

**DECODING**

**THE EU'S MOST  
THREATENING**

**CRIMINAL  
NETWORKS**



## DECODING THE EU'S MOST THREATENING CRIMINAL NETWORKS

PDF | ISBN 978-92-95236-25-7 | DOI: 10.2813/811566 | QL-05-24-250-EN-N

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2024

© **European Union Agency for Law Enforcement Cooperation, 2024**

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Union Agency for Law Enforcement Cooperation, permission must be sought directly from the copyright holders.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder. Photograph page 4 by Nicolas Peeters.

**Cite this publication:** Europol (2024), Decoding the EU's most threatening criminal networks, Publications Office of the European Union, Luxembourg.

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

[www.europol.europa.eu](http://www.europol.europa.eu)



# CONTENTS

<b>04</b>	<b>FOREWORD BY THE EUROPOL EXECUTIVE DIRECTOR</b>
<b>06</b>	<b>IDENTIFYING THE MOST THREATENING CRIMINAL NETWORKS</b>
06	Context: enhancing our understanding of criminal networks
07	A unique dataset
<b>08</b>	<b>EXECUTIVE SUMMARY</b>
09	Methodology and dataset
10	The ABCD of the most threatening criminal networks
18	A tailored approach
<b>19</b>	<b>DESCRIBING THE MOST THREATENING CRIMINAL NETWORKS</b>
19	Internal organisation and composition
27	Criminal activities
<b>39</b>	<b>WHAT MAKES CRIMINAL NETWORKS MOST THREATENING?</b>
39	Their infiltration in the legal business world for facilitation of criminal activities, as a countermeasure, or for money laundering
44	Their international reach with regional focus
47	Their survival strategies: adaptive problem solving and countermeasures
50	Their criminal cooperation model
51	Their – often combined – use of violence and corruption
55	Their resources – from money to expertise
<b>58</b>	<b>CONCLUSION</b>



**Catherine De Bolle**  
Executive Director of Europol

# FOREWORD BY THE EUROPOL EXECUTIVE DIRECTOR

I am pleased to present Europol's first report on the most threatening criminal networks active in the EU. This report distils a wealth of information on 821 criminal networks active in the EU, gathered by Europol in the context of our regular support to criminal investigations. It is also based on a targeted data collection effort, which has granted us an unprecedented intelligence picture. Its findings represent the most detailed contemporary study on the most threatening criminal networks ever undertaken by the European law enforcement community.

All EU Member States and several Europol partner countries provided intelligence on what they consider to be the most threatening criminal networks active in the EU. The data they provided followed a dedicated methodology and a common set of indicators agreed with Europol.

This enabled Europol to single out the 821 most threatening criminal networks operating in the EU. Their 25 000 members commit crimes for profit and are capable of operating in multiple countries simultaneously, impacting the lives of millions of EU citizens.

Each of the 821 identified criminal networks is unique. They vary in composition, structure, criminal activity, territorial control, longevity, types of cooperation and a range of other dimensions.

This report decodes the ABCD of the most threatening criminal networks and assesses what makes these networks most threatening – they are Agile, Borderless, Controlling and Destructive.

This analysis of over 800 criminal networks lays the foundations for tackling and disrupting their operations. Investigating and bringing them to justice is a goal that can only be achieved through a culture of police cooperation across Europe and beyond.

With this first analysis, Europol and our partners make the invisible visible and decode the inner workings of criminal networks.

# IDENTIFYING THE MOST THREATENING CRIMINAL NETWORKS

**This report is the first of its kind to analyse in depth the characteristics that make criminal actors particularly threatening. Enhancing law enforcement's understanding of their functioning and core capabilities will further strengthen the fight against serious and organised crime. It is essential as a complement to a commodity-based approach.**

## **Context: enhancing our understanding of criminal networks**

Serious and organised crime is omnipresent and continues to represent a major threat to the internal security of the European Union (EU). In order to fight it effectively, law enforcement needs to understand the key areas where it should prioritise resources. The threat posed by organised crime is often assessed through the dimension of criminal markets and criminal activities. However, the picture is incomplete without analysing the capabilities and intent of its key players. One key approach is to focus on and address the most threatening criminal networks that affect the internal security of the EU. Understanding their critical strengths is paramount as these are the criminal networks that exert significant negative impact on the societies and economies of EU Member States.

The EU Serious and Organised Crime Threat Assessment (SOCTA) 2021 brought the changing relationships between criminal actors into focus in an organised crime landscape that is characterised by a networked environment where cooperation between criminals is fluid, systematic and profit-driven.<sup>1</sup> The concept 'criminal network' reflects the nature of the current criminal landscape, which is complex and includes a variety of criminal associations. Criminal networks involve collaboration between groups and individuals – groups of different organisational character, and individuals who are either embedded within a particular network or operate outside of it.

