Higher values indicate substantial overlap, whereas lower values reveal that the forensic layer contributes novel structural insights not captured by police data (Newman, 2006).

The analysis strategy combines global and local interpretation. Global network metrics show whether FI changes the overall structure. Ego-network analysis shows how FI changes local investigative context. Crime-type profiling shows where FI contributes by offence domain. This combined approach supports a practical assessment of added value by moving beyond the question of whether FI adds data and examining whether it adds useful relational visibility.

3.2.4 Scientific results and recommendations

Task 2.2 shows that police data and forensic DNA data produce distinct network representations. The police-only network is more connected and locally clustered, reflecting operationally visible relationships based on shared individuals. The forensic DNA network is much sparser, reflecting selective trace-based relationships. The combined network is larger and more analytically informative, although the core police structure remains largely intact.

The main finding is that FI does not duplicate police knowledge. It selectively extends it. The forensic layer adds new cases and new relationships, often at the periphery of the network or in small independent components. These additions do not substantially restructure the main police-connected

component. They expand the observable relational field and identify cases that would otherwise remain outside police-based network representations.

3.2.4.1 Police-only network structure

The police-only network provides the operational reference structure for Task 2.2. It contains 2,872 cases connected by 5,344 co-involvement edges. The largest connected component contains 56 cases, indicating that the network is fragmented into many smaller components rather than organized around one dominant connected structure.

Despite this fragmentation, the police-only network shows strong local clustering. The clustering coefficient is 0.550, which indicates that cases linked through shared individuals tend to form tightly connected local groups. These groups may reflect recurring co-involvement, local co-offending structures, or repeated case relationships visible through police records. The ASPL within the largest connected component is 1.48, suggesting that cases inside the main connected component are closely linked once they are part of the same cluster.

This structure is consistent with the nature of police-recorded data. Police data capture known or recorded relationships. They are therefore effective at representing visible co-involvement, while remaining limited where cases involve unknown offenders or relationships not recognized through investigative records.

3.2.4.2 Forensic DNA network structure

The forensic DNA network provides a different representation of case relationships. It contains 3,159 cases but only 372 edges. This produces a sparse structure based on selective, high-specificity forensic connections. The largest connected component contains 9 cases, confirming that DNA matches do not produce broad network clusters in this dataset.

The clustering coefficient is 0.041 and density is 0.00007. These values show that the DNA network is not locally cohesive in the same way as the police network. The average degree is 0.24, which indicates that most cases appear once or remain unconnected. The ASPL within the largest connected component is 1.67.

This structure should not be interpreted as low value. It reflects the specific function of forensic DNA data. DNA linkages arise only where trace recurrence connects cases. These links may be sparse, although they can reveal relationships that do not depend on known suspects or recorded police co-involvement. The forensic DNA network therefore captures a distinct layer of investigative visibility.

3.2.4.3 Combined network structure

The combined network integrates police-derived and forensic DNA-derived case relationships. It contains 3,284 cases and 5,696 edges. Compared with the police-only network, this represents an increase of 412 cases and 352 additional edges. The combined network therefore provides a broader view of case relationships than the police-only network.

The largest connected component remains unchanged at 56 cases. This indicates that forensic integration did not merge the main operational clusters into a larger connected structure. Instead, forensic edges mainly attached new cases at the periphery or formed small independent components. The average degree decreases to 3.47, density decreases to 0.00106, and the clustering coefficient decreases to 0.52. These changes indicate that forensic additions are often less embedded in dense police clusters and more likely to appear as isolated or bridging ties.

The combined network should therefore be interpreted as more complete, rather than more cohesive. FI expands the observed relational field by adding new cases and non-redundant relationships. It does not substantially alter the main backbone of police-visible data in this dataset.

Table I: Structural metrics for police-only, forensic DNA, and combined networks

Metric	Police-only network	Forensic DNA network	Combined network	Δ Combined from Police
Nodes	2,872	3,159	3,284	+412
Edges	5,344	372	5,696	+352
Largest Connected Component (LCC) size	56	9	56	±0
Average degree	3.72	0.236	3.47	–0.25
Density	0.0013	0.00007	0.00106	–0.00024
Clustering coefficient	0.55	0.04	0.52	–0.03
Average Shortest Path Length (ASPL, LCC only)	1.48	1.67	1.48	±0

3.2.4.4 Structural overlap between police and combined networks

The Jaccard Similarity Index between the police-only and combined networks is 0.94. This means that approximately 93.5% of edges in the combined network were already present in the police network, while approximately 6.5% represent novel forensic connections. This result has two implications. First, the combined network remains largely police-driven. The overall structure is still anchored in police-recorded relationships. Second, the forensic layer adds a small but meaningful set of new relationships. These relationships are not redundant, because they identify links that were not visible in the police-only network. The structural overlap result is therefore important for interpretation. It shows that FI does not replace police data and does not fully restructure the observed network in this local dataset. Its contribution is targeted. It adds selected cases and links that extend the relational field and reduce linkage blindness in specific parts of the network.

3.2.4.5 Case-linkage and ego-network findings

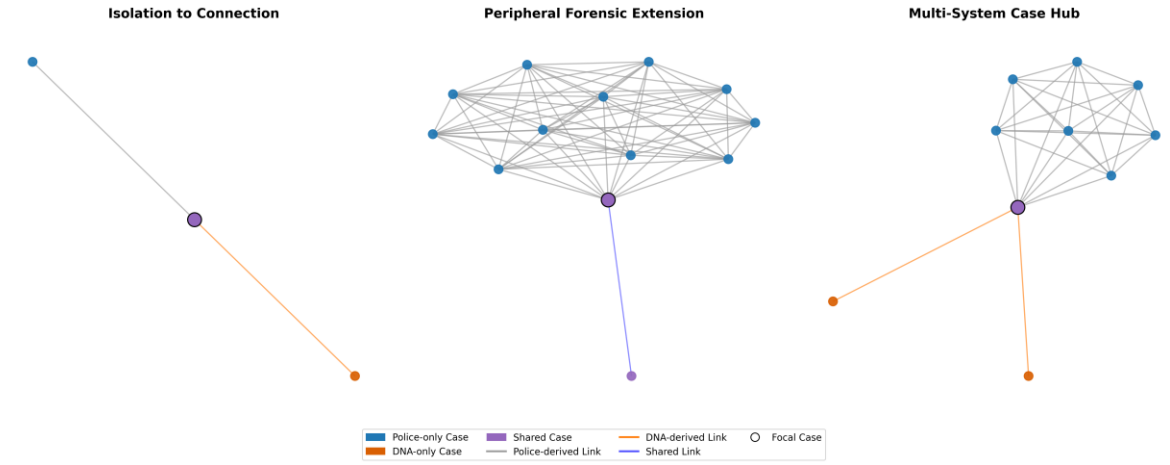
The ego-network analysis shows how FI changes the local investigative context. Three examples were selected to represent different forms of structural change after forensic integration: isolation-to-connection, peripheral forensic extension, and multi-system case hub. To guide you in understanding the following examples, please the imagery in example 3.

- Isolation-to-connection shows a case that was isolated in the police-only network. After forensic integration, it was connected to two additional cases: one police-linked and one forensic-only. This created a small triad that did not exist in the police-only representation. This demonstrates how DNA linkage can connect cases in the absence of shared suspects.

- Peripheral forensic extension shows a case already embedded in a dense police-based component. In the combined network, it retained its police connections and gained one additional forensic-based neighbor. This represents peripheral forensic extension. The police cluster remains intact, while the forensic layer adds an outward link to an external case.
- Multi-system case hub shows a case that became a multi-system hub. In the police network, the case belonged to a small, clustered group. In the combined network, it retained its police links and gained two forensic-only neighbors. This positioned the case at the intersection of police and forensic information layers.

Across these examples, FI mainly adds outward extensions and bridging ties rather than dense new clusters. This matters operationally because even a small number of forensic links can change how a case is interpreted. A case that appears isolated may turn out to be part of a broader series. A police-visible cluster may be extended for forensic purposes. A case may become a bridge between investigative domains.

Example 3: Ego Network Visualizations



3.2.4.6 Added value of FI for network visibility

The results show that FI contributes added value by expanding network visibility. The forensic layer added new cases and new links that were not present in the police-only network. These additions were not evenly distributed across the network. They appeared mainly as peripheral extensions, small independent components, and selected local bridges.

Crime-type profiling provides further evidence that forensic contributions are analytically meaningful. Among forensic-only cases introduced into the combined network, the highest representation was observed in Family and Public Morality offences, followed by Organized Crime and Serious Offences, and Theft with Violence. Mid-level contributions were also observed for Vandalism and Arson, Burglary, and Violence (See Figure 9). This indicates that FI contributes case-level information in offence domains where trace evidence and cross-case linkage may be particularly relevant. The organized crime and serious offences subgraph (Figure 10) provides a focused example. After integration, this subgraph expanded from 29 police-visible nodes to 155 nodes, and from 80 edges to 192 edges (Table 2). This represents a substantial increase in the number of visible cases and links. The largest connected component remained stable at 13 cases, while density and clustering decreased because many newly visible cases had a low degree.

These results suggest that FI does not simply make the network denser. It extends the network outward and brings additional cases into the analytical frame. This is particularly relevant for serious or complex offence categories, where missing links can affect investigative prioritization and coordination. The added value of FI in Task 2.2 is therefore specific and practical. FI enhances visibility by identifying relationships that are independent of known suspects. It supports case linkage by connecting incidents through trace recurrence. It supports local investigative interpretation by changing the ego-network structure. It supports strategic analysis by showing the offence domains in which forensic contributions are concentrated.

Figure 9: Crime-type distribution of forensic-introduced cases

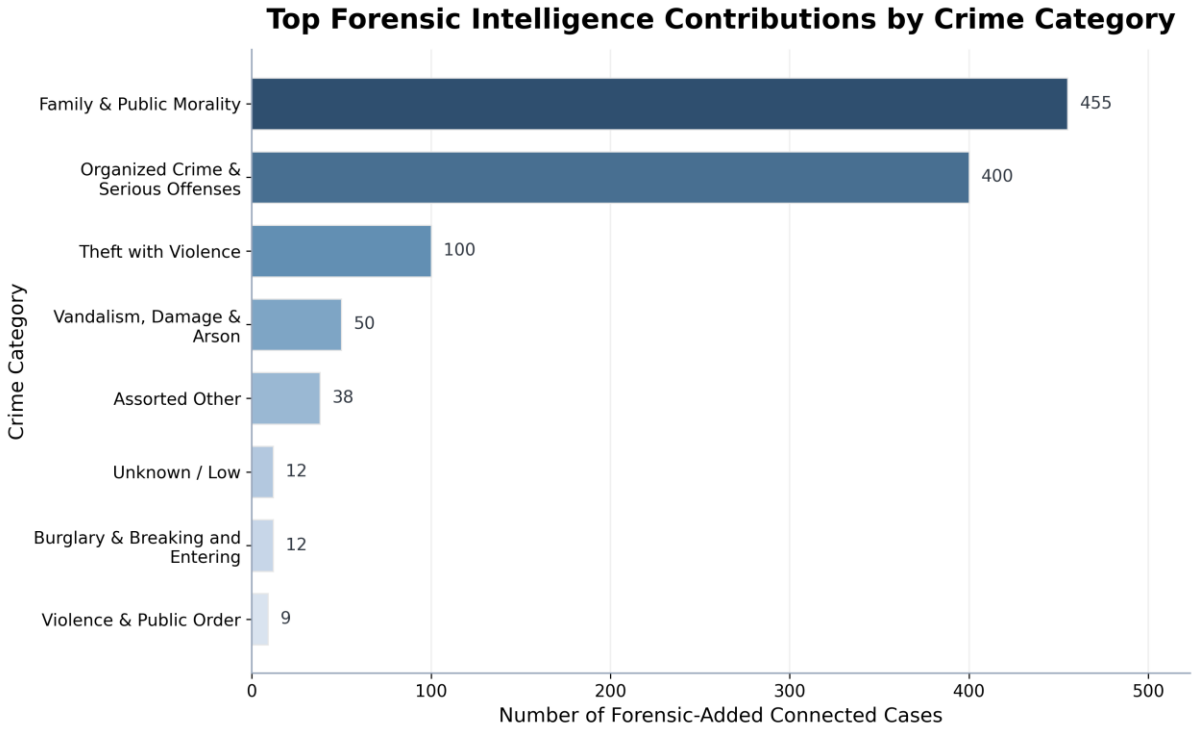
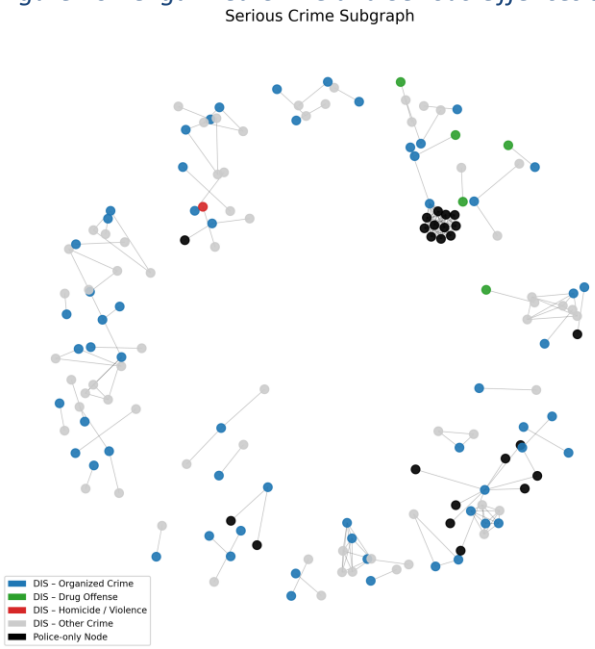


Table II: Organized Crime and Serious Offences subgraph metrics

Metric	Police Subgraph	Combined Subgraph	Δ (Combined – Police)
Nodes	29.00	155.00	+126.00 (+434.50%)
Edges	80.00	192.00	+112.00 (+140.00%)
Largest Connected Component	13.00	13.00	±0.00
Average Degree	5.52	2.48	-3.04
Density	0.20	0.02	-0.18
Clustering Coefficient	0.48	0.36	-0.12
Avg. Shortest Path Length	1.14	1.14	±0.00

Figure 10: Organized Crime and Serious Offences subgraph



3.2.5 Conclusion: implications for criminal network analysis

Task 2.2 demonstrates that police-recorded data and forensic DNA linkage data yield distinct, complementary network representations. The police-only network captures operationally visible case relationships based on shared individuals. It is more connected and more locally clustered. The forensic DNA network captures selective trace-based relationships. It is sparse, but it identifies links that do not depend on suspect identification or recorded police co-involvement.

The combined network shows that FI adds new relational visibility. It contributes additional cases and non-redundant links, while leaving the main police-visible structure largely intact. This means that FI does not replace police data. It extends the analytical field available to investigators. For criminal network analysis, the implication is clear. Network findings depend on the information layer used to construct the network. A police-only network provides one operational view of case relationships. A forensic-enhanced network provides a broader view that can reveal additional cases, local bridges, and offence-specific concentrations of forensic linkage.

For Belgium, Task 2.2 supports the development of FI as a structured analytical tool. The findings indicate that forensic DNA linkage data can improve case-linkage analysis, enrich ego-network interpretation, and identify areas where additional investigative attention may be justified. The value of FI is therefore not measured only by the number of added links. Its value lies in where those links appear, which cases they bring into view, and how they change the interpretation of criminal connectivity.

3.3 Disruption analysis and simulation of fi added value (Task 2.3)

3.3.1 Objective of Task 2.3

Task 2.3 assesses whether FI (FI) changes how criminal network disruption outcomes are measured and interpreted. Tasks 2.1 and 2.2 examined empirical police and forensic data in Belgium and showed how forensic linkage can expand the visible relational field. Task 2.3 extends this analysis through simulation. The purpose is to test, under controlled conditions, whether FI-enhanced network

representations produce different disruption outcomes than police-observed networks when the same intervention strategies are applied.

This task focuses on observability. Police-recorded networks provide a partial representation of criminal structure because they reflect detected offences, known suspects, and documented investigative links. FI can add trace-based linkages across cases, including those absent from police records. This means that the same criminal network may appear structurally different depending on the data layer used to represent it. Task 2.3 evaluates whether these differences in representation affect measured vulnerability, resilience, and disruption outcomes.

The operational research question for Task 2.3 is:

> *To what extent does integrating FI alter network vulnerability, resilience, and disruption outcomes under targeted intervention strategies?*

The task uses a controlled simulation framework to compare police-observed networks, corrected police networks, and FI-enhanced networks. The same disruption strategies are applied across network types. This allows the analysis to isolate the role of observability in shaping measured disruption effects, while holding network generation and intervention rules constant. The contribution of Task 2.3 is therefore methodological and strategic. It tests whether disruption results depend on what is visible to the analyst and whether FI provides a more complete basis for evaluating law enforcement interventions.

3.3.2 Analytical framework

Task 2.3 is grounded in the idea that disruption analysis depends on the network representation being used. Criminal networks are difficult to observe directly. Analysts usually work with reconstructed networks based on available records, such as police data, intelligence files, communications data, or forensic traces. These representations are analytically useful, although they remain partial. Missing ties, unknown actors, and unrecorded cross-case relationships can affect which nodes appear central, which parts of the network appear vulnerable, and how successful an intervention appears after disruption.

FI is treated in this task as an additional layer of observability. It expands the available network representation by adding trace-based relationships through DNA, fingerprint, or ballistics linkages. These additional linkages may reveal redundancy, alternative paths, or previously hidden connections. The analytical issue is that disruption outcomes may change when these added relationships are included. A strategy that appears highly effective on a police-only network may appear less effective once FI-derived connections are added because the enhanced representation contains additional routes for communication and coordination.

