Dismantling Organised Crime

In Physical and Digital Environments

powered by phygital-oc

ISSUE 02 | NOVEMBER 2026

phygital

EXPLORING SOLUTIONS TO TRANSNATIONAL ORGANISED CRIME



phygital-project.eu

Co-funded by the European Union

CONTENTS

04. Contributors

05. EDITORIAL — Exploring Solutions to Transnational Organised Crime

06. ARTICLE — The Future of Europe's Response to Organised Crime

08. PODCAST — Setting the Priorities for Europe's Fight Against Organised Crime

09. PAPER — Internet Organised Crime Threat Assessment

10. INFOGRAPHIC — Phygital-OC Strengthening International Cooperation

12. ARTICLE — Using Advanced Technologies to Track, Monitor and Disrupt Organised Crime

16. ARTICLE — Following the Digital Trail: How AI Helps Investigators

20. PAPER — Making Law Enforcement Fit for the Future: Strategic Priorities for Policing in the Digital Age

22. ARTICLE — Latin American Organized Crime Groups are Expanding their Presence in Europe

26. INTERVIEW — On The Frontline… Gloria Gilardoni from CAT

28. ARTICLE — Italy's Strongest Weapon Against the Mafia is its Civil Society

31. FEATURE — The Phygital-OC Alliance

32. ARTICLE — Diagnosing Evidence Gaps When Analysing Emerging Criminal Threats

34. FEATURE — EUCPN-ENAA: Preventing Youth Recruitment

38. PAPER — Disrupting Youth Recruitment into Organized Crime

39. PAPER — Decoding the EU's Most Threatening Criminal Networks – Issue 2

40. ARTICLE — What Can Strategic Communications Bring to the Fight Against Organised Crime?

44. HIGHLIGHTS — Phygital-OC Activity

45. LIBRARY — Discover more



CONTRIBUTORS

Sergio Bianchi
Agenfor International

Vincenzo Fusco
SCO

Sandro Liviero
Venice Police

Daniel Brombacher
GI-TOC

Gloria Gilardoni
CAT

Ruggero Scaturro
GI-TOC

Fook Nederveen
RAND

Shann Corbett
RAND

Maxime Hennen
EUCPN

Jonathan Benjamin
REOC



As the challenge posed by organised crime continues to evolve – with criminal groups increasingly connected, operating across borders and adopting new digital technologies – we must respond at the same pace and scale.

No single agency, country or sector can tackle transnational organised crime alone. An effective response requires closer cooperation, better information sharing and action against both criminal activity and the conditions that allow it to take root.

In the first issue of PHYGITAL, we examined how organised crime is changing and what that means for Europe. In this issue, Exploring Solutions to Transnational Organised Crime, we consider the response: what is working, where gaps remain and how different efforts can achieve more together.

Contributors explore how digital technologies can strengthen investigations, how authorities can work across borders, and how prevention can protect people from recruitment and exploitation.

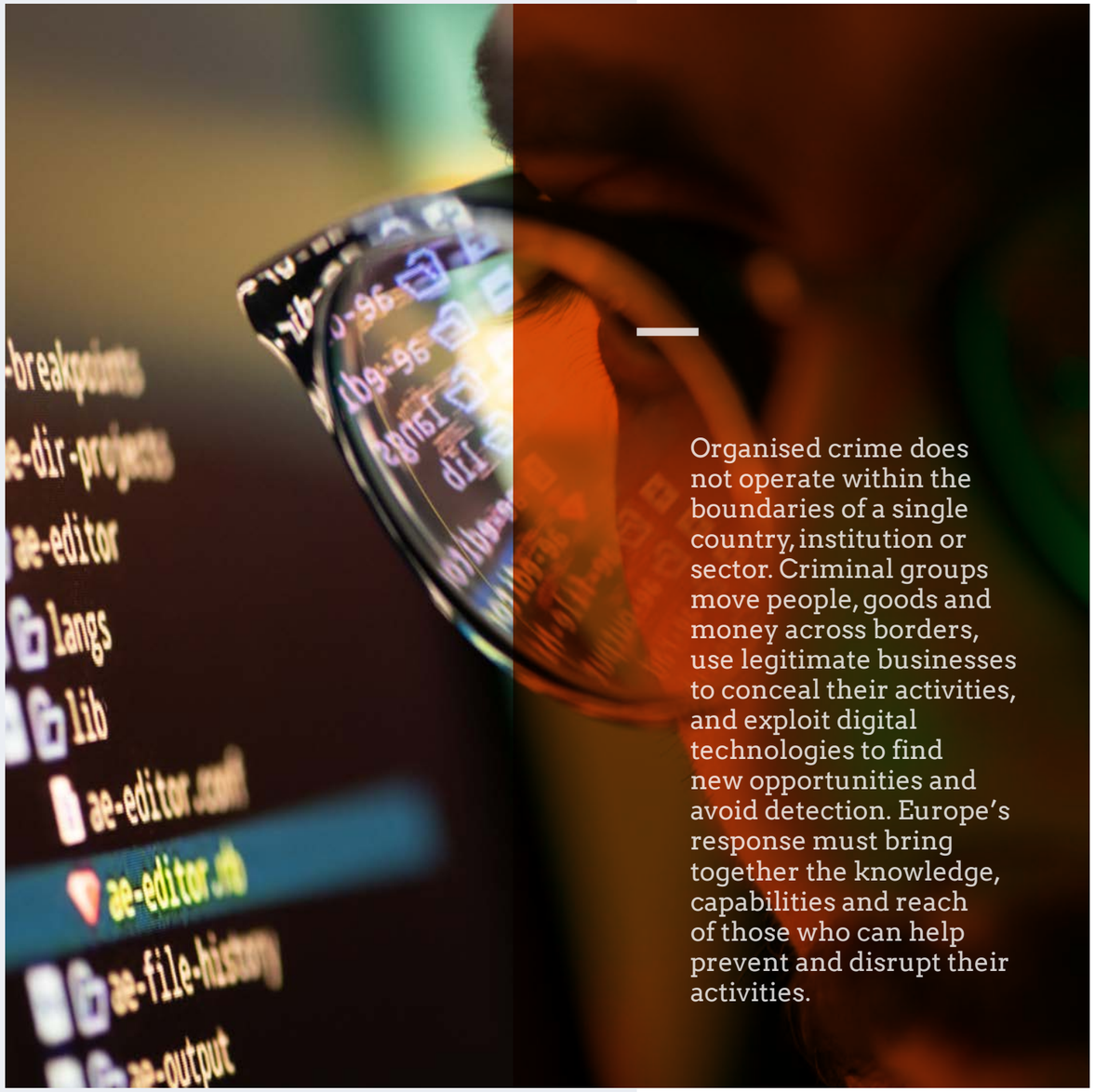
We showcase tools and approaches developed by EU-funded projects and hear from CAT Cooperativa about the realities of frontline work: reaching people facing exploitation, helping survivors rebuild their lives and connecting the services they need.

Across these contributions, a common message emerges: progress depends on combining expertise and putting it into practice. Through this magazine and the Phygital-OC Alliance, we aim to connect people and organisations, share lessons and support lasting cooperation.

Sergio
Bianchi
Agenfor
International

THE FUTURE OF EUROPE'S RESPONSE TO ORGANISED CRIME





Organised crime does not operate within the boundaries of a single country, institution or sector. Criminal groups move people, goods and money across borders, use legitimate businesses to conceal their activities, and exploit digital technologies to find new opportunities and avoid detection. Europe's response must bring together the knowledge, capabilities and reach of those who can help prevent and disrupt their activities.

Closer cooperation between law enforcement agencies is essential. But much of the information that could help authorities identify criminal activity at an early stage sits outside the police and judiciary. Civil society organisations, businesses and researchers each see different parts of the problem. The challenge is to bring those perspectives together through stronger, more structured public-private partnerships.

Turning Cooperation Into Practice

We need to move beyond occasional exchanges of information towards established ways of working together. This means agreeing how information is gathered, assessed, stored and shared, and how it can contribute to the work of police and judicial authorities. Without clear methods and the infrastructure to support them, valuable knowledge can remain fragmented or reach investigators too late.

The purpose is not for civil society or businesses to take on the responsibilities of the police. Each partner must retain its own role, responsibilities and expertise. But different organisations can pursue common goals through complementary activities. Protecting vulnerable people and disrupting the groups exploiting them, for example, are closely connected objectives.

Civil society has an important contribution to make here. Organisations supporting vulnerable migrants and victims of trafficking can encounter signs of exploitation through their everyday work. Their contact with people affected by crime can provide insight that an investigation would otherwise lack. This knowledge can help authorities understand how criminal groups operate and identify risks earlier, while supporting the protection of those being exploited.

For that contribution to be useful, cooperation must be built on clear responsibilities and lawful practices. Public authorities and other organisations operate under different data protection frameworks. These differences need to be addressed when partnerships are designed, with agreed procedures that protect individuals and allow relevant information to be used appropriately.

Connecting Digital Information With People

Technology can help strengthen these partnerships. Open-source intelligence tools, for example, can support both public authorities and other organisations in examining online activity and identifying indicators of risk. But collecting large amounts of data is only the beginning. We also need the tools and expertise to interpret it, and secure systems through which partners can work together.

Digital information must also be connected with what is happening in people's lives. Behind an online account is a person, with relationships and circumstances that cannot be understood through digital analysis alone. In Phygital-OC, we have explored an approach that connects online analysis with information gathered through interviews and engagement with local actors, including social mediators and schools. Where the findings justify further investigation, police can then use their specialist capabilities within the applicable legal framework.

The choice of technology matters too. Europe needs secure infrastructure and platforms that meet its data protection requirements and reduce the risk of sensitive information being accessed or exploited by third parties. Technology should make cooperation more effective while maintaining confidence in how information is handled.

Following The Money

Financial intelligence offers another clear reason to strengthen cooperation. Banks, notaries and other actors involved in financial transactions may encounter early signs of suspicious activity. Their knowledge can help authorities identify the financial relationships that sustain criminal networks and direct investigations towards them.

Europe's future response therefore depends on more than individual tools or investigations. We need a framework that enables public authorities, businesses and civil society to contribute their different capabilities towards shared goals. Clear methods, secure technology and stronger partnerships can help us identify criminal activity earlier, protect vulnerable people and disrupt the organisations responsible..

Sergio Bianchi is Board Member, Research and Innovation at Agenfor International, a partner on Phygital-OC.

Podcast

SETTING THE PRIORITIES FOR EUROPE'S FIGHT AGAINST ORGANISED CRIME

In this second episode of the Phygital-OC podcast series, experts from Phygital-OC and other EU-funded projects discuss how Europe can respond to transnational organised crime.

