EUROPOL

Decoding the EU's most threatening criminal networks

ISSUE **2**

The blueprint of criminal opportunism

DECODING THE EU'S MOST THREATENING CRIMINAL NETWORKS

ISSUE 2: THE BLUEPRINT OF CRIMINAL OPPORTUNISM

PDF | ISBN 978-92-9414-097-5 | ISSN 3094-6387 | doi:10.2813/3596319 | QL-01-26-005-EN-N

Luxembourg: Publications Office of the European Union, 2026

Cite this publication: Europol (2026), Decoding the EU's most threatening criminal networks - Issue 2: The blueprint of criminal opportunism, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu

Decoding the EU's most threatening criminal networks

ISSUE **2**

The blueprint of criminal opportunism

CONTENTS

FOREWORD

Jürgen Ebner,
Acting Executive Director of Europol

Over the past years, law enforcement authorities across Europe have demonstrated that organised crime can be disrupted. Many of the criminal networks identified in our 2024 assessment are no longer among the most threatening networks affecting the European Union today. This is a testament to the commitment of our law enforcement in Member States, partners countries and the power of intelligence-led cooperation.

Yet this report also delivers a clear warning. While criminal networks can be dismantled, organised crime continues to adapt, regenerate and exploit new opportunities. Criminal markets persist. New actors emerge. Criminal profits continue to fuel activities that undermine our security, prosperity and trust in institutions. This assessment shows that the most threatening criminal networks do not operate in isolation. They are embedded in a fluid criminal ecosystem that enables cooperation, resilience and rapid adaptation. At the same time, they are driven by a blueprint of opportunism, constantly identifying and exploiting vulnerabilities across our societies, economies and technologies. Understanding these dynamics is essential. It allows us not only to target the criminal actors behind organised crime, but also to reduce the opportunities that enable them to thrive.

The criminal landscape evolves, and so must our response. By combining operational disruption with a broader system-oriented approach, and by strengthening partnerships across the public and private sectors, we can build a Europe that is more resilient to organised crime and better prepared for the challenges ahead.

“

Every disrupted criminal network matters. Every target removed weakens the criminal ecosystem. Yet this report shows that organised crime adapts quickly, filling gaps and exploiting new opportunities. Our challenge is therefore not only to dismantle networks, but to stay ahead of them through intelligence, innovation and operational cooperation.”

Jürgen Ebner,

Acting Executive Director of Europol

“

Understanding the enemy is the first step to defeating it. The Decoding report gives us exactly that – and our response is already underway, from the Drugs strategy to combating migrant smuggling and digital fraud. Because while competences remain national, solutions can only be European. That is why we are also updating Europol’s mandate – to make sure that European solutions reach every Member State, faster and with more impact.”

Magnus Brunner,

European Commissioner for Internal Affairs and Migration

EXECUTIVE SUMMARY

Since Europol published its first assessment of the EU's most threatening criminal networks (MTCNs) in 2024, the criminal landscape has undergone significant change. Sustained law enforcement action across the EU has placed pressure on many criminal actors and networks. Continued monitoring and analysis of today's **731 MTCNs** have provided new insights into why the threat persists and how the approach can be further tailored.

MTCNS DECODED

The 2024 report

The 2024 Decoding the EU's most threatening criminal networks report was the first Europol assessment to systematically analyse how the EU's MTCNs operate and to identify the characteristics that make them particularly harmful.

Based on an overview of 821 MTCNs identified in 2024, the analysis pinpointed recurring patterns and characteristics that provided new insights into the criminal actors posing the greatest threat to the EU. The MTCNs were found to be **agile, borderless, controlling and destructive (A, B, C, D).**

MTCNs UNDER PRESSURE

What has happened to the 821 MTCNs since 2024?

Over the last two years, the landscape of the EU's MTCNs has changed significantly. Of the previously identified 821 MTCNs, **76%** are no longer reflected in the current list of MTCNs. This may be the result of a combination of factors, including law enforcement disruption, dissolution, restructuring, transformation into other criminal configurations, or changes in their assessed threat level.

Yet the threat persists. A **core group of 198** MTCNs identified in 2024 continues to rank among the MTCNs today, demonstrating remarkable resilience through their ability to adapt, reorganise and sustain criminal activity. This group displays characteristics commonly associated with traditional, well-established, poly-criminal and hierarchically structured criminal networks.

Furthermore, an additional **533 new** MTCNs have been identified, bringing the total number of networks currently identified across the EU to **731**. This reflects the fluid and dynamic nature of organised crime in the EU, and underscores the need to further strengthen and adapt law enforcement response.

NEW NETWORKS, PERSISTING PATTERNS

Who are today's MTCNs, what do they do, and why are they considered a threat?

The current assessment confirms the continued relevance of the ABCD framework identified in 2024. Today's 731 MTCNs continue to display a remarkably consistent threat profile, characterised by their agile, borderless, controlling and destructive nature. For example, **85%** still use legal business structures.

They continue to be primarily driven by profit. Their cohesion remains supported by this shared objective, combined with trust, regional connections, and opportunism.

They comprise more than **400 000** members representing **118** nationalities, underscoring the scale, reach and increasingly transnational nature of the threat.

Today's MTCNs operate across the **full spectrum** of serious and organised crime, including drug trafficking (over **one-third** of all MTCNs), cybercrime, migrant smuggling, trafficking in human beings, fraud, property crime and money laundering. While they continue to dominate established criminal markets, they are also increasingly exploiting emerging opportunities in the digital, financial and global environment. Less than **one-quarter** of MTCNs are poly-criminal, operating across multiple crime areas, often including drug trafficking, and demonstrating a high degree of adaptability. Some MTCNs have a link with terrorism. The increasing prominence of crime-as-a-service, particularly for financial services, further reinforces this model by enabling specialised actors to provide services to a broad criminal clientele. In doing so, it lowers the barriers to entry for criminal networks lacking the necessary expertise or capabilities.

The persistence of the ABCD characteristics demonstrates that, despite changes in the criminal landscape and its actors, and an increasing prominence of the online dimension, the factors that make these networks particularly threatening remain largely unchanged.

A FLUID CRIMINAL ECOSYSTEM

Why do MTCNs continue to resist and emerge? (part I)

Beyond understanding the threat characteristics, this updated assessment provides a deeper insight into **why** organised crime continues to resist disruption and regenerate itself.

One of the key insights to emerge from this analysis is that MTCNs **do not operate as isolated entities**. Instead, they function as part of a fluid and interconnected criminal ecosystem. When law enforcement neutralises a network, the fluid ecosystem responds: networks restructure and activities are relocated, or even changed altogether. While the arrest of key figures can destabilise a network, new actors often emerge to exploit the resulting opportunities.

Networks **cooperate**, use **countermeasures**, rely on specialised **criminal service providers**, have **international contacts**, and rapidly adapt to disruption. When law enforcement exerts pressure, some actors are removed or cease to play a significant role, but the criminal ecosystem as a whole adapts and reorganises, filling the void left behind and sustaining criminal activities. Shared criminal services strengthen the resilience of the ecosystem, but also create critical dependencies that can be targeted to generate wider operational impact.

This applies to all forms, types and structures of MTCNs, whether long-established or new, and whether flat or hierarchical. To varying extents, they are all connected to this wider criminal ecosystem. MTCNs with a Latin American connection exemplify this interconnectedness.

These insights, further reinforced by this analysis of criminal actors' operating models, underline the challenges associated with defining criminal networks and question the value of doing so through traditional concepts. Fluid criminal ecosystems transcend fixed structures, permanence and traditional roles. They facilitate ad hoc alliances, needs-based collaborations, and the exploitation of criminal opportunities as they arise.

A BLUEPRINT OF CRIMINAL OPPORTUNISM

Why do MTCNs continue to resist and emerge? (part II)

While the criminal ecosystem helps explain how criminal actors cooperate, reorganise and sustain their activities, it does not fully capture the factors that drive MTCNs to continuously identify and exploit criminal opportunities. To understand this dynamic, it is necessary to examine the enabling conditions that drive criminal adaptation.

Viewed through this lens, MTCNs can be understood as operating according to a blueprint of criminal opportunism: **driven by profit, they systematically and continuously seek and exploit vulnerabilities in the world's systems**.

Indeed, in an increasingly complex world, opportunities for criminal exploitation are both plentiful and rapidly expanding. Not only can MTCNs respond to established demands for illicit goods or services, they have also become adept at turning this complexity into criminal opportunities and engineering their response as new opportunities arise.

Digitalisation, technological innovation, global trade, geopolitical instability and the increasing overlap between legal and illegal economies provide criminal opportunities on an unprecedented scale. Criminal networks exploit digital and technological innovations such as online platforms, encrypted communication and AI to scale operations while minimising risk. Globalisation and geopolitical tensions open up new markets and routes, facilitating win-win collaborations. Criminal networks evade rules creatively, exploit loopholes, and make strategic use of key professions and businesses. At the same time, crime-as-a-service models and the exploitation of vulnerable individuals are lowering barriers to entry and increasing resilience.

A SYSTEM-ORIENTED APPROACH, IN PARTNERSHIP

Conclusion

Overall, MTCNs are becoming more adaptive, interconnected and embedded in society, while systematically taking advantage of structural weaknesses in modern systems. It enables them to sustain and expand their criminal activity – and profit – despite sustained operational pressure.

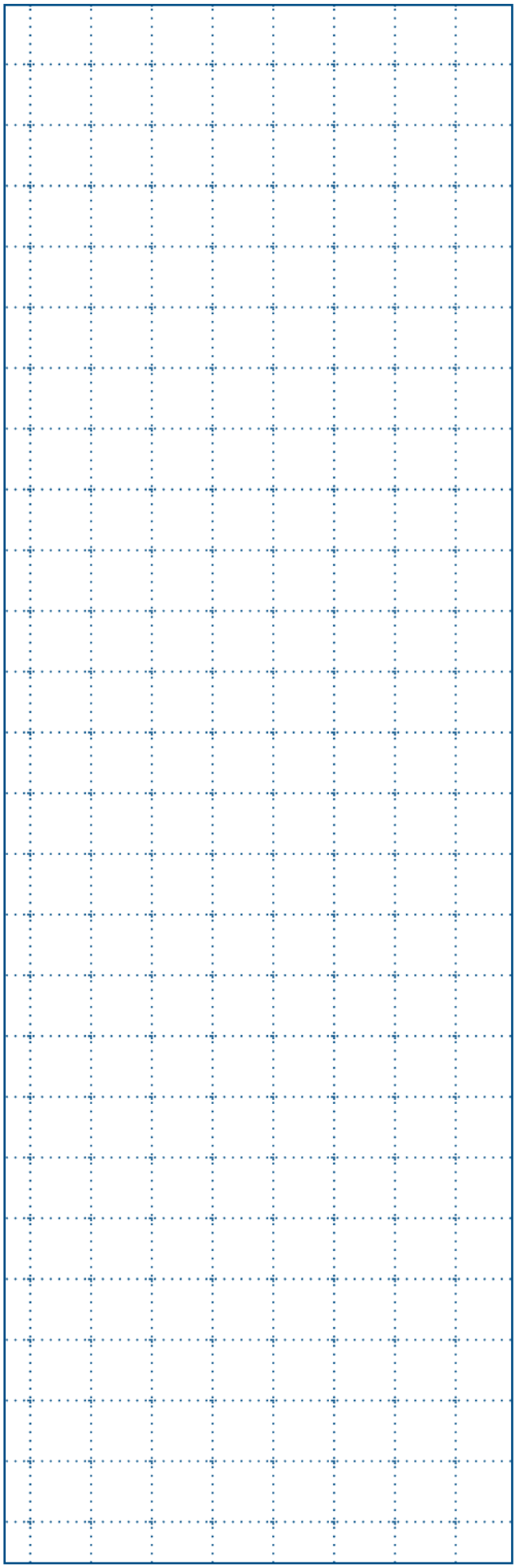
Taken together, the fluid criminal ecosystem and the blueprint of criminal opportunism help explain why organised crime remains adaptive, regenerative, and resilient. To understand organised crime today, we must look beyond individual networks to the broader environment in which they operate. Criminal actors function in a fluid ecosystem imbued with a blueprint of opportunism that enables cooperation, adaptation, and the rapid exploitation of opportunities.

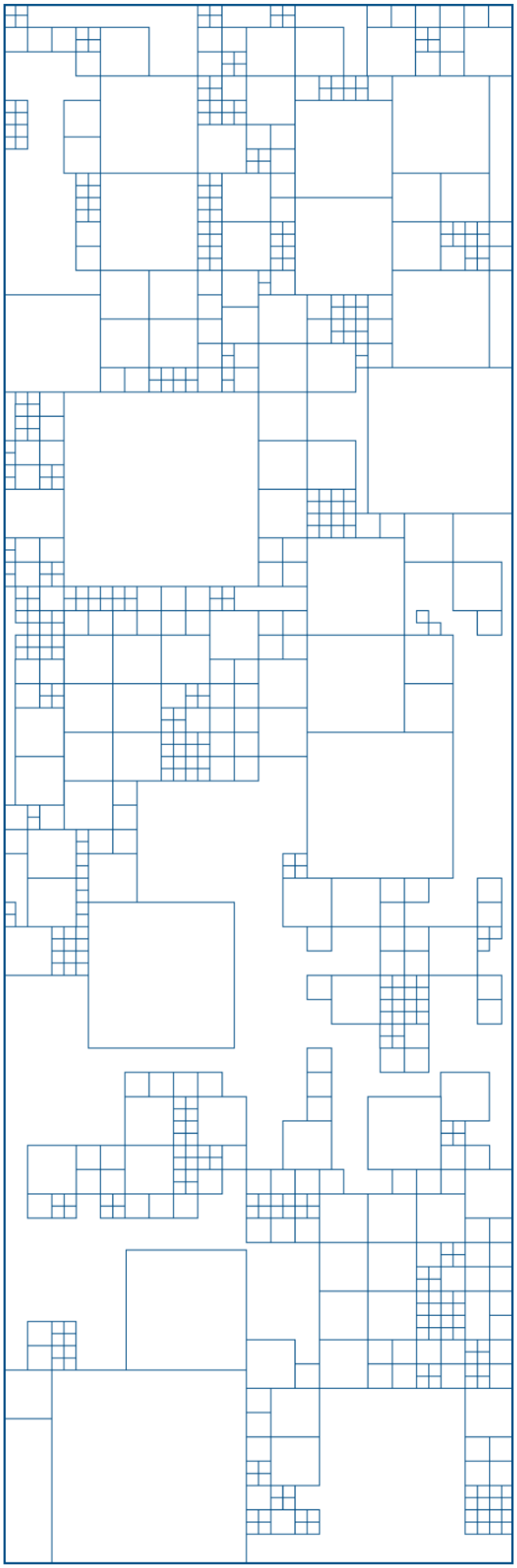
This has **direct implications for response**. Targeting high-value actors and other disruptive approaches remain essential, but are not sufficient. Criminal networks thrive by exploiting vulnerabilities in logistics, financial systems, digital infrastructure and global trade. An effective response must therefore **combine targeted disruption with systemic action**. This means not only dismantling networks but also strengthening systemic resilience and addressing the vulnerabilities that organised crime exploits. This requires a **complementary, collaborative and by-design approach** by law enforcement and partners in public and private sectors.

The reduction in the number of MTCNs identified compared with the previous assessment should therefore not be interpreted in isolation as a measure of overall threat reduction. Rather, it reflects the dynamic nature of organised crime, the effects of law enforcement action and the challenges inherent in assessing criminal networks operating within fluid and adaptive criminal ecosystems.

Understanding organised crime as both a fluid ecosystem and a blueprint of opportunism provides a **stronger foundation for future action**. By combining an actor-focused approach with a system-oriented one, the EU can increase the impact of disruption while reducing the opportunities that allow organised crime to adapt, regenerate and persist.

The composition of the MTCN landscape has changed, but organised crime remains resilient because it operates within fluid ecosystems and continually exploits emerging opportunities. Therefore, disruption of actors must be complemented by action against the systems and vulnerabilities that enable organised crime.





MTCNS UNDER PRESSURE

What has happened to the 821 MTCNs identified in 2024?

The initial analysis of the EU's MTCNs in 2024 identified 821 criminal networks posing the greatest threat to internal EU security. Law enforcement has taken coordinated international action, putting these MTCNs under pressure.