The framework therefore separates three concepts: network disruption, structural vulnerability, and resilience. Disruption refers to the intentional removal of nodes or edges. Vulnerability refers to the degree of structural degradation that follows intervention. Resilience refers to the network representation's ability to maintain communication efficiency after disruption. These concepts are assessed structurally, through graph metrics, rather than through direct behavioral outcomes such as arrests, prosecutions, or reductions in offending.

3.3.2.1 Network disruption

Network disruption is defined in Task 2.3 as a measurable structural change in a network representation following an intentional intervention. The task evaluates disruption in structural terms.

The main question is whether communication efficiency is reduced after specific actors or ties are removed.

Disruption is implemented through five strategies: high-degree targeting, high-betweenness targeting, high-closeness targeting, random targeting, and communication targeting based on edge weights. The first three strategies remove nodes based on their structural importance. High-degree targeting removes highly connected nodes. High-betweenness targeting removes nodes that lie on many shortest paths and may act as brokers. High-closeness targeting removes nodes that are, on average, close to other nodes in the network. Random targeting provides a baseline condition. Communication targeting removes the strongest edges and represents interventions aimed at key coordination channels.

All strategies are applied in a standardized single-step format. Each node-based strategy removes the top 10% of nodes according to the relevant rule. Random targeting removes 10% of the nodes selected at random. The edge-based strategy removes the top 10% of edges according to edge weight. This fixed intervention level allows outcomes to be compared across network types and forensic enhancement conditions.

3.3.2.2 Structural vulnerability

Structural vulnerability refers to the extent to which a network representation degrades measurably following disruption. In Task 2.3, degradation is assessed through changes in communication efficiency, especially Average Shortest Path Length (ASPL) (Equation 6). Higher ASPL values indicate that actors or cases are farther apart on average, which suggests reduced efficiency in the movement of information, resources, or influence across the network.

The analysis treats vulnerability as a property of the observed network configuration. A network with few alternative paths may be highly vulnerable because the removal of central nodes can quickly increase path lengths or fragment the structure. A network with more redundancy may be less vulnerable because communication can continue through alternative routes. FI matters because it may reveal additional routes that are not visible in police-only data. In that case, a police-only network may appear more vulnerable than a forensic-enhanced representation of the same underlying structure.

This approach is especially relevant for criminal network analysis because law enforcement strategies often prioritize central actors or brokers. The effectiveness of these strategies depends on whether the observed central actors are genuinely structurally critical within the broader network. If police data omit important alternative pathways, vulnerability may be overstated.

3.3.2.3 Network resilience and disruption outcomes

Network resilience refers to the extent to which a network representation retains communication capacity after disruption. In Task 2.3, resilience is assessed through post-disruption ASPL and the extent to which ASPL increases after intervention. Smaller increases in ASPL suggest that the network representation retains relatively efficient pathways. Larger increases indicate greater communication slowdown and reduced coordination capacity.

The simulation design allows resilience to be compared across police-observed and FI-enhanced networks. This matters because FI can reveal additional connections and alternative pathways. A network that appears strongly disrupted under police-only visibility may appear more resilient when FI-derived linkages are incorporated. This does not mean that the criminal network has changed. It means that the representation used to evaluate the intervention has changed.

Task 2.3, therefore, interprets disruption outcomes as visibility-dependent. The same intervention can produce different measured outcomes depending on whether the analyst evaluates the police-only network, the corrected police network with FI links reintroduced after disruption, or the FI-enhanced network where forensic links are available before targeting. This structure allows Work Package 2 to assess whether FI improves the accuracy of disruption assessment.

3.3.2.4 Added Value Gap

The Added Value Gap (Equation 8) is the primary comparative metric used to quantify FI's contribution to disruption analysis. It measures the difference in communication efficiency between corrected police networks and FI-enhanced networks after identical disruption strategies.

The Added Value Gap is defined as:

$$\boldsymbol{ASPL_3 - ASPL_{\{FI\}}} \qquad (8)$$

where:

- $ASPL_3$ represents the ASPL (Equation 6) of the corrected police network, defined as the police-observed network after disruption, with FI-derived edges reintroduced. This reflects how the disrupted network would appear if additional forensic connectivity had been observable but not used in the initial targeting and,
- $ASPL_{FI}$ represents the ASPL of the FI-enhanced network, in which forensic linkages are incorporated prior to disruption and therefore directly inform the targeting process.

In this formulation, $ASPL_3$ refers to the ASPL of the corrected police network. This is the police-observed network after disruption, with FI-derived edges reintroduced afterwards. It shows how the disrupted network would appear if additional forensic connectivity had been observable at the evaluation stage, even though it was not available during the initial targeting. $ASPL_{\{FI\}}$ refers to the ASPL of the FI-enhanced network, where forensic linkages are incorporated before disruption and can directly influence the targeting process.

Positive values indicate that the corrected police network has a higher post-disruption ASPL than the FI-enhanced network. This means that disruption under police-level observability produced greater apparent fragmentation than disruption conducted under FI-enhanced visibility. Values close to zero indicate a limited difference between the two representations. Negative values indicate simulations where the FI-enhanced disruption produced a higher post-disruption ASPL than the corrected police network. The Added Value Gap captures the difference between disruption assessed with limited observability and disruption assessed with expanded forensic visibility. It provides a practical measure of the extent to which evaluation disruption changes when FI is incorporated.

3.3.3 Methodology

Task 2.3 uses a computational simulation framework to evaluate disruption outcomes under different levels of network observability. The design generates synthetic criminal networks, applies forensic enhancements, conducts standardized disruption strategies, and compares outcomes across police-observed and FI-enhanced representations. This approach allows the analysis to vary the information available to the analyst while holding intervention rules constant.

The analysis proceeds in three comparative stages. First, baseline criminal networks are generated and interpreted as police-observed networks. Disruption strategies are applied to these networks, and

post-disruption communication efficiency is measured using ASPL. Second, FI-derived linkages are introduced into the disrupted police networks to produce corrected network representations. ASPL is recalculated to assess how previously unobserved FI connectivity changes the measured effect of disruption. Third, the same disruption strategies are applied directly to FI-enhanced networks where forensic linkages are available before intervention. These three conditions allow Work Package 2 to compare police-observed disruption, corrected post-disruption visibility, and disruption under full FI-enhanced observability.

3.3.3.1 Simulation design

The simulation dataset consists of synthetic network representations generated using the Barabási–Albert preferential attachment model. This model was selected because it produces scale-free structures with highly connected hubs and many low-degree nodes, which are common features in empirical studies of criminal and illicit networks. The simulation is not intended to reproduce one specific empirical network. Its purpose is to test disruption under structurally uneven conditions that are relevant to criminal network analysis.

A total of 1,000 base criminal networks were generated. These are the police-observed networks, labelled as “a” network. Each base network contained a random number of nodes between 150 and 200. This range was selected to represent medium-sized criminal and co-offending networks. Connectivity was set by multiplying the node count by a random value between 2 and 4. This produced moderately dense networks with variation across simulation runs. All base network edges were assigned a weight of 1, representing equal police-observed co-offending or shared crime involvement links.

The unit of analysis is the simulated network instance under a defined enhancement condition and disruption strategy. Each instance is observed before and after the disruption. This enables measuring structural change under controlled conditions and comparing disruption outcomes across network types.

3.3.3.2 Baseline police-observed networks

The baseline police-observed networks represent the relational structure available through conventional police data. They are treated as the starting point for disruption analysis because police-recorded networks commonly serve as the reference structure for operational targeting and strategic assessment.

Each baseline network uses the same construction principles. Nodes represent actors or relational units in the simulated criminal network. Edges represent police-visible relationships. Since all edges have equal weight in the baseline networks, disruption strategies based on node centrality rely on structural position rather than tie strength. The communication-targeting strategy is still applied to police-observed networks for comparability, although all police-only edges have the same weight.

The baseline networks serve two purposes. They provide the police-only condition against which FI-enhanced networks are compared, and they allow the study to assess how disruption appears when law enforcement operates with limited observability. This reflects the practical reality that disruption decisions are often based on incomplete representations of criminal connectivity.

3.3.3.3 Forensic-enhanced network variants

Three FI-enhanced sister networks were generated for each baseline network. These variants represent DNA, fingerprint, and ballistics enhancements. Each FI-enhanced network retained the same base structure as its corresponding police-observed network. Additional nodes and edges were

then introduced to represent trace-based linkages. This design keeps the baseline structure stable while allowing forensic observability to vary across enhancement types.

The DNA-enhanced networks increased node counts by a random factor of 3-5 and edge counts by a random factor of 8-10. DNA-derived edges were assigned a weight of 1.0. The fingerprint-enhanced networks increased node counts by a random factor of 2.5-4 and edge counts by a random factor of 6-8. Fingerprint-derived edges were also assigned a weight of 1.0. The ballistics-enhanced networks increased node counts by a random factor of 1.5-2.5 and edge counts by a random factor of 2-4. Ballistics-derived edges were assigned a weight of 0.8 to reflect lower specificity relative to DNA and fingerprint linkages.

These enhancement parameters were informed by empirical and case-based literature showing that different forensic modalities expand observability in different ways. DNA and fingerprint linkages are modelled as broader and higher-confidence forms of forensic visibility. Ballistics linkages are modelled as narrower and more context-dependent. The simulation, therefore, captures plausible variation in FI contributions across network instances without claiming to reproduce a single operational dataset.

Table III: FI enhancement parameters

Type	Node Increase	Edge Increase	Avg. Edge Weight
DNA	3× to 5×	8× to 10×	1.0
Fingerprint	2.5× to 4×	6× to 8×	1.0
Ballistics	1.5× to 2.5×	2× to 4×	0.8

3.3.3.4 Disruption strategies

Task 2.3 applies five disruption strategies to each network type. The strategies represent established intervention logics in criminal network research and operational policing. High-degree targeting removes highly connected actors. High-betweenness targeting removes actors positioned on many shortest paths. High-closeness targeting removes actors with short average distances to the rest of the network. Random targeting removes actors without using structural information and provides a comparison baseline. Communication targeting removes high-weight edges and represents intervention against important channels of coordination.

For the node-based strategies, nodes were ranked by degree centrality, betweenness centrality, or closeness centrality, and the top 10% were removed in a single step. Random targeting removed 10% of nodes selected at random. For the edge-based strategy, the top 10% of edges were removed according to edge weight. In FI-enhanced networks, edge weights vary by forensic modality, which enables weighted communication targeting. In police-observed networks, all edges have equal weight, so the strategy operates as a comparable edge-removal condition.

Using a single-step 10% disruption level standardized intervention intensity across all network types. This ensures that differences in outcomes can be interpreted as differences in network representation and observability, rather than differences in the amount of disruption applied.

Degree centrality (Equation 9) measures the number of direct connections an actor maintains within the network. Formally, degree centrality for a node $v$is defined as

$$\boldsymbol{C_D(v) = \frac{deg(v)}{|N| - 1}} \tag{9}$$

where $deg(v)$represents the number of edges connected to the node v, and | N |is the total number of nodes in the network.

Betweenness centrality (Equation 10) measures the extent to which a node lies on the shortest paths between other nodes, capturing the actor's potential to control information flow within the network.

$$\boldsymbol{C_B(v) = \frac{2}{(|N|-1)(|N|-2)} \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}} \quad (10)$$

where σ_{st}represents the number of shortest paths between nodes $s$and t, and $\sigma_{st}(v)$is the number of those paths that pass through node v.

Closeness centrality (Equation 11) measures how near a node is to all other nodes in the network based on geodesic distance.

$$\boldsymbol{C_C(v) = \frac{|N|-1}{\sum_{u \neq v} d(v,u)}} \quad (11)$$

where $d(v,u)$represents the shortest path distance between nodes $v$and u.

3.3.3.5 Network measures and comparison strategy

ASPL is the primary outcome measure in Task 2.3. It measures the average shortest path between pairs of nodes in the network. Lower ASPL values indicate more efficient communication. Higher ASPL values indicate longer paths, reduced communication efficiency, and greater structural degradation following disruption. ASPL is therefore used to assess whether an intervention slows or fragments the network.

The comparison strategy focuses on three conditions. The first is the disrupted police-observed network. This reflects how disruption appears when only police-visible structure is available. The second is the corrected police network, where FI-derived edges are reintroduced after police-based disruption. This shows how the evaluation of disruption changes when hidden forensic connectivity becomes visible after the intervention. The third is the FI-enhanced network disrupted under full forensic visibility. This shows how outcomes change when forensic linkages are available before targeting.

Each simulation scenario was repeated 1,000 times. Baseline and post-disruption metrics were aggregated across runs using summary statistics, including means and standard deviations. The analysis compared ASPL values across police networks, FI-enhanced networks, and corrected networks. The resulting dataset included more than 24,000 disrupted network observations, with standardized outputs programmatically combined into a unified analysis pipeline. Computations were conducted in Python using NetworkX, Pandas, NumPy, SciPy, Statsmodels, and Matplotlib.

3.3.4 Scientific results and recommendations

Task 2.3 shows that FI changes the measurement of disruption outcomes by expanding network observability. Baseline communication efficiency is broadly similar across police and FI-enhanced networks, indicating that the networks start from comparable conditions. After disruption, police-only networks show larger increases in ASPL, especially under targeted node removal. When FI-derived links are included, the magnitude of communication slowdown is reduced. This indicates that police-

only networks tend to overestimate disruption-induced fragmentation by omitting additional connectivity and redundancy.

The results also show that targeted strategies remain the most disruptive across network types. High-degree, high-betweenness, and high-closeness targeting produce the largest increases in ASPL. Random targeting and communication targeting produce limited changes. FI does not reverse the ranking of strategies. It changes the scale of measured disruption and reveals that the observed network is more connected than police-only data suggest.

3.3.4.1 Baseline differences between police and forensic-enhanced networks

Prior to disruption, baseline ASPL values were closely aligned across network types (Table 4). Police-only networks had a mean ASPL of 3.06 with a standard deviation of 0.25. DNA-enhanced networks had a slightly lower mean ASPL of 3.02 with a standard deviation of 0.34. Fingerprint-enhanced networks had a mean ASPL of 3.19 with a standard deviation of 0.47. Ballistics-enhanced networks had the highest mean ASPL at 3.42 with a standard deviation of 0.61.

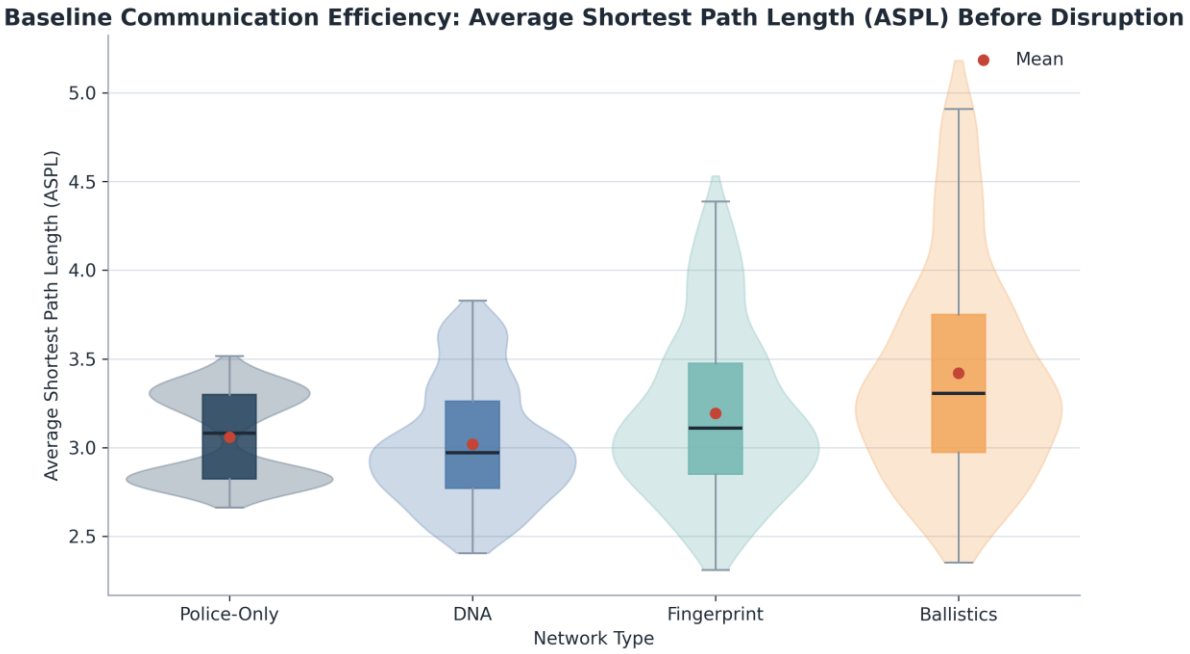
The overall range of baseline values is relatively narrow. This indicates that FI enhancements do not substantially alter global communication efficiency prior to the disruption. The main difference is variability. FI-enhanced networks exhibit greater dispersion in ASPL, especially under ballistic conditions. This suggests that forensic enhancement introduces greater structural heterogeneity across simulations, even where average communication efficiency remains comparable (Figure 11).

The practical interpretation is that FI alters the network's composition and visibility before it changes the mean level of communication efficiency. For law enforcement analysis, this is important because baseline similarity means that subsequent differences in disruption outcomes are less likely to be driven by very different starting conditions. They are more likely to reflect how additional forensic connectivity changes network response after intervention.