Recorded at the Belgian Federal Police headquarters in Brussels, the conversation explores three priorities: using technologies such as AI and open-source intelligence to strengthen investigations; preventing the recruitment of young people and building resilience in communities; and improving cooperation between law enforcement, civil society and the private sector. The contributors share examples of the work already under way and consider how these different approaches can be brought together to prevent, detect and dismantle organised crime.

Watch the podcast in full...



Paper

INTERNET ORGANISED CRIME THREAT ASSESSMENT 2026

Read more...



Europol's Internet Organised Crime Threat Assessment 2026

examines the technologies and services enabling cybercrime, alongside developments in online fraud, cyber-attacks and the sexual exploitation of children online. It describes a criminal ecosystem in which tools, stolen information and specialist services can be bought and used by different groups. Even when authorities shut down a platform, others can quickly take its place.

The report also looks at what this means for Europe's response. Europol calls for law enforcement to develop its own technological capabilities, strengthen cooperation across borders and work more closely with online service providers. The challenge is to identify and disrupt criminal activity at the speed at which it now takes place, while respecting fundamental rights and data protection.

Dismantling Organised Crime
In Physical and Digital Environments
powered by phygital-oc

Strengthening International Cooperation

to Dismantle Organised Crime

PHYGITAL-OC is creating new connections, fostering greater collaboration and enabling better coordination across borders and sectors. By bringing together insight, skills, tools and expertise, the project aims to strengthen information sharing, support joint investigations and build a more effective collective response to transnational organised crime.

Connecting Countries and Regions

Building relationships between European law enforcement agencies and counterparts around the world.

Why it Matters

Criminal networks operate between regions. Connections between authorities help build trust, understand those networks and identify opportunities for cooperation.

PHYGITAL-OC: Community of Practice Events

Connecting law enforcement and judicial authorities across Europe, the Western Balkans, Africa, Latin America and Southeast Asia.

Coordinating Across Borders

Enabling investigators, analysts and judicial authorities from different countries to share intelligence and coordinate action.

Why it Matters

An investigation in one country may reveal only part of a criminal network. Working together helps authorities connect the evidence and act against the wider organisation.

PHYGITAL-OC: Operational Task Forces and an Operative Room

Bringing together specialised teams in Italy, Spain and Greece, supported by an Operative Room in Florence, to strengthen coordination and support joint investigations.



Collaborating Across Sectors

Bringing public authorities, the private sector, technology companies and researchers together to strengthen investigative capabilities.

Why it Matters

Combining operational knowledge with technical expertise helps ensure digital tools meet investigators' needs and teams have the skills to use them effectively.

PHYGITAL-OC: Advanced Technology and Specialist Training

Procuring and adopting advanced digital technologies, and training operational teams to use them to identify, analyse and investigate criminal activity across physical and digital environments.

Cooperating With Communities

Strengthening cooperation with civil society organisations, NGOs and those supporting people affected by crime.

Why it Matters

Their reach, local insight and trusted relationships can help identify recruitment and exploitation earlier, understand people's vulnerabilities and inform prevention, protection and investigation.

PHYGITAL-OC: The Alliance and Exchange Events

Bringing civil society together with law enforcement, judicial authorities and other partners to share insights and develop cooperation, drawing on their different expertise, experience and reach.

Everyone has a role to play. Together, we can strengthen our response to organised crime and make our communities safer and more secure for everyone.



THE NEW TOOLS OF THE TRADE: USING ADVANCED TECHNOLOGIES TO TRACK, MONITOR AND DISRUPT ORGANISED CRIME

Vincenzo Fusco
SCO

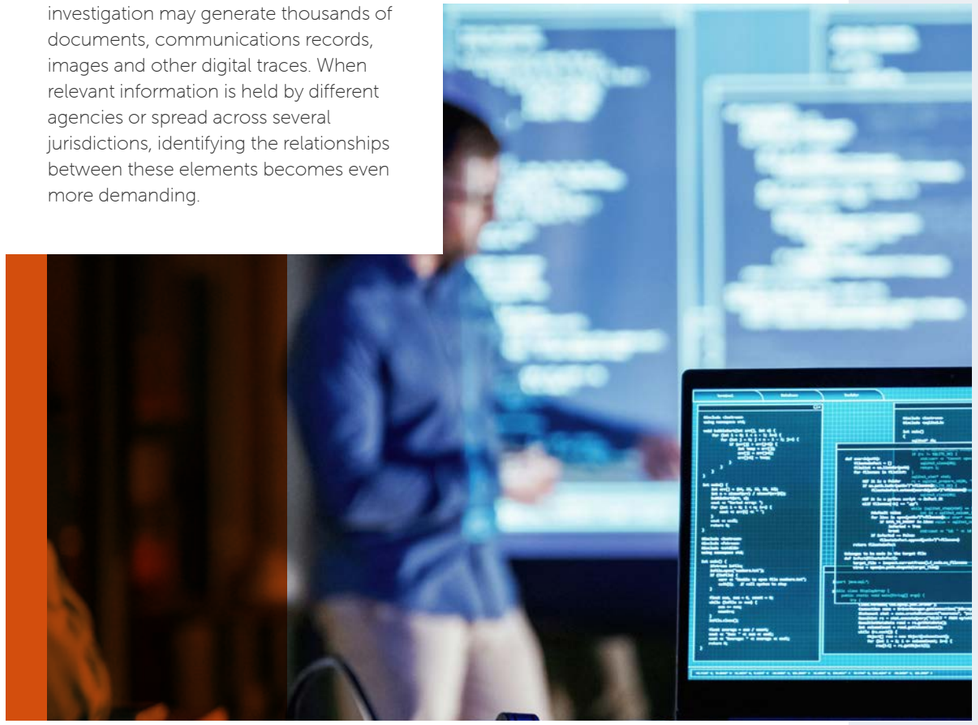
Technology does not replace investigative judgement. Its value lies in helping competent authorities make better-informed decisions...

Why Do We Need Technology?
Organised crime increasingly operates across both physical and digital environments. Criminal networks use online platforms to recruit, advertise, communicate and coordinate their activities, while people, goods and illicit proceeds move across borders. Information relevant to an investigation may be scattered across public websites, company registers, communications records, financial data, digital devices and the records held by authorities in different countries.

For law enforcement, the challenge is not simply to collect information, but to connect it, understand its significance and turn it into actionable intelligence. A single investigation may generate thousands of documents, communications records, images and other digital traces. When relevant information is held by different agencies or spread across several jurisdictions, identifying the relationships between these elements becomes even more demanding.

Advanced technologies can help investigators analyse large volumes of heterogeneous data, identify patterns and reconstruct relationships between individuals, businesses, locations and events. Combined with specialist expertise and effective international cooperation, these capabilities can help investigators develop new leads, identify links between criminal networks and support coordinated action across borders.

Technology does not replace investigative judgement. Its value lies in helping competent authorities make better-informed decisions, more efficiently and on the basis of verifiable information.



What Technologies Can Help?
Open-source intelligence, or OSINT, is an essential component of modern investigations. It involves collecting, assessing and analysing publicly available information to answer specific investigative questions. Sources can include websites, news reports, publicly accessible social media content, company registers, commercial records and other open sources.

Specialised OSINT tools can help investigators discover relevant information, monitor changes in publicly accessible content and establish connections between apparently unrelated sources. When investigations involve several countries, these capabilities can be particularly valuable for identifying cross-border links, checking identities and aliases, mapping business relationships and understanding how criminal networks use digital platforms.

Another important capability is the analysis of telecommunications records and other electronic traces. Call-detail records and related metadata, where lawfully obtained, can help investigators examine patterns of contact, communication frequency and timing, and relationships between devices or subscribers. When correlated with other investigative information, these records may help establish connections between individuals, events and locations, generate new investigative leads and test existing hypotheses.

The analysis of heterogeneous data is equally important. Link-analysis software can represent relationships between people, companies, accounts and other entities, while timelines and mapping tools can help reconstruct sequences of events and examine geographical connections.

Document-processing and language technologies can assist with extracting relevant information from large datasets and working across different languages.

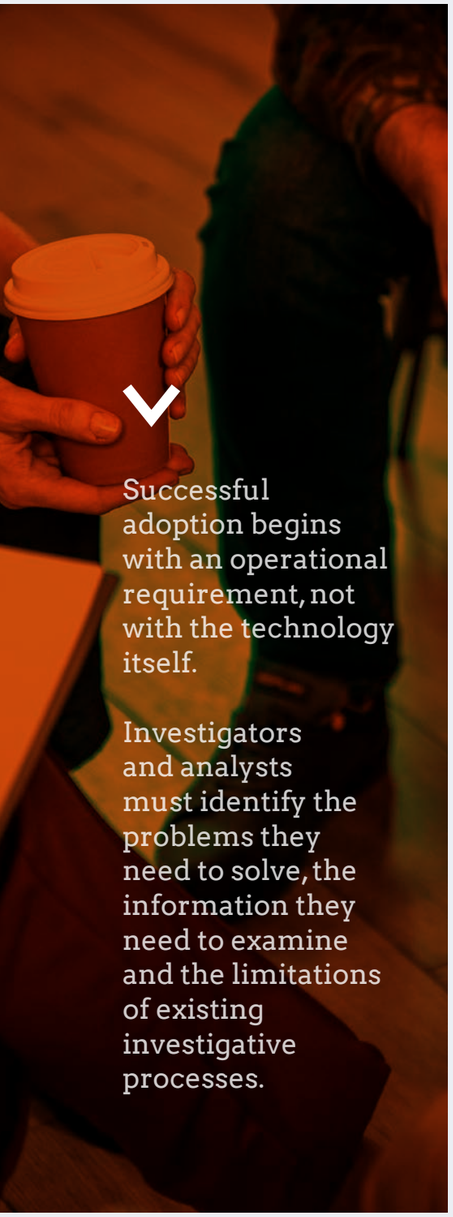
Digital forensics complements these capabilities by supporting the examination of digital devices and data obtained through lawful investigative procedures. Case-management and analytical systems can help organise information from different sources, preserve its provenance and make relevant findings accessible to authorised investigators and prosecutors.

AI may further support selected analytical tasks, but its outputs must be checked against reliable sources and the wider investigative context. An apparent pattern or connection is a lead to assess, not a conclusion to accept automatically.

The greatest value comes from combining these capabilities. OSINT may identify a potential connection, communications analysis may reveal a pattern of contact, and financial or corporate records may provide additional context. Each source contributes a different perspective, allowing investigators to develop a more complete picture of a network operating across physical and digital environments. These groups are particularly effective at building influence at the local level. By investing in businesses and real estate, they can become embedded in local economies and communities. This allows them to exert control without always using visible violence, relying instead on corruption, intimidation and economic dependency. From this position of local influence, they engage in polycrimes – including drug trafficking, human trafficking and money laundering – often in ways that remain largely out of public view.