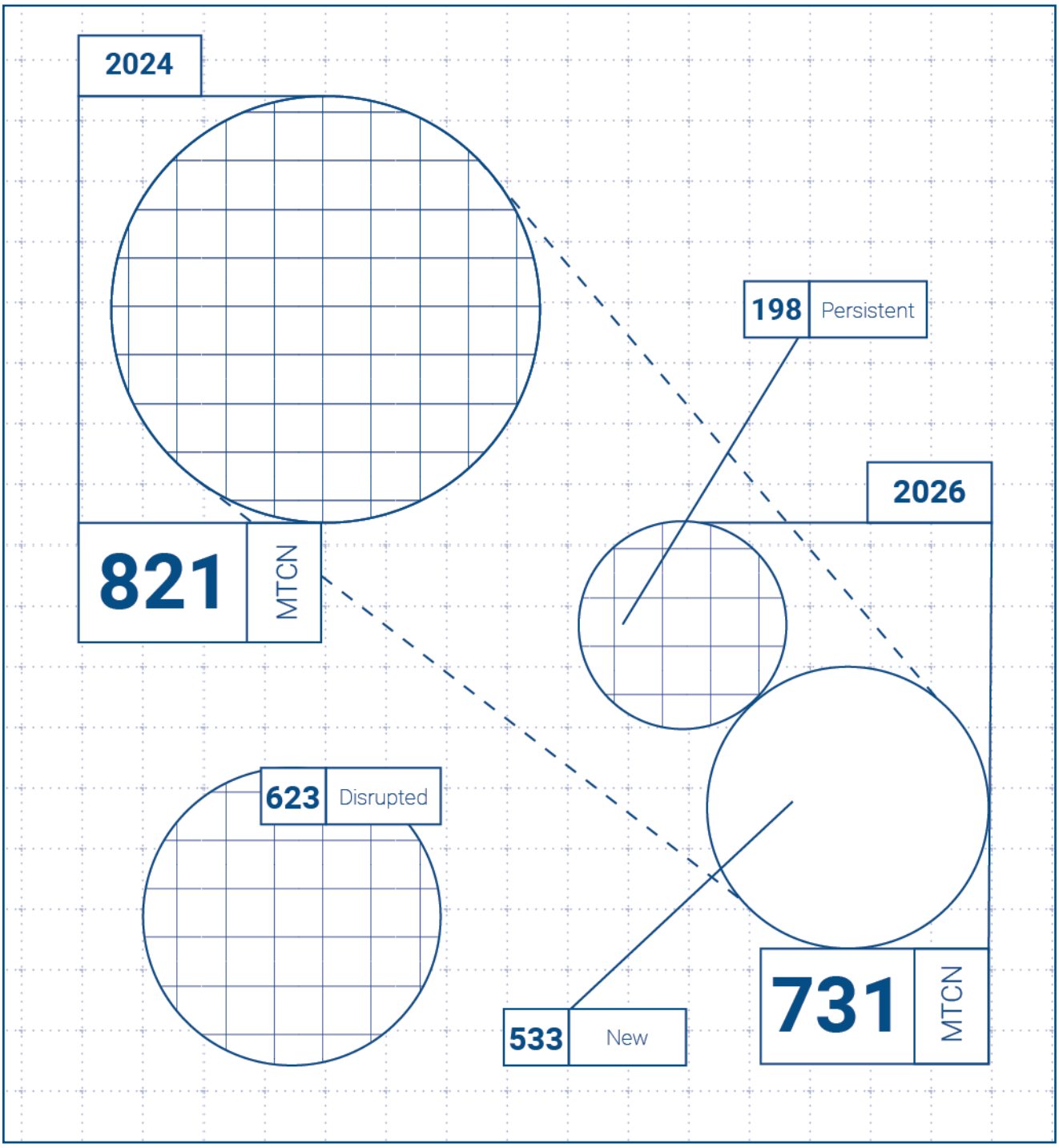
By the end of 2025, three distinct outcomes had emerged. A large proportion of MTCNs had significantly reduced their activities or were dismantled. Some, however, proved resilient despite sustained law enforcement pressure. At the same time, many newly identified networks came to the fore. Today, **731 MTCNs** have been identified.

Successful disruption

Across all EU Member States, by 2025, **three-quarters (76%)** of the MTCNs identified in 2024 were no longer considered to be among the most threatening[4].

The fact that many MTCNs have been disrupted does not indicate a decline in organised crime or a decrease in the number of MTCNs. Rather, it reflects the dynamic nature of the criminal ecosystem and demonstrates that targeted law enforcement interventions can effectively disrupt key nodes within that ecosystem.

At the same time, the analysis provides important insights into how the networks operate, where their vulnerabilities lie and how criminal markets regenerate when under pressure.



Characteristics

MTCNs identified in 2024 that are no longer among today's MTCNs were active in a range of crime areas. Between the crime areas, there are differences in the extent to which the networks have been disrupted. Higher rates for disruption are found for THB (86% of the MTCNs active in THB in 2024 have been disrupted) and migrant smuggling (82%). Among the MTCNs in fraud, drug trafficking and property crime, lower shares were disrupted, respectively 73%, 67% and 65%.

They differ from the ones that have persisted in various aspects:

- they are more often loose or organised around a core group rather than hierarchically structured;
- their geographical reach is more limited;
- only a minority have been active for decades;
- they are less inclined to work together with other networks, but when they do, it is usually in an equal partnership;
- they rarely use violence, intimidation or corruption to facilitate their criminal activities, instead using simple countermeasures.

Potential reasons for lowering the threat status

There are several reasons or a combination of factors why an MTCN identified in 2024 may not feature in today's overview. These include law enforcement disruption, dissolution, restructuring, transformation into other criminal configurations, or changes in their assessed threat level.

Disruption is primarily an indicator of the success of law enforcement. Law enforcement actions have dismantled or heavily disrupted multiple networks. A range of actions have been identified as contributing to this outcome. Typically, successful law enforcement approaches target critical vulnerabilities within the criminal ecosystem.

- **Investigations and operational taskforces (OTFs) focused on high-value targets (HVTs).** HVTs or key criminal actors within a criminal network coordinate operations or control key logistics. Once an HVT has been prioritised by law enforcement, targeted investigations are conducted, often involving international cooperation and Europol support. Investigations into HVTs may involve setting up OTFs. An OTF is a temporary group of representatives from Member States and Europol formed to carry out a specific project. The OTF coordinates intelligence and investigative efforts focusing on the criminal activities of one or more selected HVTs and members of their criminal network[5].

Case example

MIGRANT SMUGGLING NETWORK TARGETED WITH A REGIONAL OTF

A regional OTF has been established between Bulgaria, Greece, Moldova, Romania and Serbia to target migrant smuggling networks from Türkiye to Western European countries, using Bulgaria as a transit country. The leaders of the network, based in Sofia, arranged the transit across Bulgaria. They cooperated with other networks based in neighbouring countries. Migrants were smuggled across the Southern Bulgarian green border and guided to preset locations. From there, they were transported to Sofia, temporarily lodged in safehouses before being transported to various European countries. An action day end 2025 led to 16 arrests [6].

- **Parallel financial investigations.** In parallel with the original investigation into the main criminal activity of the MTCN, setting up a parallel financial investigation targeting infrastructures that enable money laundering and profit reinvestment has proven highly effective.

Case example

VIOLENT DRUG TRAFFICKING NETWORK DISRUPTED AND CRIMINAL ASSETS SEIZED

One of Scotland's most violent criminal networks was targeted in an international investigation supported by Europol and Eurojust. Law enforcement authorities from the Netherlands, Spain, Türkiye, the United Arab Emirates (UAE) and the United Kingdom (UK) joined forces to track the network's key players and finances. Continuous operational support, including from financial crime specialists, contributed to asset tracking and identifying the infrastructure underpinning the network's money laundering activities. An action day on 27 March 2026 led to the arrest of 13 suspects and the seizure of two plots of land, estimated to be worth about EUR 600 000, in Türkiye[7].

- **Investigations and action days that cover logistical nodes** such as ports, warehouses and transport networks. Coordinated action days at certain types of locations can lead to the arrest of identified suspects, the search of premises for relevant intelligence or information and the seizure of criminal assets.

Case example

SMUGGLING OF TOBACCO THROUGH PORTS

Following the seizure of 12 million counterfeit cigarettes at the port of Genoa, Italy, in September 2024, an investigation was launched. Analysis of suspicious container movements at the port led to the identification of a transnational criminal network, operating across Europe, Africa and Asia. Shipments were routed through various countries to hide the true origin of the illicit goods. Action days in 2024 targeted port workers suspected of facilitating the criminal activities. Besides port workers, the network also relied on a company in Italy to avoid inspections and an IT specialist to conceal the identities of consignees in customs documentation. An additional action day in 2026 took place across five countries and led to the seizure of over 40 tonnes of illicit tobacco products[8].

- **Investigations and action days that cover digital infrastructure**, including encrypted communication solutions or online platforms.

Case example

OPERATION CANDY

The seizure of two mobile phones from a local drug dealer in Sweden led to the discovery of multiple interconnected networks involved in drug trafficking and money laundering across Europe, Asia and Australia. The various networks were connected through shared facilitators and a web of LBSs. Forensic analysis of the devices revealed that members of the network were running a large-scale online drug distribution business with links to Thailand. Drugs destined for Australia were seized in Germany, a shipment organised by the same criminal ecosystem. And a high-value target based in Spain facilitated the large-scale drug trafficking[9].

In 2024 and 2025, Europol supported EU Member States and cooperation partners in a broad range of initiatives leading to operational success:

~ 7 000 operations supported

~ 80 OTFs set up, with investigations related to more than 50 of the EU's current MTCNs included in an OTF

~ 500 action days supported

Resulting in >1 000 arrests, including >100 HVTs, during OTF action days.

Another explanation for a criminal network's absence from today's MTCNs is a (temporary) decrease in its operational activity.

The MTCN may be disrupted by law enforcement without becoming absolutely obsolete. Following the arrest of leading figures, for example, an MTCN may appear inactive while continuing to operate under the radar. For law enforcement, the criminal network appears to be inactive. Once arrests have been made, convictions secured and the investigation has been closed, monitoring the suspects and their activities may be limited. Therefore, parts of the network may remain active, potentially operating in other locations while keeping a low profile to avoid detection by law enforcement.

This highlights the importance of continuously monitoring criminal activities and sharing intelligence and information with other countries, both during and after an investigation leading to the disruption of a criminal network. Criminal networks are known to be flexible and adaptive, exploring new areas or territories of activity in response to obstacles they encounter.

Examples of operational success notwithstanding, law enforcement pressure is not the only factor that can result in a criminal network's threat level decreasing.

This change may also be related to **developments in the criminal landscape**. Internal tensions and/or pressure from competing MTCNs may lead to a decrease in the power and influence of criminal networks. A lack of coordination may lead to fragmentation and decentralisation into smaller, less influential cells. Members who replace an arrested or deceased leader may not be as capable as their predecessor.

Finally, some **methodological considerations** could also be at play. Some contributing countries may have changed their approach to what constitutes a 'most threatening criminal network'[10].

Resilience: status quo for long-established MTCNs

Despite many MTCNs being disrupted or going under the radar, 198 of the initially identified 821 MTCNs are still considered to be among the MTCNs affecting the EU. They have resisted law enforcement pressure and demonstrated resilience.

Almost half of the persistent MTCNs are poly-criminal, compared to fewer than one in ten of the disrupted MTCNs. They are less often involved in fraud, organised property crime, migrant smuggling and THB.

These MTCNs differ from those dismantled or disrupted in various ways:

- they are more often hierarchically structured and described as mafia-style networks;
- they are larger and have a broader geographical reach;
- they are settled and have been active for decades;
- they are more likely to work together with other networks and dominate these relationships;
- they are more likely to set up legal business structures, more frequently corrupt people to facilitate their criminal activities and use innovative countermeasures strategically. These characteristics help them resist law enforcement interventions and persist for many years.

See also Persistent and fluid lifespan of MTCNs for more insights on what makes today's MTCNs long-standing.

Emergence: the rise of new players

One of the most striking findings of the dataset update is that many of the MTCNs identified in 2026 were not yet considered among the most threatening two years ago. Not fewer than 533 of today's MTCNs are either new or newly identified.

There are multiple possible explanations for this section of MTCNs, including a change in conceptualisation and incidents that bring criminal networks to the attention of law enforcement. Also, as crime is increasingly nurtured online, today more criminal networks involved in cybercrime are being identified among the ones posing the greatest threat (*see also Inside the blueprint: The cybercrime connection*).

The fact that a criminal network is new to the MTCN dataset does not necessarily mean that it is newly formed or recently established. It may have been active and even under investigation for years, but the national authorities may not have previously included it among those considered the most threatening.

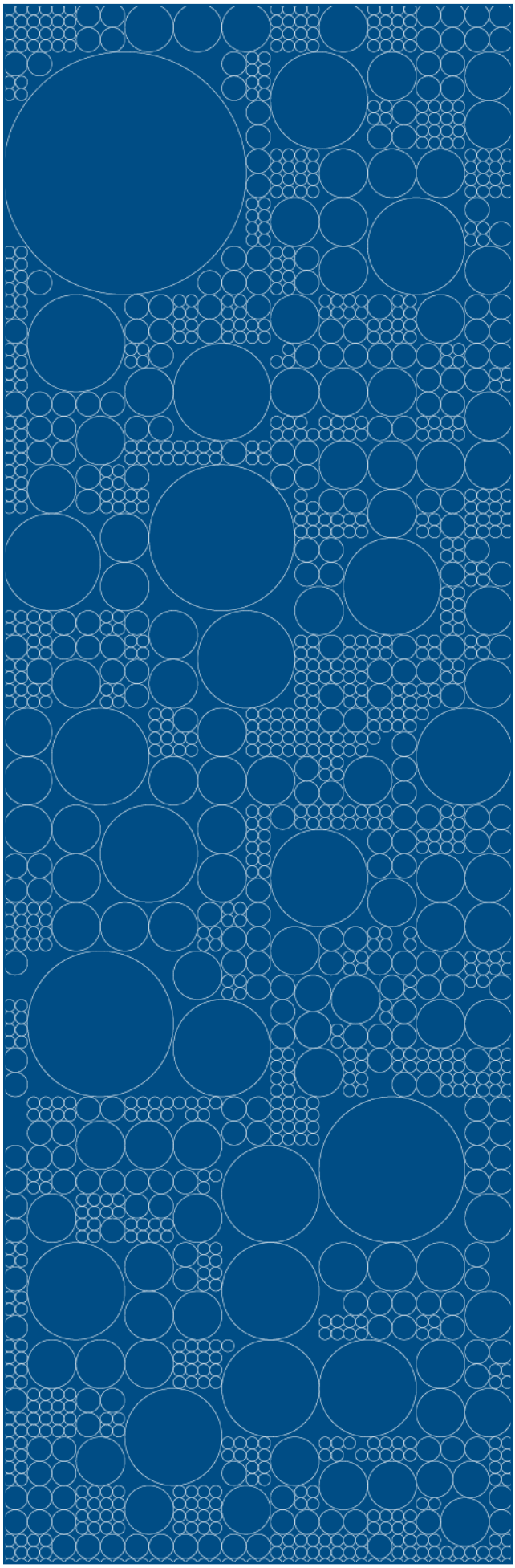
The profile of these new MTCNs is a mix between the profiles of the dismantled and persistent ones, with slightly more similarities to the dismantled MTCNs. In the group of new MTCNs, there are often more hierarchical networks compared to the group of dismantled MTCNs, but still far less compared to the persistent MTCNs. Also for other characteristics, such as the geographical scope of their activities or their longevity, the profile of the new MTCNs resembles more that of the dismantled ones than that of the persistent ones.

The emergence of many MTCNs in this overview brings forward a key insight to this analysis. It demonstrates how criminal networks fill the gaps left by dismantled networks and adapt to opportunities in their operating environment, including our societies, economies, institutions and the wider world.

Before turning to these explanations, it is important to understand the nature of today's MTCNs, the criminal activities in which they are involved, and what makes them threatening.

NEW NETWORKS, PERSISTING PATTERNS

Who are today's MTCNs, what do they do, and why are they considered a threat?



Today's criminal landscape is different than two years ago. The MTCNs identified at the time have been disrupted or some have persisted. Furthermore, many new criminal networks have emerged. Yet, the code of this largely new group remains the same. Today's MTCNs, just like those in 2024, are still agile, borderless, controlling and destructive. Their inherent threat characteristics and the criminal activities they engage in remain largely the same. Although many new actors have emerged, the old patterns have persisted.

Who are today's MTCNs: internal organisation and composition

Many of the world's nationalities are represented

The composition of criminal networks varies greatly in terms of nationality. Overall, **118 different nationalities** are represented in the 731 MTCNs, which is more than the 112 nationalities reported in 2024. This means that today, 60% of the world's nationalities are represented in MTCNs affecting the EU.

Most MTCNs have mixed membership in terms of nationality

Just under **two-thirds (63%) of MTCNs comprise multiple nationalities**. This once again highlights the borderless nature of MTCNs, which is also clearly reflected in their composition. Most often they combine EU and non-EU nationals. Some include a variety of EU nationalities. There are also MTCN composed of a variety of non-EU nationals (*see also Inside the blueprint: The Latin American connection*).

More than **one-third (37%) of the MTCNs are composed of members with one and the same nationality** – slightly more than in 2024. Most often this concerns MTCNs composed of one EU nationality, but there are also various MTCNs with members of the same non-EU nationality.

One-nationality MTCNs are more often hierarchically structured, controlling the entire criminal process, operating on a smaller scale and for a longer period of time. Interestingly, they cooperate less often with other criminal networks, and if they do, they tend to be more often dominant in the relationship.

Young perpetrators

Young perpetrators are exploited in various types of serious and organised crime, to enable the mid-level of criminal networks to sustain their criminal activity while evading law enforcement and the judiciary[11]. Young people are recruited and consequently treated as a disposable asset, often used for the execution of one-off and highly visible criminal activity.

The use of young perpetrators is not standard for all MTCNs. Even if the share of MTCNs that exploit young people seems relatively small (6%), it is still very significant: about four dozens of MTCNs are known to be linked to the criminal exploitation of young people. All the more, because in some cases, it may entail a high number of young people affected (*see also The Com network*). In all cases, it affects one of the most vulnerable groups in society.

Also among the MTCNs, young perpetrators are mostly recruited to commit low level offences. For example, in the context of drug trafficking, they are used to perform surveillance in neighbourhoods or conceal and/or distribute drugs in the streets. In some cases, which are often but not always linked to drugs, they are recruited to carry out more violent and riskier activities, including intimidation, extortion, as well as shooting and murder. They are also exploited for money laundering services, by acting as money mules or opening bank accounts to complete money laundering schemes. Young people are also recruited in the context of online fraud schemes, for purchasing stolen data on online platforms or for providing alibis.