This analysis brings to light the characteristics of those criminal networks that pose the highest threat to the EU's internal security. The aim is to strengthen our understanding of criminal networks, in order to help policy makers and law enforcement make informed policy and operational decisions to tackle them.

This report responds to several initiatives that highlight the need to enhance our understanding of what shapes the threat of criminal networks, including by the EU Justice and Home Affairs Ministers and the current Belgian Presidency of the EU Council.<sup>2</sup> The results of the analysis will complement the commodity-based assessment of the EU SOCTA 2025 with a deeper criminal-actor focused analysis. It will also support the EMPACT Operational Action Plan on High-Risk Criminal Networks on developing a methodology to identify the most threatening criminal networks. It forms part of the EU roadmap to fight drug trafficking and organised crime under Action 4.<sup>3</sup>

1 Europol, 2021, European Union Serious and Organised Crime Threat Assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg, accessible at [https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021\\_1.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf)

2 Belgian presidency, Council of the European Union, Priorities, accessed on 8 February 2024, accessible at <https://belgian-presidency.consilium.europa.eu/en/programme/priorities/>

3 European Commission, Communication from the Commission to the European Parliament and the Council on the EU roadmap to fight drug trafficking and organised crime, COM/2023/641 final, 18 October 2023, accessible at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0641>

## A unique dataset

This analysis is based on a unique dataset designed specifically for this purpose and, where relevant, illustrated with additional information already shared with Europol as the European hub for criminal information.

Based on agreed criteria from the EU SOCTA methodology, EU Member States and Europol's partner countries joined forces to identify the most threatening criminal networks active in and affecting the EU. This resulted in a unique dataset of 821 most threatening criminal networks<sup>4</sup>, with extensive information on all relevant aspects that describe them and help assess their threat. These data have a twofold significance for EU law enforcement.

The data collection has a unique importance as an intelligence-led assessment of how the most threatening criminal networks are organised, what criminal activities they engage in and how and where they operate. It provides unprecedented insights into the key features of these networks that contribute to make them particularly menacing for the EU's internal security. This will considerably strengthen our common understanding of how criminal networks operate. This assessment should help policy makers and law enforcement to make informed policy and operational decisions to tackle them. It is a starting point for future analysis of criminal actors, and will be further elaborated in forthcoming analytical products, such as the EU SOCTA 2025.

Secondly, this vast amount of criminal data collected, now centralised at Europol, further reinforces the Agency's role as a criminal information hub. It constitutes a pivotal asset in enhancing operational effectiveness, enabling law enforcement to better target and conduct criminal investigations in the framework of cross-border police cooperation. It will allow allocating investigative resources more efficiently and ultimately enhancing public security.

***The analysis is based on data on the 821 identified most threatening criminal networks affecting the EU, contributed by Member States and third countries.***

---

<sup>4</sup> Any mention of criminal networks in this report, refers to the most threatening criminal networks as identified for the purpose of this report.

# EXECUTIVE SUMMARY

The European Union's (EU) internal security continues to be threatened by serious and organised crime. To effectively prioritise resources and guide policy action aimed at addressing this issue, it is essential to build a clear understanding not only of criminal activities but also of those responsible for them. In the past, serious and organised crime has been analysed through the lens of criminal markets and activities and, in turn, their impact on the EU's economy and society. However, without a comprehensive assessment of criminal networks, the picture is incomplete. Criminal networks commit organised crime for profit, operating across borders. The current criminal landscape in the EU is complex and includes a wide variety of associations. Networks are made up of groups of different organisational structures, and individuals who are either embedded in a particular criminal network or operate outside of it.



# Methodology and dataset

This mapping exercise on the most threatening criminal networks active in and affecting the EU was conducted in four steps. First, Member States and third countries identified the most threatening criminal networks for the EU’s internal security at national level. Second, the characteristics of these groups were described. Third and most importantly, the key characteristics that heighten the threat level of criminal networks were assessed. Finally, based on these deepened insights, we highlight key areas to target in strategic, tactical, operational and proactive approaches.

**EU Member States and third countries identified a total of 821 most threatening criminal networks** active in the European Union, and affecting the region’s internal security. The total membership of the identified networks **exceeds 25 000 individuals**.

These criminal networks were selected based on criteria around the threat they pose.<sup>5</sup> This overview of 821 most threatening criminal networks is a unique feat for the European Union as it brings together details on their functioning and operations in a uniform way by all contributing countries.