The New Tools of the Trade: Using Advanced Technologies to Track, Monitor and Disrupt Organised Crime





What Can They Help Investigators Do Internationally?
International investigations often encounter a fundamental obstacle: relevant information is fragmented across countries, agencies, languages and legal systems. A relationship that is difficult to recognise within one national investigation may become apparent when information from several jurisdictions is analysed together.

Advanced analytical tools can help investigators identify these connections and develop a more comprehensive understanding of transnational criminal networks. For example, OSINT findings from one country may be compared with lawfully obtained communications records and company information available to competent authorities in another. This may reveal common associates, overlapping business interests, recurring contacts or links between activities previously investigated as separate events.

Analysis of telecommunications records and other electronic traces can also help investigators develop hypotheses about communication patterns, identify relevant relationships for further examination and establish investigative priorities. When these findings are combined with financial intelligence, digital evidence and information from partner agencies, they can support the reconstruction of a network's structure and the identification of potential organisers, intermediaries and facilitators.

These capabilities are particularly relevant to investigations involving drug trafficking, trafficking in human beings and other forms of organised crime that depend on cross-border logistics, recruitment, financial flows and local support networks.

The operational objective is not simply to exchange more information, but to make the information available to each competent authority more useful. Shared analytical methods, secure information exchange and coordinated investigative planning can help agencies compare findings, identify complementary lines of enquiry and determine where further investigative action may be appropriate.

This approach requires clear safeguards. Information must be obtained and shared in accordance with the applicable legal framework, with appropriate access controls and respect for the powers of each authority. Analytical findings must be independently assessed, and any evidence intended for judicial proceedings must meet the relevant requirements for authenticity, integrity and admissibility.

What Needs To Happen To Put These Technologies Into Use?
Tools must be selected and configured to meet those requirements. Security, reliability, interoperability, data protection, auditability and compatibility with existing systems are all important considerations. Authorities must also plan for maintenance, technical support, updates and the continued development of staff expertise.

Testing and operational evaluation are essential. Pilot activities should establish whether a tool delivers reliable results, improves analytical workflows and helps investigators answer relevant questions. Feedback from practitioners should inform its use and further development.

Training is equally important. Personnel must understand not only how to operate the tools, but also how to interpret their outputs, verify information and recognise analytical limitations. Specialist investigators and analysts need the skills to work with different types of data, while operational teams need to understand how analytical findings can inform investigative decisions.

In international investigations, these requirements extend beyond individual agencies. Partners must develop compatible working methods, agree on appropriate information-sharing procedures and understand the legal and operational constraints under which each authority works. Common training and practical exercises can help build trust, improve interoperability and make joint investigations more effective.

Ultimately, technology delivers its greatest benefit when it is integrated into an operational framework that brings together suitable tools, skilled personnel, clear procedures and effective cooperation.

How Will Phygital-OC Contribute?
Phygital-OC is an EU-funded initiative led by the Central Operational Service of the Italian Ministry of the Interior. Its objective is to strengthen international cooperation and information sharing among law enforcement agencies to help dismantle transnational organised crime networks operating across physical and digital environments.

The project focuses particularly on ethnic mafia-style organised crime groups and their activities across Europe and connected regions, including Latin America and the Caribbean, Africa and the Western Balkans. Its work addresses criminal activities such as drug trafficking and trafficking in human beings, while recognising that these networks can operate across several illicit markets and exploit digital technologies to coordinate their activities.

A central element of Phygital-OC is the establishment and equipping of specialised Operational Rooms in Rome, Athens and Murcia.

These facilities are designed to bring together investigators and analysts, providing them with advanced technological tools and analytical capabilities to support joint investigations and strengthen operational cooperation across national borders.

The technologies and specialist capabilities developed through Phygital-OC can support several complementary activities: gathering and analysing open-source information; examining telecommunications records and electronic traces; correlating information from heterogeneous sources; and identifying relationships that may connect individuals, organisations and activities across national borders.

Their international value lies in enabling investigators to move beyond isolated pieces of information and develop a more connected picture of criminal networks. When the relevant legal conditions are met, analytical findings can inform exchanges between competent authorities, help identify investigative leads and support coordinated work across jurisdictions.

Training is a further pillar of the project. Phygital-OC is developing specialist investigative capabilities through dedicated training modules and practical learning activities. Its international capacity-building work has included training for Libyan law enforcement personnel in OSINT, digital forensics, drone technologies and satellite-based surveillance. The project also aims to strengthen the capabilities of the personnel assigned to its Operational Rooms.

This combination of specialist technology, analytical expertise and international training is essential. Tools can help reveal connections, but skilled investigators must assess their significance, validate findings and determine the appropriate next steps. Shared methods and professional development can also help authorities in different countries work more consistently and exchange information more effectively.

Phygital-OC therefore seeks to strengthen the entire investigative process: from collecting and analysing information to identifying cross-border connections and supporting coordinated action by competent authorities. By connecting technological capabilities with trained personnel and stronger international partnerships, the project aims to help law enforcement respond more effectively to organised crime that operates across both physical and digital worlds.

Vincenzo Fusco is an Inspector at the Italian State Police and project coordinator for Phygital-OC.

FOLLOWING THE DIGITAL TRAIL: HOW AI CONVERSATIONS HELP INVESTIGATORS UNCOVER EVIDENCE

Sandro Liviero
Venice Police

The Forensic Investigations Unit of the Venice Local Police expects to examine around a thousand items of evidence this year.

Specialising in forensic data extraction and the analysis of telephone, internet and IP traffic, the unit supports investigations across the region and beyond, working with public prosecutors' offices and police forces.

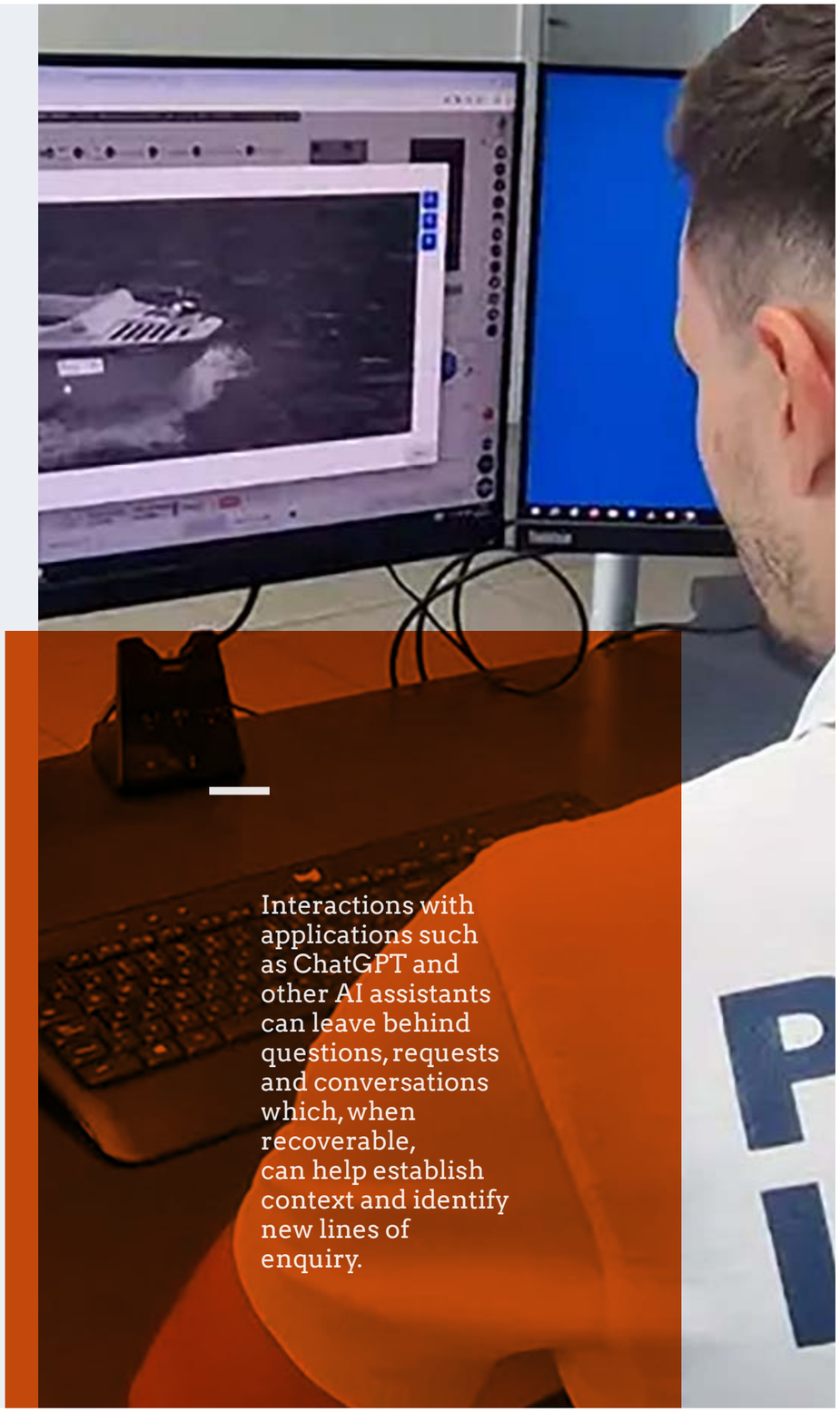
Among the digital traces its analysts examine, conversations with Artificial Intelligence chatbots are opening up new lines of enquiry. Two recent cases illustrate how these exchanges can help investigators uncover hidden evidence.

Smartphones are becoming increasingly difficult to examine. Their security systems are more sophisticated, and users are more aware of the features available to them. That awareness is fuelled by personal curiosity and information shared on social media, including short videos and reels.

For forensic investigators, acquiring data from these devices is becoming increasingly complex. Once that hurdle has been overcome, the analysis begins. At this stage, artificial intelligence can help examine large volumes of information and identify content relevant to an investigation.

Yet AI has another, less obvious role in forensic investigations: conversations between a device's owner and a chatbot can themselves provide valuable investigative leads.

Rather than serving as a tool for analysing data extracted from devices, the traces of AI use become the subject of analysis. Interactions with applications such as ChatGPT and other AI assistants can leave behind questions, requests and conversations which, when recoverable, can help establish context and identify new lines of enquiry.



Interactions with applications such as ChatGPT and other AI assistants can leave behind questions, requests and conversations which, when recoverable, can help establish context and identify new lines of enquiry.