Case example

RECRUITMENT OF YOUNG HITMEN

OTF GRIMM, launched by Europol in April 2025 to tackle violence-as-a-service and the related recruitment of young people[12], supported the arrest of two 18-year-old men in Western Sweden, who are suspected of actively recruiting youngsters for targeted killings in Sweden and Denmark. The two men are thought to have facilitated the killings, together with other suspects, by supplying the young hitmen with weapons, ammunition and safehouses. Young, vulnerable people are targeted through social media for these 'violence-as-a-service' schemes, increasingly used by criminal networks[13].

MTCNs attract young perpetrators with financial incentives and/or misleading ideological narratives that make illicit activities appear acceptable. The fact that some young people may be recruited because they are under the age of criminal responsibility limits the legal consequences for adult members of criminal networks. In some cases, the young people are the children of criminal network members and are expected to take over their parents' criminal activities in the future *(see also Enforcement service provision)*.

Most MTCNs have up to 50 members

The size of today's MTCNs varies considerably, with membership ranging between two and thousands of individuals. Yet, most MTCNs are capped at 50 members. Persistent MTCNs are often well-established groups that tend to be larger than newly emerged ones. The 731 MTCNs together have **more than 400 000 members** – a much higher absolute total than for the 2024 group of MTCNs (almost 80 000 members). This is mainly due to a few very large networks, with over 100 000 members, involved in cyber-attacks and online fraud schemes[14].

While more MTCNs are hierarchical, they are also part of an interconnected ecosystem

Today, almost **two-thirds** (**64%**, up from 57% in 2024) **of MTCNs are hierarchically structured**, with clear leaders and well-defined roles and responsibilities. Many of them are described as mafia-style or clan/family-based groups. Outlaw motorcycle gangs, Thieves-in-Law and Latin American cartels are also examples of such hierarchical networks.

However, it remains inherently challenging to determine the exact size and boundaries of a criminal network. Many of these hierarchical MTCNs operate through distributed structures composed of semi-autonomous cells, each responsible for specific operational tasks such as logistics, financial management, recruitment or enforcement. While these cells may operate under the direction of a central leadership, in many cases key functions are outsourced to specialised actors or service providers, who may support several criminal groups simultaneously. Exclusive cooperation agreements between networks further blur organisational boundaries.

Consequently, the distinction between membership, cooperation and service provision is becoming increasingly blurred, reflecting a broader shift from standalone criminal networks operating in isolation to interconnected criminal ecosystems.

What do today's MTCNs do?

MTCNs are active in all crime areas, all nurtured online, accelerated by AI, and destabilising the economy

Today's MTCNs and the suspects they are composed of engage in the full spectrum of serious and organised crime. They remain active in a range of crime areas, from traditional cross-border trafficking criminal activity such as drug trafficking, frauds, property crime, migrant smuggling, trafficking in human beings, to crime areas that predominantly take place in the online domain and are labelled as cybercrime.

Yet, in today's digital society, all types of organised crime are increasingly nurtured online. The internet and digital technology are now essential for communication between network members, for recruitment of new members or service providers, for marketing of illicit services or products, as a channel to illicitly obtain or resell digital data, or for targeting victims. The online sphere is more than a mere enabler – it has become a pillar in any criminal network's activity, and in any criminal market. MTCNs identified by EU Member States and third partners that are active in cybercrime may seem few, but any reported MTCN has a major online footprint. Also, the scale of pure cybercrime MTCNs is often larger – with often very large memberships and a truly global reach. For these reasons, the crime areas in which the MTCNs are active should not be considered to be wholly representative of the threat each crime area poses. Also crime areas in which few MTCNs have been identified, remain key threats to the internal EU security.

The rapid advancement of AI is significantly amplifying the scale and pace of organised crime, a trend that is only set to intensify. The very attributes that define AI's revolutionary potential - its accessibility, adaptability, and advanced capabilities - have also made it an appealing instrument for criminal enterprises. As AI and emerging technologies continue to reshape the landscape of organised crime, they lower the barriers to entry by democratising tools for generating text, images, and videos, as well as automating processes. This not only accelerates the speed of criminal operations but also exponentially increases their scale. This acceleration marks the beginning of a far-reaching transformation in the world of organised crime.

Organised crime is also found to be destabilising society as a whole. Among many harmful impacts, the financial destabilisation of the EU's economy is a key concern. Money laundering and criminal finances ensue from any criminal activity, as that is what turns the core objective of criminal networks – money – tangible. This analysis reconfirmed that most MTCNs launder criminal proceeds themselves (more than 90%) and some also make use of dedicated criminal networks specialising in providing money laundering services. These specialised service providers are especially useful when the money laundering techniques are more sophisticated, including for purchasing and exchanging real estate or for obfuscation methods involving crypto assets *(see also Specialised service providers)*.

Figure: MTCN involvement and average group size per crime area

This table shows per crime area, the share of MTCN's involved in each crime area, and the average size of the MTCNs per crime area.

Crime area	% of MTCNs involved	Average number of suspects per MTCN
DRUG TRAFFICKING	36.3%	
POLY-CRIMINALITY***	23.3%	
(ONLINE) FRAUD	16.4%	
ORGANISED PROPERTY CRIME	7.9%	
MIGRANT SMUGGLING	3.7%	
MONEY LAUNDERING**	2.6%	
TRAFFICKING IN HUMAN BEINGS	2.6%	
CYBER-ATTACKS	1.9%	
FIREARMS	1.0%	
EXTORTION	0.8%	
ENVIRONMENTAL CRIME	0.5%	
COUNTERFEITING	0.5%	
CHILD SEXUAL EXPLOITATION	0.3%	
OTHER*	2.2%	

1 20 000

*Includes match fixing, illegal betting , sanctions evasion, violence-as-a-service.

**Concerns the provision of money laundering as a service to other criminal networks

***Poly-criminality means that the criminal network is involved in multiple main crime areas in parallel. The multiple crime areas are all a main focus and are not in support of one main crime area, and not inherent to the modus operandi of the main crime area. An example of poly-criminality is the combination of drug trafficking and organised property crime. The combination of drug trafficking and corruption is not considered poly-criminality as the corruption supports the drug trafficking.

Most MTCNs specialise in one criminal activity of choice

More than **three quarters of MTCNs (77%)** specialise in one main criminal activity.

- Just like in 2024, **drug trafficking** continues to stand out as a key activity. Not only is more than one third (36%) of MTCNs specialised in drug trafficking, predominantly cocaine, other MTCNs also combine it as part of a poly-criminal portfolio, resulting in more than half of all MTCNs involved in drugs. These MTCNs are typically long-standing and have a global membership, operating worldwide and relying on outsourcing under a crime-as-a-service framework.

Case example

COLOMBIAN CARTEL INVOLVED IN COCAINE TRAFFICKING TO EUROPE

Prominent HVTs linked to the Clan del Golfo, a Colombian drug cartel, coordinated whole-sale cocaine trafficking from South America to Europe. Cocaine was transported by speedboats from Colombia to nearby countries, after which it was shipped in freight cargos to European ports. The network worked together with various criminal actors in South America as well as in Europe, controlling the entire chain from production in the source countries to distribution across Europe[15].

- **Fraud schemes, both online and offline**, represent the second most common form of criminal activity among today's MTCNs (16%). About half of the MTCNs involved in fraud commit online fraud, which is the fastest-growing area of organised crime. It operates as a transnational industry, utilising a range of logistical, technical and financial operations to perpetrate large-scale fraud[16]. Also prominent in this area are excise fraud and customs import fraud.

Case example

FRAUD VIA FAKE ONLINE TRADING PLATFORM

A criminal network defrauded more than 100 victims of over EUR 3 million through a fake online investment platform. The perpetrators lured victims with promises of high returns on investments. The victims made initial small deposits, after which they were pressured to invest larger amounts, manipulated by fake charts showing fictitious profits. The criminals used psychological tactics to convince the victims to transfer substantial sums of money, which were never invested but kept by the network[17].

- **Organised property crime, migrant smuggling and trafficking in human beings** also remain among the sustained criminal activities in which MTCNs engage.

Case example

CHINESE NETWORK TRAFFICKING HUMAN BEINGS FOR SEXUAL EXPLOITATION

A Chinese network targeted primarily Chinese women through call centres based in China, Spain, and France. Some victims, recruited in China, were aware of the type of work they would engage in, but misled about the conditions. Others were deceived and coerced into sexual exploitation. The network also targeted vulnerable Chinese women already staying in the EU. It has been active for several years, moving victims for short terms between apartments in different countries, a modus operandi known as 'sex tours' or 'carousels'[18].

- Interestingly, almost 3% of today's MTCNs specialise in the niche of **money laundering-as-a-service** to other criminal networks *(see also: Specialised service providers).*

- Today's MTCNs are more heavily involved in **cyber-crime** than those in the previous dataset, where such involvement was almost non-existent. In addition to online fraud schemes, there has been an increase in MTCNs involved in cyber-attacks and online child sexual exploitation (*see also Inside the blueprint: The cybercrime connection*).

Case example

MONEY MULE SERVICE PROVIDERS

A criminal network engaged in cryptocurrency investment fraud, targeting millionaires and generating huge profits, outsourced the laundering of the illicit profits to two other networks. These networks recruited money mules, who transferred the proceeds to another account or withdrew it in cash, before giving it to someone else in exchange for a commission. Europol developed the #DontBeaMule prevention campaign to raise awareness about the use of money mules[19].

Some MTCNs combine multiple main criminal activities

Less than **a quarter of today's MTCNs are poly-criminal**, in the sense that they focus on multiple criminal activities of a different nature.

Most of these poly-criminal MTCNs engage in drug trafficking alongside other criminal activities. They use the established trafficking routes and techniques to transport various commodities, including firearms and tobacco alongside drugs. Drug trafficking may also be combined with economic or financial crimes, such as fraud or counterfeiting goods. This is particularly the case for Italian mafia-style criminal networks.

The nexus between MTCNs and terrorist actors and groups

It is reported that some **5% of the MTCNs have a link with terrorism**, mainly with ethno-nationalist terrorism. However, some MTCNs also have links with jihadist terrorism. These links are often partial: specific members of the MTCNs were members of terrorist organisations, were arrested for terrorist offences, expressed support for terrorist organisations, or came from strongholds where terrorist organisations are active. Some criminal networks can be linked to terrorist financing.

Despite the fundamental differences in terms of motivation and goals between organised crime and terrorism, there are also commonalities. Both draw on the same recruitment pools and rely on the same providers of illicit goods and services. They also both leverage technology to achieve their objectives and are increasingly involving young people in their activities. Connections between terrorist and criminal networks are sporadic and opportunistic. They appear to be ad hoc and made between individuals rather than groups.

INSIDE THE BLUEPRINT

The cybercrime connection

Virtually all criminal activities are nurtured online, transforming the digital environment into a primary theatre for criminal operations. However, criminal networks that perpetrate cyber-attacks, online fraud schemes and online child sexual exploitation operate almost exclusively online. Cyber-attack perpetrators depend on digital infrastructure, which is also essential for some of the criminal processes of MTCNs involved in online fraud and child sexual exploitation. The online and offline dimensions often intertwine.

The vast majority of the MTCNs operating online are newly reported, indicating either an increase in threat level, an expanded national focus, or both.

Criminal networks operating online, whether they are involved in cyber-attacks, online fraud schemes (OFS) or online child sexual exploitation (CSE), spread their activities across borders, inflicting direct harm on individuals, businesses and the public sector.

Online operations amplify the threat of crime, as they provide criminal networks with an **extensive geographical reach** in which borders and physical distance no longer constrain activity. Members of the network, victims, infrastructure and illicit profits are distributed across jurisdictions simultaneously. This removes geographical constraints and gives criminal networks the opportunity to select the most convenient jurisdiction for the different stages of the criminal process. This is sometimes linked to regulatory shortcomings, flaws in cooperation mechanisms and the focus of law enforcement.

Case example

OPERATION ALICE

The operator of the dark web platform "Alice with Violence CP" ran more than 373 000 fraudulent websites advertising child sexual abuse material (CSAM) and cybercrime-as-a-service offerings. The investigation into the activities of the operator led to the identification of 440 customers worldwide and the seizure of 105 servers. The operator, based in China, allegedly made more than EUR 345 000 in profit from about 10 000 customers worldwide[20].

While criminal networks operating online seamlessly bypass geographical constraints, law enforcement is bound by territorial jurisdictions and national laws. Consequently, international law enforcement cooperation is vital in combatting criminal networks. However, it is often hindered by non-cooperative jurisdictions, unharmonised regulations and difficulties in accessing data for investigations.

Most of these criminal networks are either active in multiple cybercriminal activities or act as **service providers** to other criminal networks and actors. Such services include trading in breached sensitive data, which is then used to commit online fraud or gain unauthorised access to networks, as well as selling ready-to-use kits for carrying out phishing attacks.

Underage suspects are rarely involved in the activities of high-level cybercriminal networks. Although minors are likely to be indirectly involved in some cybercrime activities, there are only a handful of cases of recruit-

ment. These concern mainly OFS in which young perpetrators are recruited to carry out simple tasks, such as opening bank accounts or obtaining debit cards, to facilitate the initial transfer of victims' funds.

OFS: A transnational criminal enterprise manipulating victims en masse

51 criminal networks have been reported as being MTCNs involved in OFS, prevalently in phishing operations. However, their operations are very fluid and opportunistic. They are not usually specialised in a particular type of fraud but instead use phishing techniques as a means of carrying out various types of OFS.

Criminal networks perpetrating OFS pose an additional threat due to **the large number of victims they target, the resulting harm and the substantial financial gains generated by their activities**. They generate significant profits by directly targeting individuals, companies and public organisations and by monetising their fraudulently obtained data on both the clear and the dark web.

Due to the wide range of offences and the online dimension being used to reach as many victims as possible, these networks do not exhibit any specific geographical patterns. They can operate from anywhere, regardless of their location of their targets. However, certain nationalities tend to emerge, such as those from Eastern Europe, Western Africa and South East Asia and the Middle East.

OFS are highly profitable, and many of these schemes do not require perpetrators to be highly specialised, especially when the necessary data and services are available on an as-a-service basis within the underground economy. This enables OFS criminal networks to operate in a fluid and responsive manner, seizing opportunities as they arise. Many criminal networks engage in various schemes involving impersonation, including romance fraud and tech support scams. In several cases, the **diversification of operations** is not confined to the OFS domain but also involves other types of criminal activities, such as drug trafficking, robbery and THB.

Poly-criminal networks with OFS in their portfolio have a broad membership base, with an overall hierarchical structure comprising different cells that operate with similar internal structures and roles. These networks are particularly **resilient** to law enforcement disruption due to their diversified operations and cell-based structure across borders.

In several cases, it has become clear that the distinction between the online and offline dimensions is not as clear-cut as we might think. Despite operating primarily online, a number of these networks use **violence** both internally and externally. Internal violence is used to recruit and control members. External violence, including serious physical threats, is sometimes directed at rival criminal networks, but also at victims, law enforcement and judicial authorities' representatives with serious physical threats.

The **recruitment** of lower-level criminal network members such as money mules and call centre operators takes place in different ways, both online and offline. Online advertisements offering fake jobs or the promise of easy money are a common path of reaching young recruits. Recruitment hubs have also been established in some EU Member States, particularly for call centre operatives fluent in EU languages[21].

A few criminal networks play a crucial role by providing services that facilitate OFS and enable various criminal processes. Important criminal **service providers** include those who sell phishing kits containing ready-to-use websites that imitate official websites, and those who offer SIM-box services.

Case example

CYBERCRIME FACILITATED BY SIM-BOX SERVICE

A criminal network enabled cybercriminals globally through provision of a SIM-box service. This service offered telephone numbers from over 80 countries to cybercriminals, facilitating a wide range of telecommunication-related crimes, as well as offences such as migrant smuggling, extortion and the distribution of CSAM. More than 49 million online accounts were created with these telephone numbers, with the estimated damage done by the renters of these numbers of several million euros. The network maintained a professional website to advertise and provide their services. It relied on a highly organised network to acquire thousands of SIM cards in multiple countries worldwide to be rented out to clients[22].

As a large part of the OFS economy is based on sensitive data, these criminal actors involved in OFS can be exploited as proxies by **hybrid threat** actors to harvest important information using OFS tools and techniques.

Money laundering can involve diverse activities ranging from traditional methods to more sophisticated crimes. These MTCNs widely use crypto assets, but also traditional ML techniques such as bank transfers, investments in real estate and the purchase of high-end goods. Money mules are commonly used by OFS criminal networks, especially for investment fraud. They are often recruited online and may be underage.

The majority of the MTCNs involved in OFS in the EU are involved in **phishing**. These networks are mostly newly reported and were previously not known to law enforcement. They are extremely opportunistic and continually adapt their strategies and methods for approaching victims. The means of communication used to reach victims vary and include email, telephone, social media platforms and over-the-top (OTT) services.

When phone calls at scale are involved, call centres are established, requiring human and logistic resources. Employees of these call centres often impersonate different professional figures such as bank employees and police officers.

Several of the MTCNs are involved in **investment fraud**. Most of these are newly reported. They are a threat because their criminal activities cause significant loss to individuals, sometimes depriving individuals of their lifetime savings. The illicit profits these schemes generate are particularly high. For example, one such criminal network has inflicted damages estimated at EUR 282 million.