These networks and the suspects they are composed of are **active in a range of crime areas, such as drug trafficking, frauds, property crime, migrant smuggling and trafficking in human beings (THB), among others**. Drug trafficking clearly stands out as a key activity – **half (50 %) of the most threatening criminal networks are involved in drug trafficking, either standalone or as part of a portfolio of activities. One third (36 %) have a unique focus on drug trafficking**.

Trends around the most threatening criminal networks were identified through the analysis of the full dataset of 821 networks.

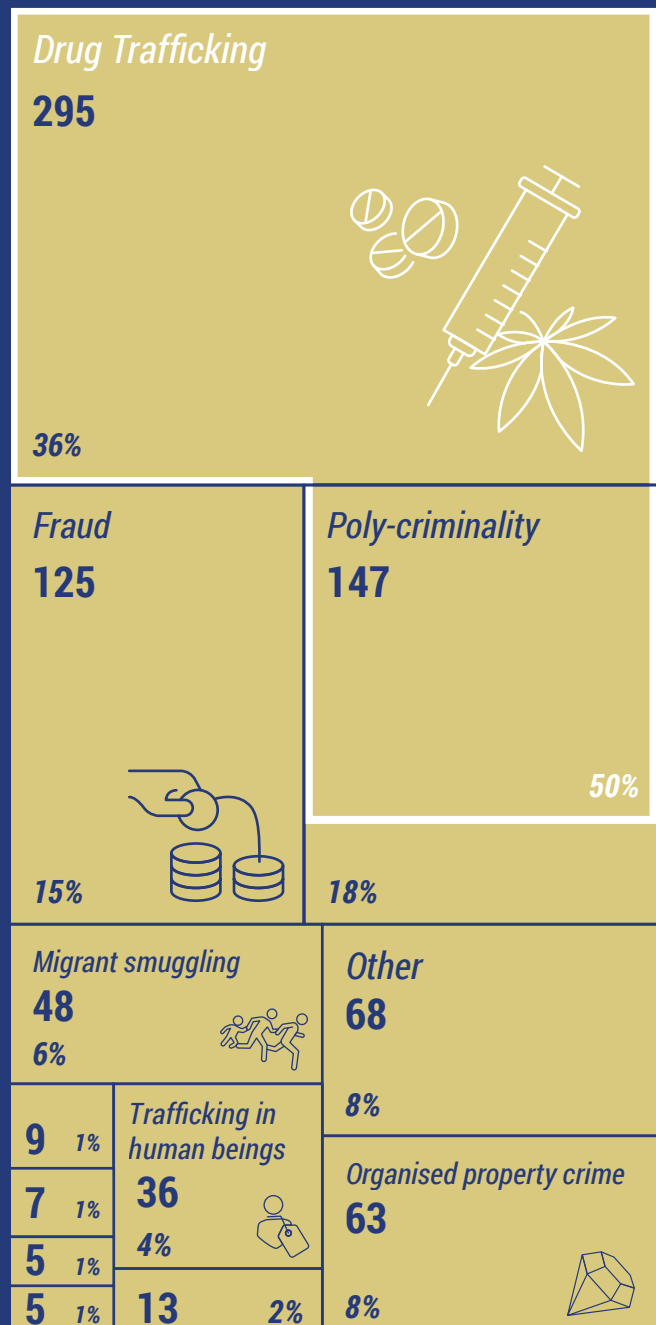
<sup>5</sup> The classification of criminal networks as most threatening and the criteria used for this assessment were left to the discretion of the national authorities. The same applies for the number of networks provided.



most threatening criminal networks active in/affecting the EU **identified**



Total membership of the identified most threatening criminal networks exceeds 25 000 **individuals**



Cybercrime  
Environmental crime  
Extortion  
Firearms  
Counterfeiting

## The ABCD of the most threatening criminal networks

This first-of-its-kind EU-wide assessment decodes the ABCD of the most threatening criminal networks – they are Agile, Borderless, Controlling and Destructive. Recognising these common traits, and using them as a starting point for further analysis and action, will help policy-makers make informed strategic decisions and help law enforcement target the most threatening criminal actors active in the EU.

### Agile

*[adjective | able to adapt to new or changing situations or changes quickly and successfully]<sup>6</sup>*

The most threatening criminal networks exhibit remarkable agility. They are able to inventively make use of opportunities in the legal world, such as by using or setting up legal business structures to facilitate or conceal their criminal activity, and to launder their money. They are able to turn challenges to their benefit, as seen in recent geopolitical crises where criminal businesses continued as usual. They combine such flexibility in operations with a high degree of resilience against law enforcement disruption, using countermeasures or corruptive practices to obtain information on law enforcement investigations or to influence judicial proceedings. With such growth and survival strategies in place, many of the most threatening criminal networks are able to maintain their power and influence over very long periods of time, sometimes even longer than a decade. This concept of agility is applicable to criminal networks of any organisational structure, setup or size.