Two cases examined by the Forensic Investigations Unit of the Venice Local Police illustrate this.

In the first, analysts discovered a conversation in which the device's owner had asked a chatbot about the safest way to store images and videos.

Initially, the assistant had suggested storage devices protected by a PIN entered on a physical keypad. When the user objected to the cost, it suggested USB sticks concealed inside small toys, providing a link to a well-known online shopping platform.

An examination of data from the shopping app confirmed an order for two USB sticks of that type. A subsequent search located the devices, allowing investigators to retrieve their contents. These yielded crucial evidence for the investigation, which was also relevant to the decision to keep the suspect in custody pending trial.

Following the digital trail: How AI conversations help investigators uncover evidence

A second case involved a conversation in which the user had asked how to conceal money above a suspended ceiling. The requests included instructions for installing such a ceiling in a small room used for storage within the home.

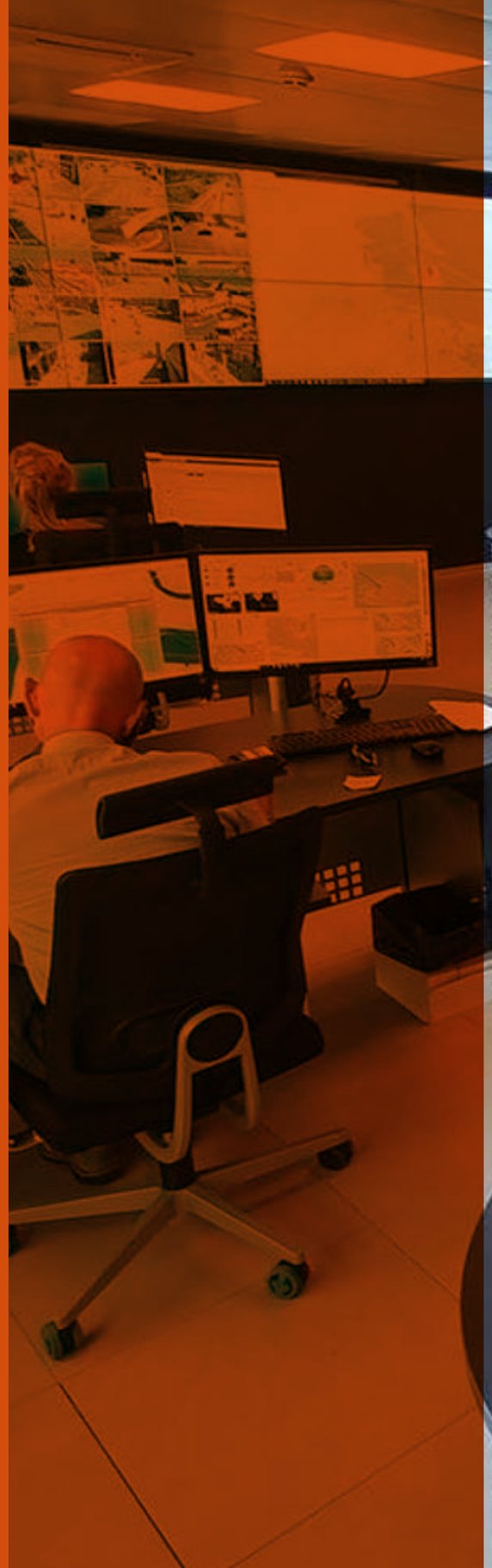
During a more thorough search, investigators identified a difference in ceiling height between that room and the main rooms. Opening up the suspended ceiling revealed the hidden money.

In both cases, the investigative value lay in connecting the recovered conversations with subsequent physical findings.

Such content must always be assessed critically. A question put to a chatbot does not, on its own, establish that something happened or that an intention was acted upon. Its significance emerges when considered alongside the other evidence gathered.

These interactions are now part of the forensic analyst's work: reconstructing events through a careful examination of digital traces in their proper context. As AI assistants become part of everyday life, the traces of those conversations offer investigators further avenues to explore.

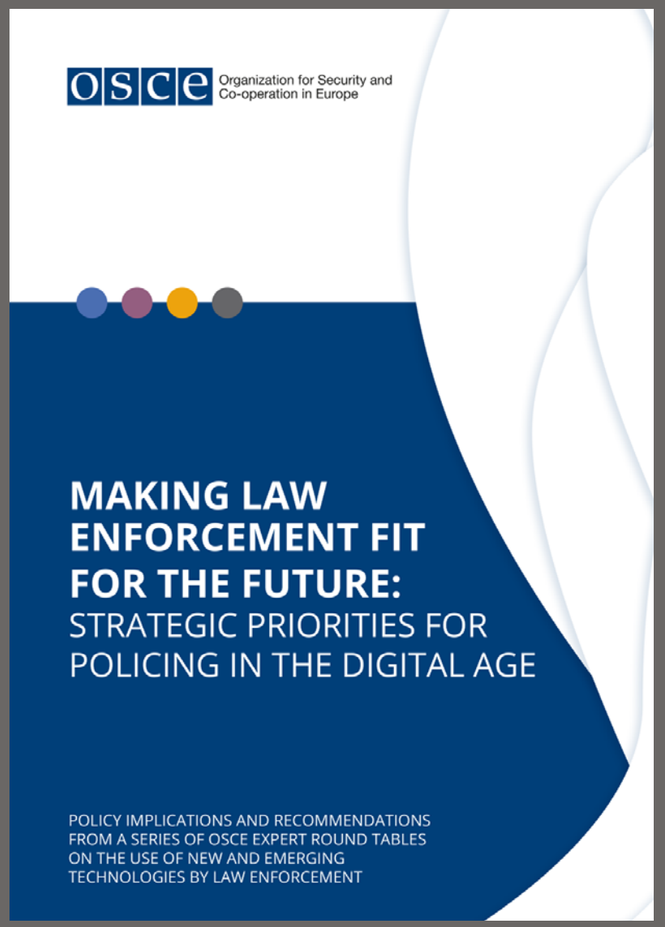
Sandro Liviero heads the Forensic Investigations Unit of the Venice Local Police.





MAKING LAW ENFORCEMENT FIT FOR THE FUTURE: STRATEGIC PRIORITIES FOR POLICING IN THE DIGITAL AGE

Read more...



The rapid evolution of new and emerging technologies is fundamentally reshaping modern law enforcement.

These technologies present both opportunities to make policing more effective and efficient, and significant challenges that demand thoughtful governance, institutional adaptation and frameworks that ensure respect for human rights and fundamental freedoms.

To explore these dynamics, the OSCE Secretariat's Transnational Threats Department/Strategic Police Matters Unit organized a series of four expert roundtable discussions between October 2024 and October 2025. This synthesis paper distils the key findings, shared challenges and common opportunities identified across the four discussions, and outlines potential activities and initiatives through which the OSCE could support its participating States in this domain.

This paper is "intended to serve as a policy-oriented resource for decision-makers, practitioners and international partners seeking to advance the responsible adoption of new and emerging technologies in law enforcement."

A TWO-WAY STREET: LATIN AMERICAN ORGANIZED CRIME GROUPS ARE EXPANDING THEIR PRESENCE IN EUROPE

Daniel Brombacher
GI-TOC

On 15 July 2026, German authorities dismantled[1] a methamphetamine laboratory in Ludwigsfelde, a small city in the state of Brandenburg, around 10 kilometres south of Berlin. With a population of around 30 000, this city had not previously been a significant location on the global organized crime map. However, police arrested three Mexican nationals at the drug-production site, pointing to the international links of the local criminal network that ran the operation.

This is not the first time that Mexican nationals have been found at drug production sites in Europe. Between 2019 and 2020, a total of 19 Mexican meth 'cooks' were arrested[2] in raids on methamphetamine laboratories in the Netherlands and Belgium. The expansion of Mexican organized crime groups into Europe was documented in a joint report[3] by the US Drug Enforcement Agency and Europol in 2022. And in 2025, authorities dismantled a synthetic drug laboratory in Marseille with alleged ties to the Sinaloa cartel[4], while in the same year four Mexican citizens were arrested[5] in Poland in connection with a methamphetamine laboratory.

Europe Now As A Destination

As early as the 1980s, Spain[6] was used by Colombian drug traffickers as a safe haven from which to build relationships with local criminal networks. Mexican organized crime groups allegedly began establishing[7] a foothold in European drug markets in the late 1990s and early noughties. However, they primarily used Europe as a transit[8] region to supply drug markets farther east[9].

But this limited scope of Latin American criminal operations in Europe appears to be undergoing fundamental changes.