Case example

PROFESSIONALLY ORGANISED CALL CENTRES INVOLVED IN INVESTMENT FRAUD

A criminal network engaged in a large-scale online fraud scheme operating several call centres in Albania. The centres were professionally organised with a clear division of tasks among dedicated teams, coordinated by team leaders and higher management, totalling around 450 employees. Advertisements on social media and search engines promoted seemingly legitimate investment platforms. Potential victims were contacted by call centre employees, often in their own language, to build trust. Once registered, they were persuaded to transfer additional amounts of money. Victims were located across Europe and worldwide, with the total financial damage estimated to be at least EUR 50 million. The criminal network was dismantled in 2026, after a two-year international investigation[23].

Most MTCNs involved in investment fraud exercise end-to-end control over their operations. These MTCNs appear to specialise in investment fraud rather than operating in multiple OFS depending on available opportunities. This is probably because efficient investment fraud schemes require specialisation, criminal infrastructure and dedicated resources. These criminal networks often establish their own LBSs or infiltrate existing ones at a high level, such as online platforms, marketing companies and call centres. Other LBS are also important for carrying out offences and are sometimes used unwittingly, such as social media platforms for advertising fraudulent investment plans.

MTCNs often target the most vulnerable citizens, with reports of **elderly fraud** increasing in several Member States. Almost all MTCNs involved in this type of fraud have a hierarchical structure, with clearly defined levels and roles reporting to network leaders. In many cases, coordination is carried out remotely, while other members are based in the countries in which they operate. Important roles include the phone operator that calls the elderly individuals, the collector who impersonates an authority figure and collects money or valuable goods from victims, and the logistical coordinator who selects victims, coordinates communication and transportation.

Elderly fraud has a strong physical component, combining online and offline steps in the criminal process. Lists of potential victims are shared online, and the victims are usually first contacted by phone before being approached at home to obtain their valuables. As this is usually jewellery and cash, the money laundering techniques used are mostly traditional. The stolen goods are transported via courier and then used to purchase real estate, luxury goods or to invest in cash-intensive businesses, banks or trading options.

Some of the MTCNs involved in OFS are more specialised, as certain types of fraud require a higher level of technical expertise to be effective. These are frauds that do not require human error to succeed as they exploit vulnerabilities in the digital systems and networks to steal funds. The MTCNs involved in **frauds against payment systems** are mostly hierarchically structured and have end-to-end control of their operations.

Cyber-attacks: successful ransomware models that remain out of reach

The MTCNs perpetrating cyber-attacks are involved in the **development, management and deployment of ransomware**. Since the ransomware criminal process is composed of different steps, some specialised actors may be involved in specific actions (e.g. intrusion). These are not exclusive to ransomware but are an essential component of it. Depending on the network's composition, the criminal actors may be part of the network or hired as-a-service.

Ransomware MTCNs are typically well-structured and built around a core group that is composed of a small number of offenders who direct and oversee the operations. They may recruit individuals to perform key functions, such as developers, penetration testers

and system administrators, while outsourcing other roles, such as accounting, finance, human resources management, recruitment and marketing, to other actors.

Once the team's structure has been established with the right people and a new code, the ransomware brand is ready to go. The team can then carry out attacks either in a **closed group** model or in a **semi-closed group** setting, with the targeted selection and recruitment of affiliates to carry out attacks using the group's infrastructure (e.g, BlackBasta[24]). A third and common business model that scales up MTCN activities is using **public ransomware-as-a-service (RaaS) programmes** that openly offer integrated code and other capabilities (e.g. leak site hosting, negotiation and money laundering services) on cybercrime underground platforms. Affiliates carry out the attacks, and the core group receives a fixed share of the profits (e.g. Akira).

Case example

BOOTER SERVICE FACILITATING DDOS ATTACKS

During a coordinated action week, Operation PowerOFF targeted over 75 000 users engaged in DDoS attacks. The action targeted booter services, that allow users to launch DDoS attacks themselves. These types of DDoS-for-hire infrastructures allow individuals with little technical knowledge to launch cyber-attacks[25].

Traditionally, investigations into ransomware MTCNs have focussed on ransomware brands, linking the brand name to the network itself. In this sense, MTCNs have had a higher turnover, which is either the result of a large number of affiliates or the capacity to attack very valuable targets and critical infrastructure, causing significant disruptions.

Nevertheless, these brands are often short-lived, with new brands emerging within a very short timeframe. Once disrupted, they demonstrate a high level of **resilience** and the ability to quickly dissolve and rebrand or create splinter groups. There are often links between popular malware strains that have been disrupted and new ones. The Akira ransomware, for example, was created by the Howling Scorpius group in 2023 and shows links to members of the Conti group – a prominent group which became defunct in 2022.

While moving away from the brand-based identification is not always easy, intelligence suggests that many of the most threatening brands are operated by a group of high-level affiliates with extensive experience and a long history of **collaboration**. These affiliates are highly resilient and collaborate to provide the most efficient cybercrime services, developing ransomware programs that are franchised to other cybercriminals in a RaaS model once they are mature.

The MTCNs involved in cyber-attacks use sophisticated **countermeasures** to evade law enforcement authorities, distancing themselves from their criminal operations and concealing their true identities while leaving as few digital traces as possible. This is the result not only of advanced knowledge but also jurisdictional barriers and regulatory that prevent, for example, the lawful interception of communication or effective law enforcement cooperation.

In many cases, jurisdictions are exploited as a form of countermeasure. While these MTCNs carry out their criminal activities exclusively online, the individuals are often located in non-cooperative jurisdictions, which makes identifying and apprehending them challenging unless they cross the border.

Most MTCNs involved in cyber-attacks are from the Commonwealth of Independent States (CIS) countries, with leadership in many cases based in countries that are out of reach for EU law enforcement agencies.

Case example

VPN SERVICE USED IN MAJOR CYBERCRIME CASES

Cybercriminals used a VPN service to conceal ransomware attacks, data theft and other cybercrimes. The service was often promoted on Russian-speaking cybercrime forums and offered anonymous payments and hidden infrastructure. Specifically meant for cybercrime, the VPN service played a role in almost every major cybercrime investigation supported by Europol in recent years. The takedown of the service exposed thousands of users linked to ransomware attacks, fraud schemes and other serious offences[26].

Several MTCNs perpetrating cyber-attacks have links with **hybrid threat** actors, which vary in degree and pattern of collaboration. In a cybercrime economy based on service providers, hybrid actors use these criminal networks as proxies for interference operations targeting strategic objectives, which may involve intrusions, data theft, ransomware and DDoS attacks. Cybercriminals may offer their services to hybrid threat actors unknowingly, others under coercion or in exchange for protection[27].

The illicit profits from these MTCNs are high and challenging to trace. RaaS programmes typically operate with an 80-20% split of the payout of each attack the affiliate carries out using a brand. A ransomware group may have a large number of affiliates. Each affiliate may carry out multiple profitable attacks. Payment is always made in cryptocurrency, which is laundered by using sophisticated techniques and services. Examples of these sophisticated **money laundering** techniques include moving funds rapidly across blockchains ('chain-hopping') and the increasing use of cryptocurrencies with built-in anonymity features (privacy coins)[28]. In some cases, money is laundered through professional money laundering networks or platforms. Furthermore, it is often reinvested to fuel further criminal operations. Some of the money is used to rent technical infrastructure for new attacks.

Due to the sophistication of the countermeasures employed and the challenges posed by uncooperative jurisdictions, there are significant intelligence gaps regarding MTCNs involved in cyber-attacks.

Case example

KIDFLIX

Kidflix was the most popular CSAM streaming platform on the dark web, taken down by law enforcement in 2025. During its activity from 2021 to 2025, the platform had more than 1.8 million users registered and about 80 000 uploaded videos. The administrator of the platform had very high-level technical knowledge. He was active in several cybercrime forums, online fraud platforms and was carrying out other cybercrime offences. It is believed that he was not driven by sexual interest in children but rather seeking for as much illicit profits as possible. The investigation was led by German authorities and supported by Europol, and involved the participation of over 35 countries. These efforts led to the seizure of the server that was hosted in the Netherlands, the identification of some 1 400 suspects of which 79 were arrested, and the safeguard of 39 children from sexual abuses[29].

CSE: fluid online networks connecting perpetrators globally

Perpetrators of CSE operate online in various ways depending on the type of offence, displaying unique networking patterns. Although their criminal operations pose a significant threat, they often do not meet the definitions of organised crime at national level and are in most cases not investigated and prosecuted as criminal networks. This is reflected in the national contributions to this report where only two MTCNs are identified as most threatening. These two MTCNs are of very diverse nature: one manages a large platform (Kidflix) for trading of CSAM, while the other incites girls aged 12–16 years into sexual activity.

Given the online nature of their operations, both groups have a prominent cross-border presence, with a **global reach** in terms of both their members and their victims.

Although both networks operate online, they are active in different environments and exploit different technologies as a **countermeasure** to conceal their activities. The Kidflix platform was hosted on the dark web and targeted offenders for financial gain. The second case involves the use of end-to-end encryption (E2EE) messaging applications to target child victims for sexual gratification.

CSE offenders are exceptionally quick in **adapting to new technologies**, including AI, both to expand and make more efficient the criminal process, but also as a countermeasure against law enforcement detection[30].

An ever-increasing number of networks dedicated to CSE are hosted on E2EE messaging applications. These applications provide a widespread environment in which to network, exchange CSAM and groom children. Thanks to E2EE they provide protection from law enforcement scrutiny, and their easier accessibility allows for a larger user base that includes offenders who would not have the technical capabilities to access the dark web[31].

The variety of CSE offences means that perpetrators can play different roles simultaneously, either acting alone or as part of a network. Although online networking is not traditionally considered organised crime, investigations show that most offenders prefer to act as part of a network[32]. Most offenders are active in several communities to obtain the largest possible volume of original CSAM and interact with like-minded individuals. They also network to discuss countermeasures against detection by law enforcement and share experiences of sexual abuse.

However, not all the communities are structured in the same way. Although platforms hosted on the dark web are well structured, with rankings and strict control measures, criminal networks operating on E2EE messaging applications tend to have a more fluid, non-hierarchical structure.

Members of the network mostly communicate with each other online and are unaware of each other's physical appearance. They avoid meeting in real life and sharing any personal details that could lead to their identification, even in private conversations with other users. They are mindful of the possibility of law enforcement infiltration. Consequently, trust is key in their relationships and usernames are the main identifier used[33].

The connections between members of CSE criminal networks are therefore fairly loose, with offenders networking for specific benefits but rarely forming closed groups. The exception is transnational child sex offenders, who cooperate closely in planning and perpetrating sexual abuse or facilitating criminal activities.

There are significant intelligence gaps regarding the networking patterns of perpetrators of live distance child abuse, where child abuse is offered on demand and, in most cases live streamed, in exchange for payment.

THE COM NETWORK

In recent years, a particularly threatening criminal network has emerged in the EU and beyond, combining serious and organised crime and violent extremism. First identified in 2021, this MTCN is commonly referred to as 'The Com' (short for 'The Community') and poses a serious threat to children and society as a whole. The network comprises a multitude of groups that leverage digital platforms to promote violence, groom children and other vulnerable categories of individuals, and recruit members on a global scale. These online communities engage in a variety of criminal activities, creating a complex landscape where CSE, cyber-attacks, extortion, assault, rape, murder and violent extremism intertwine. This results in physical and psychological harm not only to individuals, but also to society as a whole.

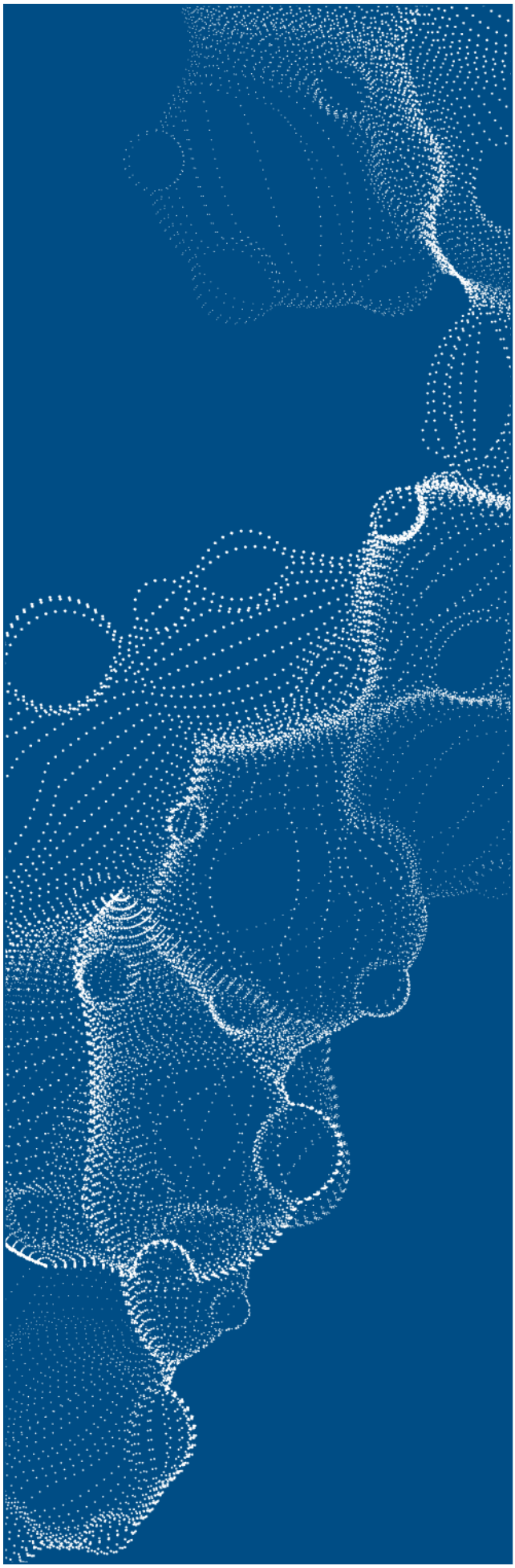
Although networking and recruitment primarily take place online, criminal offences take place both online and offline, often combining the two dimensions. Episodes involving stabbings, school attacks and violent assaults originating from these online communities are becoming increasingly prevalent in several countries. Since 2025, criminal offences involving violence that have been identified as being linked to the Com have been reported in several EU Member States. These episodes often involve children as perpetrators, either as a result of entry requirements to the groups, as a consequence of being commissioned by other members of the community, or inspired by the violence promoted in the network.

The membership of the groups forming the network is largely comprised of children and young people, aged between 8 and 17[34]. Individuals join these communities and engage in criminal activity for sexual gratification, social reward or a sense of belonging[35]. In many cases, the motivating factors for engaging in the network's criminal activities are similar to those found in gaming environments. Achieving notoriety, rivalry and seeking status are all common motivations.

Potential victims are often targeted on gaming platforms, on communication channels, and, in some cases, on channels used by youth to discuss mental health issues. The victims are first groomed, enticed and manipulated, and then threatened and coerced into complying with a variety of demands. These threats are often carried out by leveraging obtained images and personal information, which are sometimes shared among offenders, causing victims to be re-victimised by multiple offenders and perpetuating the cycle of harm[36]. In some other cases, the identified offenders have also suffered from victimisation in the past.

A FLUID CRIMINAL ECOSYSTEM

Why do criminal networks continue to resist and emerge? (part I)



Many successful law enforcement operations have recently disrupted the activities of MTCNs. Yet, the criminal enterprises typically carry on. Some networks have remained active for over a decade, demonstrating extreme resilience in the face of law enforcement action. Other networks recover or reinvent themselves, even after suffering severe setbacks. Sometimes new networks take the place of those taken down. Why?

A significant finding of this analysis is that MTCNs do not usually operate in isolation. Instead, they thrive within dynamic and interconnected criminal ecosystems. When law enforcement attempts to neutralise a network, this often triggers a response from the wider ecosystem: networks adapt by restructuring, relocating or changing their activities. While the arrest of key figures may temporarily disrupt a network, new actors quickly rise to fill the void.

This adaptable criminal ecosystem is characterised by flexible collaboration between networks and specialised service providers, such as those involved in money laundering, logistics and enforcement. It also features shared infrastructure and facilitators, the instrumental use of violence, intimidation or corruption, and operational cells spread across various countries. While some components of the ecosystem may be dismantled when law enforcement applies pressure, the overall structure responds and reorganises. It fills the gaps left by dismantled networks and continues the same criminal activities, demonstrating the ecosystem's resilience and adaptability.

About defining criminal networks

This update analysis further reinforces the insight that MTCNs do not operate in isolation, but rather as an integrated and agile ecosystem. This also reemphasises the challenges involved in defining criminal networks.

As discussed in the previous chapter, it is inherently challenging to determine the exact size and boundaries of a criminal network. Many criminal networks operate through distributed structures composed of semi-autonomous cells, each responsible for specific operational tasks such as logistics, financial management, recruitment or enforcement. While these cells may operate under the direction of a central leadership, in many cases, key functions are outsourced to specialised actors or service providers who may support several criminal groups simultaneously.

Exclusive cooperation agreements between networks further blur organisational boundaries.

As a result, it is challenging to distinguish between membership, cooperation and service provision, reflecting a broader shift from standalone traditional organised crime groups towards interconnected criminal ecosystems - notwithstanding the continued and persistent presence of certain traditional organised crime groups.