Table IV: Baseline communication efficiency by network type

Network Type	ASPL (Mean)	ASPL (Standard Deviation)
Ballistic Enhanced	3.42	0.61
DNA Enhanced	3.02	0.34
Fingerprint Enhanced	3.19	0.47
Police Data (no Enhancement)	3.06	0.25

Figure 11: Baseline ASPL distribution by network type

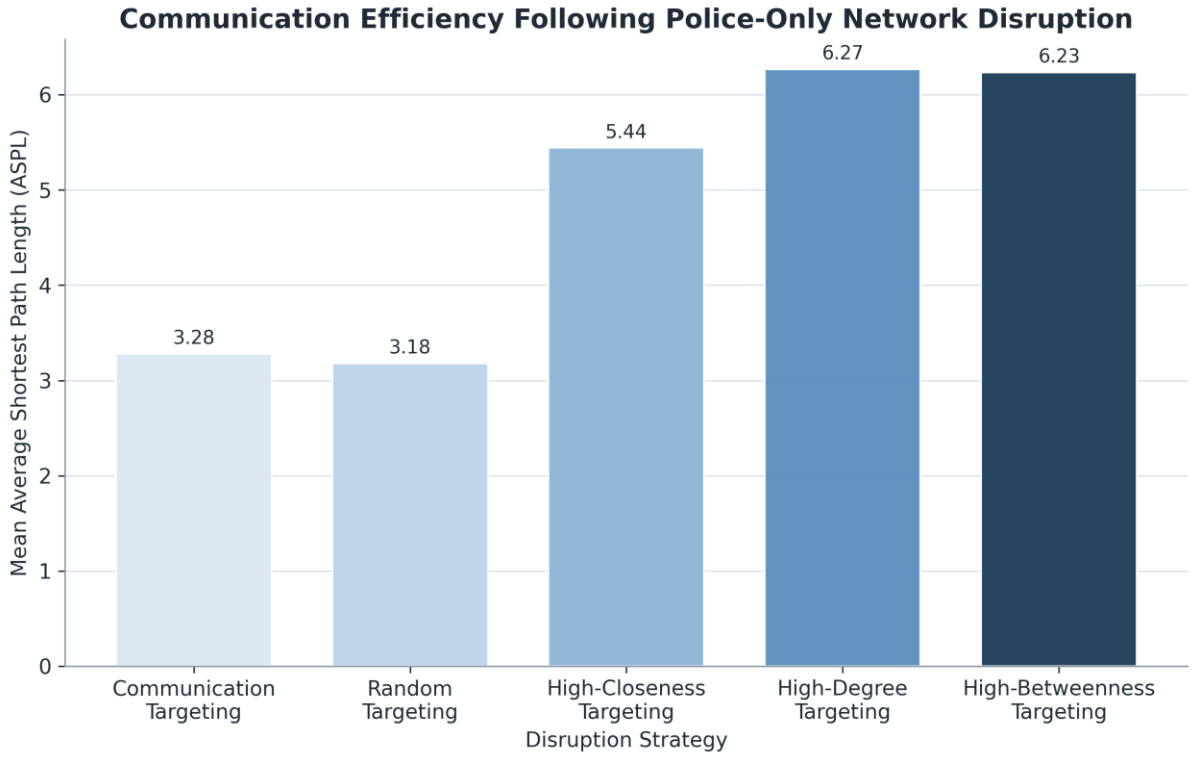


3.3.4.2 Disruption outcomes by intervention strategy

In the police-only networks, targeted node removal produced clear increases in ASPL (Figure 12). High-degree targeting increased mean ASPL from 3.06 to 6.27. High-betweenness targeting produced a comparable increase to 6.23. High-closeness targeting increased the mean ASPL to 5.44. These results indicate substantial degradation in communication efficiency after structurally informed targeting.

Random targeting and communication targeting produced much smaller changes. Random targeting increased the mean ASPL to 3.18. Communication targeting increased the mean ASPL to 3.28. The difference between targeted and non-targeted strategies is therefore substantial. Targeted node strategies increased ASPL by approximately 2.4 to 3.2 units, while random and edge-based strategies produced increases of less than 0.25 units. These results support the use of centrality-based strategies as strong disruption tests in simulation. They also show why police-only network evaluations may produce strong apparent disruption effects. When the visible network has limited redundancy, removing central nodes results in sharp increases in path length. This effect becomes more qualified once FI-derived connectivity is included.

Figure 12: Communication efficiency following police network disruptio



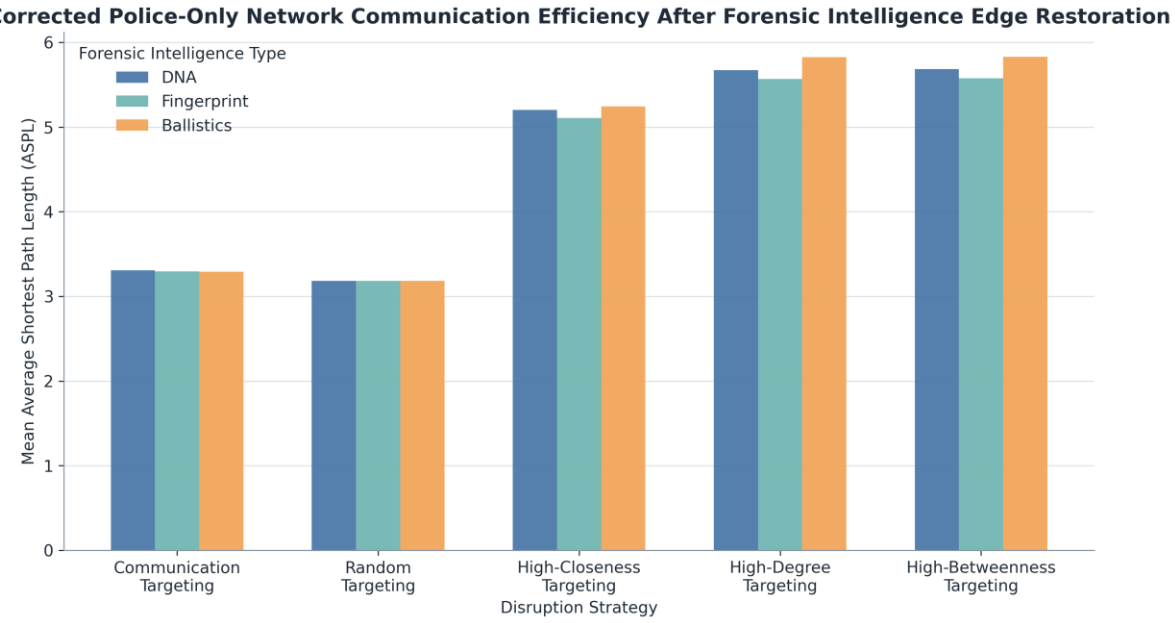
3.3.4.3 Differences between police-only and forensic-enhanced disruption outcomes

When FI-derived edges were reintroduced into disrupted police networks, post-disruption ASPL decreased across the targeted strategies. This means that adding forensic connectivity reduced the measured communication slowdown observed in police-only networks (Figure 13). Under high-degree targeting, ASPL decreased from 6.27 in the disrupted police network to 5.67 for DNA, 5.57 for fingerprint, and 5.83 for ballistics. Under high-betweenness targeting, ASPL decreased from 6.24 to 5.58-5.83 across FI conditions. Under high-closeness targeting, ASPL decreased from 5.44 to 5.11-5.24.

The reduction was not identical across forensic modalities. Fingerprint-enhanced corrections produced the largest reductions in corrected police networks, followed by DNA, with ballistics producing the smallest effects. Across all FI conditions, the same general pattern appears: forensic edge restoration reduces post-disruption path length relative to police-only disruption. For random targeting and communication targeting, differences were minimal and ASPL values remained close to baseline.

These findings show that FI-derived connectivity changes the interpretation of disruption impact. The same police-based intervention appears more disruptive before FI-derived links are considered. Once forensic connectivity is added, the network retains shorter communication paths. This suggests that police-only representations can overstate fragmentation because they do not include additional pathways visible through FI.

Figure 13: Corrected police network communication efficiency after FI edge restoration



3.3.4.4 Added Value Gap results

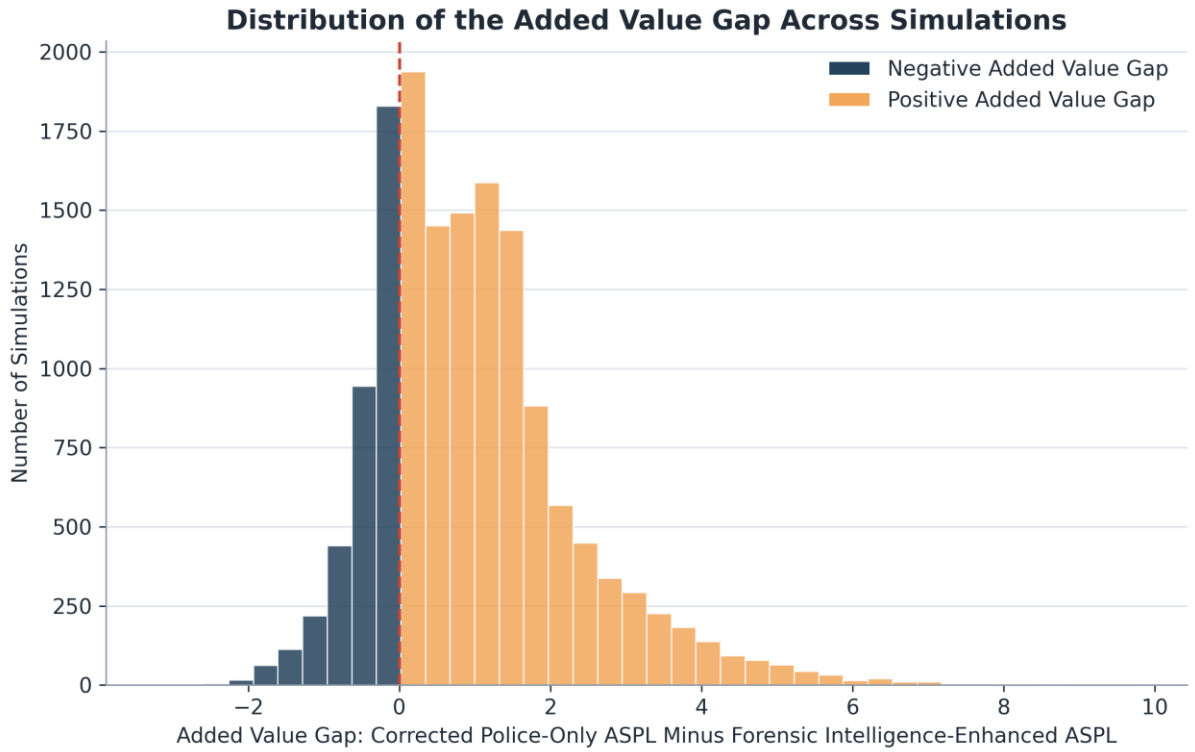
The Added Value Gap results quantify the difference between corrected police networks and FI-enhanced networks following identical disruption strategies. Across targeted strategies, Added Value Gaps are consistently positive. This indicates that FI-enhanced networks retain shorter communication paths than corrected police networks under targeted intervention. The gap is largest under high-degree and high-betweenness targeting.

Under high-degree targeting, the mean Added Value Gap is 2.33 for DNA, 1.44 for fingerprint, and 1.52 for ballistics. Under high-betweenness targeting, the mean gap is 2.34 for DNA, 1.54 for fingerprint, and 1.57 for ballistics. High-closeness targeting produces smaller values, ranging from 1.13 to 1.91 across FI types. Random targeting and communication targeting produce gaps close to zero across FI types.

Across all simulations, the distribution of Added Value Gap values is centered above zero (Figure 14). Most observations fall between approximately 0 and 2 ASPL units, with a smaller right tail extending beyond 6 ASPL units. Negative values are present, though infrequent and concentrated near zero. These cases represent simulations where FI-informed targeting produced a slightly higher post-disruption ASPL than the corrected police network.

The main interpretation is that FI changes the measured scale of disruption. Positive gaps indicate that FI-enhanced networks are less fragmented than corrected police networks after targeted intervention, as forensic visibility reveals additional connectivity. The gap is especially relevant for centrality-based targeting, where police-only representations produce the strongest apparent disruption effects.

Figure 14: Distribution of Added Value Gap across simulations



3.3.4.5 Strategic implications for law enforcement

Task 2.3 has several implications for law enforcement and FI development in Belgium.

- First, the results show that disruption assessments depend on observability. A police-only network can make targeted interventions appear more structurally disruptive by omitting forensic linkages and alternative pathways. FI-enhanced networks provide a broader view of connectivity and therefore produce a more cautious estimate of disruption effect.
- Second, targeted strategies remain operationally relevant. High-degree, high-betweenness, and high-closeness targeting consistently produce the largest changes in ASPL. This supports the continued use of structural prioritization in criminal network analysis. At the same time, Task 2.3 shows that the estimated impact of these strategies is sensitive to the data layer used to construct the network. Centrality-based targeting should therefore be interpreted alongside data quality and observability.
- Third, FI contributes to strategic assessment by reducing uncertainty. FI-enhanced networks produce more stable disruption estimates and reveal additional redundancy. This can support more realistic planning, especially when police data alone suggest that removing a small number of central actors would substantially degrade the network. In practice, FI may help analysts identify where disruption is likely to have a limited effect, even when hidden connectivity remains.
- Fourth, the findings support the development of FI tools that integrate multiple trace types. DNA, fingerprint, and ballistics enhancements produced different effects, reflecting differences in scope, coverage, and specificity.

A future Belgian FI tool should therefore preserve information about the source and confidence of forensic linkages, rather than treating all forensic links as equivalent. The purpose should be to support

better targeting, more realistic disruption assessment, and a clearer understanding of network redundancy.

3.3.5 Conclusion: implications for disruption analysis and FI

Task 2.3 demonstrates that FI changes how disruption outcomes are measured in criminal network analysis. Baseline communication efficiency is broadly similar across police and FI-enhanced networks, supporting comparisons across conditions. After disruption, police-only networks show larger increases in ASPL, especially under targeted node removal. When FI-derived connectivity is incorporated, the measured disruption effect is reduced because additional pathways remain visible. The main conclusion is that disruption effectiveness is contingent on observability. Police-based network representations can overestimate disruption-induced fragmentation when they omit forensic linkages and alternative routes. FI-enhanced representations provide a more complete basis for assessing whether targeted interventions meaningfully degrade communication efficiency.

For Work Package 2, this finding strengthens the argument that FI adds value beyond case linkage alone. FI improves the representation of criminal connectivity and changes how intervention outcomes are interpreted. Its contribution is therefore both analytical and strategic. Analytically, it reveals additional network structure. Strategically, it supports a more accurate assessment of vulnerability, resilience, and the impact of disruption. For Belgium, the implication is that future FI tools should support both disruption assessment and linkage detection. A useful FI tool should allow analysts to compare police-observed and forensic-enhanced representations, identify where forensic linkages reveal redundancy, and evaluate whether planned interventions remain effective under expanded observability. Task 2.3, therefore, provides evidence that FI can support more realistic and better-informed criminal network disruption analysis.

3.4 Legal, practical, and technical conditions for embedding fi in Belgium (Task 2.4)

3.4.1 Objective of Task 2.4

Task 2.4 identifies the legal, practical, organizational, and technical conditions required to embed FI in the Belgian policing context. This task complements Tasks 2.1, 2.2, and 2.3 by addressing the implementation environment in which a FI tool would need to operate. Tasks 2.1 and 2.2 examined whether police and forensic data can be integrated and analyzed in practice, while Task 2.3 assessed how forensic enhancement changes disruption analysis under controlled simulation conditions. Task 2.4 examines whether such a tool can be implemented responsibly, lawfully, and sustainably in Belgium.

This task is guided by two linked components. The first component is a scoping review of the international FI literature. This review examines how FI has been conceptualized and empirically applied in relation to case linkage, relational crime analysis, criminal network analysis, and disruption-relevant decision-making. The second component is a Belgian feasibility study combining legal analysis, expert interviews, and a national expert survey. This study assesses how Belgian legal frameworks, institutional structures, technical infrastructure, professional capacity, and governance conditions shape the feasibility of FI implementation.

Task 2.4 addresses two research questions:

> *How has FI been conceptualized and empirically evaluated in relation to crime linkage and criminal network analysis?*

To what extent is the integration of FI feasible within the Belgian policing context, given legal, organizational, technical, and institutional constraints?

The objective is to provide an evidence-based assessment of the conditions under which FI can be embedded in Belgium. The task does not treat FI as a single tool with one implementation pathway. It assesses FI as a range of possible models with varying levels of integration, legal risks, and operational requirements. This distinction is important for Belgian policy development because the feasibility of FI depends on the type of model being considered, the data being processed, the governance structure in place, and the safeguards attached to use.

3.4.2 Conceptual and empirical background

Task 2.4 builds on the wider Work Package 2 finding that FI adds value by expanding the observable relational field available to analysts and investigators. The international literature shows that FI can link cases, offenders, objects, places, and traces across investigations. These linkages can produce crime series, clusters, co-offending structures, and network-relevant outputs. In this way, FI contributes to intelligence-led policing by improving the information base used for prioritization, coordination, and intervention planning.

The Belgian feasibility component places this analytical potential within a specific national context. Belgium operates within a rights-based legal framework shaped by European and national data-protection rules, including the Law Enforcement Directive, the Belgian Data Protection Law of 2018, and broader protections under the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights. Belgium also has a decentralized policing and justice environment, with data, responsibilities, and operational practices distributed across institutions. These conditions mean that FI implementation requires more than technical capacity. It also requires legal authority, clear governance, standardized identifiers, reliable workflows, trained users, secure infrastructure, and public-interest safeguards.

3.4.2.1 Forensic science and FI

Work Package 2 distinguishes forensic science from FI in line with established scholarship (Baechler et al., 2020; Ribaux et al., 2006; Ribaux & Caneppele, 2017). Forensic science refers to the examination of physical traces for identification, individualization, investigative support, or evidentiary use in a specific case. Its primary orientation is case-bound and evidentiary. It supports the investigation and prosecution of individual offences.

