LEA projects cluster

Policy Scoping Brief

Working Group No.2
Criminal Networks & Financial Crime

September 2026

Privanova
Research & Consulting

www.privanova.com
comms@privanova.com
34, avenue des Champs-Elysées, Paris

Funded by
the European Union

Higlights

Criminal networks increasingly operate across interconnected financial, digital and cross-border environments, while investigative information remains fragmented.

1. The main analytical challenge is **turning fragmented information into actionable intelligence**. LEAs increasingly need to connect financial, behavioural, relational, identity and digital signals across multiple sources, systems and jurisdictions.

2. **Interoperability is not only a technical issue**. Effective cooperation also depends on compatible procedures, legal processes, terminology, communication practices and approaches to digital evidence.

3. **Emerging technologies are changing both criminal methods and investigative requirements**. Cryptocurrencies, AI-supported fraud, identity manipulation and the growing use of online environments by criminal networks create new demands for analytical and investigative capabilities.

4. **Operational uptake depends on sustained skills and organisational capacity.** New tools and methods require appropriate training, shared practices and continued awareness of changes in criminal methods and technologies.

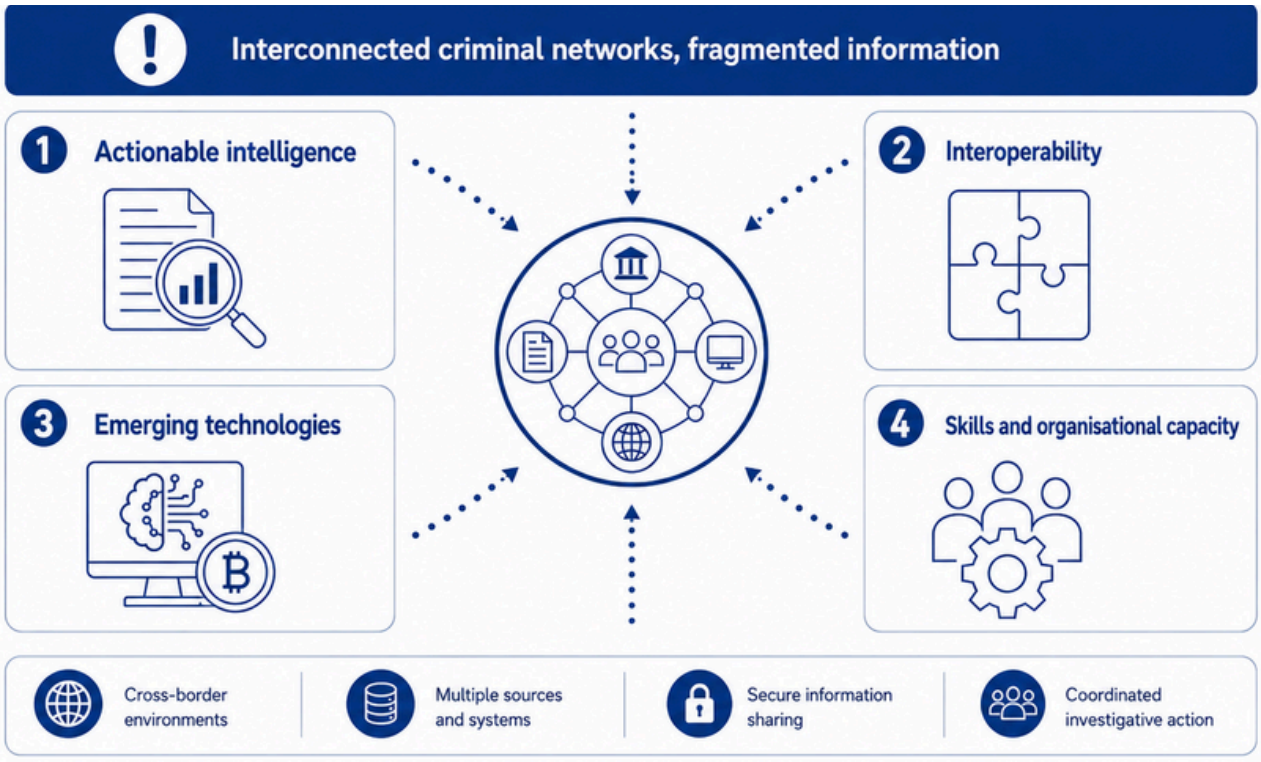

Figure 1. WG2 Highlights: Key Operational Challenges and Enabling Conditions

1. Purpose of the Scoping Brief

The present document sets out the initial policy direction and priorities identified by Working Group (WG) 2 of the LEA Projects Cluster, dedicated to Criminal Networks and Financial Crime. It constitutes the first policy output of WG2. The document builds on the initial scoping input provided by participating projects and the preliminary discussion held during the first WG2 meeting.