The fluid interconnected criminal ecosystems encountered encompassing today's MTCNs have no fixed structure, duration in time, or traditional roles. It's all about being ad hoc, collaborating where needed and continuously engineering live criminal opportunities, either by proactively scanning the environment for weaknesses or acting on demand.

The future trends foreseen by Europol in 2015[37] have become today's reality. Traditional hierarchical criminal groups are accompanied by the expansion of a virtual criminal underground made up of individual criminal entrepreneurs, which come together on a project basis and lend their knowledge, experience and expertise as part of a crime-as-a-service business model[38]. Criminal actors engage in 'co-competition', which sees competing actors interact or cooperate in the ad hoc pursuit of criminal opportunities[39].

Today's analysis of the 731 MTCNs is based on data and substantiates how these changes to the criminal landscape have materialised. It also shows how law enforcement is currently facing the challenge of dealing with a fluid criminal ecosystem that adapts and responds, resists and emerges.

It emphasises again how the current definitions of organised crime do not adequately describe the complex and flexible nature of today's criminal landscape. Furthermore, it questions the possibility and usefulness of defining criminal networks, as their nature and environment in which they function is now confirmed to be fluid in terms of organisation, and morphs according to the opportunities that it sets out to seize.

Flexible cooperation – if needed

MTCNs prefer to remain in control of their criminal enterprises. However, in the spirit of opportunism and with a view to maximising illicit proceeds, they are willing to cooperate flexibly with other criminal actors. This demonstrates adaptability through smart outsourcing.

However, not all criminal networks cooperate with others. In fact, more than one third of MTCNs do not engage in any relationships with other criminal networks. They operate autonomously and retain full control of their criminal activities. Some oversee the entire criminal process, relying on various cells to handle specific parts of the process, while others limit their activities to a particular task that does not require cooperation.

Case example

ALBANIAN DRUG TRAFFICKING NETWORK COOPERATING WITH VARIOUS OTHER NETWORKS

An Albanian clan-based criminal network was engaged in cocaine trafficking and money laundering. The network organised various multi-tonne deliveries of cocaine from Latin America to main ports in Europe, operating on a global scale. In order to facilitate these large transports, the network cooperated with multiple other networks, both within the EU and beyond. The criminal network's leader coordinated shipments from remote locations, relying on encrypted means of communication[40].

When MTCNs do cooperate, it is usually on an equal footing. Cooperation with other criminal networks often involves long-term relationships with established partners. Cooperation is usually either based on specific parts of the criminal process, such as the supply and distribution of illicit goods, or on certain expertise needed, such as chemical knowledge or money laundering expertise, which is provided as a 'crime-as-a-service' offering.

Specialised service providers

Crime-as-a-service acts both as a force multiplier for criminal networks and as a strategic vulnerability within the criminal ecosystem.

The growing use of crime-as-a-service models strengthens the criminal ecosystem by enabling networks to access specialised expertise and infrastructure on demand. While this increases adaptability, scalability and resilience, it also creates shared points of dependency. Disrupting key service providers, facilitators and enabling infrastructures offers a high-impact opportunity to weaken multiple criminal networks simultaneously and reduce the resilience of the wider criminal ecosystem.

More MTCNs now specialise in niche criminal activities that they offer to other criminal actors as part of a 'crime-as-a-service' framework (*see also Most MTCNs specialise in one criminal activity of choice*). What has changed is the level of sophistication, organisation and independence of criminal service providers, which has increased significantly. They have established themselves in the criminal landscape as autonomous operators, facilitating the criminal activities of multiple networks.

Financial service provision

Money laundering is the prime service provided to other criminal networks. It is the sole activity of 19 MTCNs. These networks are usually well organised, long-lasting and centred around one or two core members.

Expert money laundering networks have a wide geographical reach and a broad representation of EU and non-EU (including Asian) nationalities among the key members.

Case example

UNDERGROUND BANKING THROUGH MONEY MULES AND CRYPTOCURRENCY

A criminal network, led by two Ukrainian brothers, provided cash courier and underground banking services to other criminal networks. The group was made up of Ukrainian, Armenian, Azerbaijani and Kazakh nationals, as well as Chinese actors. Various Russian-speaking and Asian criminal networks made use of the money laundering services for proceeds of drug trafficking, tax evasion or the smuggling of illicit goods. Cash couriers regularly travelled between Spain, Cyprus, France and other countries with large sums of cash, abusing the temporary protection status granted to Ukrainian refugees by the EU since 2022. To avoid detection, the network increasingly moved away from cash movements to cryptocurrency[41].

Money laundering service providers often set up their own LBS or infiltrate existing companies at a high level, in various sectors (e.g. construction, transport, cleaning services, and finance) to facilitate their activities.

Logistics service provision

For certain MTCNs, the logistical supply chain has become a criminal business in itself. For example, networks producing drugs require specific equipment and chemicals; networks smuggling migrants or trafficking drugs over sea need nautical equipment and networks operating illicit cigarette factories require machines and essential components, etc. Some networks specialise in providing such materials.

Case example

SMALL BOATS SUPPLY CHAIN DISRUPTED

A criminal network arranged deliveries of nautical equipment for smuggling events via the English Channel. The equipment was produced in Asia and imported from Türkiye, arriving in bulk in Germany. There, it was stored in warehouses controlled by the network. The equipment was used to assemble unique sea smuggling packages. Each package, worth over EUR 10 000, included items such as an inflatable boat, engine, pumps, petrol jerry cans and tyre inner tubes. The criminal network delivered these to the French shores. During the investigation, authorities from Belgium, France, Germany, and the Netherlands arrested a total of 17 individuals associated with the criminal network, who were involved in low-level logistical roles. Four suspected organisers, Syrian nationals, were arrested during the action day in March 2026[42].

Enforcement service provision

Some MTCNs provide violence-as-a-service. This issue has gained extra attention in recent years, not least because of the (online) recruitment of young people for such activities. Violence-as-a-service relies on a chain of criminal roles with specific tasks[43]. The instigator typically orders the violence remotely, from a location separate from where the attack will take place. It is the responsibility of recruiters to identify and contact the perpetrator. This is often done via encrypted messaging apps or online platforms. Enablers provide the logistics, and perpetrators carry out the violent acts. These perpetrators are increasingly minors with no criminal background, deliberately recruited to avoid detection and prosecution. They are targeted through coded language, memes and gamified tasks that glamorise a luxurious lifestyle (*see also Instrumental use of violence, intimidation and corruption and Minors*).

Other types of criminal service provision

Apart from MTCNs that provide services, digital service providers and key professions such as lawyers and notaries also play a relevant role (*see also Key professions*).

Persistent and fluid lifespan of MTCNs

Most MTCNs (nearly 80%) have been active for a minimum of three years, and **one-third (34%) for 10 years or more**. These MTCNs are assessed to be in a stable position, as opposed to being rising or fading actors within the criminal landscape.

They are able to continue their activities due to redundancy (i.e. if one member is arrested, others take over their tasks) and reorganisation. Arrested or deceased members are easily replaced, even though arrested leaders may continue to exert control over the criminal activities due to the strong cohesion of the MTCNs, often based on family ties and long-standing friendships. Other core members continue to cooperate after leaders' arrests, either under remote leadership from prison, or by taking up the leadership role themselves.

Following law enforcement actions, MTCNs can diversify their criminal activities and/or relocate to other countries. Once released, arrested members may rejoin the criminal network or affiliate with others. Changes in modus operandi, including methods of operation and communication, as well as the adoption of technological innovations can also contribute to the longevity of criminal networks.

Case example

AT-SEA TRANSFERS TO AVOID LAW ENFORCEMENT DETECTION

To avoid law enforcement detection methods at EU ports, criminal networks increasingly make use of complex at-sea transfers whereby commercial ports are avoided all together. Using this method, drugs are picked up by large mother vessels in Latin America and transferred to smaller vessels, sometimes multiple, mid-ocean. The latter bring the drugs on shore, using fast-moving vessels and favourable entry points such as remote beaches, river systems and small marinas in order to avoid detection. Once on shore the drugs are further distributed across the EU[44].

A high level of awareness, as well as calculated and strategic use of countermeasures also contributes to the persistence of MTCNs. These are mainly used against law enforcement authorities and other government bodies (e.g. tax offices, authorities in logistical nodes), and rival criminal networks.

The types of countermeasures put in place by MTCNs vary and include the use of encrypted phones and communications, VPNs and residential proxy services. They also include frequently changing contact details, utilising aliases, using fake identities on social media accounts and phones, complex movement patterns, and concealment of criminal activities, for instance through the use of front companies, underground banking systems or decentralised blockchain solutions, and relocating criminal activities. Some criminal networks infiltrate law enforcement authorities or provide them with false information to law enforcement officers to mislead investigations, obtain information to facilitate criminal activities or identify members who collaborate with law enforcement. They also seek professional legal advice to exploit the legal system and facilitate their illicit activities, as well as to engage in legal procedures such as civil and commercial disputes against competitors.

Instrumental use of violence, intimidation and corruption

While violence is part of the modus operandi of some MTCNs, this is not always the case. More than 70% of MTCNs using violence is associated with drug trafficking. Smaller proportions are associated with migrant smuggling (4%) and fraud (6%). Although criminal networks may see the use of extreme, externally directed violence as a way to assert their power, such actions can pose a risk to the network if they result in civilian casualties and attract significant public attention. Such actions attract greater scrutiny from law enforcement, resulting in more thorough investigations and the disruption of criminal activities, which can lead to the exposure of members. Even if the leadership outsources violence to young perpetrators or other providers of violence-as-a-service, this still represents a risk (*see also Young perpetrators*).

When violence is used (e.g. kidnapping, arson or murder), it is usually – but not exclusively – directed against rival criminal networks in order to establish and/or expand one's own criminal enterprise while damaging those of one's rivals.

Case example

USE OF VIOLENCE AGAINST WITNESS

A Western Balkan criminal network involved in trafficking and distributing drugs and supplying weapons and explosives to other criminal networks in the EU committed various violent crimes. The network's leader was incarcerated after a major crackdown, but kept coordinating the group's activities from prison. After his release, he went underground and continued to lead the network, allegedly organising and coordinating the assassination of a witness. A month later, the HVT was taken into custody by law enforcement, together with several of his criminal associates[45].

Many MTCNs that engage in high levels of violence against rivals also tend to use violence internally against members and collaborators in cases of non-compliance with orders. Punishment is used with the intention of setting an example. Physical and psychological violence, torture and other types of abuse are used against victims, especially in areas of crimes involving the exploitation of victims.

Intimidation is directed at rival criminal networks, the private sector, witnesses and members of the network itself. Acts of intimidation, such as threats, shootings and attacks on houses using explosives, are intended to pressure on, coerce and scare rivals and members alike.

As regards violence and intimidation, not all MTCNs rely on corruption. Those that resort to corruption typically do so to obtain information on law enforcement investigations and judicial proceedings, to secure favours, to further their criminal activities (e.g. shipping and extracting drugs from port containers trafficking illegal

goods via customs), to infiltrate public procurement proceedings and obtain public contracts, and to facilitate the movement of members of criminal networks.

Case example

SWEDISH FUGITIVE ARRESTED AS NEW OTF GRIMM TARGETS ADDED TO EU MOST WANTED

A Swedish fugitive linked to the Foxtrot criminal network was arrested in Tunisia following cooperation between Swedish and Tunisian authorities. The suspect was wanted for murder and conspiracy to commit murder and was believed to recruit individuals for violent criminal acts. His profile had recently been published on the EU Most Wanted website. Following the arrest, two additional HVTs linked to violence-as-a-service networks have been added to the platform, both wanted in connection with serious violent offences[46].

Operational cells in multiple countries

MTCNs often operate across national borders. Overall, **76% are active in up to seven countries**, while approximately a quarter are active in more than seven countries. More than half are active in both EU and non-EU countries.

Some jurisdictions may offer strategic advantages to MTCNs, such as opportunities to conceal criminal assets or establish legitimate businesses that can be used as fronts for illicit activities.

Although MTCNs are transnational in nature, most maintain a relatively focused geographical footprint. By concentrating their activities in a limited number of countries, they may be better able to maintain control over their operations.

Hierarchical networks tend to have a wider geographical reach than loosely structured networks or those centred around a core group. This may be because they are often more established and have gradually expanded their presence over time. Operating in multiple countries allows these networks to establish local cells and cooperate with local intermediaries where logistical support or local expertise is required.

Migrant smuggling networks also tend to have a broad geographical scope, with cells based in different countries, having control over the entire route from the country of origin to the final destination.

The extensive geographical reach of MTCNs is also reflected in the geographical footprint of their leadership. For those of which the location of the leaders is known, they are based in 64 different countries, including all EU Member States (465 MTCNs) and 37 non-EU countries (146 MTCNs).

For the majority of MTCNs, leadership is based in one of the countries in which they operate, indicating a tendency to maintain close control over criminal activities. The choice of the specific country from which the operations are managed is a strategic choice, influenced by factors such as the ability to evade law enforcement or ensure the success of major criminal operations.

The leadership of 86% of the MTCNs is settled either in the main country of activity[47] or the country of origin of the key members[48]. This implies that only for 14% of MTCNs, the leadership is located elsewhere. Such remote coordination can take place from non-EU countries, but also from within the EU.

The international reach of MTCNs is also evident in their composition. Members of these criminal networks represent 118 nationalities, including those of all EU Member States and 91 non-EU countries. Many MTCNs have mixed nationalities (*see also Who are today's MTCNs*).

INSIDE THE BLUEPRINT

The Latin American connection

A key feature of the MTCNs affecting the EU is that they are borderless. They operate in multiple countries, both within and outside the EU, and their members are often of various nationalities. Some networks strategically deploy members abroad, collaborate with criminal networks based outside the EU or use specialised services provided by non-EU criminal actors. Latin America is a key region of interest, being an important source of drugs, as well as having interconnections with THB and organised property crime. The individuals who steer these interconnections are also part of a fluid criminal ecosystem, but the nature of these interconnections should be considered in more detail.

One in five MTCNs has a Latin American connection

As many as one in five of the MTCNs affecting the EU (149 out of 731) have ties with Latin America. These MTCNs deploy criminal activities in both the EU and in Latin America and/or have Latin American members. This makes Latin America one of the regions most closely connected to the EU in terms of organised crime.

In Latin America, these MTCNs carry out their criminal activities across a wide range of countries and overseas regions. In the EU, their operations are dispersed throughout most EU Member States.

But what does the Latin American connection entail?

The Latin American perspective

Interregional criminal connections are often perceived from a Latin American perspective. Latin American cartels are entrenched within the national and regional criminal landscape. They have several common characteristics that emphasise their strength and influence. They are hierarchically structured, with internal systems of control and discipline, and they are very large, ranging in size from 1 000 to 20 000 members. They exert extended control at a national level and are active in several countries in the region. They also have global links.

While they are all poly-criminal in nature, their strong involvement in cocaine trafficking is where their international connections are most clearly evident. Indeed, some of the cartels have links with the EU, and Latin American law enforcement partners consider some of these to affect the EU significantly too.

The Colombian Clan del Golfo and the Brazilian Primeiro Comando da Capital (PCC), in particular, have close ties with EU-based criminal networks typically at common cocaine entry points. There are furthermore indications that the PCC is trying to establish cells in various European countries, including for money laundering purposes. These cartel-style MTCNs are known to control every stage of the criminal process, facilitating cocaine trafficking by setting up LBSs, including in the EU. They systematically use corruption and intimidation to facilitate cocaine trafficking.

The links that Latin American cartels have with the EU go hand in hand with the region's position as the world's leading producer of cocaine. Logically, cartels that dominate national and regional handling have transaction-based contact with EU-based receiving counterparts, or individuals may be present to broker transactions. This collaborative and transactional approach does not transpose the cartel's structure, hierarchy, modus operandi or use of violence to EU territory.

Case example

CRIMINAL NETWORK LINKED TO LOS LOBOS CARTEL

A drug trafficking network, linked to the Ecuadorian 'Los Lobos' cartel, was targeted in an international investigation. The network, led by a person considered as a high-value target, used fruit exporting companies as cover for the illicit activities, concealing the drugs within legitimate cargo. Alerts regarding suspicious containers led to targeted inspections and seizures at major ports in Europe. The Ecuadorian network cooperated with an Albanian network. Members of the latter regularly travelled to Ecuador to negotiate deals. Criminal cells operating in various European countries handled the logistics and the further distribution of the drugs within the EU[49].

A nuanced view

The analysis of the 149 MTCNs with Latin American links provides a more nuanced view. The Latin American perspective cannot simply be transposed to the European situation.

It shows that the EU-Latin American connection is not limited to cartels but is multidirectional and goes beyond drug trafficking. It also demonstrates how global criminal actors converge within a fluid criminal ecosystem where networks, groups and individuals collaborate opportunistically and flexibly to maximise profits and ensure the continuity of criminal enterprises. The issue is not that Latin American cartels are copying their business model in the EU, but that actors on both sides are collaborating using their respective strengths and transforming demand and opportunities into illicit earnings.

This fluid interregional ecosystem contains MTCNs with Latin American nationals among their members who may or may not have individual links to established Latin American cartels, criminal networks that are composed of other nationalities but that engage in criminal activities in Latin America, and/or criminal networks whose leadership operates from Latin America.

Latin American nationals are part of MTCNs affecting the EU

The analysis of the membership of EU's MTCNs reveals that around one in 10 (67 MTCNs) have Latin American members. A variety of Latin American nationalities are represented in the EU's MTCNs. They operate in a range of EU Member States. They are mostly engaged in cocaine trafficking, and some are also involved in organised property crime and other crimes.