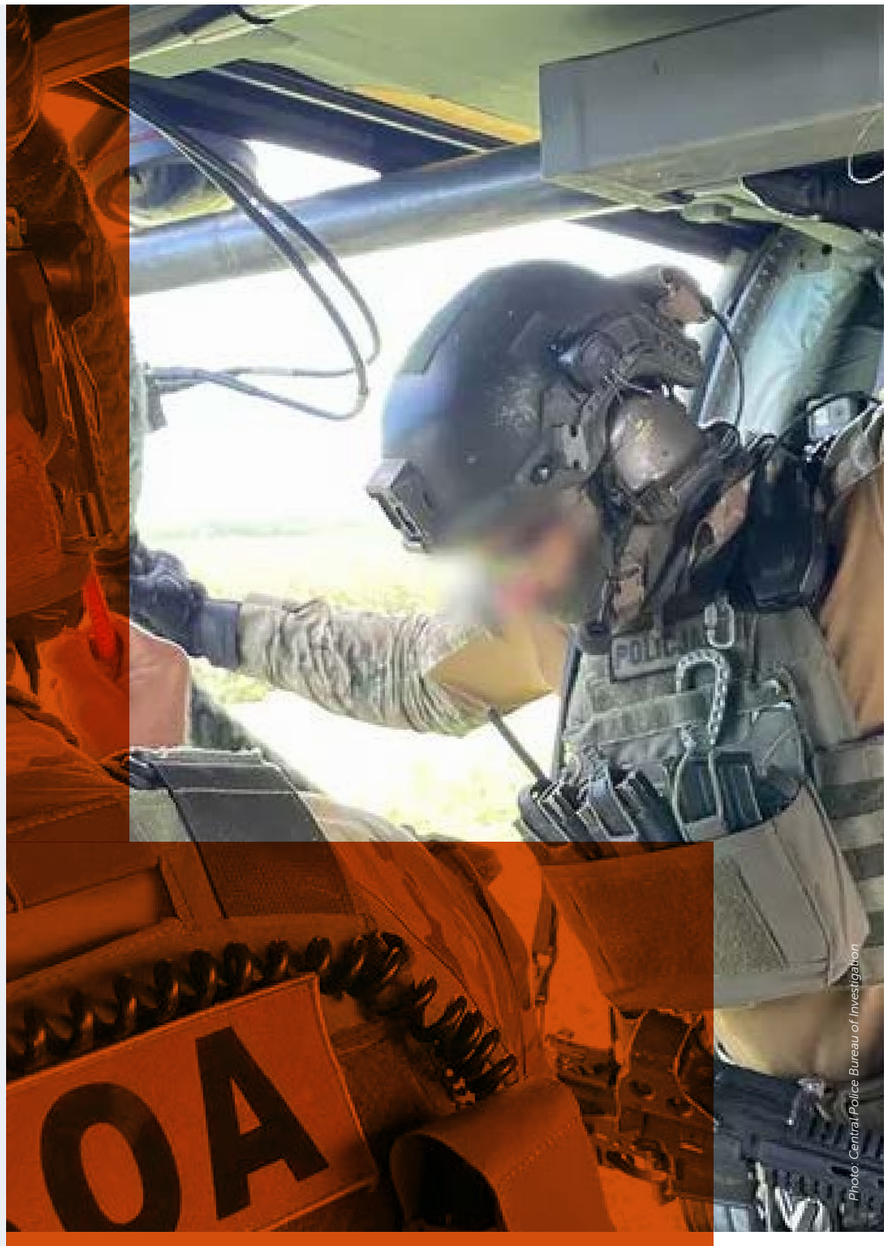


Photo: Central Police Bureau of Investigation

While Spain was long the European gateway for criminal networks from the region, some groups have expanded towards Central and Eastern Europe, with Romania[10] and Bulgaria reportedly becoming key hubs. The CJNG and the Sinaloa cartel have built up local networks[11] in these countries[12], which are strategically positioned along the Balkan route, one of Europe's principal drug trafficking corridors.

This goes hand in hand with a new level of threat: Europe is no longer merely a transit hub for Latin American criminal actors or a destination for criminal specialists such as methamphetamine chemists. There are growing signs that Latin American criminal groups are establishing operational hubs in Europe to exploit the continent's diverse criminal revenue opportunities.

Given the United States' increased pressure on Latin American organized crime groups and the region's widespread return to more heavy-handed responses to organized crime[13], the enhanced European operations of Latin American criminals may be[14] a direct consequence of their shrinking spaces in the Americas. Although the 2025 US designation of Latin American organized crime groups as foreign terrorist organizations has had little impact[15] on criminal behaviour in the region, Europe may have become less risky for some criminal activities, such as money laundering and other private-sector related activities. Relocating parts of their operations to Europe reduces risk and enables expansion into a thriving criminal ecosystem in which Latin American expertise and networks are often welcomed by European counterparts.

References

1. berlin.de
2. dw.com
3. europol.europa.eu
4. europol.europa.eu
5. polskieradio.pl
6. insightcrime.org
7. brookings.edu
8. europol.europa.eu
9. insightcrime.org
10. milenio.com
11. businessinsider.com
12. brookings.edu
13. theconversation.com
14. washingtontimes.com
15. globalinitiative.net

A two-way street: Latin American organized crime groups are expanding their presence in Europe



Photo: PAP/Artur Reszko

There are already signs of organized crime groups on both sides of the Atlantic learning from each other, and crime-as-a-service models have become a key driver in building new networks between Latin American and European criminal groups.

A Widening Criminal Footprint

Mexican criminal organizations have reportedly[16] moved beyond producing methamphetamine, forming partnerships with a wide range of domestic criminal networks in the lucrative cocaine market. Although Colombian networks still play a decisive role in supplying Europe with cocaine, Mexican groups such as the Jalisco New Generation Cartel (CJNG) have increased[17] their involvement in Spain's cocaine trade while remaining active in the methamphetamine market, as recent arrests[18] in Catalonia show.

But their involvement in European criminal markets goes beyond drugs. In August 2026, four alleged CJNG members were arrested[19] in Prague for reportedly seeking to procure military-style weapons. Similarly, in April 2025, Spain extradited a Bulgarian national to the United States who had been charged[20] with conspiracy to supply military-grade weapons to the CJNG.

Criminal actors from other Latin American countries are also becoming increasingly active in Europe. In 2021, Spanish authorities arrested[21] 'Pipo' Chavarría, the leader of the Ecuadorian gang Los Lobos, in Málaga, where he had been hiding after faking his own death. In November 2025, Portuguese authorities arrested[22] 'Hulk', a leading figure in the Brazilian organized crime group Primeiro Comando da Capital (PCC), which is believed to have a substantial presence[23] in Portugal. Also in November 2025, Spanish authorities dismantled[24] a local chapter of the Venezuelan gang Tren de Aragua in Barcelona and several other Spanish cities.

The previous year, authorities in Barcelona detained[25] the brother of Tren de Aragua leader Héctor 'Niño' Guerrero, who was killed[26] in a joint US–Venezuelan operation in June 2026.

While the European expansion of Los Lobos, the PCC and Tren de Aragua still appears to be focused on Spain and Portugal, the same was originally true for other Latin American networks that subsequently integrated into European criminal ecosystems. The European organized crime landscape is highly fragmented and, with a few exceptions, is characterized by relatively flat structures and fluid networks. This makes it easier for external groups to integrate into lucrative local markets.

There are already signs of organized crime groups on both sides of the Atlantic learning from each other, and crime-as-a-service models have become a key driver in building new networks between Latin American and European criminal groups, for example in the synthetic drugs and cocaine markets. Criminal groups in Mexico have a long trajectory of increasing expertise in drug production and are generally quick adapters and learners.

The tendency of some Latin American organized crime groups to use violence to control and access markets could contribute to the growing trend[27] of drug-related violence in Europe. While much attention has recently been paid to the expansion[28] of European organized crime groups into Latin America, this trend now appears to be unfolding in reverse, exposing Europe to an additional criminal challenge in an already complicated threat landscape.

The geopolitical effects of the United States' clampdown on Latin American organized crime groups, coupled with heavy-handed responses to crime in Latin America, are likely to be felt even more strongly in Europe in the years ahead.

Europe must therefore remain vigilant and strengthen its resilience to the displacement of criminal activity from the Western Hemisphere.

Daniel Brombacher is the Director of the Europe Observatory for the Global Initiative Against Transnational Organised Crime, a partner on the Phygital-OC project. The article was first published by GI-TOC[29].

References

16. brookings.edu
17. agendapublica.es
18. interior.gob.es
19. cbsnews.com
20. globalinitiative.net
21. elpais.com
22. euronews.com
23. smallwarsjournal.com
24. interior.gob.es
25. interior.gob.es
26. globalinitiative.net
27. globalinitiative.net
28. rosalux.org.ec
29. globalinitiative.net

ON THE FRONTLINE... GLORIA GILARDONI

Helping Survivors of Trafficking Rebuild Their Lives.

Gloria is a project coordinator at C.A.T. Cooperativa Sociale, a Florence-based social cooperative NGO which supports survivors of human trafficking in Italy.

From what you see on the ground, how is the problem of human trafficking evolving?
In my experience as a social worker and anthropologist tackling human trafficking and smuggling, what stands out is how quickly traffickers adopt new methods. New technologies and artificial intelligence have transformed the problem and reshaped traditional harm-reduction work. Trafficking is increasingly facilitated by digital technology.

What changes in the way criminal groups recruit, control and exploit people concern you most?
The rapid shift of recruitment, control and exploitation into digital environments, particularly in sexual exploitation.

Criminal groups use social media, encrypted messaging apps and deceptive job advertisements to reach vulnerable people while remaining anonymous and reducing the risk of detection.

Control no longer relies solely on physical presence or force. It also involves constant tracking, taking over social media accounts, threatening to share intimate material without consent, or using digital payment platforms to deny people control over their own money. Prostitution and exploitation have moved from the streets into private apartments advertised on dedicated websites, alongside entirely online forms of exploitation, such as forced webcam performances.

For street outreach teams and protection services, this shift presents an enormous challenge. Without a physical point of contact, reaching potential victims, recognising signs of distress and building the trust needed to help someone disclose their situation and reach safety have become extremely difficult.

Are frontline services equipped to identify exploitation and respond? Where are the biggest gaps?
Frontline services have considerable experience and dedication, but are not fully equipped for this shift. The main difficulty is reaching people: traditional street outreach is less effective when exploitation moves online or into private premises.

The biggest gaps include insufficient training in digital outreach, including virtual outreach teams, online monitoring and tools to identify requests for help on social networks or messaging apps.



Formal victim identification and access to protection often take longer than the urgent action needed to bring someone to safety. Services are also frequently understaffed, with limited budgets restricting investment in new technologies, specialist training, language skills and cultural knowledge.

While sexual exploitation has historically been more widely recognised, there are still considerable difficulties in promptly identifying hidden labour exploitation, forced begging and exploitation within related illegal activities.

What helps people escape exploitation, and what can prevent them from reaching safety?
Escaping exploitation requires secure legal status, social and economic inclusion, and the means to live independently.

A valid residence permit is fundamental, alongside access to civil rights, healthcare, housing, psychological support and legal assistance. Regular, fairly paid employment is crucial to financial independence.

Conversely, insecure immigration status is a major barrier to safety. Traffickers repeatedly use it to threaten people and discourage them from reporting abuse or approaching the police. Language and cultural barriers deepen isolation, preventing people from understanding their rights or communicating with the outside world.

What does it take to help someone rebuild their life after exploitation?
Helping someone rebuild their life requires long-term support that extends well beyond the initial emergency.
The foundation is helping people regain control over their lives in two parallel ways: economic independence, through training, language learning and decent employment; and emotional independence.

Specialist, ongoing psychological support to process trauma is essential. It helps people overcome psychological dependence, rebuild self-esteem and address the deep emotional wounds left by violence. A strong local social and community network is also vital. Building healthy relationships and a sense of belonging, beyond support services and away from isolation, enables people to reclaim their future and avoid becoming trapped in exploitation again.

Where are survivors being let down by the systems meant to protect them?
Survivors are particularly let down when bureaucracy and fragmented services delay their reintegration. The main problem is the slow issuing and renewal of residence permits and other documents. This leaves people in legal and financial limbo, preventing them from accessing regular employment and basic services.

For particularly vulnerable groups, including trans women and sex workers, social stigma and systemic discrimination create barriers that are often almost impossible to overcome. These can prevent timely and meaningful access to employment, even when someone is already receiving protection and support.