A key threat vector is criminal networks' strategy to infiltrate the legal business world – as a facilitator to commit their crimes, as a front to disguise their crimes, and as a vehicle for laundering criminal profits.

**86 % of the most threatening criminal networks make use of legal business structures (LBS).** The majority infiltrate LBS at a high level or set up their own LBS. The sectors most vulnerable to infiltration by organised crime include construction, hospitality and logistics. Legal businesses are also key in laundering illicit proceeds – with money laundering methods misusing real estate (investments), retail (investments in high value goods) and cash-intensive businesses (transactions). A few of the most threatening criminal

networks engage in money laundering as their sole criminal business, also offering it as a service to other criminal actors. The more the misuse of legal companies, the stronger and more resilient they become.

They are agile because of the flexibility they can apply to their operations and their capacity to withstand disruptions. **34 % of the most threatening criminal networks have been active for more than 10 years.** During such extended periods of time, they are able to maintain their influence and power, even if leaders and members are detained. They are often aware of law enforcement initiatives and actively apply countermeasures – potentially also aided by corruptive practices to obtain information from or infiltrate law enforcement or the judiciary.

Such resilience and agility are underpinned by strong cohesion between network members who work together towards a criminal objective over time. **Cohesion is present in networks no matter how they are organised. The most threatening criminal networks have an organisational set-up that includes all possible variations on the spectrum of vertical and horizontal, and small to large.** The majority of the most threatening criminal networks are vertical and hierarchical in nature, with a layered power structure, strong system of internal control and central leadership. Criminal networks organised more horizontally, around a core group of central figures or in a decentralised manner, are also found in this group. The most threatening criminal networks can range from very few to many members. While an exact membership count is often not feasible, they often range between 8 and 38 members.

Agility also refers to their ability to adopt new technologies. The quality of the most threatening criminal networks' tools and expertise is often thought of as sophisticated and high-level, but case examples point to flexibility and ingenuity as more important means that help accomplish their criminal objectives.