The purpose of this document is threefold.

1. **First**, it consolidates the main thematic areas that should guide WG2 work during the next phase.

2. **Second**, it identifies the main operational gaps and barriers affecting the investigation and disruption of serious criminal networks and financial crime.

3. **Third**, it defines an initial set of EU policy and cooperation priorities for validation with law enforcement agencies, EU institutions and international partners.

The role of the Scoping Brief is to establish a structured starting point for further consultation, expert exchange and policy formulation. The findings will be further developed through targeted engagement with law enforcement agencies, EU and international institutional stakeholders.

2. Policy and Cluster Context

EU-funded security research generates valuable knowledge and tools to combat serious and organised crime, but its impact can be limited by fragmentation across projects, themes and stakeholder communities. The LEA Projects Cluster addresses this by fostering cooperation between research projects, law enforcement, and policy actors through three thematic Working Groups aligned with the **EMPACT 2026-2029 crime priorities**.

WG2 focuses on Criminal Networks and Financial Crime, covering areas such as financial investigations, money laundering, asset recovery, fraud, and identity and document fraud. The initial consultation highlighted key priorities based on participating projects' expertise and operational experience.
Together with the other Working Groups on Cyber and Digital Crime, and Human Security and Environmental Crime, WG2's findings will contribute to the future LEA Projects Cluster Cross-WGs Policy Paper, "Innovation and Cooperation for a Secure and Resilient Europe".

The Cluster methodology follows an evidence-based sequence of **(i) mapping**, **(ii) consultation**, **(iii) thematic analysis**, and **(iv) integration.** WG2 is currently at the initial consultation stage. This Scoping Brief presents the first synthesis of project input and expert discussions, providing a basis for further consultation with law enforcement practitioners and policy development.

3. Core Thematic Areas

The consultation confirmed that criminal networks and financial crime cannot be examined through isolated crime categories or individual sources of intelligence.

Participants described an operational environment in which financial transactions, identities, behavioural patterns, relationships between individuals, digital evidence and cross-border activities increasingly need to be analysed together. Understanding serious criminal networks therefore depends on the **ability to connect different forms of information and translate them into a coherent investigative picture.**

3.1 Financial Investigations and Illicit Financial Flows

Financial investigations remain central to identifying, understanding and disrupting criminal networks. Participants particularly highlighted the **growing relevance of cryptocurrencies and other forms of digital financial activity** in criminal investigations.

Tracing cryptocurrency flows presents significant operational challenges due to the technical complexity of virtual assets and the methods used to obscure transactions and ownership.

Effective investigation therefore requires access to appropriate tracing capabilities, together with practitioners who understand how to interpret transaction patterns and connect financial information with other investigative evidence.

The discussion also highlighted the wider value of financial intelligence. Financial traces can contribute to identifying relationships between individuals, uncovering wider criminal structures and supporting the analysis of trafficking, fraud and other organised criminal activities. The challenge is therefore not limited to following individual transactions. LEAs increasingly need the analytical capacity to connect financial information with identities, relationships and other intelligence in order to understand the structure and activities of criminal networks.

3.2 Criminal Network Analysis

Serious criminal investigations increasingly require a deeper understanding of how individuals, roles and relationships interact within criminal structures. **Participants highlighted the difficulty of combining large volumes of heterogeneous information and identifying meaningful behavioural, relational and contextual patterns.**

Relevant signals may be dispersed across records, communications, identities, previous criminal activity and other sources. Behavioural and forensic psychological approaches can complement criminal intelligence by helping investigators assess roles, identify suspicious patterns and understand situational factors. AI-supported analysis can further help process complex information and prioritise leads for investigation.

The operational challenge is to transform different signals into actionable intelligence, particularly when information is dispersed across systems, organisations and jurisdictions. Understanding criminal networks should therefore go beyond identifying individual offenders to analysing relationships, roles, patterns and evolving modus operandi, supporting more effective investigation and disruption.

3.3 Identity and Document Fraud

Identity and document fraud represent an increasingly important component of investigations involving organised criminal activity, border control and immigration processes. Participants highlighted the growing use of techniques supported by AI, including morphing and presentation attacks, which can make fraudulent identities more difficult to detect through conventional visual inspection.

Remote and unsupervised identity processes may create additional vulnerabilities, particularly where weaknesses at one stage of the identity management process affect the reliability of subsequent verification.