Which partnerships make the biggest difference to the people you support?
Each person's route out of exploitation must reflect their needs and pace. Consistent, constructive dialogue with provincial police headquarters and the territorial commissions responsible for assessing asylum claims is essential to navigating immigration procedures, which still take far too long. Relationships within our local communities are equally important. They help challenge prejudice and create real opportunities for integration and employment.

I coordinate accommodation for cis and trans women in a mountain village. Every day, I see the difference partnerships with local businesses make. They build practical connections and provide genuine employment opportunities.

What would help agencies and organisations work together more effectively, from first contact through to long-term support?
Shared operational protocols and direct communication between voluntary organisations, provincial police headquarters and local services would help overcome bureaucratic delays.

Joint training and regular meetings would build common understanding, coordinate responses to complex cases and ensure continuous support.

How can survivors have a stronger voice in shaping the response?
The first essential step is to recognise survivors fully as people with social and civil rights and as full members of society, creating the conditions for meaningful participation. This means involving survivors as advisers with lived experience in designing services, developing peer-support programmes and ensuring their direct participation in the institutional forums where policies and responses are decided.

What more needs to be done, and what support would help?
We need sustained, multi-year funding that moves beyond fragmented projects and allows for long-term planning.

Organisations like ours need ongoing support for specialist staff training, dedicated resources to help people access employment and live independently, and simpler administrative procedures.

Easier cooperation with institutions would free us to focus on supporting people and building local networks.

ITALY'S STRONGEST WEAPON AGAINST THE MAFIA IS ITS CIVIL SOCIETY

Ruggero Scaturro
GI-TOC



For much of the world's imagination, Italy's fight against organized crime is embodied by courageous prosecutors, dramatic police raids and the names of anti-mafia heroes such as Giovanni Falcone and Paolo Borsellino.

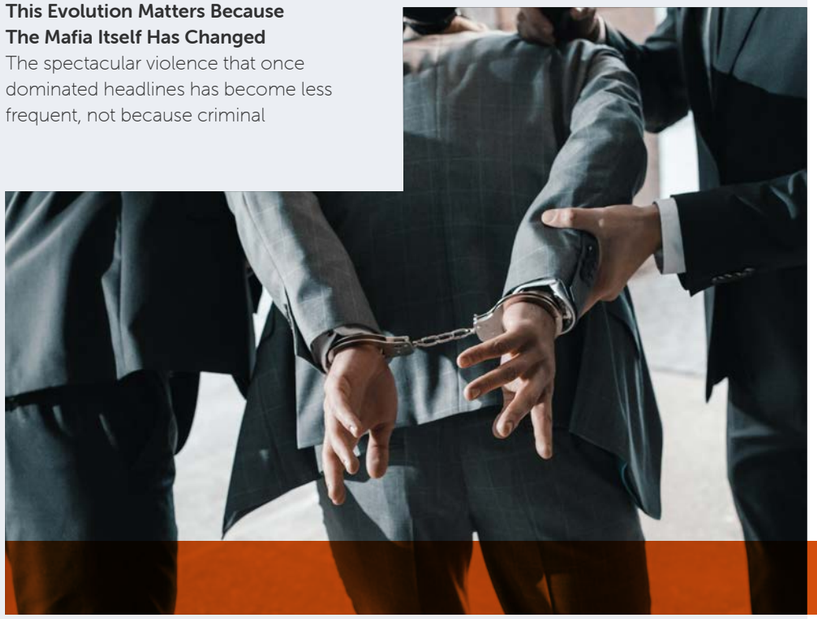
These remain essential symbols of the country's struggle against criminal power. Yet they tell only part of the story.

Over the past three decades, Italy has built something arguably more remarkable: a resilient civil society that has become one of the country's most effective defences against organized crime. While criminal organizations continue to evolve, infiltrating legitimate markets and exploiting globalization, Italian citizens, associations, journalists, entrepreneurs and educators have increasingly transformed anti-mafia action from a law-enforcement mission into a broader democratic project.

This Evolution Matters Because The Mafia Itself Has Changed

The spectacular violence that once dominated headlines has become less frequent, not because criminal organizations have weakened, but because many have become more sophisticated. Today's mafia groups derive much of their power not from bombs and assassinations, but from their ability to infiltrate public procurement, logistics, construction, waste management, financial services and international trade. Increasingly, they operate as business enterprises embedded within the legal economy while maintaining strategic alliances with foreign criminal networks.[1]

The latest assessments by Italian authorities show that traditional rivalries between mafia organizations are increasingly giving way to pragmatic cooperation.[2] Rather than competing over territory alone, criminal groups collaborate where it serves mutual economic interests, particularly in drug trafficking, money laundering and public contracts. This transformation makes organized crime less visible but no less dangerous.



Law enforcement remains indispensable in confronting these threats. Italy's anti-mafia institutions are among the most advanced in the world, combining specialized prosecutors, preventive measures, witness protection programmes and one of the most extensive systems for confiscating criminal assets. Major operations continue to demonstrate the state's capacity to dismantle criminal structures, including the large-scale operation against Cosa Nostra in Palermo in early 2025, which highlighted both the resilience and the continued adaptability of Sicily's historic mafia.[3] Yet every successful investigation also reminds us that arrests alone cannot eradicate the social and economic conditions that allow organized crime to regenerate.

Recent Events Illustrate This Uncomfortable Reality

In 2024, the death of Indian farm worker Satnam Singh shocked Italy after he was abandoned by his employer following a devastating workplace injury.[4] Barely two years later, four Pakistani agricultural workers were killed in Calabria in what investigators believe was retaliation linked to labour exploitation networks.[5] These tragedies were not isolated acts of violence but manifestations of criminal systems that continue to exploit vulnerable workers, particularly migrants employed in sectors where legality, labour rights and organized crime intersect.

It Is Precisely Here That Civil Society Has Become Indispensable

Organizations such as Libera have transformed confiscated mafia assets into schools, farms, cooperatives and community centres, demonstrating that territories once controlled by criminal organizations can be returned to the public.[6] Across Italy, teachers integrate anti-mafia education into classrooms, journalists continue investigating criminal infiltration despite intimidation, and local associations monitor public spending and procurement. Cultural initiatives such as the fifteenth edition of the Trame Festival in Lamezia Terme—dedicated in 2026—further demonstrate how civic engagement, public debate and collective memory remain central components of Italy's anti-mafia movement.
These initiatives do more than raise awareness; they reduce the social legitimacy upon which organized crime ultimately depends.[7]

Perhaps the greatest achievement of the Italian anti-mafia movement has been changing public expectations. In previous generations, silence, resignation or accommodation often characterised the relationship between communities and criminal organizations.


Photo: libera.it

Today, in many parts of the country, citizens increasingly expect transparency, accountability and institutional integrity. This cultural transformation cannot be measured through arrest statistics, yet it may represent one of Italy's most significant long-term victories.

Italy's strongest weapon against the mafia is its civil society



None Of This Means The Battle Has Been Won

Digital technologies, online financial services, encrypted communications and increasingly global criminal supply chains have expanded the opportunities available to organized crime. Criminal organizations have become more entrepreneurial, less hierarchical and more internationally connected. At the same time, corruption, labour exploitation and environmental crime continue to provide profitable opportunities for criminal infiltration even where traditional mafia violence is absent.

These developments require resilience to evolve as well. Civil society can no longer focus exclusively on opposing traditional mafia organizations; it must also strengthen democratic institutions against corruption, protect investigative journalism, promote transparency in public procurement and defend vulnerable communities from exploitation.

Resilience today means safeguarding not only communities from organized crime, but also the integrity of democratic governance itself.

Italy's experience offers an important lesson far beyond its borders. Every country confronting organized crime tends to invest in stronger policing, tougher legislation and enhanced intelligence capabilities. These are all necessary.

Italy demonstrates that lasting success depends equally on citizens who refuse to normalize criminal influence in everyday life.

The country's most enduring anti-mafia innovation is therefore not a particular law or investigative technique. It is the emergence of a society that increasingly recognizes that organized crime is not simply a criminal justice problem but a democratic challenge requiring collective responsibility.

That lesson has never been more relevant than it is today.

Ruggero Scaturro is a Senior Analyst at the Global Initiative against Transnational Organized Crime (GI-TOC), a partner on Phygital-OC.

References

1. *Europol, The Changing DNA of Serious and Organised Crime, 2025.*
2. *Direzione Investigativa Antimafia (DIA), Relazioni semestrali, Italian Ministry of the Interior, accessed 7 July 2026.*
3. *Ruggero Scaturro, Palermo strikes back, GI-TOC, 27 February 2025.*
4. *Romolo Tosiani and Alvise Armellini, Death of Indian labourer highlights... , Reuters, 20 June 2024.*
5. *Reuters, Deadly attack on migrants highlights issue of labour abuse in Italy, 3 June 2026.*
6. *libera.it*
7. *tramefestival.it*

Dismantling Organised Crime
In Physical and Digital Environments
powered by phygital-oc
Alliance



Connecting Efforts Against Organised Crime

Criminal groups operate across borders, form multinational networks, engage in multiple forms of crime and exploit digital technologies. Responding requires the knowledge and capabilities of many different organisations, and stronger connections between them.

Planned for launch in early 2027, the Dismantling Organised Crime Alliance (DOC Alliance) will bring together organisations across Europe working to prevent, detect and dismantle organised crime. It will connect law enforcement and judicial authorities, civil society, researchers, policymakers and the private sector. The aim is to bridge silos between professional communities, strengthen existing efforts and support cooperation beyond the life of individual projects.

The idea grew out of Phygital-OC, an EU-funded project working to strengthen responses to organised crime across physical and digital environments. Through exchanges with other EU-funded projects, we found a shared appetite for closer connections and more lasting collaboration. The Alliance will build on that interest, connecting networks and initiatives that may have limited opportunities to work together.

It will provide a space for members to share insights, learn from one another and identify opportunities for practical cooperation. Regular online exchanges and informal networking will help build relationships across sectors.
Initial activities could include sharing observations on emerging threats and bringing practitioners, researchers and technology providers together to develop and test solutions. Members will help shape these priorities.

Ahead of the launch, we are inviting established networks and organisations to help develop the Alliance and identify others who could contribute. We want to connect those conducting investigations and developing new tools with those preventing recruitment, supporting victims and building resilience in communities.

By bringing these perspectives together, the Alliance aims to build a lasting community that supports its members' work and creates opportunities for cooperation across sectors and borders.

To find out more or express an interest in joining

Contact:

info@phygital-project.eu

Phygital-OC Alliance

FIVE KINDS OF NOTHING: DIAGNOSING EVIDENCE GAPS WHEN ANALYSING EMERGING CRIMINAL THREATS

How do you respond to a criminal threat when you do not yet have sufficient data to understand it?