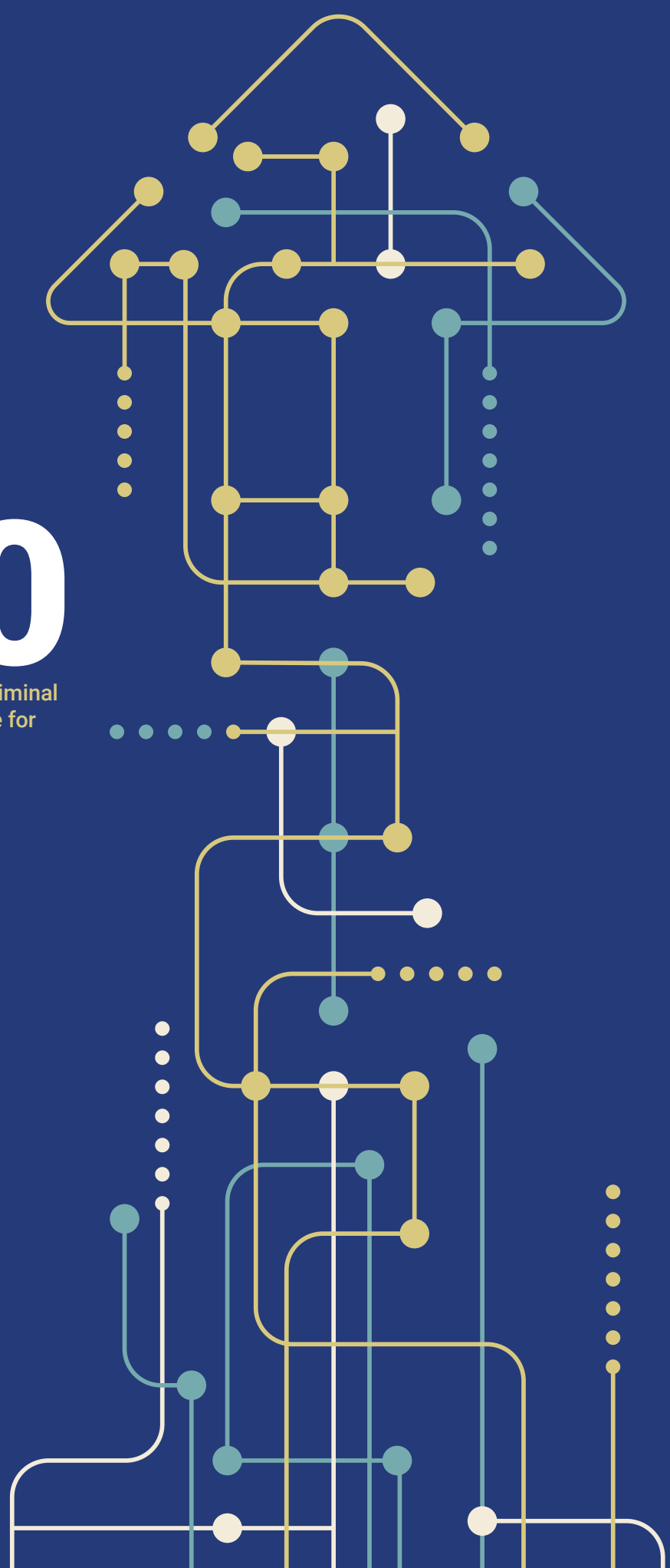
# ~280

of the most threatening criminal networks have been active for 10+ years



# 86%

are able to infiltrate the legal business world to disguise their activities and launder criminal profits



## Borderless

*[adjective | used to describe a situation in which the border between countries is not important, usually in relation to the movement of goods, people, etc.]<sup>7</sup>*

7 Ibid.

The most threatening criminal networks run borderless criminal operations. Their activities touch many countries and their composition is very international, with network members from many countries of the EU and the world cooperating within networks. They have an international, and often global reach, yet they contain their criminal activity to a region or a limited number of countries.

The 821 most threatening criminal networks affect all 27 EU Member States. The majority have a reach that extends beyond the EU, particularly to countries in the EU neighbourhood, but also more distant locations. This global reach is also reflected in criminal networks' composition, with **112 nationalities represented** among the members of the 821 most threatening criminal networks. **68 % of networks are composed of members from multiple nationalities, while 32 % have members from only one country.** Multinational criminal networks are often composed of nationalities of neighbouring countries or of nationalities with large diaspora

communities present in the country, and some are made up of very mixed, international membership. The networks with members from only one country are mostly EU nationals. A strong cohesion based on nationality is valid for some of the most threatening criminal networks, but not all.

**76 % of the most threatening criminal networks are present or active in two to seven countries.**

This means that they maintain geographical focus and do not extend their activities too broadly. Less than a quarter operate in more than seven countries.