Some of the MTCNs (22 MTCNs) are predominantly made up of Latin American nationals. Organised property crime is a key criminal activity for some, and cocaine trafficking for others.

EU or other third-country nationals expand their control of criminal activities in Latin America

Seventy-five MTCNs that operate both in the EU and in Latin America do not have any Latin American members. Some EU-based MTCNs, or MTCNs from regions neighbouring the EU, have established themselves in Latin America in order to source cocaine directly from local counterparts. This is particularly the case for Italian and Western Balkan networks. The Italian 'Ndrangheta, for instance, has set up extensive cocaine trade routes in Latin America and uses Albanian criminal networks to oversee these deals on the ground. Consequently, they have succeeded in establishing a dominant position in drug trafficking from Latin America, ensuring end-to-end control of the criminal process. Some Albanian networks have settled in Latin America and continue to benefit from their transactional relationships with cartels. Other Western Balkan networks have also expanded their involvement in the cocaine trafficking business.

Case example

LARGE-SCALE DRUG TRAFFICKING FROM SOUTH AMERICA TO EUROPE

A criminal network orchestrated the trafficking of large amounts of cocaine from Colombia, Brazil and Ecuador to the EU. The shipments went to logistical hubs in Western Africa and the Canary Islands. From there, the drugs were further distributed via handling centres in Belgium, Croatia, Germany, Italy and Spain. The coordinators and brokers, originating from the Western Balkan region, relied on a broad network of criminal associates, posted in various locations on a long-term basis, to facilitate the drug trafficking operations. International law enforcement cooperation was crucial to disrupt this transnational criminal network[50].

MTCN leadership is settled in Latin America in order to control and hide – and vice versa

Importantly, a number of MTCNs have their leaders based in Latin America. This is the case, logically, for the cartel-style MTCNs that predominantly operate from Latin America and have some individual contacts in the EU.

However, the same applies to MTCNs based in the EU or its neighbourhood that are involved in criminal activities affecting the EU. Some MTCNs reported by EU Member States have leadership based in Latin America.

Having leadership functions based in Latin America facilitates the criminal process, particularly for drug trafficking. Key departure and transit points are targeted in order to control and secure the movement of drugs. Having a presence in Latin America can also facilitate access to specific expertise, such as the ability to incorporate and extract cocaine into carrier materials.

The leadership of EU-centred MTCNs has also been found to relocate to Latin America to avoid law enforcement action in Europe. This, combined with the benefits of managing the criminal process at source, represents a double win.

Conversely, Latin American MTCNs have also settled in the EU, from where they direct operations that affect the EU. This is particularly the case for mobile criminal networks involved in organised property crime.

Drug trafficking, but not only

Cocaine trafficking involves cooperation between Latin American and EU-based MTCNs

These interregional MTCNs are primarily involved in the trafficking of cocaine. They have been established for many years, use sophisticated countermeasures and either set up their own LBS or infiltrate them at high level.

As Latin America is a source region for cocaine, it follows that it commonly acts as a hub for cocaine trafficking networks. Of the 111 MTCNs operating (partly) in Latin America, 89 are engaged in cocaine trafficking alongside other types of drugs.

Latin American nationals are typically responsible for arranging and providing specialised services related to drug trafficking to Europe. These services may include specialised skills related to concealing or extracting drugs upon arrival in Europe. Another very specialised trafficking method involves constructing semi-submersibles for crossing the Atlantic. These semi-submersibles are usually manned by Latin American nationals[51].

Latin American nationals also provide specialised services related to cocaine production in Europe, including extracting cocaine from various carrier materials or the processing of trafficked coca paste. They also bring expertise in producing synthetic drugs, such as methamphetamine. This expertise encompasses both technical and logistical know-how.

Latin American networks linked to drug trafficking are also involved in other types of crime, including violence-as-a-service.

A significant aspect of cocaine trafficking involves the exploitation of LBSs. Criminal networks establish legal companies in both Latin America and Europe to use as a cover for cocaine trafficking.

Organised property crime by Latin American MTCNs targeting the EU

Latin American networks are involved in organised property crime in EU Member States. They are particularly active in domestic burglaries and theft by deception, as well as pickpocketing and theft from shops and robberies. They focus on loot that can be disposed of quickly, such as cash, jewellery, watches, and designer goods. The stolen goods are either resold via existing fencing structures in the EU, or sent back to their home countries, primarily via parcel shipments.

Being primarily active in EU Member States in the southern and western part of the EU, criminal networks composed of Latin American suspects are often very mobile and travel through several EU Member States to commit burglaries and thefts. These MTCNs are not hierarchically structured, but rather exhibit characteristics of a flexible, loose and fluid network, with group composition frequently changing.

While some networks and their leaders are based in EU Member States, most offenders are likely to enter the Schengen area legally for a limited period of time[52] to carry out their criminal activities. They use short-stay accommodation and rental vehicles to move between crime locations. Some return to their home country within the legally permitted timeframe, while others overstay.

They use fraudulent documents to hide their identities and often use rental cars, sometimes rented through straw men, to travel between countries and commit organised property crimes.

Latin American MTCNs exploit Latin American victims in the EU for sexual and labour exploitation

Latin American MTCNs are active in trafficking in human beings (THB) across the EU, exploiting victims for sexual and labour purposes. They mostly exploit Latin American victims, who are generally recruited on social media platforms. Victims of THB for sexual exploitation are typically aware of what to expect in the EU, as advertisements openly promote sex work alongside attractive salary and accommodation packages. In cases of labour exploitation, victims may be aware that they are going to work illegally in the EU, but not that they will be exploited.

The Latin American MTCNs involved in THB have a networked structure. They are organised into cells and sub-cells based in different countries, both within and outside the EU. These cells work closely together, each performing a specific function within the organisation, such as operating call centres, handling money transfers and money laundering, and posting online adverts to recruit victims. Call centres play a crucial role in the exploitation of victims by criminal networks across EU countries. The call centre operators act as coordinators among the cells, offering victims' services on adult service websites and managing their online profiles. Latin American THB criminal networks use popular messaging applications or advanced encrypted communication platforms to communicate with each other and with victims.

Transportation to the EU is generally arranged by MTCNs using regular commercial flights, without however ruling out the possibility that THB victims may, in some cases, arrange transportation to the EU on their own. Criminal networks also provide victims with practical guidance on how to avoid checks at airports and/or how to behave if they are checked by border authorities. In many cases, victims of THB for sexual exploitation leave the EU before the 90 days of their legal visa-exempt stay expire, only to return later for another three months. Once in the EU they either travel alone by public transport or are driven by members of the criminal networks to the cities and countries where they will be exploited. Latin American THB criminal networks rotate victims throughout the EU and neighbouring countries.

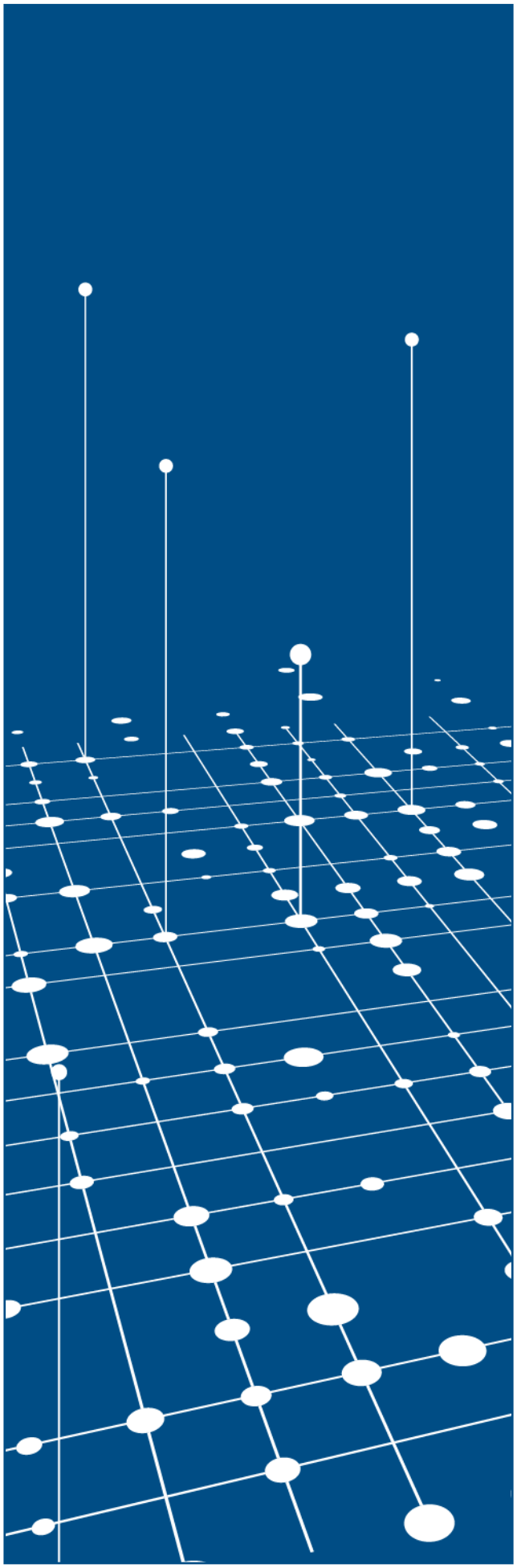
Exploitation involves a combination of psychological manipulation and physical violence. Victims are offered a seemingly convenient 50:50 split of the profits between exploiters and victims. Most victims are already working in prostitution in their home countries and are lured to the EU by the prospect of higher earnings and better living conditions. Yet, once in the EU, victims incur high expenses (travel costs to reach and travel within Europe, daily living expenses, rent, etc.) and become indebted. The level of physical violence experienced varies depending on the country of origin.

Case example

COLOMBIAN NETWORK FORCES VICTIMS INTO SEXUAL EXPLOITATION

Members of a human trafficking network advertised their victims and the services they could offer via adult sexual websites. Call centre agents negotiated prices and services with potential clients. The victims were forced to comply and provide all requested sexual services. If they did not comply with the expectations, severe physical violence followed and was filmed to intimidate other victims. Threats and violence against the victims' families in Colombia was also used[53].

Former victims sometimes become members of the criminal network. In these cases, they are mainly used to transport and control victims and, less frequently, to work in call centres arranging appointments for victims.



A BLUEPRINT OF CRIMINAL OPPORTUNISM

Why do criminal networks continue to resist and emerge? (part II)

Recognising that MTCNs are not isolated entities, but instead form part of a fluid criminal ecosystem, does not fully explain why some continue to thrive and why new players regularly emerge. It is also essential to look beyond this criminal ecosystem in which the MTCNs interact, and to consider the broader, underlying context. It then becomes clear that the MTCNs are imprinted with a blueprint of opportunism.

This latest report takes the analysis one step further. Having examined how criminal networks operate and their criminal environment, we have turned our attention to the systems that underpin them. While the criminal actors change, the conditions that enable them to emerge and thrive are continuously scanned for weaknesses to be exploited by the MTCNs. Beyond the code of threatening characteristics – being agile, borderless, controlling and destructive – MTCNs are imbued with a blueprint of opportunism that enables them to identify system weaknesses and maximise their proceeds.

The blueprint outlines the broader context in which criminal networks are able to operate and turn a profit. They achieve their objective of making money by either responding to a demand for illicit goods or services, or by proactively taking advantage of opportunities as they arise.

Such opportunities are plentiful and growing rapidly. The world's systems (digital, financial, technological and geopolitical) are becoming increasingly complex and MTCNs are better than ever at exploiting this complexity. Digitalisation, technological innovation, global instability and the growing convergence of the legal and illegal economies are creating unprecedented criminal opportunities. Criminal networks exploit online platforms, encrypted communication and AI to scale their operations while minimising risk. Globalisation and geopolitical tensions open up new markets, routes and collaborations. They evade rules creatively, exploit loopholes, and corrupt key professions and businesses to their advantage. Meanwhile, crime-as-a-service models and the exploitation of vulnerable individuals are lowering barriers to entry and increasing resilience. Overall, MTCNs are becoming more adaptive, interconnected and embedded in society, and are systematically taking advantage of structural weaknesses in modern systems.

Digital and technological opportunities

Today, criminal activities are increasingly being nurtured online (*see also What do today's MTCNs do?*)[54]. An ever-more complex digital infrastructure sustains serious and organised crime, functioning as both an enabler and a countermeasure against law enforcement detection.

While some criminal activities, such as cyber-attacks, online fraud and the distribution of CSAM occur primarily online, other MTCNs involved in trafficking or production are also increasingly using digital tools. These networks exploit online infrastructure for recruitment, advertising, trade, and financial transactions. These activities are often carried out by technical specialists, either in an established role within the criminal network or in a crime-as-a-service cooperation setting.

To shield themselves from law enforcement, MTCNs develop or use dedicated encrypted communication platforms designed to provide an E2EE that prevents external interception. They are also increasingly abusing commercial E2EE communication platforms, which are legally designed to protect users' privacy[55]. In the cybercrime environment, actors strategically leverage a variety of hosting models designed specifically to avoid detection. These include bulletproof hosting services nested across multiple jurisdictions and multi-layered routing schemes via residential proxies[56].

Case example

ENCRYPTED MESSAGING SERVICE USED BY CRIMINALS TAKEN DOWN

A coordinated operation by Dutch and French authorities, supported by Eurojust and Europol, led to the take down of the encrypted messaging service MATRIX at the end of 2024. The infrastructure of this service was technically more sophisticated than that of previous platforms such as SkyECC and EncroChat, and consisted of more than 40 servers in multiple countries. Law enforcement authorities were able to monitor the activity on the service for three months, intercepting more than 2.3 million messages in 33 different languages[57].

In the digital domain, MTCNs are also heavily involved in targeting personal, institutional and business data. Unauthorised access, data brokers and data markets play a central role in the illicit data ecosystem. Demand for data is skyrocketing, and the illicit trade in data is expected to become the biggest underground economy in the near future[58].

The evolution and increasing accessibility of AI-powered tools continues to create opportunities for serious and organised crime, expanding criminals' capabilities exponentially. As generative AI becomes more advanced and user-friendly, the scope and potential of a wide range of crimes are changing significantly, especially in terms of scale of operations and damage potential. In the context of large language models, dark AI – open-source AI systems without safeguards that are tailored to criminal use cases – may increasingly be offered as 'crime-as-a-service' tools[59]. Furthermore, integrating AI automation tools into legitimate security contexts and business applications creates new vulnerabilities and avenues for criminal exploitation[60].

Leveraging financial opportunities and exploiting systemic vulnerabilities

MTCNs sustain themselves through an opaque financial ecosystem established to facilitate their operations across national borders, circulate their illicit proceeds among members, facilitators and associates, and keep their wealth as far away as possible from law enforcement detection. This opaque financial ecosystem replicates the legal one while severely impacting the very foundations of the EU and its society[61], and undermining the strength of legitimate financial institutions and the fair competitiveness of legal markets. Overall, it weakens the Union's economy and its internal security. The fact that the confiscation of criminal proceeds remains low is clear evidence of the existence of a robust underground criminal financial system.

A key factor in the resilience of MTCNs is their ability to capitalise on every opportunity and exploit all vulnerabilities in the legal economic and financial systems. Money laundering and corruption are the key cornerstones of this exploitation mechanism, fuelling organised crime operations and contributing to its resilience.

This parallel financial system is increasingly facilitated by digital platforms and enhanced by emerging technologies[62]. MTCNs make use of the most innovative commercial tools and the latest financial technologies, which allow for the quick and easy transfer of illicit funds across continents. They take advantage of weak regulatory frameworks and uneven anti-money laundering standards across jurisdictions.

The use of cryptocurrencies in organised crime is evolving rapidly in response to advancements in blockchain technology, decentralisation, and anonymisation tools. Cryptocurrencies provide a layer of pseudo-anonymity, which makes it challenging to trace illicit transactions. Techniques such as chain hopping, crypto-swapping, and the use of privacy-focused coins further obscure the opacity of these transactions. Crypto assets are no longer solely a facilitator of cybercrime, but are now a well-established means of obfuscation in the wider serious and organised crime landscape[63].

Blurred boundaries between legal and illegal activities

One of the characteristics of the MTCNs is that they tend to blur the boundaries between legal and illegal activities in order to commit and conceal crimes, and to reinvest profits in legitimate businesses and influence otherwise legal markets. To this end, they exploit opportunities provided by seemingly legitimate companies and professionals who, knowingly or unknowingly, contribute to the criminal activities.

The misuse of LBS persists

The vast majority of the MTCNs **use LBSs (85%)**. They most often do so at a high level by setting up their own LBS, infiltrating existing LBSs at management level, or colluding with or coercing key high-level individuals within the structures, in order to gain access to or control over the LBS. Some MTCNs infiltrate the LBS at a low level by colluding with or coercing employees, or by misusing the LBS unknowingly.

All areas of crime are subject to the misuse of LBSs. However, it is strongly concentrated among drug-related criminal networks. While drug trafficking represents the single largest crime area among MTCNs abusing LBSs, a substantial proportion of poly-criminal networks are also primarily engaged in drug-related activities. Taken together, these findings indicate that drug related organised crime accounts for the majority of identified LBS abuse. Given that drug-related networks constitute approximately half of all MTCNs, their predominance among LBS-abusing networks suggests a particular reliance on legal business structures to facilitate criminal operations.