These developments increase the need for advanced identity and document authentication capabilities. At the same time, their operational use requires practitioners to understand the strengths, limitations and appropriate application of automated detection methods. **The challenge therefore concerns both technological capability and institutional readiness.**

Effective uptake requires suitable training, organisational awareness, clear procedures and approaches that support the trustworthy use of AI within identity management and investigative settings.

3.4 Trafficking Networks

Trafficking in human beings also provides an important example of the complexity of modern criminal networks. Within WG2, trafficking is considered specifically through the lens of criminal network structures, financial activity, relationships between actors and evolving modus operandi. **Participants highlighted the growing role of digital environments in recruitment and exploitation, alongside activities that take place across physical locations and national borders.** Investigations may therefore require the analysis of multilingual and multimedia information, behavioural indicators, identities, locations and relationships between individuals.

A central operational gap is the limited integration of these different intelligence streams. Fragmented information can make it more difficult to identify relationships, recognise emerging patterns and develop a timely understanding of how trafficking networks operate. Participants therefore emphasised the value of coordinated and cross-border approaches to understanding criminal groups, including greater use of social and behavioural analysis and more consistent data inputs. Such approaches can strengthen understanding of traffickers' roles and methods and support better informed investigative and preventive strategies.

4. Initial Operational Gaps and Barriers

The consultation indicates that the main barriers affecting investigations of criminal networks and financial crime are closely interconnected. Analytical complexity is intensified by fragmented information, while differences in systems, procedures and legal interpretation can limit the ability to combine intelligence across organisations and jurisdictions. At the same time, emerging technologies create new investigative requirements, while limited training and inconsistent working practices can reduce the operational value of available tools and methods.

4.1 Analytical Complexity and Fragmented Information

A central concern identified by participants was the difficulty of turning large volumes of heterogeneous information into actionable intelligence. Investigations involving criminal networks and financial crime may require practitioners to connect financial transactions, identities, behavioural indicators, relationships between individuals, digital evidence and other investigative information. Relevant signals may be distributed across different databases, organisations and jurisdictions, making correlation difficult and time consuming.

The challenge is therefore not simply access to more data. Investigators need to identify relevant connections, assess the significance of different signals and develop a coherent understanding of criminal structures and activities. Fragmented information can reduce the ability to identify relationships, prioritise persons of interest, understand roles within criminal networks and recognise wider patterns of activity. This becomes particularly significant in complex and cross-border investigations where no single organisation holds a complete operational picture.

4.2 Interoperability Across Systems, Procedures and Jurisdictions

Interoperability emerged as one of the strongest cross-cutting concerns during the consultation. Participants emphasised that the problem extends beyond technical compatibility between information systems. Effective cooperation also depends on compatible procedures, legal processes, information exchange practices and organisational workflows across different teams, authorities and jurisdictions.

Cross-border investigations are often complicated by differences in national procedures, data protection requirements, information exchange and judicial processes. These barriers can limit the wider use of tools and information across Europe. WG2 should therefore view interoperability as a **broader operational requirement** covering technical systems, data exchange, procedures, legal frameworks and organisational cooperation.

4.3 Emerging Technological Challenges

Participants identified several technological developments that are increasing the complexity of investigations. Cryptocurrencies and other forms of digital financial activity create new requirements for tracing and analysing criminal financial flows. At the same time, AI-supported fraud, morphing attacks, presentation attacks and other forms of identity manipulation can make fraudulent activity increasingly difficult to detect through conventional methods.

The growing use of online environments by criminal networks also expands the range of information that may need to be assessed, including multilingual and multimedia content, digital identities and behavioural indicators.

These developments affect both criminal methods and investigative practice. LEAs therefore need capabilities that can respond to changing technologies while remaining operationally usable and suitable for integration into existing investigative processes.

The challenge is not only the availability of new analytical tools. Practitioners also need to understand when such tools are appropriate, how their outputs should be interpreted and what limitations should be considered when they inform investigative decisions.

4.4 Skills, Training and Operational Uptake

Training and capacity building were repeatedly identified as major barriers to the effective uptake of available solutions.

Participants highlighted the need for practitioners to remain informed not only about new tools, but also about changes in criminal methods, technologies and investigative techniques. Limited personnel and uneven access to specialised knowledge can make it difficult for organisations to maintain this level of capability. The consultation also indicated that training requirements extend beyond specialist users.

Technologies related to cryptocurrency tracing, AI-supported identity analysis, behavioural assessment and digital evidence may need to be understood by different actors involved in investigative and criminal justice processes.