FI refers to the structured analytical use of forensic trace data to identify patterns, link events, and generate relational knowledge across investigations. Its defining feature is cross-case integration. FI uses traces such as DNA, fingerprints, ballistics, chemical profiles, digital traces, or other forensic indicators to identify relationships that may not be visible through case-by-case investigation. These outputs can support tactical decisions, strategic analysis, investigative prioritization, and disruption planning.

In Work Package 2, FI is therefore understood as a relational information layer derived from trace data. This definition is important because it places FI within the broader objective of improving criminal network analysis. The value of FI does not depend only on the scientific reliability of a trace in a single file. It also depends on whether forensic data can be transformed into lawful, interpretable, and useful cross-case information.

3.4.2.2 Existing conceptualizations of FI

The literature identifies several ways in which FI can be organized. At the most basic level, traditional forensic data analysis uses existing laboratory workflows to compare traces across cases. This model can produce intelligence through cross-case comparisons of DNA, fingerprints, ballistics, drug profiles, or other forensic materials. It normally builds on existing laboratory systems and professional practices, which makes it the most immediately feasible model in many jurisdictions.

A second model is information-sharing and forensic integration. This model links forensic data with police, investigative, or intelligence information through shared databases, interoperable systems, and formal communication channels. It requires stronger coordination between institutions and more developed governance arrangements. Its value lies in improving cross-agency visibility and reducing information silos.

A third model is the holistic data-view model. This model integrates multiple forensic, police, intelligence, digital, financial, and situational data streams within a single analytical environment. It offers the greatest analytical reach because it can support complex, multi-domain analysis. It also creates the highest legal, organizational, and technical demands because it requires large-scale processing of sensitive data, strong access controls, clear legal authorization, advanced cybersecurity, and mature oversight.

These models should be understood as a progression in integration intensity. Traditional forensic data analysis is closest to current practice. Information-sharing models require structured interoperability. Holistic data-view systems require major institutional, legal, and technical capacity. For Belgium, this distinction is central because the feasibility of FI depends on the level of integration being proposed.

3.4.2.3 FI, case linkage, and criminal network analysis

The scoping review shows that FI primarily functions as a linkage mechanism. Across the included studies, forensic data were used to connect cases, offenders, objects, or identifiers through exact matching, similarity-based comparison, clustering, or aggregation. DNA studies commonly use exact profile matches to connect incidents or offenders. Ballistic and digital studies used shared identifiers, signatures, or artefacts. Chemical and behavioral studies often relied on similarity thresholds or clustering methods.

These linkages are directly relevant to criminal network analysis because they generate relational structures. Some studies produced formal networks with nodes, edges, and network measures. Others produced network-adjacent outputs such as linked case sets, crime series, clusters, or co-offending patterns. Both types of output matter for Work Package 2 because they show that FI can produce cross-case relational knowledge even when the original study does not describe the output as a network.

The scoping review also shows that FI can reveal previously unobserved cases, actors, and cross-jurisdictional connections. These findings align with the empirical results of Tasks 2.1 and 2.2, which showed that forensic DNA data expanded the visible relational field beyond police-recorded case relationships. They also support the simulation logic of Task 2.3, where FI was treated as an added layer of observability that changes how disruption outcomes are assessed.

3.4.3 Methodology

Task 2.4 uses two complementary research components. The first is a scoping review of international empirical studies on FI, case linkage, relational crime analysis, and disruption-relevant decision-making. The second is a Belgian feasibility assessment based on legal analysis, expert interviews, and a national expert survey.

Together, these components allow Task 2.4 to connect the international evidence base with the Belgian implementation context. The scoping review identifies what FI does analytically and where the literature shows added value. The feasibility study identifies the requirements for implementing FI in Belgium under current legal, organizational, technical, and governance conditions.

3.4.3.1 Scoping review methodology

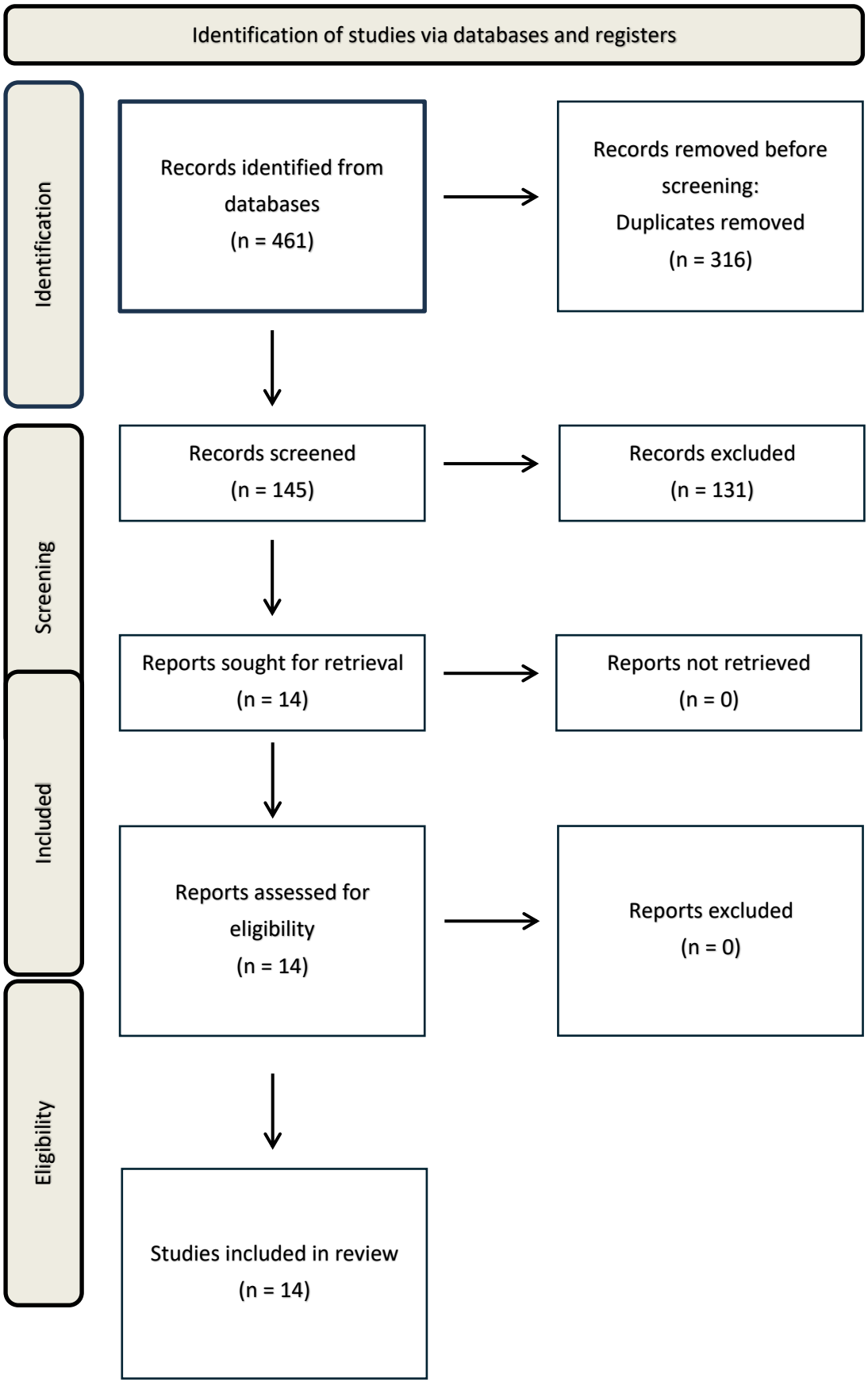
The scoping review was designed to map how FI has been used in empirical research to generate relational crime structures and support criminal network understanding. A scoping review design was selected because the literature is fragmented across criminology, forensic science, policing studies, legal scholarship, computer science, and network research. The purpose was to identify concepts, applications, and gaps rather than estimate the effect of a single intervention.

The review followed PRISMA-ScR guidance (Tricco et al., 2018). Searches were conducted in JSTOR, PubMed, Scopus, and Web of Science. The search strategy focused on FI modalities such as DNA, fingerprints, ballistics, drug profiling, digital FI, communication metadata, and financial or transaction-based data, combined with terms related to case linkage, crime linkage, series linkage, co-offending, clusters, criminal networks, and intelligence-led policing.

The review identified 461 records (Figure 15). After duplicate removal, 145 records were screened. Studies were included where they used at least one FI modality in an investigative or intelligence-led capacity, applied that modality to cross-case linkage or relational analysis, and reported empirical material relevant to criminal network understanding, relational crime analysis, or disruption-relevant decision-making. Studies focused only on single-case forensic identification, laboratory validation, or purely technical performance were excluded. The final corpus included 14 empirical studies.

Data extraction recorded publication details, jurisdiction, forensic modality, unit of analysis, linkage method, analytical approach, type of relational output, and relevance to disruption or intelligence-led policing. The extracted data were synthesized thematically. Four themes structured the analysis: FI as a linkage mechanism, FI revealing otherwise unobserved structures, FI altering network topology, and FI supporting targeting logic in intelligence-led policing.

Figure 15: PRISMA flow diagram for the scoping review



3.4.3.2 Interview methodology

The Belgian feasibility study included eight semi-structured expert interviews. Participants were selected through purposive expert sampling because the objective was to capture informed views from professionals directly involved in forensic practice, policing, criminal analysis, legal governance, data protection, or technical system design. This approach was appropriate because FI implementation depends on the interaction of legal, operational, technical, and institutional actors.

The interviews explored the current police and forensic data landscape in Belgium, experiences with data-sharing and information silos, views on traditional forensic data analysis, information-sharing models, and holistic data-view systems, and perceived legal, technical, organizational, cultural, and governance barriers. They also examined the conditions required for successful implementation, including standardized identifiers, access control, training, data quality, infrastructure, and oversight.

Interview data were analyzed thematically. The initial coding framework was informed by the research questions and by the National Institute of Justice FI program elements, including policies, forensic laboratory workflow, data sharing, training, and resources (Garvey et al., 2023). This deductive framework was refined during analysis to capture themes emerging from the interview data. The analysis focused on identifying perceived enablers and barriers for each FI model and on comparing views across professional domains.

3.4.3.3 Survey methodology

A national online expert survey was conducted to provide broader empirical coverage across relevant professional sectors in Belgium. The survey used purposive, expert-oriented sampling. The target population included law enforcement personnel, forensic scientists, legal professionals, policy and government actors, and IT or data science specialists involved in justice or security-related work.

The survey measured perceptions of the current Belgian police and forensic data landscape, awareness of FI, perceived usefulness of FI, technical feasibility, expected impact on interagency collaboration, compatibility with Belgian legal frameworks, and infrastructure requirements. Respondents also evaluated three FI models: traditional forensic data analysis, information-sharing and integration, and a holistic data-view model. For each model, respondents assessed usefulness, realism of implementation, and legal or ethical security.

The survey was administered in English, French, and Dutch. Responses from the three language versions were exported, cleaned, and merged into a single anonymized dataset. The final analytic sample included 51 respondents. Closed-ended responses were analyzed descriptively using frequencies and percentages. Open-ended responses were coded into recurring themes, including legal barriers, data silos, training and expertise, infrastructure and resources, organizational culture, public trust, and security concerns.

3.4.3.4 Analytical strategy

The analytical strategy integrated the scoping review and feasibility study at the level of interpretation. The scoping review established what FI can contribute in principle and in international empirical practice. The feasibility study assessed whether and how these contributions can be translated into the Belgian context.

The analysis was structured around legal feasibility, organizational feasibility, technical feasibility, governance feasibility, and overall implementation feasibility. This structure allows Work Package 2

to distinguish between analytical value and practical implement ability. A model may be useful in principle while still requiring legal authorization, organizational reform, technical infrastructure, or stronger governance before it can be implemented. The three FI models were used as the main comparative framework. Traditional forensic data analysis was assessed as the lowest-integration model. Information-sharing and integration was assessed as a medium-integration model. Holistic data-view systems were assessed as the highest-integration model. This structure allows Task 2.4 to provide phased recommendations for Belgium.

Table V: Analytical framework for assessing FI feasibility in Belgium (Adapted from (Garvey et al., 2023))

Program Element	Evaluation Factors
Policies	Policies and procedures established for: - Sharing data. - Reviewing products. - Communicating between intelligence and forensic science units. - Feedback between intelligence, investigative, and forensic science units.
Forensic Laboratory Workflow	Workflow changes implemented to produce timely data on: - Firearms - Chemistry (e.g., drugs, toxicology) - DNA - Latent Prints
Data Sharing	- Establish the types of data that are available. - Procedure for data transfer (manual or automated). - Establish timeframes for the date-sharing routine. - Procedures for data requests.
Training	- Presence of an internal training program. - Number of trainings held. - Number of personnel trained (intelligence, forensic science, and investigative).
Resources	Staffing for: - Forensic scientists. - Intelligence analysts. - Investigators. - Analytic technology platform specialists. - Infrastructure (laboratory space, analyst workstations).

3.4.4 Scientific results and recommendations

Task 2.4 finds that FI has clear analytical value and broad professional support in Belgium, although implementation feasibility varies by model. The scoping review shows that FI can generate cross-case relational structures and strengthen the information base for disruption-relevant decisions. The Belgian feasibility study shows that traditional forensic data analysis is the most immediately feasible model, information-sharing and forensic integration is feasible under strengthened governance and infrastructure, and holistic data-view systems remain a longer-term objective requiring substantial legal, technical, and organizational development.

The overall finding is that Belgium can move toward FI through a staged approach. Immediate implementation should focus on strengthening existing forensic comparison capacity and standardizing case-linkage processes. Medium-term implementation should focus on controlled

interoperability between police and forensic systems. Long-term development can prepare the conditions for more integrated analytical environments, provided that legal authorization, oversight, cybersecurity, and institutional capacity are in place.

3.4.4.1 Findings from the scoping review

The scoping review identified 14 empirical studies that met the inclusion criteria. Most studies used quantitative approaches, including statistical modelling, clustering, or network analysis. DNA-based FI was the most common modality, followed by studies using chemical or drug profiling, ballistics, digital FI, and multi-source forensic approaches.

The review shows that FI is most consistently used to generate linkages. These linkages connect cases, offenders, objects, devices, or traces across investigations. FI therefore supports the construction of crime series, clusters, co-offending structures, and formal network representations. This finding is directly relevant to Work Package 2 because it supports treating FI as a relational information layer.

The review also shows that FI expands understanding of the criminal network. Across the included studies, FI identified previously unlinked cases, unknown or previously unseen actors, cross-jurisdictional series, and trace-based relationships that were absent from police records. This means FI can reduce linkage blindness and improve the completeness of the intelligence picture used for analysis.

The evidence for direct disruption outcomes remains limited. Most studies show that FI supports targeting, prioritization, early detection, and coordination, while few directly test whether FI-informed interventions produce better disruption outcomes than police-only approaches. This gap supports the wider design of Work Package 2. Tasks 2.1 and 2.2 provide empirical evidence on police and forensic data integration, while Task 2.3 uses simulation to assess how forensic enhancement changes disruption outcomes.

Table VI: Summary of scoping review findings

Analytical theme	Finding	Evidence from the review
Linkage mechanism	FI primarily operates by linking cases, offenders, objects, traces, or identifiers. These links are produced through exact matching, similarity-based comparison, or algorithmic clustering.	Exact matching was the most common approach, particularly in DNA-based studies where identical genetic profiles were used to link crimes or offenders (De Moor, 2018, 2020; Lammers, 2014; Lavergne et al., 2022, 2024; Lovell et al., 2017, 2018), and in ballistic or digital contexts where exact identifiers or signatures were used (Gagliardi, 2012; Quick and Choo, 2017; Thorpe & Bernard, 2017). Similarity-based linkage was used in chemical profiling and behavioral comparison studies (Morelato et al., 2013; Popovic et al., 2022; Woodhams & Labuschagne, 2012). Algorithmic clustering and aggregation were used to group related entities into clusters or communities (Popovic et al., 2022; Ribaux et al., 2022; Thorpe & Bernard, 2017).
Unobserved structures	FI can reveal relationships that may not be visible through police-recorded data alone, including linked cases, series, clusters, co-offending relations, and object-based connections.	Case identification was reported in 11 studies (Gagliardi, 2012; Lammers, 2014; Lavergne et al., 2022; Lovell et al., 2017, 2018; De Moor et al., 2018; Morelato et al., 2013; Popovic et al., 2022; Quick and Choo, 2017; Ribaux et al., 2022; Woodhams & Labuschagne, 2012). Co-offending identification was present in six studies (Lammers, 2014; Lavergne et al., 2022, 2024; Lovell et al., 2017; De Moor et al., 2020; Thorpe & Bernard, 2017). Cluster detection or grouping was present in seven studies (Gagliardi, 2012; Lovell et al., 2018; Morelato et al., 2013; Popovic et al., 2022; Ribaux et al., 2022; Thorpe & Bernard, 2017; Woodhams & Labuschagne, 2012).
Network topology	FI can generate formal network models and network-adjacent relational outputs. These outputs enable analysis of how forensic links shape the structure of crime relationships.	Eight studies constructed explicit network graphs with defined nodes and edges and applied network-analytic measures (Gagliardi, 2012; Lavergne et al., 2022, 2024; S. Moor et al., 2018, 2020; Popovic et al., 2022; Quick and Choo, 2017; Thorpe & Bernard, 2017). Six studies produced network-adjacent outputs, including crime series, clusters, or linked case sets, without formal graph modelling (Lammers, 2014; Lovell et al., 2017, 2018; Morelato et al., 2013; Ribaux et al., 2022; Woodhams & Labuschagne, 2012).