LBSs provide drug-trafficking networks with access to logistics, transport, storage and commercial infrastructures that can be used to conceal illicit activities and support the movement of drugs and criminal proceeds.

Fraud emerges as a secondary area of exploitation, while all other crime areas account for comparatively limited shares of identified LBS abuse.

Case example

OPERATION ADMIRAL 2

A criminal network was involved in large-scale VAT fraud. The suspects allegedly set up companies in 15 EU Member States, selling electronic devices via online marketplaces worth over EUR 1.48 billion. The end customers paid VAT, but the selling companies did not fulfil their tax obligations. Other companies subsequently claimed VAT reimbursement, resulting in an estimated loss of EUR 297 million. This network of companies is also believed to have been used for the laundering of illicit proceeds from drug trafficking and different types of cybercrime. The international investigation was coordinated by the European Public Prosecutor's Office with law enforcement authorities from 165 countries and with Europol support[64].

The sectors most at risk of misuse are cash-intensive businesses (including hospitality), logistics (including transport and import/export) and real estate/construction sectors[65].

Abuse of LBSs and money laundering are closely connected. The sectors most exploited for money laundering are real estate and those that handle large amounts of cash. In both sectors, the MTCNs invest their illicit proceeds in order to integrate them into the legitimate economy. These networks purchase properties via front identities or private companies, or they establish businesses either via intermediaries or in the names of network members. Often, MTCNs use a combination of money laundering techniques, e.g. via the use of digital assets, high-value goods and money transfers (bank transfers, informal value transfer systems and hawala).

Key professions

Some professions, such as lawyers, real estate agents, accountants and logistics experts play a pivotal role as enablers of MTCN activities. They provide yet another layer in the MTCNs' blueprint of opportunism by linking them to the legal economy.

As they hold key positions and have access to valuable information and expertise, they can be valuable assets for MTCNs. They provide entry points for MTCNs in the professional domains of the economy and law. These experts can leverage their professional knowledge to provide information to criminal networks, to set up financial structures to hide money flows, and to give various illicit activities a façade of legality.

Misuse occurs along a spectrum, ranging from deliberate collusion to coercion and negligence, often blurring the boundary between licit and illicit activity. The targeting and misuse of such professionals highlights how MTCNs make strategic use of systemic vulnerabilities to further their criminal activities.

Geopolitical crises open up criminal opportunities

Criminal networks are increasingly acting as proxies for hybrid threat actors, exploiting vulnerabilities to destabilise the EU and its Member States from within[66]. These shadow alliances are mutually beneficial: the criminal actors gain money, protection and/or infrastructure. The hybrid threat actors gain plausible deniability.

Although connections between the 731 MTCNs and hybrid threat actors have occasionally been reported, the nature of these links is often unclear or insufficiently substantiated. Nevertheless, some MTCNs have been found to maintain direct or indirect relationships with both State and non-State actors. This is for example the case for certain criminal networks active in cybercrime. Data stolen online and shared on dedicated platforms may be used to indirectly serve the interests of state entities and disrupt our societies. Alternatively, cyber-attacks may be carried out in service of external threat actors (*see also Cyber-attacks: successful ransomware models that remain out of reach*). State actors may recruit members of the MTCNs to leverage their resources and expertise.

Russia's war of aggression against Ukraine has contributed to shifts in the activities and geographical distribution of some Russian-speaking criminal networks. These developments may have increased the presence within the EU of certain criminal actors, including individuals associated with the Thieves-in-Law criminal milieu.

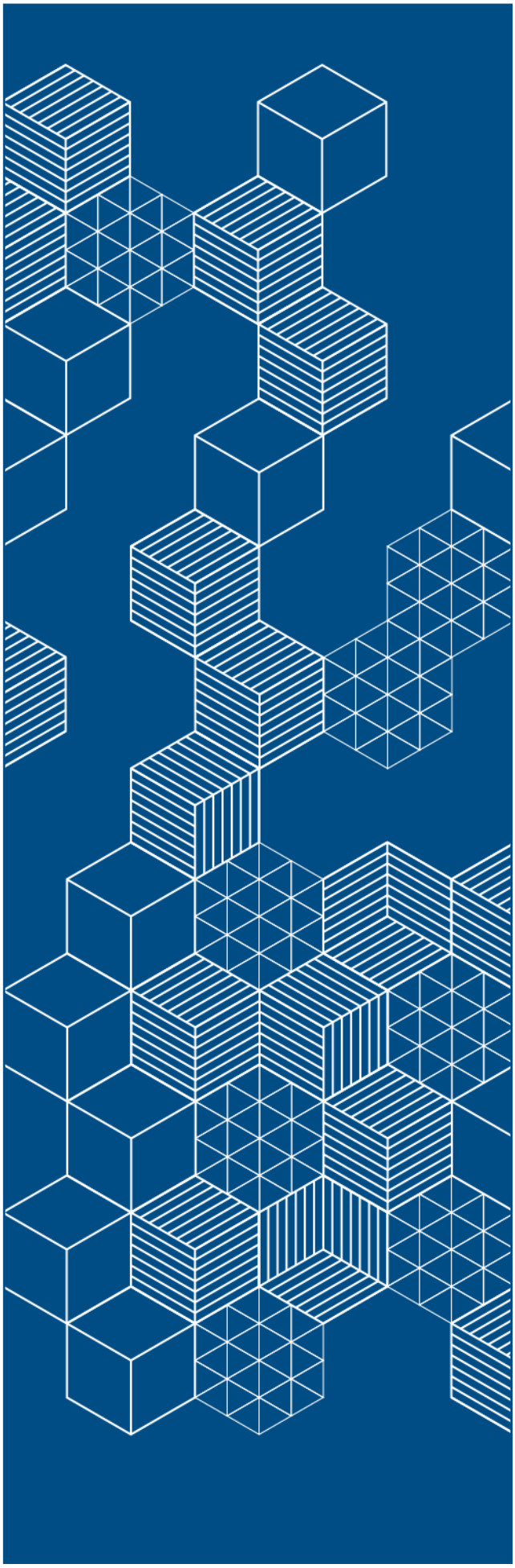
Russian-speaking MTCNs are predominantly involved in drug trafficking, fraud, organised property crime and cybercrime.

Case example

KEY FIGURE IN RUSSIAN-SPEAKING CYBERCRIME ARRESTED

The administrator of one of the world's most influential Russian-speaking cybercrime platforms was arrested in Kyiv. The platform, used by the most active and dangerous cybercriminal networks, served as a central marketplace for stolen data, hacking tools and criminal services, with more than 50 000 registered users. The suspect is also thought to have run a private messaging service for cybercriminals and acted as an arbiter for criminal disputes. In his almost twenty years of activity, the man is estimated to have made over EUR 7 million in advertising and facilitation fees[67].

To gain a comprehensive understanding of the diverse characteristics of criminal networks operating within the EU landscape and involving Russian-speaking suspects, it is crucial to examine their operational contexts, specific activities, and tactics. While it is important to consider the national backgrounds of the individuals involved, it is equally vital to recognise that these networks are often not homogeneous but rather composed of various nationalities. Focusing on the dominant nationalities within these networks can provide insights into their activities and the threats they pose to EU internal security. This approach allows for a more informed and nuanced assessment of their role within the broader context of organised crime involving Russian-speaking individuals and their activities in the EU.



Conclusion:

A SYSTEMIC APPROACH, IN PARTNERSHIP

Law enforcement has been successful in the fight against MTCNs. However, this alone is not sufficient. A more systemic approach is needed to complement the focus on criminal actors, particularly those at the top of the MTCN hierarchy. This report has shown that MTCNs swiftly reorganise within a fluid criminal ecosystem and continuously seek out criminal opportunities. Their opportunistic blueprint enables them to rapidly identify and exploit emerging criminal opportunities. A more comprehensive, systemic approach involving law enforcement and its partners is essential.

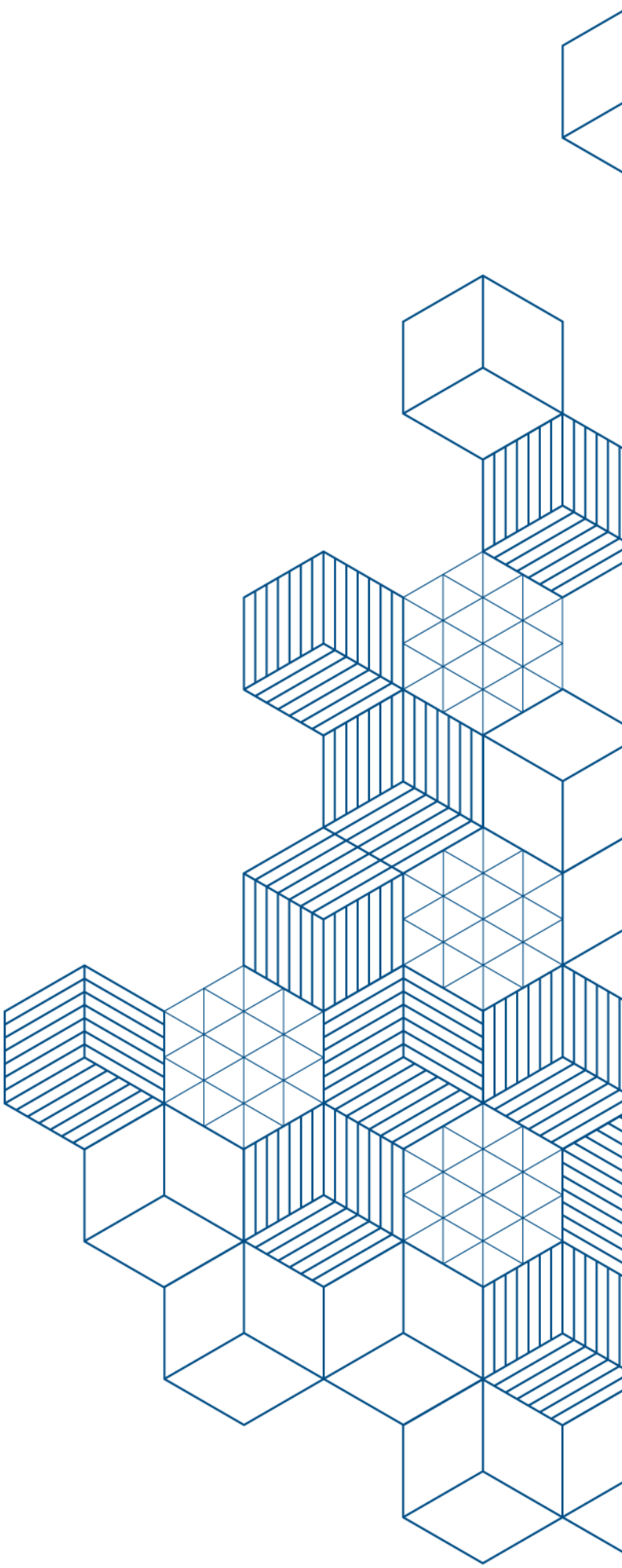
This updated report highlights two key insights. Firstly, it acknowledges the successes of law enforcement: many of the previously identified MTCNs have been disrupted and new ones are already under pressure.

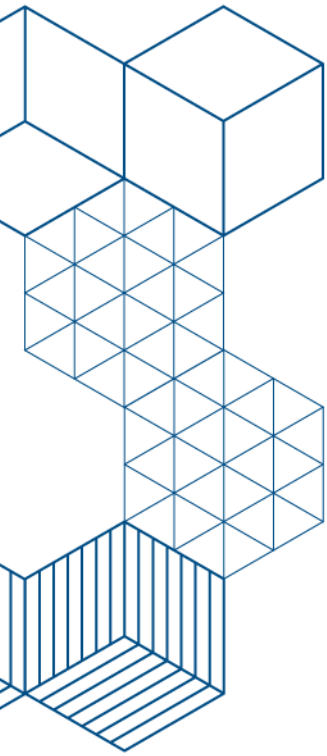
At the same time, it recognises that this is not enough to stop criminal markets from flourishing. New actors swiftly take the place of those who have been taken down and criminal businesses continue to thrive. Particularly resilient are well-established hierarchical MTCNs that remain deeply embedded within legitimate and illicit structures. The current approach appears less effective against some of these networks, whose leadership structures often remain resilient despite action against lower- and mid-level members.

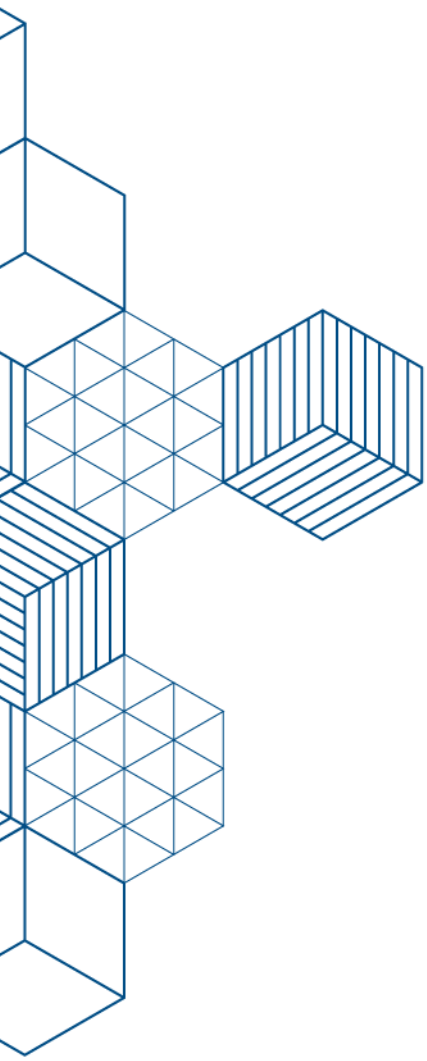
Secondly, this report provides evidence that MTCNs are not isolated entities, but function and interact in a fluid criminal ecosystem. A defining characteristic of this ecosystem is its opportunistic blueprint, which conditions criminal actors to continuously and proactively identify and exploit systemic vulnerabilities for financial gain.

Continuous efforts are needed to disrupt the activities of criminal networks. While arrests of key players can have a significant impact, more must be done. Given the adaptability of MTCNs, reducing criminal opportunities by addressing systemic vulnerabilities should complement efforts targeting criminal actors. Remedying these weaknesses is essential for effectively disrupting criminal activities and markets.

In today's globalised, complex, and volatile society, vulnerabilities that can be exploited by criminal actors are extensive and touch upon all societal dimensions. This report highlights how MTCNs opportunistically misuse companies, infrastructure, digital and technological advancements, and professionals with access to information, expertise or legal provisions. They increasingly operate within digital environments that facilitate criminal activities, misusing online platforms, encrypted communication tools and AI without any regulation or restrictions to enhance the scale, speed and resilience of their operations. This assessment also demonstrates how MTCNs adapt rapidly to changing circumstances, modifying their modus operandi, find better routes, develop new cooperation schemes or create alternative markets for their illicit goods or services. MTCNs systematically scan for structural weaknesses in modern systems, further embedding and interconnecting themselves in society.







Addressing these challenges effectively calls for a broader, more integrated approach beyond conventional law enforcement methods. The complex nature of organised crime requires a tailored approach that targets its core: the actors, HVTs and the MTCNs as a whole, while also protecting the sectors and communities most affected by organised crime. Combining the already mature and effective actor-oriented approach with a system-oriented approach can support a Europe-wide response to organised crime by combining reactive disruption and systemic prevention. Only by combining approaches that tackle HVTs, investigate the criminal networks as a whole, and reduce criminal opportunities, can we build a response that is stronger than the sum of its parts.

Tackling these vulnerabilities requires a broad range of approaches to complement a purely law enforcement-based approach on HVTs and MTCNs. This includes an **administrative approach** to halting organised crime's exploitation of legal businesses or other legal provisions. It includes a **preventive approach** with room for the development of awareness campaigns and prevention initiatives to protect victims and to dissuade vulnerable people from participating in organised crime. It is of key importance today to embed **innovation** and **technology** in our approaches, by investing in research and development to ensure that the tools used by law enforcement and other relevant partners in the fight against serious and organised crime leverage today's digital and technological advances. A **data-oriented and intelligence-led approach** is also required. This includes facilitating lawful access to data for law enforcement purposes and improving consistency in data retention practices where appropriate, recognising the central role of data in investigations and operational activities. A **financial approach** with strengthened asset tracing is another essential prerequisite. A **legal focus** is necessary to close jurisdictional gaps alongside with developing robust legislation where necessary. And through all of this, a **collaborative approach** is required: law enforcement must join forces with other public authorities and the private sector. It must continue to bring together relevant authorities from around the globe to exchange information and collaborate continuously.

The findings of this report demonstrate that tackling MTCNs requires a coordinated and whole-of-society approach. This involves joining forces with all relevant partners to address the root causes of criminal activities in the long term, while continuing to target key criminal actors and networks in the short term to limit their destructive impact on our societies and prevent them from developing criminal hegemony.

Such a complementary, multi-disciplinary approach should also be incorporated by design. By design means that when setting up new legislation, policies, initiatives, or when implementing technology, we should think ahead of potential criminal misuse.

An effective response to criminal networks requires sustained cooperation between law enforcement, public authorities, private-sector partners and civil society, combining disruption of criminal actors with measures that reduce criminal opportunities and strengthen societal resilience.

BACKGROUND

Breaking the code

In April 2024, Europol published its first in-depth analysis of the criminal networks posing the greatest threat to the EU's internal security[1].

The report provided a detailed description of the organisational structures of the most threatening criminal networks (MTCNs), their criminal activities, and their operational patterns and locations. It also assessed the specific characteristics of these criminal networks, which are instrumental to understanding the threat they pose.