A further concern is the fragmentation of training efforts across individual research projects. Participants suggested that greater coordination between projects could support more consistent and reusable training materials rather than multiple isolated resources addressing similar operational needs. Strengthening operational uptake therefore requires sustained capacity building alongside the development of technical solutions.

4.5 Communication, Terminology and Digital Evidence Practices

Differences in terminology and communication practices can create additional barriers when information and digital evidence move between teams, organisations or jurisdictions. Participants highlighted the absence of common terminology for digital evidence and the difficulty of communicating complex technical information to actors with different professional backgrounds and levels of technical expertise.

This can create a risk of misunderstanding, inconsistent interpretation and reduced efficiency when investigators, digital forensic specialists, prosecutors or other practitioners need to work with the same evidence or analytical findings. Clearer communication practices, more consistent terminology and common approaches to handling digital evidence could therefore strengthen cooperation across investigative teams and jurisdictions.

Within WG2, this represents the semantic and professional dimension of the wider interoperability challenge. Technical systems can enable information exchange, but effective cooperation also requires shared terminology, clear communication and a common understanding of how information and digital evidence should be interpreted and used.

5. Initial Policy Priorities for EU-Level Action

The gaps identified point to **five areas** where EU-level action could strengthen existing national and project efforts addressing criminal networks and financial crime. These priorities remain subject to further validation and should not yet be read as final recommendations.

5.1 Improve Data Integration and Interoperability

Participants identified improved data integration and interoperability as one of the highest-priority areas for further action.

Complex investigations increasingly depend on information held across different systems, organisations and jurisdictions. The operational value of this information depends on the ability to connect relevant financial, identity, behavioural, relational and digital signals and interpret them within a coherent investigative context. EU-level action should therefore support greater interoperability between relevant systems and investigative environments. This should extend beyond technical compatibility and consider procedures, information exchange practices, legal processes and organisational workflows. Greater consistency in these areas could reduce fragmentation and strengthen the ability of LEAs to correlate information across cases and jurisdictions.

5.2 Strengthen Analytical and Investigative Capabilities

The changing nature of criminal activity requires analytical capabilities able to process increasingly complex forms of information. Participants highlighted particular needs related to cryptocurrency tracing, fraud detection, identity and document analysis, behavioural and relational intelligence, and the analysis of complex criminal networks. EU-level support should contribute to strengthening these capabilities while encouraging their integration into existing investigative practices. This includes supporting methods and tools that help practitioners identify relevant patterns, relationships, roles and financial flows within large and heterogeneous datasets. The objective should be to strengthen the ability of investigators to transform fragmented information into operationally meaningful intelligence rather than simply increase the volume of information available to them.

5.3 Strengthen Training and Capacity Building

The effective use of new analytical capabilities depends on practitioners having the knowledge and skills required to apply them appropriately. Training should address both emerging technologies and changes in criminal methods. Areas identified during the consultation include cryptocurrency tracing, AI-supported analysis, identity fraud detection, behavioural analysis and digital evidence.

Participants also highlighted the value of greater coordination between EU-funded projects developing training materials. More consistent and reusable resources could reduce duplication and provide practitioners with clearer pathways for developing relevant capabilities. EU-level action could therefore support coordinated training approaches, knowledge exchange and stronger links between research projects, LEAs and practitioner training organisations.

5.4 Develop Common Approaches for Digital Evidence and Communication

Common terminology and communication practices are important for investigations involving multiple teams, professional disciplines and jurisdictions. Participants highlighted difficulties that can arise when complex digital or technical findings need to be communicated between investigators, forensic specialists and other actors within the criminal justice process. EU-level cooperation could support more consistent terminology, clearer communication practices and common approaches for handling and discussing digital evidence. Greater consistency could reduce misunderstanding and support more effective cooperation when evidence and analytical findings move between teams, institutions or national systems.

5.5 Support Cross-Border Understanding of Criminal Networks

Serious criminal networks often operate across borders, while relevant intelligence remains distributed across organisations and jurisdictions. Participants highlighted the need for stronger cross-border cooperation to better understand criminal structures, relationships, roles, financial activity and evolving modus operandi. EU-level action could support the exchange of operational knowledge, compatible analytical approaches and stronger cooperation between authorities, helping connect intelligence and identify patterns that may not be visible within a single national context. The objective should be to strengthen the collective understanding of criminal networks and support more informed investigative, preventive and disruption strategies.

6. Implications for EU Security Research and Innovation Projects

The WG2 discussion has direct implications for EU-funded security research projects working on criminal networks, financial investigations, fraud, identity management, trafficking and related analytical capabilities.