Fook Nederveen
Shann Corbett
RAND

When a police cybercrime unit set out to profile the Eastern European and Russian hackers behind a wave of ransomware attacks, investigators ran into a familiar problem. There is no shortage of information about the attacks themselves, the victims, or the tools used. What is missing is the people: the offenders who got away leave almost no trace in any official record, frustrating the police response.

As organised crime policy researchers, we are often asked to study such emerging threats: cases where law enforcement or policymakers have picked up a signal - a new criminal tactic, set of targets, or way of operating - but lack the evidence base needed to properly understand or tackle new threats.

The reflexive answer is always "we need more data." But that is not always possible, and often not even true. Instead, it is worth starting with a blunter question: what kind of 'nothing' do we have? The absence of evidence has more than one cause, and each cause points to a different response.

Some threats are simply too new to register. The criminal activity may already be occurring, but not for long enough, or at sufficient volume, to have left a trace in anyone's records; a reporting field or an offence code must exist before anything can be counted. At RAND Europe, for example, we are currently studying gold tokens for the UK's Foreign, Commonwealth & Development Office - an emerging crypto-asset class that links the physical scarcity of bullion to the reach of a blockchain. The market remains small but is expanding, and many of the basic indicators needed to understand its risk of criminal misuse have not yet been created.

In other cases, nobody has been tasked to look. In our research into the Dutch government's approach to human trafficking, we found that priorities, capacity and ways of working vary so much between regions that no coherent national picture of the problem exists, even though the activity itself is well documented. A related version of this gap shows up when an entire market moves faster than anyone has been assigned to watch it; new psychoactive substances, for instance, can appear and spread before monitoring or regulatory systems catch up. What looks like a sudden new threat is sometimes simply a shift in where attention happens to be pointed.

Other threats are structurally hard to detect, because opacity is the whole point of the method. Cybercrime is the clearest example. In a RAND study of organised cybercriminals from Eastern Europe, we found that the evidence base depends almost entirely on the minority of offenders who have been identified, investigated, or exposed through leaked internal communications. Offenders who avoid all three are invisible to the people trying to study them.

The opposite problem also exists: good data, but no recognition that it constitutes a problem. We encountered this studying the sudden rise of poor-quality counterfeit banknotes carrying inconspicuous disclaimers that they are fake, sold openly on e-commerce sites and advertised on social media. Every one of these notes used in legitimate transactions eventually passes through a point in the cash cycle where it gets checked, so the scale of the problem is known with real precision. What is missing is not data but the shared understanding that passing off a note that does not meet central banking rules as currency is counterfeiting, and should be prosecuted as such.

Finally, a threat can simply be rare. Criminals sometimes have cheaper or less risky ways of reaching the same outcome, and the apparent gap in evidence reflects nothing more than low volume.

Each of these gaps in police and policy understanding of the changing patterns of criminality calls for a different fix. A genuinely new threat needs a baseline: one or two indicators that can signal growth in scale or a change in form, with clear ownership of who monitors them and what triggers a response. An overlooked threat needs administrative repair - reporting requirements, clear ownership, better coordination among the people who should already be watching - not more data collection. A structurally opaque threat calls for triangulating every unconventional source, from service-provider data and offender-generated material to arrest records and expert elicitation. A threat that is recorded but not recognised needs someone to trace where cases fall out of the pipeline between detection and conviction, and why. And a threat that looks rare should be treated as such until researchers can document the search and explain why offenders would choose a different method.

None of this tells police or policymakers the full nature of the threat in front of them. What it does is tell them which questions are worth asking, and which interventions are worth recommending.

Fook Nederveen and Shann Corbett are policy researchers at RAND Europe, a nonprofit, nonpartisan research institute.

RAND Europe is not a partner in the Phygital-OC Alliance; the authors write here as independent researchers whose recent work for European government clients - including the UK Foreign, Commonwealth & Development Office and the Dutch Ministry of Justice and Security - spans several of the evidence gaps described above.





In a landscape where criminal activity increasingly moves across the same physical and digital seams that make it hard to track activity in the first place - what this magazine has termed "phygital" crime - that diagnostic step is not a delay before the real work starts. It is the real work.



EUCPN-ENAA: PREVENTING YOUTH RECRUITMENT INTO ORGANISED CRIME: FROM EUROPEAN KNOWLEDGE TO LOCAL PRACTICE



Maxime Hennen
EUCPN

Across Europe, the involvement of children and young people in organised crime has become an increasing concern for policymakers, law enforcement and professionals working with young people.

Reports from several countries point to their participation in activities ranging from drug distribution and violence to other forms of criminal exploitation.

Against this backdrop, the European Crime Prevention Network (EUCPN) and the European Network on the Administrative Approach (ENAA) are bringing together knowledge and promising practices from across the European Union to strengthen the prevention of youth recruitment into organised crime. Its work highlights a range of approaches that can help practitioners intervene earlier, while recognising that different countries and communities require different responses.

Understanding The Recruitment Process

Understanding why and how young people are recruited is an essential starting point for prevention. Organised crime groups can offer financial rewards, social status, excitement or a sense of belonging. For young people facing exclusion, instability at home or limited work or educational opportunities, these promises may be particularly attractive.

Recruitment does not follow one single pathway. It may be facilitated by existing relationships. Family members, friends or peers may introduce young people to criminal networks, making criminal activity appear normal or necessary. Online platforms can expand the reach of recruiters, allowing them to contact young people beyond their immediate social environment. Online recruitment should not, however, be considered separately from offline realities. Online contact may be the final step in a process that begins with social or economic vulnerabilities.

Young people may actively seek involvement in criminal activity, but they may also be drawn into it through grooming, coercion, threats or debt bondage. It is therefore important not to view young people involved in organised crime solely as offenders: they may also be victims of exploitation, even where their involvement initially appears voluntary.

There is therefore no single profile of a recruited young person and no single intervention that can prevent recruitment on its own.

From Knowledge To Prevention

Traditional criminal justice responses often intervene after recruitment or offending has already taken place. Preventing recruitment requires to act early, by reducing vulnerabilities, strengthening protective factors and creating credible alternatives to organised crime.

One of the EUCPN's latest outputs is a practical toolkit[1] on the recruitment of young people, highlighting a range of prevention approaches, reflecting the different pathways into organised crime and the different levels at which intervention may be needed.

Community-based prevention can help identify vulnerabilities early and strengthen relationships between young people and the people and institutions around them. Schools, youth workers, local authorities, community organisations and the police can all contribute to creating safe environments and improving access to support. The French LIMITS project, for example, illustrates how different actors can be brought together, with interventions adapted to local circumstances.

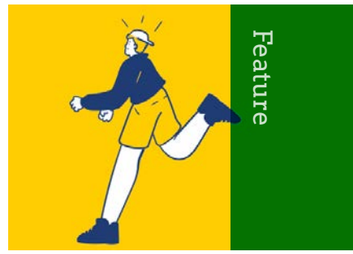
Family support is another important element. Families can be both risk and protective factors. Conflict, instability or other pressures can increase a young person's vulnerability, while supportive family relationships can provide protection against the influence of criminal networks. Family-based interventions therefore aim to strengthen communication, guidance and support within the family.





Traditional criminal justice responses often intervene after recruitment or offending has already taken place. Preventing recruitment requires to act early, by reducing vulnerabilities, strengthening protective factors and creating credible alternatives to organised crime.

EUCPN-ENAA: Preventing youth recruitment into organised crime: From European knowledge to local practice



For young people already involved in, or at risk of becoming involved in, criminal activity, diversion and alternatives to traditional criminal justice responses can offer a different pathway. These approaches may include mentoring, education, employment support, training, positive activities and engagement with trusted professionals. Their purpose is not simply to avoid punishment. They should also address the needs that organised crime exploits, such as the need for income, recognition, identity and belonging. In Ireland, youth diversion initiatives, including the work of Foróige, illustrate how early intervention and structured support can provide alternatives to continued involvement in crime.

Focused deterrence may be appropriate for young people facing a particularly high risk of serious violence or organised criminal involvement. These approaches combine clear communication about the consequences of continued offending with support and opportunities to exit criminal activity. The Group Violence Intervention approach in Sweden illustrates how targeted deterrence can be combined with support and cooperation between relevant actors.



The online environment also requires attention. Social media and other platforms can give recruiters access to young people beyond their immediate social environment and may be used to facilitate contact, grooming or the promotion of criminal lifestyles. Prevention can therefore include digital awareness, cooperation with platforms and action against harmful recruitment content. However, online measures should be connected to offline support: removing content or disrupting online contact will not, by itself, address the vulnerabilities that make recruitment possible.

The Importance Of Cooperation

Preventing youth recruitment requires cooperation beyond the criminal justice system. No single organisation is likely to have all the information, resources or relationships needed to respond effectively. Schools, youth workers, social services, police and local authorities may each see a different part of the picture.

Coordinated action and appropriate information-sharing can help professionals identify risks earlier and avoid fragmented responses. The administrative approach can complement these preventive efforts by addressing the environments and legitimate structures that organised crime seeks to exploit.

This multi-agency perspective is central to EUCPN–ENAA's work. By bringing together expertise from crime prevention and the administrative approach, the networks look beyond individual interventions to the wider conditions in which organised crime can recruit and operate.

Turning Knowledge Into Action

The EUCPN–ENAA project brings together knowledge and promising practices from across the European Union and translates them into practical resources for practitioners. Since Member States have different legal frameworks, institutional structures and local realities, the project does not promote a single model to be copied. Instead, it supports practitioners in understanding different approaches and adapting relevant lessons to their own context.

By sharing knowledge, examining what works and supporting the implementation of evidence-based practices, EUCPN–ENAA helps connect European experience with prevention at national and local level.

The objective is to strengthen the capacity of professionals and communities to intervene earlier and reduce vulnerabilities.

Ultimately, preventing youth involvement in organised crime is not only about disrupting recruitment. It is about offering young people meaningful alternatives for belonging, identity and purpose.

About EUCPN[2] And ENAA[3]

The European Crime Prevention Network (EUCPN) promotes evidence-based knowledge and practices in crime prevention, improves the effectiveness of prevention activities, and serves as a first point of contact for crime prevention expertise.

The European Network on the Administrative Approach (ENAA) strengthens understanding of the administrative approach and promotes its application across the European Union, at both national and European levels.