In doing so, the analysis decoded the ABCD of the MTCNs affecting the EU.

A	**stands for agile.**

MTCNs combine flexibility and adaptability, with a very high degree of resilience. They exploit legal opportunities to their advantage and are capable of persisting for many years.

B	**stands for borderless.**

MTCNs operate in multiple countries, some having a global reach. However, they have a regional focus and do not expand their activities as part of their risk management strategy.

C	**stands for controlling.**

MTCNs control their activities through specialisation, close management and end-to-end control, cooperation with equals or outsourcing what is beyond their reach or exposes them.

D	**stands for destructive.**

Criminal activities, corrupt practices and related violence damage the EU's internal security, rule of law and economy. They have a direct impact on EU citizens' lives.

This analysis has triggered further information exchange and international cooperation, strengthening investigations through international collaboration and access to additional resources.

Deepening the insights

In June 2024, the Council of the European Union issued new Council conclusions on mapping the most threatening criminal networks[2]. The Council tasked the Member States and Europol with delivering follow-up reports, including on the misuse of legal business structures[3]. In addition, the Council ensured continuous follow-up of this actor-focused analytical perspective, by requesting the mapping exercise of the MTCNs on a biennial basis.

This report is the first update in this biennial series. Its actor-based perspective complements the findings of the EU Serious and Organised Crime Threat Assessment (EU-SOCTA). The analytical findings set out in this report will in its turn inform the EU-SOCTA Interim Report on new, changing and (re)emerging threats 2027, as well as the subsequent EU biennial EMPACT Operational Action Plans.

Recalibration

The 2026 dataset comprising the EU's most threatening criminal networks is a recalibration of the 2024 dataset.

Each dataset represents a snapshot of the criminal networks that EU Member States and partner countries currently consider to be the most threatening. EU Member States and third partners autonomously decide how many MTCNs to contribute and which criteria to use to select them, based on national priorities and information.

Updating the dataset

The initial analysis in 2024 was based on a unique dataset. It drew on information provided by EU Member States and third countries with which Europol has cooperation agreements. The analysis was specifically designed to improve the understanding of what makes each MTCN particularly threatening.

For this second issue, this dataset was thoroughly updated by our law enforcement partners and complemented by relevant information available at Europol as a criminal information hub.

Firstly, the 821 MTCNs identified in 2024 were updated with a focus on their current status. Are they still considered to be some of the most threatening criminal networks? If so, how has their status evolved? If not, why not? What actions have been taken to tackle the criminal network?

Secondly, the EU Member States and partner countries added information on newly identified criminal networks that are considered to be the most threatening.

Thirdly, this dataset was enriched with operational and strategic information provided to Europol in support of serious and organised crime investigations at an international level. In 2025, Europol supported more than 4 000 investigations, including those involving high-value targets (HVT) and operational taskforces (OTF).

As a result, an updated set of 731 criminal networks were identified that are currently considered to be the most threatening ones affecting the EU. These include:

- 198 MTCNs were already considered MTCNs in 2024;
- 533 MTCNs have been newly identified as MTCNs.

This report is based on the analysis of the dataset comprising the **731** most threatening criminal networks identified for the 2026 update. It also draws on the 2024 dataset to assess operational follow-up.

ENDNOTES

1 Europol, 2024, Decoding the EU's most threatening criminal networks, accessible at https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks.

2 Council of the European Union, Council conclusions on mapping the most threatening criminal networks (14 June 2024), 11153/24, accessible at https://data.consilium.europa.eu/doc/document/ST-11153-2024-INIT/en/pdf.

3 Europol, 2024, Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures, accessible at https://www.europol.europa.eu/publications-events/publications/leveraging-legitimacy-how-eu%E2%80%99s-most-threatening-criminal-networks-abuse-legal-business-structures.

4 For a number of the initial MTCNs, no update was provided. These have been considered as no longer being among the MTCNs.

5 Europol, 2025, Europol in brief, accessible at https://www.europol.europa.eu/publication-events/main-reports/europol-in-brief#downloads

6 Europol, 29 January 2026, Large migrant smuggling operation in Bulgaria leads to 16 arrests, accessible at https://www.europol.europa.eu/media-press/newsroom/news/large-migrant-smuggling-operation-in-bulgaria-leads-to-16-arrests

7 Europol, 27 March 2026, Major operation targets one of Scotland's most violent crime networks, accessible at https://www.europol.europa.eu/media-press/newsroom/news/major-operation-targets-one-of-scotland%E2%80%99s-most-violent-crime-networks

8 Europol, 24 March 2026, Five-country operation targets cigarette smuggling network operating from the UK, accessible at https://www.europol.europa.eu/media-press/newsroom/news/five-country-operation-targets-cigarette-smuggling-network-operating-uk

9 Europol, 6 March 2026, From a small Swedish town to a global crime network: international operation strikes top-tier organised crime, accessible at https://www.europol.europa.eu/media-press/newsroom/news/small-swedish-town-to-global-crime-network-international-operation-strikes-top-tier-organised-crime

10 Stricter criteria for inclusion in the MTCN list may have resulted in the declassification of a number of criminal networks. As there are no common criteria between countries on what constitutes an MTCN, law enforcement authorities can decide based on their national criteria and priorities.

11 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime#downloads

12 Significant progress has been made in the first year of operation: 280 suspects have been arrested, and over 14 000 accounts linked to violence-as-a-service have been taken down. This has disrupted the activities of various criminal networks operating in multiple countries.

13 Europol, 19 June 2025, Teenagers recruited as hitmen: Denmark and Sweden strike back at violence-as-a-service, accessible at https://www.europol.europa.eu/media-press/newsroom/news/teenagers-recruited-hitmen-denmark-and-sweden-strike-back-violence-service

14 In the 2024 report, MTCNs with 1 000 members or more were disregarded in the calculation as they were considered outliers, bringing the total number at 'more than 25 000'.

15 Europol, 8 October 2025, Five central suspects arrested in whole-sale cocaine trafficking case, accessible at https://www.europol.europa.eu/media-press/newsroom/news/five-central-suspects-arrested-in-whole-sale-cocaine-trafficking-case

16 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads.

17 Europol, 13 May 2025, International crackdown dismantles multimillion-euro investment scam, accessible at https://www.europol.europa.eu/media-press/newsroom/news/international-crackdown-dismantles-multimillion-euro-investment-scam

18 Europol, 28 November 2025, 29 suspects arrested in two blows against human trafficking networks, accessible at https://www.europol.europa.eu/media-press/newsroom/news/29-suspects-arrested-in-two-blows-against-human-trafficking-networks

19 Europol, 31 May 2024, International crackdown dismantles multimillion-euro investment scam, accessible at https://www.europol.europa.eu/media-press/newsroom/news/international-crackdown-dismantles-multimillion-euro-investment-scam

20 Europol, 20 March 2026, Global cybercrime crackdown: over 373 000 dark web sites shut down, accessible at https://www.europol.europa.eu/media-press/newsroom/news/global-cybercrime-crackdown-over-373-000-dark-web-sites-shut-down

21 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads.

22 Europol, 17 October 2025, Cybercrime-as-a-service takedown: 7 arrested, accessible at https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

23 Europol, 29 April 2026, Call centres dismantled and ten arrested in EUR 50 million online fraud case, accessible at https://www.europol.europa.eu/media-press/newsroom/news/call-centres-dismantled-and-ten-arrested-in-eur-50-million-online-fraud-case

24 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads.

25 Europol, 16 April 2026, Europol-supported global operation targets over 75 000 users engaged in DDoS attacks, accessible at https://

www.europol.europa.eu/media-press/newsroom/news/europol-supported-global-operation-targets-over-75-000-users-engaged-in-ddos-attacks

26 Europol, 21 May 2026, Cybercriminal VPN used by ransomware actors dismantled in global crackdown, accessible at https://www.europol.europa.eu/media-press/newsroom/news/cybercriminal-vpn-used-ransomware-actors-dismantled-in-global-crackdown

27 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads.

28 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads

29 Europol, 2025, Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users, accessible at https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users

30 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads

31 Ibid.

32 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime#downloads

33 Ibid.

34 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads.

35 FBI, 2025, Public Service Announcement, Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe, accessible at https://www.ic3.gov/PSA/2025/PSA250306.

36 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads

37 Europol, 2015, Exploring tomorrow's organised crime, accessible at https://www.europol.europa.eu/publications-events/publications/exploring-tomorrow%E2%80%99s-organised-crime.

38 Ibid.

39 Ibid.

40 Europol, 12 August 2025, Internationally active Albanian organised crime network busted – 10 arrests, accessible at https://www.europol.europa.eu/media-press/newsroom/news/internationally-active-albanian-organised-crime-network-busted-10-arrests

41 Europol, 27 January 2025, 23 underground bankers arrested, accessible at https://www.europol.europa.eu/media-press/newsroom/news/23-underground-bankers-arrested

42 Europol, 25 March 2026, Small boats supply chain disrupted: 21 arrested for supplying Channel smugglers with nautical equipment, https://www.europol.europa.eu/media-press/newsroom/news/small-boats-supply-chain-disrupted-21-arrested-for-supplying-channel-smugglers-nautical-equipment

43 Europol, 14 August 2025, From instigator to perpetrator: how violence-as-a-service operates, accessible at https://www.europol.europa.eu/media-press/newsroom/news/instigator-to-perpetrator-how-violence%E2%80%91%E2%80%91%E2%80%91service-operates.

44 Europol, 27 January 2026, Diversification in maritime cocaine trafficking modi operandi, accessible at https://www.europol.europa.eu/publications-events/publications/diversification-in-maritime-cocaine-trafficking-modi-operandi and Europol, 8 May 2026, Atlantic 'Cocaine Highway' broken in coordinated maritime operation, accessible at https://www.europol.europa.eu/media-press/newsroom/news/atlantic-cocaine-highway-broken-in-coordinated-maritime-operation

45 Europol, 28 February 2025, Criminal ringleader and nine associates arrested after killing a witness, accessible at https://www.europol.europa.eu/media-press/newsroom/news/criminal-ringleader-and-nine-associates-arrested-after-killing-witness

46 Europol, 13 May 2026, Swedish fugitive arrested as new OTF Grimm targets added to EU Most Wanted, accessible at https://www.europol.europa.eu/media-press/newsroom/news/swedish-fugitive-arrested-new-otf-grimm-targets-added-to-eu-most-wanted

47 This is the country investigating the MTCN.

48 The leadership is settled in the main country of activity for 64% of the MTCN and in the country of origin of the key members for 22%.

49 Europol, 3 March 2026, Europol supports takedown of cocaine trafficking network linked to Los Lobos cartel, accessible at https://www.europol.europa.eu/media-press/newsroom/news/europol-supports-takedown-of-cocaine-trafficking-network-linked-to-los-lobos-cartel

50 Europol, 13 June 2024, Cocaine cartel collapses after final arrests in Spain, accessible at https://www.europol.europa.eu/media-press/newsroom/news/cocaine-cartel-collapses-after-final-arrests-in-spain

51 Europol, January 2026, Diversification in maritime cocaine trafficking modi operandi, accessible at https://www.europol.europa.eu/publications-events/publications/diversification-in-maritime-cocaine-trafficking-modi-operandi

52 Most citizens of South American countries can enter the Schengen zone visa-free for up to 90 days in any 180-day period for tourism, business and family visits.

53 Europol, 08 September 2025, Dozens of sex trafficking victims in Austria – five arrests in Colombia, accessible at https://www.europol.europa.eu/media-press/newsroom/news/dozens-of-sex-trafficking-victims-in-austria-%E2%80%93-five-arrests-in-colombia

54 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025 – The changing DNA of serious

and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime#downloads.

55 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025 – The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime#downloads

56 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads.

57 Europol, 3 December 2024, International operation takes down another encrypted messaging service used by criminals, accessible at https://www.europol.europa.eu/media-press/newsroom/news/international-operation-takes-down-another-encrypted-messaging-service-used-criminals

58 Europol, 2025, Internet Organised Crime Threat Assessment (IOCTA) 2025. Steal, deal and repeat. How cybercriminals trade and exploit your data, accessible at https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data.

59 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU-SOCTA 2025), accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime#downloads.

60 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads.

61 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU-SOCTA 2025), accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime#downloads.

62 Ibid.

63 Europol, 2026, Internet Organised Crime Threat Assessment (IOCTA) 2026, accessible at https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape#downloads.

64 Europol, 28 November 2024, 400 companies part of EUR 297 million VAT fraud network, accessible at https://www.europol.europa.eu/media-press/newsroom/news/400-companies-part-of-eur-297-million-vat-fraud-network

65 These three sectors represent 70% of the misused LBSs; 24% in the cash-intensive sector, 23% in the logistics sector and 22% in the real estate sector.

66 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU-SOCTA 2025), accessible at at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime#downloads.

67 Europol, 23 July 2025, Key figure behind major Russian-speaking cybercrime forum targeted in Ukraine, accessible at https://www.europol.europa.eu/media-press/newsroom/news/key-figure-behind-major-russian-speaking-cybercrime-forum-targeted-in-ukraine

GETTING IN TOUCH WITH THE EU

IN PERSON

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

ON THE PHONE OR IN WRITING

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls)
- at the following standard number: +32 22999696
- via the following form: www.european-union.europa.eu/contact-eu/write-us_en

FINDING INFORMATION ABOUT THE EU

ONLINE

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU PUBLICATIONS

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU LAW AND RELATED DOCUMENTS

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU OPEN DATA

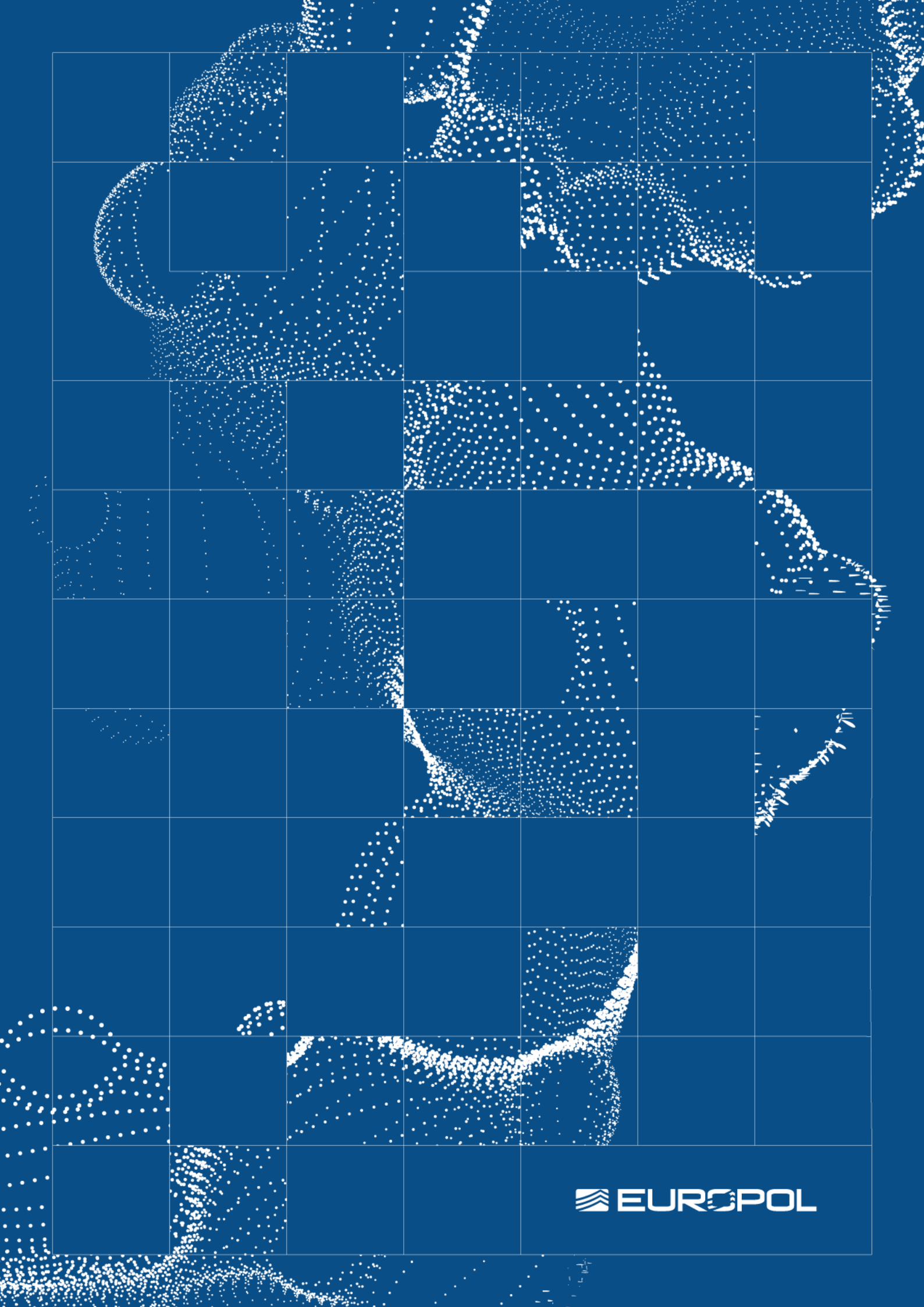
The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Your feedback matters.

By scanning the embedded QR code you can fill in a short user survey on the received strategic report.

Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/eus_strategic_reports


EUROPOL