1. **Projects should design analytical tools with integration and interoperability in mind from the start**, considering not only technical compatibility but also the procedures, terminology and organisational environments in which information will be used.
2. **Projects should support the combination of different forms of intelligence,** including financial, behavioural, relational, identity and digital information. The operational value of individual tools increases when their outputs can contribute to a wider understanding of criminal structures and activities.
3. **Training and capacity building should be developed alongside technical solutions**. Practitioners need support to understand emerging technologies, interpret analytical outputs and apply new methods within existing investigative practices.
4. **Projects should strengthen cross-border relevance and operational validation** by involving law enforcement and other end users from different jurisdictions. This can help identify procedural, legal and organisational barriers that may affect wider uptake.
5. **Greater coordination between projects could also support shared terminology, reusable training materials and complementary operational practices**, reducing duplication and helping research results contribute to more consistent capabilities across the European security ecosystem.
6. **Sustainability requires clearer pathways from research outputs to operational use**, including continued engagement with LEAs, practitioner networks, EU and international institutions, training organisations and future funding or implementation mechanisms.

7. Initial Conclusions

The first phase of WG2 confirms that criminal networks and financial crime should be addressed as interconnected analytical, operational, technological and cross-border challenges. The consultation highlighted five central messages.

First, complex criminal investigations increasingly depend on the ability to connect different forms of information. Financial, behavioural, relational, identity and digital signals may each reveal only part of a wider criminal structure. Their combined analysis can provide a more complete understanding of relationships, roles and patterns of activity.

Second, fragmented information remains a major barrier to actionable intelligence. Relevant data and intelligence may be distributed across different systems, organisations and jurisdictions, limiting the ability of investigators to identify connections and develop a coherent operational picture.

Third, interoperability extends beyond technical systems. Effective cooperation also depends on compatible procedures, legal processes, terminology, communication practices and approaches to handling digital evidence.

Fourth, emerging technologies are changing both criminal methods and investigative requirements. Cryptocurrencies, AI-supported fraud, identity manipulation and the growing use of digital environments by criminal networks require LEAs to continuously adapt their analytical capabilities and investigative practices.

Fifth, operational uptake depends on sustained skills and organisational capacity. Training, knowledge exchange and common operational practices are necessary for practitioners to understand new technologies, interpret analytical outputs and integrate innovative methods into existing workflows.

These findings will be further validated with practitioners, EU and international stakeholders, and participating projects before being translated into more concrete policy recommendations.

Contributors

The present document also reflects the expertise and perspectives shared by the following contributors under the LEA Projects Cluster during the WG2 consultation process:

- Prof. Constantinos Patsakis, Athena Research Center, representing the **SafeHorizon Project**;
- Amy Long and Megan O'Neill, University of Dundee, representing the **CLARUS Project**;
- Chris Antoniou, European Dynamics, representing the **CRYPTOACTION Project**;
- Eileen Murphy, Trilateral Research, representing the **EINSTEIN Project**;
- Marina Papaefthymiou, AEGIS IT RESEARCH, and Youssef Bouali and Steven Ormston, Polish Platform for Homeland Security (PPBW), representing the **GANNDALF Project**;
- Alexander Nikolov, SYNYO GmbH, representing the **NOTIONES Project**;
- Nikolaos Avgerinos, Performance Technologies, representing the **TRACY Project**;
- Theoni Spathi, Theodora Tsikrika and Despina Chatzakou, CERTH, representing the **VANGUARD Project**.

The WG2 consultation process, facilitation of the Working Group discussions and drafting of the present Scoping Brief were coordinated by Kristina Isakzay, **LEA Projects Cluster** Coordinator at **Privanova**, who also contributed to the consultation representing the **IAMI**, **SafeHorizon** and **SECUR-EU** projects.

About the Cluster

The **LEA Projects Cluster**, led by **Privanova**, brings together more than 54 EU-funded security research and innovation projects to strengthen Europe's collective capacity to address emerging security challenges. The LEA Projects Cluster contributes to addressing fragmentation in EU security research by connecting projects, law enforcement authorities, and institutional stakeholders.

The Cluster enhances the visibility of available capabilities, facilitates knowledge exchange, and supports alignment between research outputs, policy priorities, and operational needs.

Join the LEA Projects Cluster

If your organisation coordinates or participates in an EU-funded security research project and would like to learn more about the **LEA Projects Cluster** or explore opportunities for collaboration, please contact Cluster Coordinator **Kristina Isakzay:** **kristina.isakzay@privanova.com**.