Policy Scoping Brief

Working Group No.1 Cyber and Digital Crime

August 2026

Privanova
Research & Consulting

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

Funded by
the European Union

Higlights

Innovation is advancing faster than operational adoption.

1. The main gap is operational, not only technological. Tools and research outputs exist, but their impact depends on skills, procurement, interoperability, internal procedures and implementation capacity.

2. Digital capability is now required across the criminal justice chain. Digital evidence is no longer handled only by specialist cybercrime units; investigators, forensic experts, prosecutors and judicial actors all need relevant capacity.

3. Cross-border access to digital evidence remains a critical pressure point. Delays reduce the operational value of data and can affect the identification of suspects, victims and criminal networks.

4. AI brings both investigative value and evidential risk. Its use requires operational validation, transparency, meaningful human oversight and alignment with forensic and legal standards.

1. Purpose of the Scoping Brief

The present document sets out the **initial policy direction and priorities** identified by Working Group (WG) 1 of the LEA Projects Cluster, dedicated to Cyber and Digital Crime. It constitutes the first policy output of WG1. The document builds on the initial scoping input provided by participating projects and the preliminary discussion held during the first WG1 meeting.

The purpose of this document is threefold.

1. First, it consolidates the **main thematic areas** that should guide WG1 work during the next phase.
2. Second, it identifies the **main operational gaps and barriers** that affect law enforcement and criminal justice responses to cyber and digital 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 significant knowledge, tools and operational insights relevant to law enforcement innovation. However, **the impact of this work is often limited by fragmentation** across projects, project timelines, thematic areas and stakeholder communities. The LEA Projects Cluster addresses this gap by supporting cooperation between research projects, law enforcement, and institutional and policy actors. It has established **three thematic Working Groups** aligned with the EMPACT 2026–2029 crime priorities.[1]

WG1 focuses on Cyber and Digital Crime, addressing emerging online threats and digital resilience. The other Working Groups focus respectively on Criminal Networks and Financial Crime, and Human Security and Environmental Crime. Their collective findings and gathered insights will establish the analytical basis for 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. WG1 is currently at the initial consultation stage. The present Scoping Brief therefore captures the first synthesis of stakeholder input before moving towards deeper expert consultation and policy development.

[1] For further information on the crime priorities under the EMPACT Cycle 2026-2029, see: https://eucrim.eu/media/news/pdf/eucrim-news-crime-priorities-under-the-empact-cycle-2026-2029.pdf

3. Core Thematic Areas

The consultation confirmed that **cyber and digital crime can no longer be understood through isolated crime categories**.

Instead, participants described an operational environment where investigations, intelligence, digital evidence, and online infrastructures are increasingly interconnected.

3.1 Online cybercrime ecosystems

Participants highlighted the growing professionalisation and accessibility of cybercrime. Criminal actors increasingly operate through interconnected online ecosystems that combine ransomware services, darknet marketplaces, cyber-enabled fraud, anonymisation technologies, cryptocurrencies and digital communication platforms.

The discussion emphasised that many operational challenges no longer stem from individual criminal incidents, but from the **ability of offenders to exploit complex digital infrastructures** that transcend jurisdictions and facilitate collaboration, monetisation and concealment.

The widespread use of VPNs, encrypted communications, virtual private servers, privacy-enhancing technologies and cryptocurrency financial flows was repeatedly identified as a significant obstacle to attribution, evidence gathering and disruption activities.

3.2 Digital investigations

Digital investigations are no longer confined to specialised cybercrime units. Digital evidence, online traces, platform data and technical artefacts increasingly appear within a wide range of investigations and affect the full criminal justice chain. The growing use of manipulated and AI-generated content adds a further evidential dimension. Digital investigations increasingly require practitioners not only to identify relevant content, but also to establish its authenticity, reliability and evidential value.

These developments create **practical challenges beyond access to tools.** Technical findings must be understood, communicated and translated into legally usable investigative outputs.

Differences in terminology, working practices and levels of technical understanding can create friction between technical experts and non-technical actors, increasing the risk of delay, misinterpretation or loss of evidential value.

WG1 should therefore address digital investigations as a technical, evidential and coordination challenge. Clearer procedures, shared terminology, stronger cross-team practices and capacity building across law enforcement, prosecution and judicial actors are necessary to ensure that digital evidence can be handled consistently, understood correctly and used effectively.

3.3 Real-time intelligence

Real-time intelligence refers to the ability to collect, process and interpret large volumes of open-source and digital information in time to support investigations. Participants noted that **the main challenge is not only access to data,** but the ability to filter relevant signals, verify information and turn it into lawful, reliable and actionable investigative insight. This area also connects to AI-supported analysis, digital evidence integrity, prevention before cyber incidents occur, and post-incident recovery.

