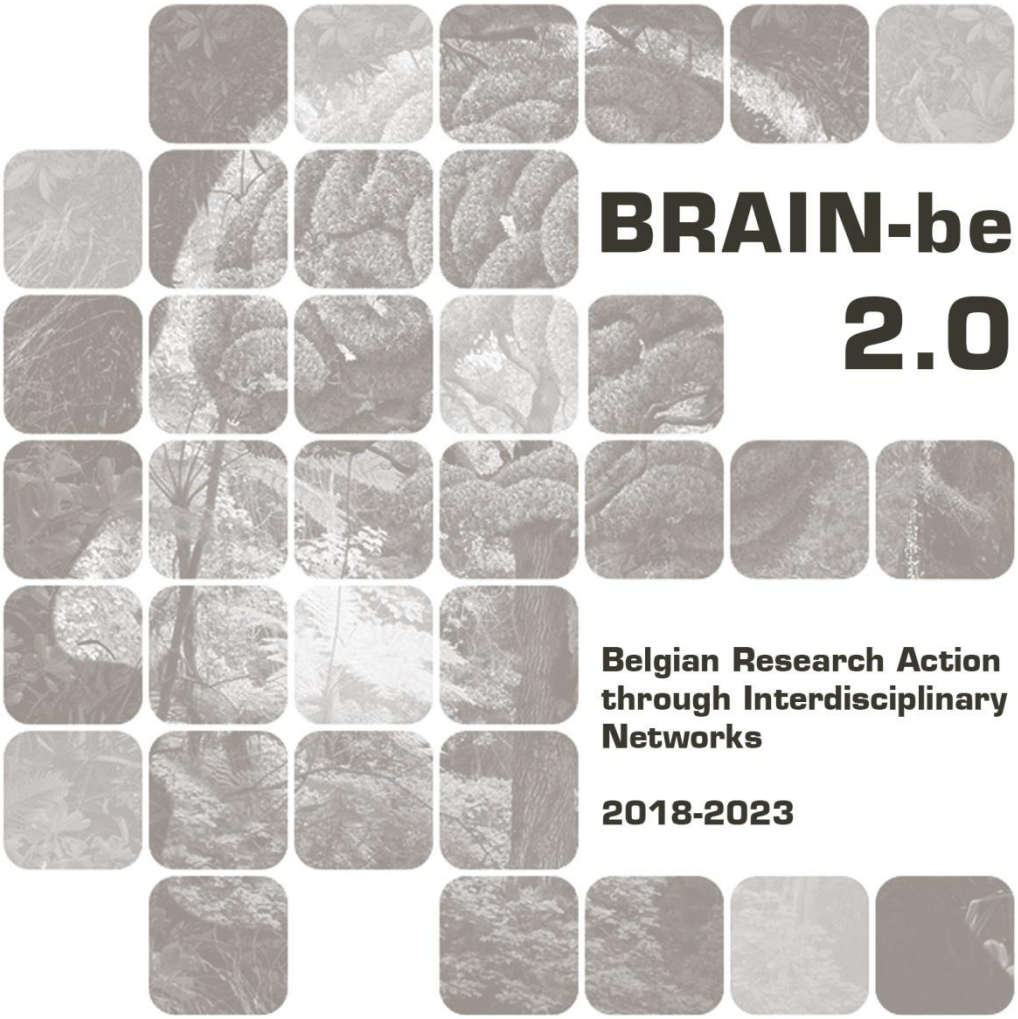


# Be-ForIntel

## 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

**Contract - B2/223/P3/BeForIntel**

## SUMMARY

belspo .be

**Keywords:** *forensic intelligence; crime analysis; case linkage; criminal networks; DNA database; intelligence-led policing; data integration; network analysis; Belgium; NICC; Federal Police; GDPR; forensic data governance; institutional mapping; roadmap*

## Context

Forensic science in Belgium is well established for evidentiary purposes, yet forensic data is exploited almost exclusively on a case-by-case basis in support of judicial proceedings. The potential to use the same data for cross-case linkage, pattern recognition, and intelligence-led policing, collectively referred to as 'forensic intelligence', remains largely unrealized. This gap results from a combination of institutional fragmentation (data stored in incompatible silos across the NICC, the Federal Police, and local police zones), cultural barriers (a justice-oriented, zero-error culture incompatible with the probabilistic reasoning inherent in intelligence work), legal ambiguity (no clear legal basis for cross-case forensic data exploitation under Belgian law), and insufficient resources.

The Be-ForIntel project was initiated against this background. Funded under the BRAIN-be 2.0 program of the Belgian Science Policy Office (BELSPO) and co-funded by the Federal Public Service Justice, it brought together researchers from the NICC, Ghent University, and the University of Lausanne. The project ran from 2021 to 2026 and is the first Belgian research project specifically dedicated to building the foundations of a forensic intelligence system. It faced severe constraints: the Federal Police ultimately refused access to national police data, limiting the empirical scope of WP2 to a local police zone and NICC forensic DNA data. The project team explicitly notes that this refusal, justified on GDPR grounds despite formal authorization from the College of Prosecutors General, constitutes a significant research finding in itself and reflects a broader democratic deficit in the governance of scientific access to police data.