Targeting logic	FI can support prioritization and intervention by identifying linked cases, central actors, recurring objects, relevant clusters, and cross-case patterns. Direct evaluation of disruption outcomes remains limited in the reviewed literature.	The review found that FI supports case linkage, co-offending identification, cluster detection, communication or interaction mapping, and network construction (Gagliardi, 2012; Lammers, 2014; Lavergne et al., 2022, 2024; Lovell et al., 2017, 2018; De Moor et al., 2018, 2020; Morelato et al., 2013; Popovic et al., 2022; Quick and Choo, 2017; Ribaux et al., 2022; Thorpe & Bernard, 2017; Woodhams & Labuschagne, 2012). The evidence supports FI as a basis for targeting and prioritization, while direct tests of disruption outcomes remain limited.

3.4.4.2 Legal feasibility conditions

The Belgian legal framework does not prevent all forms of FI. It creates conditions that any FI system must respect. The Data Protection Law of 2018, the Law Enforcement Directive, Article 44/11/3 of the Law on Police Services, and broader European rights protections require lawfulness, necessity, proportionality, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, oversight, and accountability.

Article 44/11/3 is particularly relevant because it allows common police databases for strategic, tactical, or operational purposes where processing is necessary, relevant, and proportionate. This provides a possible legal basis for certain FI information-sharing models. It also imposes clear design limits. Any FI system must define its purpose, restrict access, justify the data included, and maintain appropriate safeguards. Interview participants and survey respondents identified legal restrictions as a central barrier, particularly for models that require broader data integration. Experts stressed that pseudonymized data remains personal data when it can be linked to identifiable persons. This means that encoded identifiers, forensic profiles, police records, and judicial data remain subject to data-protection rules. Legal feasibility, therefore, depends on clear authorization, defined data controllership, auditable access, proportionality assessment, retention rules, and safeguards against misuse. The legal feasibility of FI varies by model. Traditional forensic data analysis aligns most closely with current practice and can be strengthened under existing legal structures. Information-sharing models are conditionally feasible if governance, access control, and purpose limitation are clearly established. Holistic data-view systems would require the strongest legal foundation, including explicit authorization for multi-domain processing and high-assurance oversight.

3.4.4.3 Organizational feasibility conditions

The feasibility study shows that organizational fragmentation is a major barrier to FI implementation in Belgium. Interviewees described forensic work as largely case-centered, with laboratories and police services focusing on individual judicial files rather than systematic cross-case linkage. Experts also described fragmented information systems, uneven feedback between institutions, and limited mechanisms for analysts to identify trace-based links across cases in real time. This fragmentation reflects the structure of the Belgian justice and policing environment. Relevant data are held by different institutions, including forensic laboratories, local police zones, federal police services, judicial authorities, and specialized units. These actors have different mandates, workflows, priorities, and

legal responsibilities. FI implementation, therefore, requires institutional coordination, not only data access.

The interviews and survey responses indicate that any FI tool must fit existing workflows. Frontline police and forensic staff already face workload constraints. A system that adds new reporting duties without reducing administrative burden is unlikely to be sustainable. Experts, therefore, supported tools that reuse data already generated in ordinary forensic and police practice, with automated or semi-automated linkage where possible. Training is also an organizational condition. Respondents noted that magistrates, police officers, analysts, and forensic practitioners may not share the same level of scientific, legal, or technical knowledge. FI products require careful interpretation. A forensic link does not automatically mean shared offender identity, direct co-offending, or legal grounds to merge judicial files. Training is needed to help users understand both the value and the limits of FI outputs. Governance actors should Treat FI as an institutional reform process. Implementation should include workflow mapping, role clarification, cross-sector training, and procedures for feedback between forensic laboratories, police analysts, investigators, and judicial actors.

3.4.4.4 Technical feasibility conditions

The feasibility study identifies several technical conditions for FI implementation. The most important thing is the availability of common or harmonized identifiers. Experts repeatedly noted that case numbers, dossier numbers, laboratory identifiers, police records, and judicial references are not always aligned. Without stable identifiers, forensic and police information cannot be reliably linked across systems.

Technical feasibility also depends on data quality. Interviewees highlighted that poor data quality, inconsistent coding, incomplete fields, or incompatible systems can reduce the value of FI. If data are inaccurate or poorly mapped, integration can create false confidence in unreliable outputs. Data quality control is, therefore, a core technical requirement.

System interoperability is another condition. Forensic information may be stored in laboratory information management systems, comparison tools, statistical software, local police databases, federal systems, or separate analytical tools. These systems were generally designed for case management or evidentiary reporting, not for cross-case intelligence analysis. FI implementation requires interfaces that allow the lawful and secure exchange of selected data fields.

Security requirements increase as integration becomes more advanced. Traditional forensic data analysis can often be strengthened within existing laboratory systems. Information-sharing models require secure interfaces, access controls, audit logs, and standardized data exchange rules. Holistic data-view models require advanced cybersecurity, clearance management, retention controls, and continuous monitoring because they combine more sensitive and heterogeneous data. It is essential to prioritize technical foundations before pursuing advanced integration. These foundations include harmonized case identifiers, data quality standards, interoperable data formats, secure transfer procedures, audit logging, and system designs that support privacy by design.

3.4.4.5 Governance and implementation conditions

Governance is the central condition connecting the legal, organizational, and technical requirements. The feasibility study shows that FI cannot be implemented only through software or laboratory capacity. It requires rules defining who may access data, who controls data, who processes data, how outputs are reviewed, how errors are corrected, how long data are retained, and how compliance is monitored.

The NIJ FI program elements provide a useful framework for Belgium. They identify policies, forensic laboratory workflow, data sharing, training, and resources as core implementation domains. These domains align with the Belgian findings. Experts identified the need for formal data-sharing policies, timely forensic workflows, standardized exchange procedures, cross-disciplinary training, adequate staffing, analyst capacity, and technical infrastructure.

A governance framework should also preserve source provenance. Analysts must be able to distinguish police-derived information from forensic-derived information and understand the confidence levels associated with each type of linkage. This is important for interpretation, accountability, and legal defensibility. It also prevents FI outputs from being treated as automatic conclusions.

Implementation should proceed incrementally. A phased model would allow Belgium to strengthen existing forensic comparison systems first, then develop controlled information-sharing mechanisms, and only later consider broader integration. This approach fits Belgium's legal and institutional environment and reduces the risk of overbuilding a system before the necessary safeguards are in place. From this there is a recommendation to Establish a national FI governance roadmap. This roadmap should define short-, medium-, and long-term objectives, assign institutional responsibilities, establish oversight mechanisms, and require evaluation before expanding to higher levels of integration.

3.4.4.6 Feasibility of FI in the Belgian policing context

The combined evidence indicates that FI is feasible in Belgium if implemented in a model-specific, phased manner. Traditional forensic data analysis is the most immediately feasible option. It aligns with existing laboratory practice, has strong professional support, and can be improved through investment in capacity, standardization, and cross-case comparison procedures.

Information-sharing and forensic integration are feasible as medium-term objectives. This model responds directly to the problem of data silos. It would allow police and forensic information to be connected more systematically while maintaining controlled access and source-specific interpretation. Its feasibility depends on governance, identifier harmonization, infrastructure investment, training, and legal safeguards.

Holistic data-view systems are the least feasible in the short to medium term. Experts recognized their analytical value, while also identifying substantial legal, organizational, security, and political risks. A fully integrated system would require explicit legal authorization, advanced cybersecurity, mature oversight, national-level governance, and major reforms to data architecture and professional workflows.

The findings, therefore, support a progressive FI strategy for Belgium. The most realistic path is to strengthen traditional forensic data analysis first, develop structured information-sharing next, and lay the groundwork for longer-term conditions for more integrated models. This approach allows Belgium to improve FI capacity while respecting legal obligations and institutional constraints.

Table VII: Feasibility assessment of FI models in Belgium

FI model	Current feasibility	Main requirements	Recommended implementation horizon
Traditional forensic data analysis	High	Laboratory capacity, standardized coding, cross-case comparison procedures	Short term
Information-sharing and forensic integration	Moderate	Governance, interoperability, harmonized identifiers, access control, training	Medium term
Holistic data-view system	Low to conditional	Explicit legal authorization, advanced cybersecurity, national oversight, major infrastructure reform	Long term

3.4.5 Conclusion: conditions for embedding FI in Belgium

Task 2.4 shows that FI has clear conceptual, empirical, and practical relevance for Belgium. The scoping review demonstrates that FI is consistently used internationally to generate cross-case linkages, reveal previously unobserved structures, support network-relevant analysis, and strengthen the informational basis for intelligence-led policing. The Belgian feasibility study shows that professionals across relevant sectors recognize the value of FI, especially for reducing data silos, improving case linkage, and supporting better coordination.

The main conclusion is that FI is feasible in Belgium when treated as a staged institutional development. Traditional forensic data analysis is the most realistic short-term model because it builds on existing laboratory and judicial practices. Information-sharing and forensic integration provide a credible medium-term pathway if Belgium invests in governance, interoperability, standardized identifiers, and training. Holistic data-view systems remain a long-term objective that should only be pursued after stronger legal, technical, and organizational foundations are in place.

For Work Package 2, Task 2.4 provides the implementation framework for the empirical and simulation findings. Tasks 2.1 and 2.2 show that forensic data can add relational visibility when integrated with police data. Task 2.3 shows that forensic enhancement changes how disruption outcomes are assessed. Task 2.4 shows the conditions under which these analytical benefits can be translated into a Belgian FI tool. The overall implication is that Belgium can develop FI capacity in a legally compliant and operationally useful way, provided that implementation is phased, governed, secure, and proportionate.

3.5 General conclusion of work package 2

3.5.1 Summary of findings across tasks

Work Package 2 assessed the feasibility and added value of an FI approach for Belgian crime analysis. Across Tasks 2.1 to 2.4, the findings show that FI can strengthen crime analysis by expanding the information available to analysts, improving case linkage, and supporting a more accurate

understanding of criminal network structure. At the same time, its contribution depends on the quality, availability, and lawful integration of the data used.

Task 2.1 showed that police and forensic data can be prepared, harmonized, and integrated into combined datasets under secure and anonymized research conditions. This task confirmed that data integration is possible when common case identifiers can be established and when clear procedures are used for data cleaning, linking, and storage. It also showed that data integration is a practical task, not only a technical one. The process depends on institutional workflows, consistent identifiers, and clear data governance.

Task 2.2 demonstrated that integrating forensic DNA linkage data alters the observable structure of criminal case networks. The police-only network remained the main structural backbone, while forensic DNA data added new cases and links that were not visible in police data alone. The combined network, therefore, provided a broader relational view, especially at the level of case linkage and ego networks. The results showed that FI adds value by extending visibility into selected parts of the network, especially where trace-based links connect cases that would otherwise appear isolated or weakly connected.

Task 2.3 extended this analysis to disruption and structural vulnerability. The simulation results showed that forensic-enhanced networks can alter how disruption outcomes are measured. Police-only networks may overestimate the apparent effect of targeted interventions because they do not capture all possible relational pathways. When FI is added, additional connections and redundancy become visible. This changes how vulnerability, resilience, and disruption effectiveness are interpreted. The main value of FI in this task is therefore its ability to produce a more realistic basis for assessing disruption strategies.

Task 2.4 examined the legal, organizational, technical, and governance conditions for embedding FI in Belgium. The scoping review confirmed that FI is understood in the literature as the structured use of forensic data for linkage, analysis, and decision-making across cases. The Belgian feasibility study showed that implementation is possible, although it must be gradual, legally grounded, and supported by clear governance arrangements. Expert interviews and survey findings indicated that legal compliance, data protection, technical interoperability, analytical capacity, and institutional coordination are all necessary conditions for meaningful implementation.

Taken together, the tasks show that FI is feasible and useful in Belgium when it is treated as an integrated intelligence capability. Its contribution is strongest when it is introduced early, integrated into police analytical workflows, and supported by institutional capacity to interpret and act on relational information.

3.5.2 Added value of FI for Belgian crime analysis

The main added value of FI in Work Package 2 is improved observability. Police-recorded data provide an essential basis for crime analysis, but they reflect only what has been reported, detected, recorded, and attributed through investigative processes. FI adds a different form of relational information. It links cases through traces rather than only through known suspects, co-offending records, or police-recorded relationships. This contribution is important because criminal network analysis depends on what is visible in the data. If the available data are incomplete, the resulting network representation may understate the number of relevant cases, miss links between events, or misidentify which parts of a network are structurally important. FI helps reduce this limitation by adding cross-case linkages generated from forensic traces. In Work Package 2, this was most clearly demonstrated through the integration of forensic DNA linkage data with police-recorded case data.

The added value was not uniform across the entire network. The empirical results showed that FI did not completely restructure the police-derived network. Instead, it added a smaller set of non-redundant links and cases. These additions were analytically meaningful because they expanded the observed network outward, identified additional case relationships, and improved the interpretation of selected ego networks. This is especially relevant for serious, complex, or trace-rich forms of crime, where forensic links may reveal relationships that are not available through police data alone.

The simulation results further show that the value of FI is not limited to identifying more links. It also changes how analysts evaluate intervention and disruption. When forensic-enhanced networks reveal additional pathways, disruption strategies may appear less effective than they do in police-only networks. This does not mean that FI weakens disruption. It means that FI provides a more complete and cautious assessment of network vulnerability. For Belgian crime analysis, this is a significant contribution because it reduces the risk of overconfidence in conclusions drawn from police data alone. In line with WP1's conceptual work, these findings support the view that FI can operate at the tactical, operational, and strategic levels. At the tactical level, it can support case linkage and investigative leads. At the operational level, it can help identify recurring patterns across cases. At the strategic level, it can support broader assessments of criminal structures, vulnerabilities, and intervention priorities.

3.5.3 Feasibility of FI implementation in Belgium

Work Package 2 shows that FI implementation in Belgium is feasible, provided that it is developed within clear legal, organizational, and technical boundaries. The findings do not support an immediate move toward a fully integrated intelligence system. They support a phased approach that begins with structured forensic data analysis and targeted case-linkage capabilities.

The legal feasibility of FI depends on lawful purpose, proportionality, necessity, data minimization, and access control. Belgian and European data protection requirements do not prevent FI, but they require careful design. Any system that links forensic and police information must have a clear legal basis, defined users, limited access rights, secure storage, and transparent governance. These safeguards are not secondary issues. They are core conditions for implementation. Organizational feasibility is equally important. The findings show that FI cannot function as a purely laboratory-based output or as an isolated technical product. Its value depends on cooperation between forensic institutions, police services, judicial actors, data protection experts, IT specialists, and analysts. A FI tool must be embedded in workflows where the results can be interpreted and used. Without trained analysts and clear routes from analysis to action, additional forensic links may remain descriptive rather than operationally useful. Technical feasibility depends on interoperability, data quality, harmonized identifiers, and secure analytical systems. Task 2.1 demonstrated that combining data is possible, though integration requires substantial preparation. The data must be cleaned, structured, and linked through reliable identifiers. This has direct implications for future implementation. A Belgian FI tool would require consistent data standards, agreed linkage rules, and technical systems capable of handling sensitive information in a secure and auditable way.

The most feasible short-term model is therefore an incremental model. Belgium can begin by strengthening structured forensic data analysis and cross-case linkage within existing legal and institutional frameworks. More advanced models, such as broader multi-source integration or holistic data-view systems, require further governance development, stronger interoperability, and long-term institutional investment.

3.5.4 Recommendations for future FI development

A phased implementation strategy should be used to develop forensic intelligence gradually and realistically. A strong starting point would be a controlled pilot focused on a single jurisdiction or crime domain where forensic traces are already operationally relevant, such as serious violence, organized crime, burglary series, sexual offences, or drug-related networks. This pilot should compare police-only and forensic-enhanced outputs so that the added value of forensic intelligence can be assessed rather than assumed. Forensic intelligence should also be embedded directly within the intelligence function of policing, rather than treated solely as a laboratory service or late-stage evidentiary tool. Its value depends on timely integration into analytical workflows, allowing forensic links to inform case linkage, prioritization, and network interpretation at an early stage. To support this, Belgium should invest in analytical capacity by training analysts who understand forensic data, police data, network analysis, legal constraints, and operational decision-making. These teams should be cross-disciplinary and include analysts, investigators, forensic experts, and legal or data protection professionals who share a common understanding of forensic intelligence. At the same time, governance should be developed before any large-scale technical expansion. Clear rules are needed for data access, ownership, retention, auditability, quality control, and oversight, and these rules should align with legal, operational, and technical actors from the outset. Finally, future research should continue to test forensic intelligence using comparative designs. The findings from Work Package 2 show that added value is clearest when police-only, forensic-only, and combined datasets or networks are compared directly. This approach should therefore be used in pilot projects and future evaluations to help policymakers and practitioners identify where forensic intelligence meaningfully improves analysis, where its contribution is limited, and where further investment is justified.

3.5.5 Final conclusion

Work Package 2 shows that FI has clear potential to strengthen Belgian crime analysis. Its value lies in changing what can be observed, linked, and assessed within criminal networks. By integrating forensic linkage data with police-recorded crime data, FI can expand network visibility, identify additional case relationships, and support more cautious assessments of disruption and vulnerability.

The findings show that this added value is conditional. FI is most useful when trace data are available, when data can be lawfully linked, when analytical capacity exists, and when outputs are connected to operational decision-making. Its implementation in Belgium should therefore be gradual, governed, and evidence-led. The central conclusion of Work Package 2 is that FI can contribute to Belgian crime analysis by improving the investigative picture available to police and analysts. It does not provide a complete view of criminal activity, nor does it automatically produce better disruption outcomes. FI's practical value is realized when it helps institutions see connections that were previously hidden and when those connections can be interpreted within lawful, secure, and operationally meaningful processes.