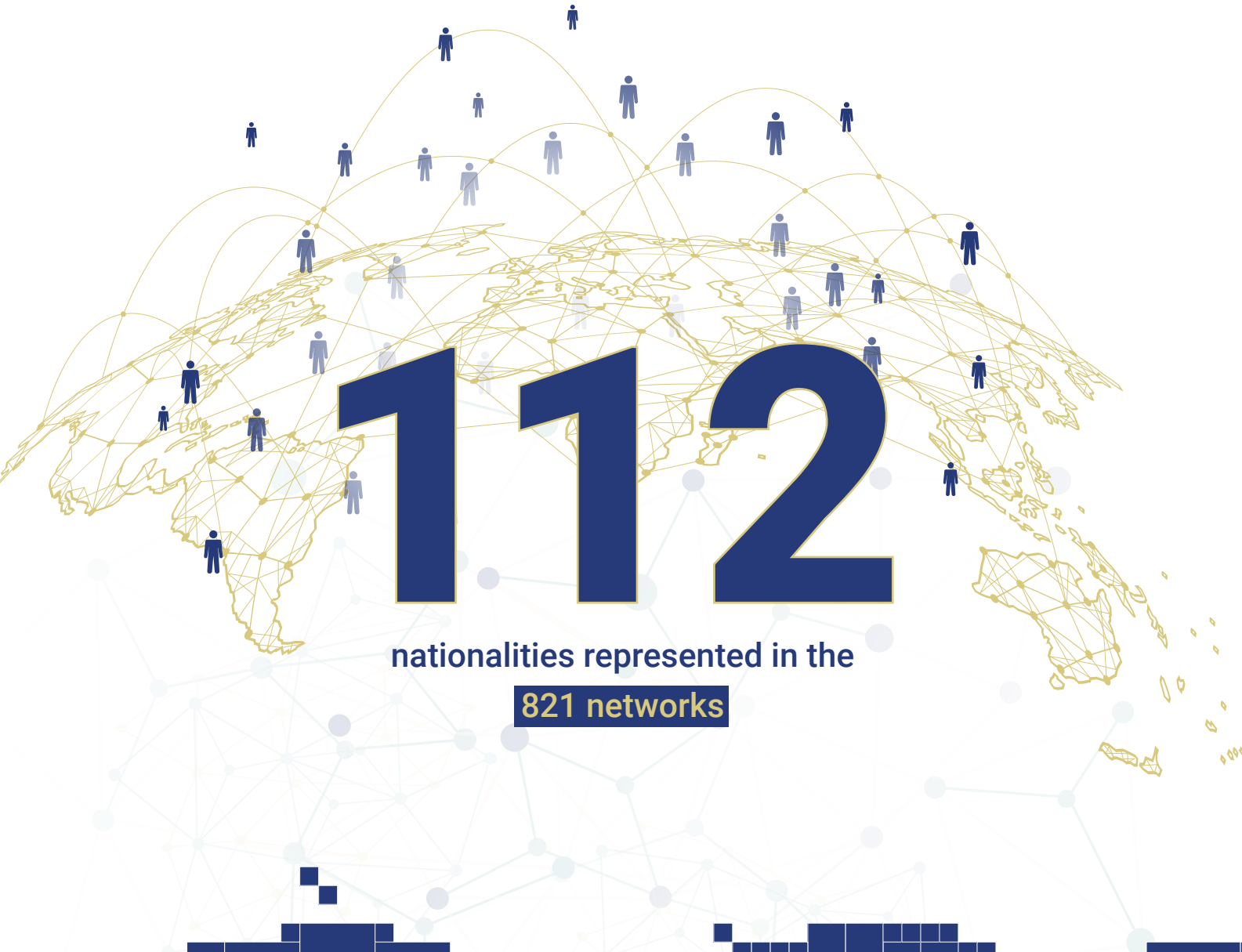
**68%**

are composed of members from multiple nationalities



**32%**

have members from only one country



nationalities represented in the  
**821 networks**



**76%**

are present or active in two to seven countries

## Controlling

[adjective | ordering, limiting, or ruling something, or someone's actions or behaviour]<sup>8</sup>

8 Ibid.

The most threatening criminal networks exert strong control and focus over their criminal operations. They tend to specialise in one main criminal business – truly poly-criminal networks are exception rather than rule. They are characterised by a strong leadership that is often close to operations, but can also keep command and control remotely from global locations. Under a strong lead, networks often operate independently and tend to keep complete control over their activities, including essential support activities such as the laundering of their illicit proceeds. When they do cooperate, they do so in balanced, equal partnerships, often under the crime-as-a-service framework, in order to obtain specific technical or on-the-ground support.

Strong leadership is a key determinant for the most threatening criminal networks. It is not necessarily linked to a specific type of organisational structure or to a specific individual. Leaders of the most threatening criminal networks ensure close control over operations. **The leadership of 82 % of the most threatening criminal networks is settled either in the main country of activity or the country of origin of the key members.** Some distance themselves as a countermeasure or because they are detained, while still ensuring control and command remotely. **Around 6 % of the most threatening criminal networks have a leadership that coordinates operations from outside the EU** – a deliberate choice to move away from law enforcement reach as they feel the pressure.

The cooperation model of the most threatening criminal networks emphasises self-reliance or balanced partnerships. **They remain independent and keep close control over their main activities. When they do cooperate, they do so in balanced, equal partnerships.**

Such a cooperation model likely increases criminal efficiency and allows for a high degree of independence in controlling the full criminal business process, from start to end. **A majority of the most threatening criminal networks tend to have end-to-end control over the majority of their activities or over the main part of the criminal process.**

When in need of technical expertise or low-level executors, they delegate parts of the criminal process to external service providers. This crime-as-a-service business model further heightens their threat, as all their needs can be catered for by other criminal actors through financial exchange. It allows them to delegate and gain outside expertise for part of the criminal process or to support criminal activities. Crime as a service often revolves around a niche activity that requires a certain technical specialisation, or a low-level activity that is outsourced as a countermeasure. A few criminal networks offer crimes to other networks as their main activity – particularly money laundering or acts of violence, including threats to life as a service.

Also fitting with the characteristic of control is the finding that a large majority of the most threatening criminal networks keep a focus on one main criminal activity. Truly poly-criminal networks are the exception rather than the rule. **82 % of networks deal in one main criminal activity, making only 18 % poly-criminal.** This focus also means that they are often well-established in terms of their influence and dominance exerted over criminal markets.

The most threatening criminal networks remain involved in other types of crime that support, strengthen, or conceal their main crimes. Firearms trafficking, for example, is often committed together with drug trafficking or in support of violent activities such as extortion and racketeering. As profit is the main objective uniting criminal actors, money laundering is a key part of criminal enterprises, and **nearly all (96 %) networks launder their criminal proceeds themselves.**



**82%**

the leadership is settled  
either in the main country  
of activity or the country of  
origin of the key members



**18%**

poly-criminal



**82%**

one main criminal activity



**96%**

most threatening criminal  
networks launder their criminal  
proceeds themselves



## Destructive

[adjective | causing, or able to cause, damage]<sup>9</sup>

The criminal activities and corruptive practices of the most threatening criminal networks inflict significant damage on the EU's internal security, rule of law, and economy. They do not operate in an isolated criminal underworld but directly impact EU citizens' lives. Examples include the increase of drug-related violence and turf wars on the streets of many EU cities, the abuse of vulnerable youngsters and other strata of vulnerable populations in organised crime, and the victimisation of many people in crimes like trafficking in human beings or frauds. Their power and influence have serious social ramifications, with citizens often fearing the consequences of reporting organised crime and feeling pressured to comply with it. Meanwhile, criminal networks continue to accumulate illicit proceeds and further invest them in both criminal activities and the legal world.