4. Initial Operational Gaps and Barriers

The consultation indicates that the **identified barriers are mutually reinforcing rather than independent**. Technical complexity increases demand for specialised skills, while legal fragmentation, procurement constraints and organisational capacity limit the operational uptake of available solutions.

4.1 Skills and access to tools

A central concern was the **uneven level of digital skills** across the wider law enforcement and criminal justice system. This can affect investigation speed, evidence handling, communication with technical specialists and the practical uptake of research tools.

As digital evidence becomes relevant to a wider range of investigations, basic digital literacy and investigative understanding are increasingly required across a broader group of practitioners.

This affects not only investigation speed, but also the quality of evidence handling, the ability to communicate with technical specialists, and the practical uptake of research tools.

Limited access to suitable and affordable tools was also identified as a major barrier. Even when relevant tools exist, law enforcement agencies may face high costs, limited procurement, flexibility, licensing constraints, interoperability issues, and difficulties assessing whether new solutions are sufficiently mature, compliant and operationally useful.

4.2 Tool overload and implementation fatigue

A particularly important point emerging from the discussion was **the problem of too many tools**. Participants noted that law enforcement agencies are often presented with multiple platforms, pilots, prototypes and technical solutions, but do not always have the resources or knowledge to implement them in real operational settings. This creates a risk that tools remain available in theory but unused in practice. **The issue is not simply innovation supply; it is the ability of receiving institutions to integrate, maintain, and operationalise new capabilities**.

In this respect, WG1 should pay specific attention to the gap between tool development and tool adoption. A law enforcement perspective also highlighted that internal policies on information sharing may limit the adoption of new tools. In some cases, agencies prefer existing and proven tools because they are already

embedded in internal workflows, accepted by practitioners, and supported by established procedures.

This suggests that future EU-funded innovation should be designed with stronger attention to operational integration, institutional constraints and end-user confidence.

4.3 Anonymisation, encryption and technological complexity

The widespread use of anonymisation tools, encrypted communications and cryptocurrencies reduces visibility into criminal networks and limits the effectiveness of traditional investigative approaches.

At the same time, AI-generated content, synthetic identities and manipulated media make it increasingly difficult to verify information, establish authenticity and assess evidential value.

The challenge is therefore not limited to a specific technology. Rather, participants highlighted a broader loss of investigative visibility and traceability in digital environments.

The emerging gap is not simply the absence of detection tools, but the **lack of sufficiently validated and interoperable forensic capabilities able to produce transparent, reproducible and legally defensible results**. This limits the consistent integration of AI-supported analysis into investigative and judicial workflows.

4.4 Cross-border and legal constraints

Cyber and digital crime routinely crosses national borders. Digital evidence, user accounts, communication services, hosting infrastructure and financial traces may be located across multiple jurisdictions.

Participants identified delays in European Investigation Orders[2], limited legal cooperation with third countries, and inefficient access to account and transaction data as recurring barriers.

Faster and more effective cross-border judicial cooperation was identified as one of the highest-priority areas for EU-level action. The practical need is clear: investigations often depend on timely access to digital data. Delays can lead to loss of evidence, reduced operational value, and difficulties identifying suspects, victims or criminal networks. At the same time, faster access must remain legally sound and rights-compliant.

4.5 Data volume, real-time analysis and operational communication

The volume of digital data available in investigations is increasing rapidly. Participants highlighted that law enforcement agencies often struggle to analyse large volumes of data in real time. This affects their ability to detect patterns, prioritise evidence, generate intelligence and act within operationally relevant timeframes.

---

[2] For further information on the European Investigation Order (EIO), see: https://www.eurojust.europa.eu/judicial-cooperation/instruments/european-investigation-order

The challenge is not only technical. It also concerns communication and interpretation across teams. Digital investigations often involve investigators, analysts, forensic experts, prosecutors, cybersecurity specialists, private sector providers and sometimes international partners. Without common terminology, interoperable workflows and shared procedures, information cannot be consistently interpreted, shared and transformed into operational intelligence across the criminal justice chain.

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-level efforts. These priorities remain subject to further validation and should not yet be read as final recommendations.

5.1 Faster and More Effective Cross-Border Judicial Cooperation

Cyber and digital crime investigations require timely access to data across borders. EU-level action should support faster, clearer and more predictable cooperation mechanisms for digital evidence, account information and transaction data. This includes improving the practical functioning of existing instruments, addressing delays, and supporting cooperation with third countries where relevant.

The objective should be to strengthen operational effectiveness while maintaining legal certainty, accountability and fundamental rights safeguards.