4. WP 3: DEVELOPING A ROADMAP WITH GUIDELINES TO IMPLEMENT A FORENSIC INTELLIGENCE SYSTEM IN BELGIUM

This work package aims to define guidelines for actors and recommendations emerging from the examination of the theory, practice and potential institutionalization of forensic intelligence in Belgium. Forensic intelligence, as a systematic exploitation of forensic data to support proactive and strategic criminal investigations, remains underdeveloped in the Belgian context despite its significant demonstrated potential in comparable international jurisdictions.

The research was grounded in an extensive conceptual review, an analyze of integrating police-recorded crime data and forensic DNA linkage data, qualitative fieldwork with forensic practitioners and judicial actors, and institutional mapping across the Belgian forensic ecosystem. A central finding of the project is that the obstacles to forensic intelligence development in Belgium are not primarily technical or scientific in nature. Rather, they are cultural, organizational, and legal: a persistent disconnect between forensic scientists, investigators, and the judiciary; a dogmatic interpretation of data protection legislation that inhibits cross-case data exploitation; insufficient resources within the institutions most capable of carrying forensic intelligence work; and an absence of shared definitions and governance frameworks.

Recommendations are structured across three interconnected levels: (1) global, systemic recommendations addressing the normative and legal conditions for forensic intelligence; (2) intermediate recommendations addressing institutional, organizational, and cultural conditions; and (3) a practical project-design canvas for institutions seeking to initiate specific forensic intelligence activities. Together, these levels constitute a pragmatic roadmap that any institution with the mandate and resources could follow, independently of whether a large-scale, multi-agency system is achievable in the near term.

4.1 Conceptual foundations

4.1.1 Operational definition

Forensic intelligence is defined in this project as the systematic exploitation of forensic data, including DNA profiles, ballistic comparisons, toxicological findings, digital traces, and physicochemical markers, beyond their use in individual case files, with the aim of identifying criminal series, patterns, and phenomena in support of tactical, operational, and strategic decision-making.

This definition entails a shift in the epistemological orientation of forensic science: from a predominantly reactive, case by case logic to a proactive, phenomenon-oriented logic. This shift is not a rejection of traditional forensic rigor but an extension of it into new analytical territory.

4.1.2 Functional levels of forensic intelligence

The research team identified four functional levels at which forensic intelligence operates. These levels are cumulative: higher levels presuppose the conditions established at lower levels, but each level also has independent value.

Level	Orientation	Description
1. Tactical	*Reactive*	Opening and supporting activity within a single case file; basic evidential linking (e.g., DNA matching, ballistic comparison). Most current Belgian practice operates at this level.

2.	**Intra- file potential**	*Reactive+*	Maximizing the investigative potential of forensic data within a bounded dossier; profiling to identify further leads within a single case.
3.	**Phenomenological**	*Proactive*	Cross-case analysis of criminal phenomena; identification of series, patterns, and networks across multiple dossiers (e.g., linked shootings, drug supply routes, serial burglaries).
4.	**Strategic - Systematic**	*Anticipatory*	Longitudinal exploitation of forensic data to support criminal policy, resource allocation, and long-term law enforcement strategy.

4.1.3 The central misunderstanding: a structural diagnosis

A key finding of the qualitative research is that the development of forensic intelligence in Belgium is blocked not primarily by a lack of will or capability, but by a fundamental structural misunderstanding between the actors whose collaboration is indispensable. This misunderstanding operates at several levels simultaneously. Institutional actors acknowledge the value of forensic intelligence in the abstract while consistently declining to assume the practical, legal and organizational responsibilities it entails.

The misunderstanding manifests in at least three forms. First, there is a definitional misunderstanding: actors use the term 'forensic intelligence' to mean very different things, ranging from enhanced case support (Level 1–2) to genuine phenomenon analysis (Level 3–4). Second, there is a mandates misunderstanding: institutions are assigned forensic intelligence functions without the resources, legal frameworks, or strategic direction to carry them out. Third, there is an expectation misunderstanding: when a new post or unit is created in response to an emerging phenomenon (as with the NICC Drug Expertise Centre), the expectations placed on it are frequently far broader than any realistic resourcing allows, creating conditions for burn-out and institutional disillusionment.

4.1.4 Key conceptual challenges

Four key conceptual challenges can be detected in the research results:

1. *Linkage blindness:* The systematic failure to recognize connections between cases due to institutional, organizational, or cognitive barriers. Forensic intelligence is specifically designed to address this failure; it is also undermined by it.
2. *Temporality and utility:* The operational value of forensic intelligence is highly time-sensitive. Analytical products that arrive after the investigative window has closed have limited tactical utility, even if they retain strategic or academic value.
3. *Top-down versus bottom-up dynamics*: The research consistently identifies risks associated with exclusively top-down implementation of forensic intelligence frameworks. Practitioners must be involved in defining analytical priorities and output formats. A bottom-up or iterative co-design model is more likely to produce sustainable and actionable results.
4. *Scientific legitimacy and institutional positioning*: Forensic intelligence products must meet standards of scientific rigor equivalent to those applied to other forensic outputs. If a central institution such as the NICC is perceived as the sole author of forensic intelligence recommendations, other actors (police laboratories, university partners) may resist, not because the recommendations are wrong, but because the institutional framing is contested. International and peer-reviewed literature should be used to anchor findings in broader scientific consensus rather than institutional authority alone.

4.2 Global recommendations: systematic and normative conditions

The following recommendations address the structural prerequisites for forensic intelligence development in Belgium. They are applicable at the level of the national policy and legislative framework, irrespective of which institution initiates specific projects.

R1

Establish a shared, legally grounded definition of forensic intelligence

A common operational definition of forensic intelligence must be developed and formally adopted by the relevant Belgian authorities. This definition should clearly distinguish between case-level forensic support (Levels 1–2) and proactive, cross-case forensic intelligence (Levels 3–4). The definition should be embedded in legal texts, institutional protocols, and training curricula to prevent definitional drift and mandate misalignment.

R2

Develop an adequate legal basis for cross-case forensic data exploitation

The current Belgian legislative framework does not provide a clear and specific legal basis for the collection, retention, cross-referencing, and analysis of forensic data for intelligence purposes, as distinct from their use in individual criminal proceedings. This legislative gap must be addressed. A dedicated legal instrument, or an explicit amendment to existing legislation (DNA Act, Police Function Act, Code of Criminal Procedure), is required, in full conformity with the GDPR, the EU Law Enforcement Directive, and constitutional protections. The current dogmatic and overly restrictive interpretation of GDPR by institutional actors, which fragments data that could lawfully be combined, must be addressed through legal guidance and, where necessary, legislative clarification.

R3

Counter linkage blindness through formalized inter-institutional data sharing

Dedicated mechanisms should be established to enable the sharing of forensic data across institutional boundaries for intelligence purposes. These mechanisms must be built on explicit legal bases, standardized data formats, and agreed access protocols. The Belgian DNA Database and the SDB provide a partial precedent but is insufficient in scope. Extension to ballistic, toxicological, and digital forensic data, and to intelligence-oriented querying rather than purely case-specific matching, is required.

R4

Move from a reactive to a phenomenon-oriented forensic strategy

Belgian forensic institutions should develop the capacity to identify and respond to emerging criminal phenomena, not only in reaction to judicial mandates, but proactively, through systematic monitoring of forensic data trends. The model of reactive response to an already-critical phenomenon (e.g. Antwerp drug violence) is inefficient: it generates high-intensity engagement that is not sustained and does not build durable intelligence capacity. A structured, proactive monitoring function at Level 3–4 should be progressively established.

R5

Define measurable evaluation criteria for all forensic intelligence activities

Any forensic intelligence initiative should specify, in advance, its intended outcomes and the criteria by which these will be evaluated. Outcomes may be tactical (suspect

identification, case linkage), phenomenological (characterization of a criminal series), or strategic (policy revision). The absence of predefined evaluation criteria makes accountability impossible and impedes evidence-based resource allocation. This evaluation criteria must be a combination of qualitative and statistical key performance indicators e.g. number of profiles entered, but also an assessment of the impact on reducing crime.

4.3 Intermediate recommendations: institutional and cultural conditions

The research identified a set of intermediate-level conditions — situated between broad policy commitments and the design of specific projects, which must be addressed for forensic intelligence to take root within Belgian institutions. These conditions are primarily organizational and cultural.

4.3.1 Institutional positioning of the NICC

The NICC occupies a structurally advantageous position in the Belgian forensic ecosystem: it holds multi-domain scientific expertise and a national mandate. The following recommendations concern the NICC's specific role:

R6

Position of the NICC as a forensic intelligence knowledge hub, not a monopoly

The NICC should develop an explicit forensic intelligence mandate that positions it as a knowledge hub, providing methods, standards, training, and analytical support, rather than as the sole operational producer of forensic intelligence. This framing is essential to maintain legitimacy with police laboratories, university partners, and other stakeholders. Where possible, forensic intelligence recommendations should be attributed to internationally validated methodologies and scientific literature, rather than exclusively to NICC institutional authority.

R7

Embed forensic intelligence as a transversal capacity, not a standalone unit

Forensic intelligence should not be created as a separate department but as a transversal analytical function embedded across existing scientific sections. Domain-specific intelligence capabilities (ballistic intelligence, DNA intelligence, drug trend analysis, digital forensic intelligence) should be developed incrementally within existing teams, drawing on established expertise and building analytical capacity progressively.

R8

Start small: identify the section with the best current conditions for a pilot

Rather than attempting a simultaneous, institution-wide transformation, institutions should identify the section or unit where the conditions for forensic intelligence are currently most favorable in terms of data availability, practitioner motivation, judicial demand, and legal clarity, and concentrate initial efforts there. Based on the research, the Drug Expertise Centre at the NICC presents itself as a strong candidate, given the existing judicial mandate (the National Drug Commissioner), the volume and diversity of forensic data, and the demonstrated interest of forensic staff. However, the research also notes that this unit is already overstretched, and that any pilot must be

accompanied by dedicated resources to avoid replicating the 'Pandora's box' dynamic identified below.

4.3.2 Addressing the 'Pandora's box' dynamic

One of the most significant operational risks identified in the research concerns what participants described as the 'Pandora's box' effect: the moment at which an institution commits to forensic intelligence, the volume and diversity of external demands, from prosecutors, police, customs, schools, festivals, health authorities, and international partners, immediately exceeds the institution's capacity to respond. This dynamic is not hypothetical: it was observed in the genesis of the NICC Drug Expertise Centre, where staff were deployed without clear strategic direction or adequate resources.

R9

Define the scope of forensic intelligence activities explicitly and protect staff

Any institution launching a forensic intelligence function must explicitly define: (a) what types of requests fall within scope; (b) what types of requests should be redirected; and (c) what the realistic output capacity is given available resources. These boundaries should be communicated formally to all potential requestors (judicial, police, policy), before the function is activated. Staff in new forensic intelligence roles should receive strategic guidance, dedicated time allocation, and structured peer support to mitigate the risk of professional overload.

R10

Resource forensic intelligence functions adequately before activation

The research documents repeated instances in which forensic intelligence functions were initiated without sufficient human, technical, or legal resources. Launching a forensic intelligence unit or project without the resources to sustain it produces worse outcomes than not launching at all: it generates false expectations, depletes staff, and discredits the forensic intelligence concept. A realistic resource assessment, including staffing, IT infrastructure, legal support, and training, is a prerequisite for any institutional commitment to forensic intelligence.

4.3.3 Overcoming cultural and cultural-institutional barriers

The research identified several persistent cultural barriers that impede the development of forensic intelligence, independent of the legal and resource constraints:

R11

Bridge the cultural gap between forensic scientists, investigators, and the judiciary

Forensic scientists, investigators, and magistrates operate within distinct professional cultures, each with different logics of relevance, different time horizons, and different risk tolerances. Forensic intelligence requires sustained collaboration across these cultures. This cannot be achieved through formal protocols alone: it requires shared training, joint working groups, and critically the progressive development of a shared vocabulary and shared understanding of what forensic intelligence can and cannot provide. Forensic Advisors could play a key role in mediating across these cultural boundaries.

R12

Engage magistrates and police leadership as early adopters, not passive recipients

The research documents a pattern of judicial and police disengagement from forensic intelligence initiatives, even when actors acknowledge their potential value in principle. The Federal Prosecution Service, arguably the primary beneficiary of a national forensic intelligence system, has shown limited institutional engagement with the research project. Police actors, while initially enthusiastic, have retreated to GDPR concerns as a barrier. Engagement strategies must move beyond information provision to active co-design: magistrates and police leadership should be involved in defining the analytical questions that forensic intelligence is expected to answer, not merely informed of its outputs after the fact.

R13

Address GDPR as a governance challenge, not a definitive barrier

The GDPR is frequently invoked by Belgian institutional actors as a reason to avoid cross-case forensic data exploitation. While data protection obligations are real and must be scrupulously observed, the research finds that the current interpretation of GDPR in the Belgian forensic context is frequently more restrictive than the law requires. A targeted legal analysis, clarifying what is lawful under GDPR and the Law Enforcement Directive in the specific context of forensic intelligence, should be commissioned and disseminated to relevant institutional actors. The deliberate fragmentation of data to ensure GDPR compliance is, in many cases, neither legally required nor scientifically justified.

4.3.4 Mapping and network development

Forensic intelligence is structurally a collective, network-dependent activity. No single institution holds all the forensic data, contextualizing knowledge, or analytical capacity required to produce comprehensive forensic intelligence. The following recommendations address this systemic dependency:

R14

Conduct a systematic actor mapping before initiating any specific project

Prior to launching a forensic intelligence project, a structured mapping of all relevant actors for this specific project should be conducted to establish: who holds the raw forensic data; who holds contextualizing data (police operational intelligence, criminal network information, epidemiological data); who has the analytical capacity to interpret combined datasets; and who is the legitimate recipient of outputs. This mapping should identify both existing actors and actors that may need to be newly engaged or whose roles may need to be formally defined.

R15

Anticipate and prepare for non-habitual partnerships

Some forensic phenomena will require collaboration with actors outside the established forensic-judicial ecosystem. The research illustrates this with the example of firearms: a forensic laboratory detecting a new type of weapon or ammunition cannot independently interpret the strategic significance of this finding without engaging police intelligence units, Europol arms-trafficking analysts, customs authorities, or criminological researchers. Institutional readiness to engage such non-habitual partners, including private-sector actors in digital forensic intelligence contexts, should be built into project governance from the outset.

4.4 Implementation canvas for specific forensic intelligence projects

This section presents a structured project-design canvas: a systematic set of questions that any institution wishing to initiate a specific forensic intelligence project should work through before committing resources. The canvas does not prescribe answers, it identifies the questions that must be explicitly addressed if a project is to be coherently designed, legally compliant, and operationally sustainable.

The canvas reflects a core methodological commitment of the research team: rather than issuing specific operational prescriptions, which would require detailed contextual knowledge that varies by institution, by criminal phenomenon, and by legal environment, the project's primary contribution is to provide a structured thinking tool that enables institutions to develop their own well-designed projects. The canvas is also intended as a diagnostic instrument: it can be applied to existing initiatives to identify gaps in their design.

Canvas Dimension	Key questions to be answered
1. WHAT?	
Subject – phenomenon	What is the phenomenon? What are its geographic, temporal, and typological boundaries? How does it relate to existing case data and institutional priorities?
Measurable objectives	What specific, measurable outcomes does the project aim to produce? Are these tactical, operational or strategic? How will success be defined, measured and communicated?
2. WHO?	
Central and peripheral actors	Who are the central actors implicated in the phenomenon? Who are the peripheral actors whose data or knowledge is relevant? Which institutions, public and private, hold actionable forensic data? Who can collect the data and integrate them?
Institutional host and governance	Governance responsibility for design, execution, quality assurance, and output dissemination? How will the project be formally authorized?
Mandate and commissioning	Is the project initiated proactively (internal initiative) or in response to an external mandate (judicial, police, policy)? What constraints does the mandate impose on scope, methods, and outputs? Is the mandating authority also the primary recipient?
Recipient network	Who are the intended recipients of the forensic intelligence outputs? What is the appropriate format and security classification for each recipient category? How will output be communicated and actioned?
3. STRUCTURE	
Legal and regulatory basis	Is there a clear legal basis for collecting, retaining, and cross-referencing the relevant data? Are data protection obligations (GDPR, Law Enforcement Directive) fully addressed? Is a Data Protection Impact Assessment (DPIA) required?

Resources	What are the resources available?
4. WHEN?	
Reference period	What is the temporal scope of the analysis? Is this a retrospective study, a current snapshot, or a prospective monitoring protocol? What are the implications for data availability and analytical validity?
Sustainability and mutation	What happens when the criminal phenomenon evolves or disappears? How will the project be adapted? Is there a mechanism for reviewing and updating the analytical framework as the phenomenon changes?
Intensity	What intensity reflects the temporal nature of the analysis? The combability between the analysis and real time.
5. HOW?	
Data requirements	What specific data sources are required, and where are they held? What are the applicable data quality standards? Are there known gaps, biases, or access restrictions in the available data?
Tools and Infrastructure	What analytical tools and IT infrastructure are required? Are these existing or to be developed? What are the data security, access control, and logging requirements?
Process	What are the different steps and methodology to use? Determining where to place the tool: is an existing database available?
Skills	What skills are required for analysis (data metrics)?
Feedback	Who will feedback be provided to different actors involved?
6. EVALUATION	How will the project be evaluated? What are the indicators of impact at tactical, operational, and strategic levels? Who is responsible for evaluation and on what timeline?

4.5 Governance and quality standards

4.5.1 The federated model

The research recommends a federated governance model for forensic intelligence in Belgium, in which one institution plays a coordinating, standard-setting, and capacity-building role, while operational forensic intelligence activities are distributed across institutions according to their domain expertise and mandate. This model avoids both the fragmentation of a fully decentralized approach and the institutional capture risks of a fully centralized one.