**Half of the most threatening criminal networks are involved in drug trafficking as (one of) their main criminal activity(-ies). Other relevant crime areas include fraud, property crime, migrant smuggling and trafficking in human beings (THB).** The impact of these crime areas is extensive and affects all layers of our society, including directly harming the lives of millions of EU citizens.

Not all of the most threatening criminal networks use violence and/or corruption. When they do, it further extends their threat level. Corruption and violence mutually reinforce each other. **71 % of networks engage in corruption to facilitate criminal activity or obstruct law enforcement or judicial proceedings.** Corruption facilitates all criminal activity and may be targeted towards the private and public sectors. Corruption serves as a means to obtain information or to obstruct investigations and/or judicial proceedings. Corrupted individuals often become embedded in and part of criminal networks, as they become intertwined in the network's activities. An exit from the network is difficult, also because corruptive practices are often closely interlinked with violence and intimidation.

**68 % of networks use violence and intimidation as an inherent feature of their modus operandi. 32 % do not use violence to avoid detection by law enforcement.** The use of violence is particularly applicable to drug trafficking, where it is also often more strategic and extreme. Some networks offer violent acts as a service to other criminal actors.

Some of the most threatening criminal networks **recruit from a young strata of the vulnerable population, even minors**, and abuse them to execute tasks in drug trafficking or to exploit them in criminal activities. They often do this as a countermeasure to avoid prosecution and/or identification of core network members or leadership.

The destructive nature of the most threatening criminal networks is already leaving its impact on EU citizen's lives and our society as a whole. The more visible presence of organised crime in cities instils fear in some and tempts others to participate in criminal activities, lured by the promise of a rich lifestyle or pressured by (the threat of) violence.

They are able to obtain large amounts of illicit profits and deploy these alongside other (human, material or technical) resources and expertise to further invest in their criminal capabilities.







# 50%

of the most threatening criminal networks are involved in drug trafficking  
*(36% engage in drug trafficking as sole main activity)*

# 71%

engage in corruption

# 68%

use violence



## A tailored approach

A better understanding of the threat-generating aspects of the myriad of criminal networks active in the EU will assist law enforcement in better tailoring their operational approach and directing resources where they are needed most.

The ABCD of criminal networks highlights important elements to guide policy and operational action. A key component is to further strengthen international cooperation to tackle the borderless nature of the most threatening criminal networks, both regionally within the EU as well as with non-EU partners. Investigations and operational activities can be more focused on the most threatening criminal networks, examining their high-value targets and from there, dismantling the complete network. Parallel investigations should also tackle the broader crime infrastructure<sup>10</sup> that supports and enables the main criminal business, such as money laundering and firearms trafficking. As the most threatening criminal networks are agile and have integrated themselves into our society, we cannot fight them in an isolated way. Law enforcement must strengthen their partnerships with other actors to form comprehensive, all-encompassing approaches that tackle the roots of serious and organised crime, such as the administrative approach.<sup>11</sup>

While this analysis from the perspective of criminal actors is a first and already brings clear added value, the approach can be further refined by continuing the exchange of information, collecting more representative data, analysing in-depth the threat vectors for criminal networks and their implications on crime areas, and maximising operational action to dismantle these most threatening criminal networks in cross-border investigations.

---

10 Crime infrastructure refers to the enablers of crime, such as corruption, violence, money laundering, and misuse of legal business structures. These tools make it easier to commit crime or avoid apprehension.

11 The administrative approach entails equipping local administrations with necessary tools (such as revoking licenses) to avoid that criminals abuse the legal infrastructure. See also European Network on the Administrative Approach, accessible at <https://administrativeapproach.eu>

# DESCRIBING THE MOST THREATENING CRIMINAL NETWORKS

A description of the key characteristics of the most threatening criminal networks is the first step in reaching this report's objective. This chapter focuses on the characteristics that allow us to strengthen our understanding of the most threatening criminal networks but do not necessarily influence their threat level. These include organisational setup, composition in terms of citizenships of network members, and the type of criminal activities they engage in.