5.2 Access to Affordable and EU-Compliant Tools for LEAs

Law enforcement agencies need access to tools that are affordable, compliant with EU law, operationally usable and sustainable beyond project lifecycles. EU funding can support this objective, but funding should be more closely aligned with operational priorities and implementation realities.

Future support should not focus only on developing new tools. It should also address validation, interoperability, training, procurement readiness, maintenance, user support and integration into existing workflows.

5.3 Shared EU-level Capabilities and Platforms

Participants identified a need for shared EU-level capabilities, particularly in cybercrime intelligence and reporting. Such capabilities could support better situational awareness, reduce duplication and help smaller or less-resourced agencies access expertise and information that may otherwise remain fragmented.

This area should be approached carefully. Shared platforms must be designed around clear governance, data protection, access control, accountability, operational relevance and trust between participating institutions.

5.4 Support for Innovation and AI Deployment in Law Enforcement

AI can support cyber and digital crime investigations by helping process large datasets, detect patterns, support triage, analyse open-source information, identify anomalies and assist decision-making.

However, participants also noted that AI deployment must be aligned with regulatory requirements, evidential standards and institutional readiness. EU-level support should therefore focus on responsible AI deployment, including regulatory alignment, validation, transparency, human oversight, risk management, and the strengthening of EU-based technological capabilities for law enforcement.

Where AI outputs may influence the assessment of digital evidence, responsible deployment should include common requirements for operational validation, explainability, documented limitations and human oversight.

5.5 Common EU Approaches for Digital Evidence Handling and Terminology

The lack of common terminology and practices in digital evidence handling creates challenges across teams, institutions, and borders.

EU-level guidance, training, and standardisation are needed to strengthen cooperation, improve evidence quality, and ensure consistent assessment of manipulated and AI-generated media through shared approaches and benchmarks.

6. Implications for EU Security Research and Innovation Projects

The WG1 discussion **has direct implications** for EU-funded security research projects working on cybercrime, digital investigations, digital evidence, cyber resilience and law enforcement tools.

- **Projects should design outputs for implementation from the start**, ensuring that tools are innovative, usable, explainable, maintainable and compatible with law enforcement workflows.”.

- **Projects should engage a broader range of practitioners**, including analysts, investigators, prosecutors, judicial actors, and operational managers, as cyber and digital crime is no longer limited to specialised units.

- **Training, documentation and organisational guidance should be developed alongside tools**. Without these elements, technical outputs may remain underused.

- **Interoperability and terminology should be addressed early**, avoiding isolated systems or concepts that cannot integrate with existing operational, legal, and institutional environments.

- **Sustainability requires clear pathways beyond the project duration**, including links with EU agencies, practitioner networks, procurement, training institutions, standardisation initiatives and future funding mechanisms.

7. Initial Conclusions

The first phase of WG1 confirms that cyber and digital crime should be addressed as a combined operational, legal, technical and organisational challenge. The discussion highlighted **five central messages.**

First, **cyber and digital crime capabilities must be strengthened within the wider criminal justice system**, not only within specialist cyber units.

Second, access to tools remains important, but **tool adoption depends on additional factors**, such as training, procurement, interoperability, institutional policies, implementation capacity.

Third, **cross-border access to digital evidence** remains one of the most urgent operational barriers.

Fourth, **AI offers new investigative capabilities** but also raises evidential challenges requiring validation, transparency, human oversight, and legal alignment.

Fifth, **common EU approaches to digital evidence handling, terminology** and interoperability would **significantly improve cooperation and operational effectiveness.**

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 reflects the expertise and perspectives shared by the following contributors under the LEA Projects Cluster during the WG1 consultation process:

- Amy Long, Megan O'Neill from University of Dundee, representing the **CLARUS Project**;
- Antonia Koumpoti, CERTH, representing the **DETECTOR** Project;
- Amélie Cathier, Liana-Miruna Predut, representing the **ENDURANCE** Project;
- Carlos Cilleruelo, Ioannis Chalkias, representing the **ENSEMBLE** Project;
- Michael O'Callaghan from University College Dublin (UCD), representing the **HOPLITE** Project;
- Prof. Constantinos Patskais from Athena Research Center, representing the **SafeHorizon** Project;
- Ulrich Seldeslachts, representing the **INCIDENTRON** Project;
- Carlos Urquizo from the Basque Country Police, representing **PRESERVE** Project;
- Jean-Michel Chapon, Information Security Forum; Robert-Stefan Sandru, National Directorate for Cyber Security (DNSC), Romania; Khalimatou Samirah, National Standards Authority of Ireland (NSAI), representing the **TrustBoost** Project.

The WG1 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**.