In a federated model, the coordinating institution's role would include developing and maintaining methodological standards for forensic intelligence; providing training and analytical support to partner institutions; facilitating data-sharing agreements; hosting cross-institutional coordination meetings; and producing strategic forensic intelligence assessments on criminal phenomena of national significance.

4.5.2 Scientific rigor and quality assurance

Forensic intelligence products must meet standards of scientific rigor equivalent to those applied to other forensic outputs. This entails traceability of data sources and analytical methods; transparent documentation of uncertainty and confidence levels; peer review of analytical conclusions before dissemination; and clear separation between empirical findings and interpretive recommendations. The risk of confirmation bias, in which analysts selectively attend to data that confirms existing investigative hypotheses, is particularly acute in intelligence contexts and must be addressed through structured analytical techniques.

4.5.3 Ethical and human rights dimensions

The systematic exploitation of forensic data for intelligence purposes raises significant ethical and human rights concerns, which the research does not dismiss but contextualizes. Key concerns include: the risk of discriminatory profiling based on biometric or behavioral data; the erosion of the presumption of innocence through probabilistic association rather than individualized evidence; and the potential for forensic intelligence to extend surveillance beyond legally authorized boundaries.

These concerns do not argue against forensic intelligence per se, but they do require robust governance: independent oversight mechanisms; transparent communication to judicial and legislative authorities about the methods and scope of forensic intelligence functions; and engagement with civil society organizations and academics in the design of governance frameworks.

4.6 Priority research and development agenda

The Be-ForIntel project has identified a number of areas where further empirical research, legal analysis, and institutional development are required before the recommendations in this document can be fully operationalized.

R16 **Commission a targeted legal analysis of the Belgian forensic intelligence framework**

A comprehensive legal analysis is required to map the existing Belgian legislative framework as it applies to forensic intelligence, with specific attention to: the DNA Act; the Police Function Act; the Code of Criminal Procedure; the National Security Council framework; and relevant European instruments (GDPR, Law Enforcement Directive, European Firearms Directive, Prüm Convention). The analysis should identify specific legislative gaps, propose concrete amendments or new instruments where required, and provide clear guidance to practitioners on what is currently lawful.

R17 **Develop and test domain-specific forensic intelligence pilot protocols**

Building on the canvas developed in Section 5, pilot forensic intelligence protocols should be developed and tested in domain-specific contexts (recommended: the Drug Expertise Centre and the Forensic Advisory at the NICC). Each pilot should include: a formal project design using the canvas; a legal compliance review; a structured evaluation framework; and a debriefing process to extract transferable lessons.

R18 **Conduct a systematic comparative analysis of forensic intelligence governance models**

A systematic comparison of forensic intelligence models in comparable jurisdictions, with particular attention to the Netherlands, the United Kingdom, Australia and Switzerland, should be conducted to provide an evidence base for Belgian institutional design choices.

R19

Develop a forensic intelligence training curriculum for Belgian practitioners

A needs assessment for forensic intelligence training should be conducted across the relevant practitioner groups: forensic scientists, Forensic Advisors, criminal investigators, and prosecutorial actors. Based on this assessment, a structured training curriculum should be developed, drawing on existing international programs (Interpol FIND, Europol forensic intelligence modules, academic programs in forensic science and intelligence studies) and adapted to the Belgian institutional and legal context.

R20

Engage the National Drug Commissioner and comparable commissioners in strategic dialogue

The recent appointment of a National Drug Commissioner in Belgium, whose budget funds the NICC Drug Expertise Centre, represents a significant opportunity to align forensic intelligence development with a well-resourced and politically supported institutional mandate. A structured engagement process between the research team, the NICC, and the Commissioner's office should be initiated to ensure that the Commissioner's strategic vision for drug intelligence is informed by the forensic intelligence framework developed in this project, and that the Drug Expertise Centre's activities are guided by a coherent and achievable strategic plan.

4.7 Scientific Research on Justice and Policing

The difficulties encountered in conducting the Be-ForIntel research serve as significant warning signs that Belgium is no longer a conducive environment for scientific research when it comes to using judicial or police data. The considerable obstacles to accessing federal police data, in the name of compliance with the GDPR, show that the problems already identified 10 years ago during the Be-Gen project have worsened. The dogmatic approach to the GDPR within the federal police demonstrates the existence of a climate of mistrust toward scientific research, even when the research results could benefit this institution, and even when specialized members of the federal police wish to support the research. This lack of transparency, conversely, risks fostering mistrust toward the police and thus constitutes a critical democratic issue.

R21

Establishment of a legal framework and practical procedures to ensure access to the judicial and police data necessary for scientific research

There is an urgent need to establish a dialogue between law enforcement and judicial authorities, on the one hand, and scientific research institutions, on the other, to create both the legal conditions and the practical arrangements necessary to conduct scientific research on police and judicial practices.

Creating these legal, structural, and practical conditions for access to judicial and police practices for scientific research requires the proactive involvement of judicial authorities, police authorities, and scientific institutions, as well as political will (on the part of the Minister of Justice and the Minister of the Interior) to bring this dialogue to fruition through the adoption of legal and concrete measures that define specific points of contact for the entire scientific community within these judicial and police institutions.

4.8 Conclusion

The Be-ForIntel research project has produced a detailed and evidence-based account of the conditions for, and obstacles to, forensic intelligence development in Belgium. Its central finding is simultaneously sobering and constructive: the obstacles are real, substantial, and structurally entrenched, but they are not insurmountable. The scientific expertise, forensic infrastructure, institutional goodwill, and judicial demand for forensic intelligence exist in Belgium. What is currently lacking is the coherent framework, definitional, legal, organizational, and evaluative within which these assets can be systematically and sustainably deployed.

The recommendations in this document are not a blueprint for a finished system. They are a structured set of starting points, grounded in empirical research, comparative analysis, and direct engagement with Belgian practitioners, from which institutions can develop their own forensic intelligence initiatives in a legally compliant, scientifically rigorous, and organizationally realistic manner. The implementation canvas in Section 5 is the core practical tool: it does not tell institutions what to do, but it ensures that they have asked all the right questions before they act.

The research team emphasizes one final point. The misunderstanding identified as the central structural problem of forensic intelligence in Belgium, the gap between scientific ambition, institutional mandate, legal framework, and operational reality, cannot be resolved by scientific recommendations alone. It requires political will, sustained institutional leadership, and a commitment to long-term investment in forensic intelligence capacity. The Be-ForIntel project provides the scientific and methodological foundation for that investment. The decision to make it remains with the institutional and political actors whose cooperation the research has, throughout, sought in vain to secure, and who, it is hoped, will find in this document the structured arguments required to make that decision with confidence.

5. DISSEMINATION AND VALORISATION

PRESENTATIONS

Ballèvre, N., Renard, B., & Ribaux, O. (2024, Septembre). *Forensic intelligence and its uses, perceptions and representations by forensic practionners* [Presentation]. 24th Annual Conference of the European Society of Criminology 2024.

Ballèvre, N., Ribaux, O. & Renard, B. (2025, May). *Forensic intelligence and its uses, perceptions, and representations by forensic practitioners* [Presentation]. EAFS.

Harvey, D. (2023). *Building the foundations of a forensic intelligence tool in Belgium* [Poster]. Research Day Law and Criminology 2023, Ghent, Belgium.

Harvey, D., Madjlessi, J., Kumar, K., & Vandeviver, C. (2024). *Criminal network disruption: A scoping review* [Poster]. Research Day Law and Criminology 2024, Ghent, Belgium.

Harvey, D. (2025). *Police view vs. forensic view: The network you think exists vs. the network that actually exists* [Poster]. Research Day Law and Criminology 2025, Ghent, Belgium.

Harvey, D., Vandeviver, C., Stappers, C., Mauquoy, M., & Renard, B. (2025, Septembre). *Leveraging forensic intelligence to disrupt criminal networks: A simulation study* [Poster]. 25th Annual Conference of the European Society of Criminology.

Mauquoy, M., Stappers, C., & Renard, B. (2025). *Be-ForIntel: Building the foundations of a Forensic Intelligence tool in Belgium: The organisation of forensic data in Belgium*. ESC.

Renard, B., & Ribaux, O. (2024, May 21). *Be-ForIntel: Construire les bases d'un outil de renseignement forensique en Belgique* [Presentation]. AICLF 2024.

Renard, B., Stappers, C., Mauquoy, M., Harvey, D., Kumar, K., Vandeviver, C., Vander Beken, T., Gason, F. & Ribaux, O. (2024, May). Be-ForIntel: Building the foundations of a Forensic Intelligence tool in Belgium [Poster]. AICLF 2024.

Renard, B., Stappers, C., Mauquoy, M. (2026, May), Construire les fondements d'une démarche de renseignement forensique en Belgique – Une question de définition (The Be-ForIntel Project) [Presentation]. AICLF 2026.

Stappers, C., Harvey, D., Kumar, K., Vandeviver, C., Vander Beken, T., Gason, F., Ribaux, O., & Renard, B. (2023, september). *Be-ForIntel: Building the foundations of a Forensic Intelligence tool in Belgium* [Poster]. 23rd Annual Conference of the ESC.

Stappers, C., Harvey, D., Kumar, K., Vandeviver, C., Vander Beken, T., Gason, F., Ribaux, O., & Renard, B. (2025, May). *Be-ForIntel: Building the foundations of a Forensic Intelligence tool in Belgium* [Poster]. EAFS.

Stappers, C., Mauquoy, M., & Renard, B. (2025). *Be-ForIntel: Building the foundations of a Forensic Intelligence tool in Belgium the organisation of forensic data in Belgium* [Presentation]. EAFS.

Stappers, Caroline, & Renard, B. (2023, June). *Be-ForIntel: Building the foundation of a forensic intelligence tool in Belgium*. Network Intelligence Manager Federal Police.

Vandeviver, C. (2023). The future of big data policing for law enforcement agencies [Lecture].

PUBLICATIONS

Ballèvre, N., Renard, B., & Ribaux, O. (Under Review). Representations and perception of forensic intelligence among Belgian forensic practitioners**.** Forensic science international.

Harvey, D., Madjellessi, J., Kumar, K., & Vandeviver, C. (2024). Disrupting criminal networks: A scoping review [Preprint]. CrimRxiv. https://www.crimrxiv.com/pub/cofzjnzx/release/1

Harvey, D., Geeraert, J., & Vandeviver, C. (2026). Observability and disruption in criminal networks: A simulation study of forensic intelligence [Preprint].

Harvey, D., Madjlessi, J., Kumar, K., & Vandeviver, C. (2026). Enhancing criminal network disruption through forensic intelligence: A scoping review [Preprint].

Harvey, D., Vander Beken, T., Kumar, K., & Vandeviver, C. (2026). Feasibility of forensic intelligence in Belgium: A mixed-methods assessment of legal, organizational, and technical constraints [Preprint].

Harvey, D., & Vandeviver, C. (2026). Examining observability in forensic-enhanced criminal networks: Evidence from empirical network reconstruction [Preprint].

Harvey, D., & Vandeviver, C. (2026). The added value of forensic intelligence in criminal network analysis: Evidence from empirical network reconstruction [Preprint].

Klymentiev, R., Harvey, D., Rocha, L. E. C., & Vandeviver, C. (2025). A systematic review and Bayesian meta-analysis of co-offending characteristics. Nature Human Behaviour, 9(10), 2135–2152. https://doi.org/10.1038/s41562-025-02244-z

POLICY BRIEFS

Harvey, D., Geeraert, J., & Vandeviver, C. (2026). How forensic intelligence transforms criminal network disruption: A policy brief [Policy brief].

Harvey, D., Vanderbeken, T., Kumar, K., & Vandeviver, C. (2026). The feasibility of a forensic intelligence tool in Belgium: A policy brief [Policy brief].

Harvey, D., & Vandeviver, C. (2026). Comparing police, DNA, and combined case networks: Understanding the added value of forensic intelligence: A policy brief [Policy brief].

Harvey, D., & Vandeviver, C. (2026). How forensic DNA transforms criminal networks: A policy brief [Policy brief].

6. ACKNOWLEDGEMENTS

The Be-ForIntel research team would like to thank Emmanuèle Bourgeois and Aziz Naji from BELSPO for managing and providing follow up to the project.

The research team would like to thank the Follow-up Committee for their valuable input during the different stages of this project.

The research team is thankful to all organizations that helped by granting access to the necessary data (DNA data, police records and criminal records). Special thanks are extended to the DIS service of the NICC, the College of Prosecutors General, the Local Police of Bruges, the Federal Police DJSOC and the Technical and Scientific Police (DJT).

The research team would also like to thank all the participants in the interviews.

Special thanks to Samuel Waltener from NICC for his assistance in preparing the data, and Stefan Lambrechts from DJT for going above and beyond in his efforts (which ultimately were unsuccessful) to obtain the data from the federal police.

BIBLIOGRAPHY

Agius, A., Jones, K., Epple, R., Morelato, M., Moret, S., Chadwick, S., & Roux, C. (2017). The use of handwriting examinations beyond the traditional court purpose. Science & Justice, 57(5), 394–400. https://doi.org/10.1016/j.scijus.2017.05.001

Agius, A., Morelato, M., Moret, S., Chadwick, S., Jones, K., Epple, R., Brown, J., & Roux, C. (2018). Using handwriting to infer a writer's country of origin for forensic intelligence purposes. Forensic Science International, 282, 144–156. https://doi.org/10.1016/j.forsciint.2017.11.028

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 [Doctoral dissertation, Université de Lausanne]. https://serval.unil.ch/resource/serval:BIB_149C1AFE9092.P001/REF.pdf

Baechler, S. (2024, April). ProFID — Forensic profiling of fraudulent identity and travel documents.

Baechler, S., Boivin, R., & Margot, P. (2015). Analyse systématique des faux documents d'identité à des fins de renseignement criminel: Vers la construction de connaissances sur la criminalité par l'étude de la trace matérielle. Revue Internationale de Criminologie et de Police Technique et Scientifique, 68(3), 315–337

Baechler, S., & Caneppele, S. (2017). Forensic intelligence. In The Routledge international handbook of forensic intelligence and criminology (pp. 212–224). Routledge. https://doi.org/10.4324/9781315541945-18

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. https://doi.org/10.1057/sj.2015.26

Baechler, S., Morelato, M., Gittelson, S., Walsh, S., Margot, P., Roux, C., & Ribaux, O. (2020). Breaking the barriers between intelligence, investigation and evaluation: A continuous approach to define the contribution and scope of forensic science. Forensic Science International, 309, 110213. https://doi.org/10.1016/j.forsciint.2020.110213

Baechler, S., Morelato, M., Ribaux, O., Beavis, A., Tahtouh, M., Kirkbride, K. P., Esseiva, P., Margot, P., & Roux, C. (2015). 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. Forensic Science International, 250, 44–52. https://doi.org/10.1016/j.forsciint.2015.02.021

Baechler, S., Ribaux, O., & Margot, P. (2012). Toward a novel forensic intelligence model: Systematic profiling of false identity documents. Forensic Science Policy & Management: An International Journal, 3(2), 70–84. https://doi.org/10.1080/19409044.2012.744120

Baechler, S., Terrasse, V., Pujol, J.-P., Fritz, T., Ribaux, O., & Margot, P. (2013). The systematic profiling of false identity documents: Method validation and performance evaluation using seizures known to originate from common and different sources. Forensic Science International, 232(1–3), 180–190. https://doi.org/10.1016/j.forsciint.2013.07.022

Bollé, T., & Casey, E. (2018). Using computed similarity of distinctive digital traces to evaluate non-obvious links and repetitions in cyber-investigations. Digital Investigation, 24, S2–S9. https://doi.org/10.1016/j.diin.2018.01.002

Braga, A. A. (2008). Gun enforcement and ballistic imaging technology in Boston. In D. L. Cork, J. E. Rolph, E. S. Meieran, & C. V. Petrie (Eds.), Ballistic imaging: Appendix A. National Academies Press.

Bright, D., Greenhill, C., & Levenkova, N. (2014). Crime and networks. In Crime and networks (pp. 148–162). Routledge. https://doi.org/10.4324/9781315885018-11

Broséus, J., Baechler, S., Gentile, N., & Esseiva, P. (2016). Chemical profiling: A tool to decipher the structure and organisation of illicit drug markets: An 8-year study in Western Switzerland. Forensic Science International, 266, 18–28. https://doi.org/10.1016/j.forsciint.2016.04.008

Broséus, J., Huhtala, S., & Esseiva, P. (2015). First systematic chemical profiling of cocaine police seizures in Finland in the framework of an intelligence-led approach. Forensic Science International, 251, 87–94. https://doi.org/10.1016/j.forsciint.2015.03.026

Bruenisholz, E., Delémont, O., & Ribaux, O. (2015). Repetitive deliberate fires: Critical review of the situation and proposal of a follow-up process and systematic analysis. Forensic Science Policy & Management: An International Journal, 6(3–4), 79–90. https://doi.org/10.1080/19409044.2015.1069424

Bruenisholz, E., Delémont, O., Ribaux, O., & Wilson-Wilde, L. (2017). Repetitive deliberate fires: Development and validation of a methodology to detect series. Forensic Science International, 277, 148–160. https://doi.org/10.1016/j.forsciint.2017.06.009

Bruenisholz, E., Prakash, S., Ross, A., Morelato, M., O'Malley, T., Raymond, M. A., Ribaux, O., Roux, C. P., & Walsh, S. (2016). The intelligent use of forensic data: An introduction to the principles. Forensic Science Policy & Management: An International Journal, 7(1–2), 21–29. https://doi.org/10.1080/19409044.2015.1084405

Bruenisholz, E., Wilson-Wilde, L., Ribaux, O., & Delémont, O. (2019). Deliberate fires: From data to intelligence. Forensic Science International, 301, 240–253. https://doi.org/10.1016/j.forsciint.2019.05.046

CGIC. (2017). 5 things to know about Crime Gun Intelligence Centers. Gun Crime Intelligence Centers. https://crimegunintelcenters.org/wp-content/uploads/2017/12/5-THINGS-to-Know-About-Crime-Gun-Intelligence-Centers.pdf

CGIC. (2022). How GunStat can complement Crime Gun Intelligence Center (CGIC) operations. Crime Gun Intelligence Centers. https://crimegunintelcenters.org/wp-content/uploads/2022/03/How-GunStat-Can-Complement-a-CGIC.pdf

Collins, M. (2017). Illicit drug profiling: The Australian experience — Revisited. Australian Journal of Forensic Sciences, 49(6), 591–604. https://doi.org/10.1080/00450618.2017.1348009

Collins, M., Huttunen, J., Evans, I., & Robertson, J. (2007). Illicit drug profiling: The Australian experience. Australian Journal of Forensic Sciences, 39(1), 25–32. https://doi.org/10.1080/00450610701324924

Crispino, F., Rossy, Q., Ribaux, O., & Roux, C. (2015). Education and training in forensic intelligence: A new challenge. Australian Journal of Forensic Sciences, 47(1), 49–60. https://doi.org/10.1080/00450618.2014.906655

De Alcaraz-Fossoul, J., & Roberts, K. A. (2017). Forensic intelligence applied to questioned document analysis: A model and its application against organized crime. Science & Justice, 57(4), 314–320. https://doi.org/10.1016/j.scijus.2017.04.003

De Moor, S. (2018). Forensic DNA databases as data sources for criminological research [Doctoral dissertation, Ghent University].