## Objectives

The project pursued three main objectives, each operationalized through a dedicated work package:

- WP1 – Mapping: to clarify the concept of forensic intelligence through international literature reviews; to map all forensic data produced by the NICC and the Federal Police (DJT and DJSOC); and to assess existing forensic intelligence practices and future opportunities in Belgium.
- WP2 – Feasibility and added value: to empirically assess, through data integration and network analysis, whether combining police-recorded crime data with forensic DNA linkage data reveals additional relational information; to simulate disruption analysis; and to identify the legal, technical, and organizational conditions for embedding forensic intelligence in Belgian crime analysis.
- WP3 – Roadmap: to develop actionable guidelines and recommendations for practitioners, policymakers, and judicial authorities, enabling the phased and legally compliant implementation of forensic intelligence in Belgium.

## Methodology

The project employed a mixed-methods, multi-team design. WP1 combined systematic literature reviews (using Scopus, PubMed, Cairn, and NVivo-assisted qualitative analysis) with semi-structured interviews with forensic practitioners at the NICC and Federal Police, and qualitative analysis of internal documentation. WP2 built three relational datasets, police-only, forensic DNA-only, and

combined, from pseudonymized administrative records, then applied network analysis (structural metrics, ego-network analysis, offence-type profiling) and Monte Carlo simulations of network disruption. WP3 integrated qualitative fieldwork (expert interviews, survey of practitioners), a scoping review of the forensic intelligence legal and organizational literature, and co-design workshops to produce a structured roadmap and implementation canvas.

## Results

WP1 findings: The literature review yielded an operational definition of forensic intelligence (Ribaux et al., 2006) and a conceptual framework articulating three functional levels (tactical, operational, strategic) and six key elements (utility, circularity, temporality, multi-data integration, alternative data integration, and collaboration). The international mapping identified four models (Australia: top-down centralized; USA: top-down decentralized; Switzerland/Canada: bottom-up decentralized), with Belgium currently lacking a dedicated governance structure. The Belgian data mapping revealed rich forensic data held by the NICC (DNA, ballistics, drugs, toxicology, fibers, paints, gunshot residues, security inks, IT forensics) and the Federal Police (fingerprints/biometrics via BIS/AFIS, footwear and ear prints via SDB, violent crime linkage via ViCLAS, document forensics via OCRF). Six implicit forensic intelligence practices were identified (DNA database comparisons, ballistic case linkage, European amphetamine profiling, SDB trace comparison, BIS fingerprint matching, ViCLAS crime linkage), all operating at the tactical level and none systematically integrated with each other or with police operational data.

WP2 findings: The integration of police and forensic DNA data into a combined network demonstrated that forensic data adds relational visibility beyond what police data alone provides. Forensic DNA linkages connected cases, including cases with unknown suspects, that remained isolated or weakly connected in the police-only network. Disruption simulations showed that forensic-enhanced networks change how network vulnerability and intervention effectiveness are assessed: police-only networks may overestimate the apparent disruption achieved by targeted interventions because they fail to capture all relational pathways. The added value of forensic intelligence was clearest for serious, trace-rich crime types, and depended on the availability of validated case-linkage information and clear data governance.

WP3 findings: Qualitative fieldwork confirmed that the central obstacle is a structural misunderstanding between institutional actors: definitional confusion about what forensic intelligence means; mandate misalignment between assigned functions and available resources; and expectation misalignment when new units are created without sustainable resourcing. The 'Pandora's box' dynamic, whereby any institutional commitment to forensic intelligence immediately generates demand exceeding capacity, was identified as a recurrent operational risk. The research recommends a federated governance model in which one institution (positioned as the NICC) plays a coordinating role without becoming a monopoly.

## Conclusions and Recommendations

The project concludes that forensic intelligence is both technically feasible and analytically valuable in Belgium, but that implementation requires addressing structural conditions that are currently absent. The 21 recommendations are organized at three levels:

Global/normative level: Establish a shared legal definition of forensic intelligence (R1); create a dedicated legal basis for cross-case forensic data exploitation compliant with GDPR and the Law

Enforcement Directive (R2); formalize inter-institutional data-sharing mechanisms (R3); shift from a reactive to a proactive, phenomenon-oriented forensic strategy (R4); define measurable evaluation criteria for all forensic intelligence activities (R5).

Institutional/cultural level: Position the NICC as a knowledge hub rather than a monopoly (R6); embed forensic intelligence as a transversal capacity across existing teams rather than a standalone unit (R7); start with a well-resourced pilot in the section with the best current conditions, likely the Drug Expertise Centre (R8); explicitly define the scope of forensic intelligence activities to avoid the 'Pandora's box' dynamic (R9); resource forensic intelligence functions adequately before activation (R10); bridge cultural gaps between forensic scientists, investigators, and the judiciary through shared training and co-design (R11); engage magistrates and police leadership as active co-designers (R12); address GDPR as a governance challenge rather than a definitive barrier through targeted legal guidance (R13); conduct systematic actor mapping before initiating any project (R14); and prepare for non-habitual partnerships (R15).

Research and development level: Commission a comprehensive legal analysis of the Belgian forensic intelligence legislative framework (R16); develop and test domain-specific pilot protocols (R17); conduct systematic comparative governance analysis (R18); develop a forensic intelligence training curriculum (R19); engage the National Drug Commissioner in strategic dialogue (R20); and establish legal and procedural frameworks for scientific access to police and judicial data (R21).

The project also provides a practical implementation canvas, a structured set of questions covering the what, who, structure, when, how, and evaluation dimensions of any forensic intelligence project, intended as a diagnostic and design tool for practitioners.