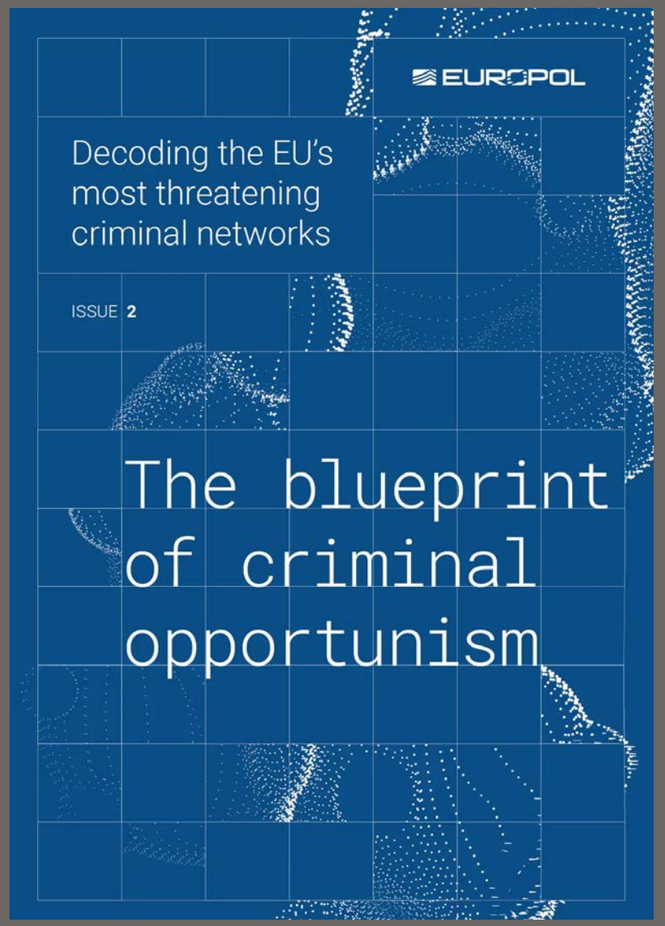
Both networks conduct research, provide training, organise activities such as field visits and facilitate cooperation among actors in the field.

References

1. eucpn.org
2. eucpn.org
3. administrativeapproach.eu

THE BLUEPRINT OF CRIMINAL OPPORTUNISM: DECODING THE EU'S MOST THREATENING CRIMINAL NETWORKS ISSUE 2

Read more...



Europol's latest assessment explores how Europe's most threatening criminal networks operate, adapt and exploit new opportunities.

Building on its 2024 report, the paper examines their activities, connections and use of digital technologies, alongside the financial systems and legitimate businesses that help them conceal their operations and reinvest criminal profits.

The report shows why disrupting individual groups does not necessarily remove the wider threat. Criminal networks operate within interconnected systems that allow them to cooperate, replace lost capabilities and rebuild. Digital platforms, encrypted communications and artificial intelligence are helping them expand their activities while reducing their exposure to law enforcement.

The findings underline the need for a response that tackles both criminal networks and the opportunities that sustain them. This means stronger cooperation between law enforcement, public authorities and the private sector, investment in investigative tools, and preventive action to address the weaknesses criminals exploit.

DISRUPTING YOUTH RECRUITMENT INTO ORGANIZED CRIME

Read more...

This paper explores how to prevent young people from being recruited into organised crime

drawing on insights from policymakers and practitioners across South-Eastern Europe, Latin America and the Caribbean. It highlights the recruitment of increasingly young children and the use of social media to promote criminal lifestyles, exploit vulnerabilities and draw young people into serious crime.

The recommendations emphasise the need to act early, with support tailored to each child's circumstances. Closer cooperation between law enforcement, schools, social services and child protection, supported by joint training, can help practitioners identify risks and intervene sooner.

The paper also calls for stronger public-private partnerships: working with social media platforms to disrupt online recruitment, and with businesses to provide training and employment opportunities for vulnerable young people. Greater cooperation across borders, credible voices challenging the glamorisation of crime, and sustained support for children and families are central to the response.



WHAT CAN STRATEGIC COMMUNICATIONS BRING TO THE FIGHT AGAINST ORGANISED CRIME?





An organised crime ecosystem can involve many different actors: criminal groups and their facilitators; people vulnerable to recruitment or exploitation; consumers of illicit goods and services; businesses and professionals who may knowingly or unknowingly enable activity; and communities affected by criminality.

Jonathan Benjamin
REOC

Lessons and opportunities from P/CVE, behaviour change and other complex security challenges.

Organised crime is constantly evolving. Criminal networks operate across borders, exploit new technologies and adapt their methods in response to enforcement. Increasingly, their activities also move fluidly between physical and digital environments.

Responding to that complexity requires an equally broad range of capabilities: law enforcement, intelligence, technology, international cooperation, prevention and engagement with affected communities.

There is also an interesting opportunity to consider what lessons strategic communications and behavioural approaches can bring to this wider toolkit.

At REOC, much of our work over the past decade has involved communications in complex security and policy environments, including preventing and countering violent extremism (P/CVE), migration and sanctions compliance. These are very different challenges from organised crime, and approaches developed in one field should never simply be transplanted into another.

Nevertheless, there are useful parallels; particularly in understanding the relationship between information, human behaviour and complex networks.

Start With behaviour, Rather Than Communications

One lesson from behaviourally informed strategic communications is deceptively simple: don't begin by asking what do we want to say?

Begin by asking: what is happening, who is involved, what behaviours matter and what influences them?

An organised crime ecosystem can involve many different actors: criminal groups and their facilitators; people vulnerable to recruitment or exploitation; consumers of illicit goods and services; businesses and professionals who may knowingly or unknowingly enable activity; and communities affected by criminality.

These are not one audience. Nor will information affect all of them in the same way.

Behavioural frameworks can help break this complexity down. What enables a particular behaviour? What opportunity exists to undertake it? What motivates it? What barriers might prevent it?

The value of this approach is that it helps identify where communications might contribute, and equally, where another intervention is required.

What Can Strategic Communications Bring to the Fight Against Organised Crime?



Understand The Information Environment
A second parallel with fields such as P/CVE is the importance of understanding the information environment in which behaviour takes place.

People do not encounter institutional communications in isolation. Their perceptions are shaped by friends, family, communities, news, social media, messaging applications and increasingly complex online networks.

Criminal actors can inhabit the same environments. Digital platforms may be used to identify or recruit people, advertise illicit services, establish trust, facilitate transactions or misrepresent the risks and rewards associated with criminal activity.

This physical-digital convergence is central to the EU-funded Phygital-OC project, which is exploring the changing nature of organised crime and how capabilities and cooperation can continue to evolve in response.

For strategic communicators, it raises an important question: where within that wider information environment might communications create useful leverage?



Look Beyond Awareness
A third lesson is the distinction between awareness and behaviour.

In many complex policy areas, simply informing someone that an activity is illegal, harmful or risky does not necessarily alter what they do.

Behavioural approaches encourage us to look deeper.

What does someone believe about the likelihood of detection? Who do they trust? What social norms influence them? What perceived benefit makes a behaviour attractive? What misinformation or misunderstanding affects their choices?

This opens up a wider range of possible communications interventions.

Depending on the audience and context, communications might help make consequences more salient, challenge misconceptions, increase confidence in legitimate alternatives, strengthen resilience to recruitment or exploitation, equip trusted intermediaries with better information, or amplify credible evidence of successful enforcement.

The appropriate intervention will be different in every case. The common principle is that communications is designed around an identified behavioural objective rather than communications activity being an end in itself.

Insight, Intervention And Learning
There is another useful parallel with P/CVE: the importance of treating communications as an iterative process.

Insight informs an intervention. The response is observed. Evidence is gathered. The approach is refined.

That becomes particularly interesting in the context of increasingly digital organised crime.

The same technologies and analytical capabilities that help us understand networks and activity can potentially deepen understanding of the information environments surrounding them.

For strategic communications, this creates opportunities for much closer integration between research, behavioural insight, communications, technology and operational expertise.

It also encourages better evaluation. Reach and engagement remain useful measures, but where communications has a behavioural purpose, we should also seek to understand whether relevant perceptions, confidence, intentions or behaviours have changed.

An Opportunity For Cross-Disciplinary Learning
None of this suggests that approaches developed for P/CVE provide a ready-made communications model for organised crime. The actors, incentives, legal environments and behaviours can be very different.

But that is precisely why cross-disciplinary exchange is valuable.

Across Europe, considerable expertise already exists in behavioural science, strategic communications, prevention, digital analysis, community engagement and law enforcement. Projects such as Phygital-OC create opportunities to bring different parts of that expertise together and explore what can usefully be learned across disciplines.

As organised crime continues to evolve across physical and digital environments, the response will necessarily evolve with it.

Strategic communications is one part of that much larger picture. The opportunity is to continue exploring where it can add value: understanding audiences and behaviours, identifying points of influence, supporting prevention and disruption, and learning systematically from what works.

For those of us working in strategic communications, that is an exciting challenge, and one where the experience accumulated in adjacent fields may have much to contribute.

Jonathan Benjamin is a Director at REOC Communications, a Brussels-based strategic communications agency, and partner on Phygital-OC.

CALENDAR OF EVENTS

Explore upcoming events around the world which take a look at the latest challenges in dismantling organised crime, and register your interest to attend Phygital-OC events.

Community of Practice Event 4

November 3
Bogota

The last of four regional Community of Practice events which will bring together local law enforcement agencies...

Phygital-OC Exchange Event 5

December 2
Online 12pm - 1pm CET

Representatives from law enforcement agencies (LEAs), judicial authorities, civil society organisations (CSOs) and experts...

94th Session of the INTERPOL General Assembly

November 30 - December 3
Hong Kong

Delegates appointed by the governments of our 196 member countries...

DISCOVER MORE...



Latin American organised crime 'may operate in 16 European countries'

October 13, 2026 | The Guardian



50 arrested as police target Western Balkan network linked to killings

October 9, 2026 | Europol



Calls for Stronger Cooperation to Prevent Youth Recruitment...

October 1, 2026 | Phygital-OC



Latin American organized crime groups are expanding their presence in Europe

September 23, 2026 | GI-TOC



World Day Against Trafficking in Persons Highlights the Growing Threat...

July 30, 2026 | Phygital-OC



Podcast Explores Europe's Response to Transnational Organised Crime

July 1, 2026 | Phygital-OC



Criminal opportunism: how the EU's most threatening criminal networks exploit society

June 28, 2026 | Europol



Phygital-OC Delivers Advanced Training to Strengthen Libya's Response to Organised Crime

June 25, 2026 | Phygital-OC



View More



The Phygital-OC Project is being led by a consortium of leading European agencies involved in dismantling serious organised crime, including the Central Operational Service of the Italian Ministry of the Interior (SCO), Agenfor International, the Global Initiative against Transnational Organized Crime (GI-TOC), Policia Murcia, Center for Security Studies (KEMEA), CAT Cooperative Sociale, and REOC Europe.