De Moor, S., Vandeviver, C., & Vander Beken, T. (2018). Integrating police-recorded crime data and DNA data to study serial co-offending behaviour. European Journal of Criminology, 15(5), 632–651. https://doi.org/10.1177/1477370817749499

De Moor, S., Vandeviver, C., & Vander Beken, T. (2020). Assessing the missing data problem in criminal network analysis using forensic DNA data. Social Networks, 61, 99–106. https://doi.org/10.1016/j.socnet.2019.09.003

Dégardin, K., Roggo, Y., & Margot, P. (2015). Forensic intelligence for medicine anti-counterfeiting. Forensic Science International, 248, 15–32. https://doi.org/10.1016/j.forsciint.2014.11.015

Delémont, O., Bitzer, S., Jendly, M., & Ribaux, O. (2018). The practice of crime scene examination in an intelligence-based perspective. In The Routledge international handbook of forensic intelligence and criminology (pp. 86–101). Routledge.

Delgado, Y., Price, B. S., Speaker, P. J., & Stoiloff, S. L. (2021). Forensic intelligence: Data analytics as the bridge between forensic science and investigation. Forensic Science International: Synergy, 3, 100162. https://doi.org/10.1016/j.fsisyn.2021.100162

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., & Morelato, M. (2023). The potential of using the forensic profiles of Australian fraudulent identity documents to assist intelligence-led policing. Australian Journal of Forensic Sciences, 55(6), 720–730. https://doi.org/10.1080/00450618.2022.2074138

Devlin, C., Morelato, M., & Baechler, S. (2024). Forensic intelligence: Expanding the potential of forensic document examination. WIREs Forensic Science, 6(5), e1528. https://doi.org/10.1002/wfs2.1528

Egger, S. A., & Doney, R. H. (1990). Serial murder: An elusive phenomenon. Praeger.

Esseiva, P., Ioset, S., Anglada, F., Gasté, L., Ribaux, O., Margot, P., Gallusser, A., Biedermann, A., Specht, Y., & Ottinger, E. (2007). Forensic drug intelligence: An important tool in law enforcement. Forensic Science International, 167(2–3), 247–254. https://doi.org/10.1016/j.forsciint.2006.06.032

Flippin, M. R., Katz, C. M., & King, W. R. (2022). Examining the impact of a crime gun intelligence center. Journal of Forensic Sciences, 67(2), 543–549. https://doi.org/10.1111/1556-4029.14952

Gagliardi, P. (2012). Transnational organized crime and gun violence: A case for firearm forensic intelligence sharing. International Review of Law, Computers & Technology, 26(1), 83–95. https://doi.org/10.1080/13600869.2012.646801

Garvey, T., LaBerge, G., & Wartell, J. (2023). Forensic intelligence models: Assessment of current practices in the United States and internationally. National Institute of Justice. https://www.ojp.gov/pdffiles1/nij/305898.pdf

Goswami, S., Murthy, C. A., & Das, A. K. (2018). Sparsity measure of a network graph: Gini index. Information Sciences, 462, 16–39. https://doi.org/10.1016/j.ins.2018.05.044

Grossrieder, L. (2017). Intégration des méthodes computationnelles en renseignement criminel — Application sur la détection de problèmes à travers les tendances dans les activités criminelles [Doctoral dissertation, Université de Lausanne]. https://www.unil.ch/files/live/sites/esc/files/Fichiers%202017/The%CC%80se_Grossrieder.pdf

Hachem, M., Mizouni, R., Alawadhi, I. M., & Altamimi, M. J. (2023). Digital forensic intelligence for illicit drug analysis in forensic investigations. iScience, 26(10), 108023. https://doi.org/10.1016/j.isci.2023.108023

Hochholdinger, S., Arnoux, M., Delémont, O., & Esseiva, P. (2019). Forensic intelligence on illicit markets: The example of watch counterfeiting. Forensic Science International, 302, 109868. https://doi.org/10.1016/j.forsciint.2019.06.026

Houck, M. M. (2020). Front-end forensics: An integrated forensic intelligence model. In B. Fox, J. A. Reid, & A. J. Masys (Eds.), Science informed policing (pp. 161–180). Springer. https://doi.org/10.1007/978-3-030-41287-6_8

Ioset, S., Esseiva, P., Ribaux, O., Weyermann, C., Anglada, F., Lociciro, S., Hayoz, P., Baer, I., Gasté, L., Terrettaz-Zufferey, A.-L., Delaporte, C., & Margot, P. (2007). Establishment of an operational system for drug profiling: A Swiss experience. Bulletin on Narcotics, 57(1–2), 121–147.

Jiang, J., Zhuang, A. C., Holme, P., Mucha, P. J., & Schwarze, A. C. (2025). Robustness of “small” networks. arXiv. https://doi.org/10.48550/arxiv.2509.23670

Kelty, S. F., Julian, R., & Ross, A. (2013). Dismantling the justice silos: Avoiding the pitfalls and reaping the benefits of information-sharing between forensic science, medicine and law. Forensic Science International, 230(1–3), 8–15. https://doi.org/10.1016/j.forsciint.2012.10.032

Lammers, M. (2014). Are arrested and non-arrested serial offenders different? A test of spatial offending patterns using DNA found at crime scenes. Journal of Research in Crime and Delinquency, 51(2), 143–167. https://doi.org/10.1177/0022427813504097

Lavergne, L., Boivin, R., Baechler, S., Jeuniaux, P., Fiola, K., Séguin, D., Lefebvre, J.-F., & Milot, E. (2022). Determining the impact of unknown individuals in criminality using network analysis of DNA

matches. Forensic Science International, 331, 111142. https://doi.org/10.1016/j.forsciint.2021.111142

Lavergne, L., Boivin, R., Baechler, S., Séguin, D., Lefebvre, J.-F., Fiola, K., & Milot, E. (2024). DNA databanks as a source of information about the criminal behavior of individuals who have been linked to crimes but not identified by police. Canadian Journal of Criminology and Criminal Justice, 66(1), 1–28. https://doi.org/10.3138/cjccj-2022-0049

Legrand, T., & Vogel, L. (2015). The landscape of forensic intelligence research. Australian Journal of Forensic Sciences, 47(1), 16–26. https://doi.org/10.1080/00450618.2014.928830

Lopez, B. E., McGrath, J. G., & Taylor, V. G. (2020). Using forensic intelligence to combat serial and organized violent crimes. National Institute of Justice Journal, 47–58.

Lovell, R., Flannery, D. J., & Luminais, M. (2018). Serial offending and sexual assault kits. In The Cambridge handbook of violent behavior and aggression (pp. 399–417). Cambridge University Press. https://doi.org/10.1017/9781316847992.023

Lovell, R., Luminais, M., Flannery, D. J., Overman, L., Huang, D., Walker, T., & Clark, D. R. (2017). Offending patterns for serial sex offenders identified via the DNA testing of previously unsubmitted sexual assault kits. Journal of Criminal Justice, 52, 68–78. https://doi.org/10.1016/j.jcrimjus.2017.08.002

Malsh, M., Lammers, M., & Van den Berg, T. (2018). De meerwaarde van handpalmafdruken voor de opsporing en vervolging. Expertise en Recht, (1), 4–11.

Marclay, F. (2014). Perspectives for forensic intelligence in anti-doping and the emergence of smokeless tobacco consumption in sport [Doctoral dissertation, Université de Lausanne]. https://iris.unil.ch/handle/iris/136950

Marclay, F., Mangin, P., Margot, P., & Saugy, M. (2013). Perspectives for forensic intelligence in anti-doping: Thinking outside of the box. Forensic Science International, 229(1–3), 133–144. https://doi.org/10.1016/j.forsciint.2013.04.009

Meola, S., & Esseiva, P. (2022). What is the future of illicit drug profiling in Switzerland? Condemned to disappear or forgotten treasure. Drug Testing and Analysis, 14(3), 411–415. https://doi.org/10.1002/dta.3167

Meola, S., Huhtala, S., Broséus, J., Jendly, M., Jalava, K., Aalberg, L., & Esseiva, P. (2021). Illicit drug profiling practices in Finland: An exploratory study about end users' perceptions. Forensic Science International, 324, 110848. https://doi.org/10.1016/j.forsciint.2021.110848

Mireault, C., Dumont, P., & Delémont, O. (2025). From traces to intelligence: Forensic science contributions to counterfeiting understanding through profiling of counterfeit goods. WIREs Forensic Science, 7(1), e70002. https://doi.org/10.1002/wfs2.70002

Morelato, M., Baechler, S., Ribaux, O., Beavis, A., Tahtouh, M., Kirkbride, P., Roux, C., & Margot, P. (2014). Forensic intelligence framework — Part I: Induction of a transversal model by comparing illicit drugs and false identity documents monitoring. Forensic Science International, 236, 181–190. https://doi.org/10.1016/j.forsciint.2013.12.045

Morelato, M., Beavis, A., Tahtouh, M., Ribaux, O., Kirkbride, P., & Roux, C. (2013). The use of forensic case data in intelligence-led policing: The example of drug profiling. Forensic Science International, 226(1–3), 1–9. https://doi.org/10.1016/j.forsciint.2013.01.003

Morelato, M., Cadola, L., Bérubé, M., Ribaux, O., & Baechler, S. (2023). Forensic intelligence teaching and learning in higher education: An international approach. Forensic Science International, 344, 111575. https://doi.org/10.1016/j.forsciint.2023.111575

Morselli, C. (2009). Inside criminal networks. Springer. https://doi.org/10.1007/978-0-387-09526-4

Moulin, S. L., Ertan, E., Martin, D., & Baechler, S. (2024). Cross-border forensic profiling of fraudulent identity and travel documents: A pilot project between France and Switzerland. Science & Justice, 64(2), 202–209. https://doi.org/10.1016/j.scijus.2024.01.003

Moulin, S. L., Weyermann, C., & Baechler, S. (2022). An efficient method to detect series of fraudulent identity documents based on digitised forensic data. Science & Justice, 62(5), 610–620. https://doi.org/10.1016/j.scijus.2022.09.003

Musawi, A. F. A., Roy, S., & Ghosh, P. (2023). Examining indicators of complex network vulnerability across diverse attack scenarios. Scientific Reports, 13(1), 18208. https://doi.org/10.1038/s41598-023-45218-9

Newman, M. E. J. (2006). Finding community structure in networks using the eigenvectors of matrices. Physical Review E, 74(3), 036104. https://doi.org/10.1103/physreve.74.036104

Ngo, H. Q., & Le-Khac, N.-A. (2023). Ontology-based case study management towards bridging training and actual investigation gaps in digital forensics. Forensic Science International: Digital Investigation, 47, 301621. https://doi.org/10.1016/j.fsidi.2023.301621

Popovic, A., Morelato, M., Baechler, S., De Grazia, A., Tahtouh, M., Roux, C., & Beavis, A. (2022). Understanding Australian methylamphetamine drug markets through relational, temporal and spatial analyses. Drug Testing and Analysis, 14(3), 481–495. https://doi.org/10.1002/dta.3181

Porreca, A., Maturo, F., & Ventre, V. (2025). Fuzzy centrality measures in social network analysis: Theory and application in a university department collaboration network. International Journal of Approximate Reasoning, 176, 109319. https://doi.org/10.1016/j.ijar.2024.109319

Quick, D., & Choo, K.-K. R. (2017). Pervasive social networking forensics: Intelligence and evidence from mobile device extracts. Journal of Network and Computer Applications, 86, 24–33. https://doi.org/10.1016/j.jnca.2016.11.018

Quick, D., & Choo, K.-K. R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT + OSINT): A timely and cohesive mix. Future Generation Computer Systems, 78, 558–567. https://doi.org/10.1016/j.future.2016.12.032

Ribaux, O., Baechler, S., & Rossy, Q. (2022). Forensic intelligence and traceology in digitalised environments: The detection and analysis of crime patterns to inform practice. In The handbook of security (3rd ed., pp. 81–100). Palgrave Macmillan.

Ribaux, O., Baylon, A., Roux, C., Delémont, O., Lock, E., Zingg, C., & Margot, P. (2010). Intelligence-led crime scene processing. Part I: Forensic intelligence. Forensic Science International, 195(1–3), 10–16. https://doi.org/10.1016/j.forsciint.2009.10.027

Ribaux, O., Crispino, F., & Roux, C. (2015). Forensic intelligence: Deregulation or return to the roots of forensic science? Australian Journal of Forensic Sciences, 47(1), 61–71. https://doi.org/10.1080/00450618.2014.906656

Ribaux, O., Girod, A., Walsh, S. J., Margot, P., Mizrahi, S., & Clivaz, V. (2003). Forensic intelligence and crime analysis. Law, Probability and Risk, 2(1), 47–60. https://doi.org/10.1093/lpr/2.1.47

Ribaux, O., & Talbot Wright, B. (2014). Expanding forensic science through forensic intelligence. Science & Justice, 54(6), 494–501. https://doi.org/10.1016/j.scijus.2014.05.001

Ribaux, O., Walsh, S. J., & Margot, P. (2006). The contribution of forensic science to crime analysis and investigation: Forensic intelligence. Forensic Science International, 156(2–3), 171–181. https://doi.org/10.1016/j.forsciint.2004.12.028

Ross, A. (2015). Elements of a forensic intelligence model. Australian Journal of Forensic Sciences, 47(1), 8–15. https://doi.org/10.1080/00450618.2014.916753

Rossy, Q., Ioset, S., Dessimoz, D., & Ribaux, O. (2013). Integrating forensic information in a crime intelligence database. Forensic Science International, 230(1–3), 137–146. 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(3), 335–356. https://doi.org/10.1007/s10610-020-09438-3

Roux, C., Bucht, R., Crispino, F., De Forest, P., Lennard, C., Margot, P., Miranda, M. D., NicDaeid, N., Ribaux, O., Ross, A., & Willis, S. (2022). The Sydney declaration — Revisiting the essence of forensic science through its fundamental principles. Forensic Science International, 332, 111182. https://doi.org/10.1016/j.forsciint.2022.111182

Roux, C., Crispino, F., & Ribaux, O. (2012). From forensics to forensic science. Current Issues in Criminal Justice, 24(1), 7–24. https://doi.org/10.1080/10345329.2012.12035941

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks, 13(3), 251–274. https://doi.org/10.1016/0378-8733(91)90008-h

Spaulding, J. S., & Morris, K. B. (2019). Integration of DNA, fingerprint, and firearm databases into forensic intelligence networks for a real-time case assessment model. Journal of Policing, Intelligence and Counter Terrorism, 14(1), 39–61. https://doi.org/10.1080/18335330.2018.1548770

Talbot-Wright, B., Baechler, S., Morelato, M., Ribaux, O., & Roux, C. (2016). Image processing of false identity documents for forensic intelligence. Forensic Science International, 263, 67–73. https://doi.org/10.1016/j.forsciint.2016.03.054

Tapps, M., Piat, O., Matte, A.-A., & Volery, R. (2024). Succeeding together: The power of collaboration between forensic and criminal intelligence. Forensic Sciences Research, 9(4), owae054. https://doi.org/10.1093/fsr/owae054

Taylor, M., Turbett, G. R., Lee, J., & Sears, A. (2024). Forensic intelligence in Australia and New Zealand: Status and future directions. Forensic Science International, 364, 112207. https://doi.org/10.1016/j.forsciint.2024.112207

Thorpe, S., & Bernard, M. (2017). Graph mining for forensic databases. SoutheastCon 2017, 1–10. https://doi.org/10.1109/secon.2017.7925340

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K., Colquhoun, H., Levac, D., Moher, D., Peters, M., Horsley, T., Weeks, L., Hempel, S., Akl, E., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M., Garritty, C., … Tunçalp, Ö. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. Annals of Internal Medicine, 169(7), 467–473. https://doi.org/10.7326/m18-0850

Woodhams, J., & Labuschagne, G. (2012). A test of case linkage principles with solved and unsolved serial rapes. Journal of Police and Criminal Psychology, 27(1), 85–98. https://doi.org/10.1007/s11896-011-9091-1

Yin, H., Benson, A. R., & Leskovec, J. (2019). The local closure coefficient. Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining, 303–311. https://doi.org/10.1145/3289600.3290991