## Internal organisation and composition

### Organisational setup: unity in diversity

The organisational setup of criminal networks is very diverse. Some are strictly hierarchical, while others are loose, decentralised and informal. Some are composed of just 3 network members, while others have more than 100. How criminal actors are organised and how large or small the networks are, does not necessarily correlate to the threat they pose. Nonetheless, to understand how to identify, prioritise and tackle criminal networks, it is relevant to outline these characteristics.

More than half of the most threatening criminal networks have a hierarchical structure, with various layers of power and responsibilities, a clear division of tasks and internal systems of control and discipline. Most of these networks are described as mafia type organisations, outlaw motor cycle gangs (OMCGs), Thieves in Law or cartels.

The other half of the most threatening criminal networks are more fluidly organised, either around a central core group, or loose and decentralised. Criminal networks organised in such a way have come more to the fore since 2020, when the analysis of communications between criminals using cryptophones revealed this more networked, fluid landscape of criminal actors.

The size of most threatening criminal networks varies a lot. The exact size and boundaries are difficult to determine – network members can remain under the radar, membership evolves over time, and some individuals may be external service providers rather than embedded in the network.

The largest groups are often hierarchically structured, and on many occasions are family or clan-based (such as mafia-families) or OMCGs. The extent to which all members are involved in criminal activities and form part of the criminal network requires further information and analysis.

Smaller networks often operate at a regional or local level, relying on external partners, while larger networks can operate at an international level and carry out more complex operations. Drug trafficking operations rely on fluid networks of contacts that connect different levels of activity. The sharing of responsibilities at various points in the trafficking chain across different networks means that trafficking operations are more complex than if they were organised end-to-end by a single group.

## What glues networks together? Cohesion and leadership

Criminal network members come together as they find each other in a common criminal enterprise. However, some criminal networks are bound by more than a common criminal goal. Several aspects can contribute to a criminal network's cohesion: a common regional area of activity, a common nationality, a shared origin or cultural background, a common language, family ties, or belonging to a subculture or organisation. References to clans, cartels, mafia, confraternity, street gang, Thieves in Law, OMCs, all imply this sense of belonging and connection, strengthening criminal networks' cohesion.

Higher cohesion makes criminal networks more agile and resilient. It allows them to rely on a community, comprising assets and illicit affiliations within diasporas and groups of associates situated in different places, to establish their criminal operations. The cohesion is further strengthened and guided by the presence of strong leadership.

*The network's cohesion can be based on one aspect or a combination of factors. Below we provide examples of aspects strengthening criminal networks' cohesion based on the available data on the 821 most threatening criminal networks. The categories are not exhaustive and not mutually exclusive – one criminal network can have multiple factors contributing to its cohesion.*

### Regional cohesion

Most networks are highly diverse in terms of nationality composition. 68 % of the criminal networks contain members of multiple nationalities, ranging anywhere between 2 to 10 nationalities, and sometimes even more. The main nationalities are Albania, Belgium, France, Germany, Italy, the Netherlands, Poland, Spain, Türkiye and Ukraine. Most criminal networks are made up of both EU and non-EU nationals. A smaller share is made up of several EU nationalities and a handful are made up of a combination of non-EU nationalities.

Among these multi-national most threatening criminal networks, some are composed of nationalities of neighbouring countries. These neighbours join forces on criminal projects capitalising on regional opportunities. What are the most common combinations?

- ◇ **A distinct group are Belgo-Dutch criminal networks, built around key members<sup>12</sup> from Belgium and the Netherlands.** Some of the elements connecting them are their common language, close proximity and good road infrastructure between relevant locations (such as the port of Antwerp and Rotterdam). Several key members of these criminal networks with Belgian or Dutch nationality originate from other countries, mainly Morocco and Türkiye. The criminal networks also include key members from other nationalities such as Albanian, British, Italian, Moroccan and Turkish. These networks are mainly active in cocaine trafficking, and to a lesser extent in cannabis trafficking and money laundering. They are present in more than 40 countries, with main operations in Belgium, Germany, the Netherlands and Spain in the EU, and the United Arab Emirates outside the EU.

<sup>12</sup> Key members of the criminal network refers to those members that perform a key role in the network and/or are in a key position.

- ◇ **Eastern European nationals of Belarus, Czechia, Hungary, Moldova, Poland, Russia, Slovakia and Ukraine often cooperate in changing compositions. The dominant nationalities<sup>13</sup> within these criminal networks are often Polish or Ukrainian.**
  - ◇ Criminal networks with Ukrainian key members often include Belarussian, Polish, Russian and Slovakian criminals who take up key positions in these networks. Moldovan nationals collaborate with Ukrainian nationals as low-level members in the criminal network. These networks are mostly active in tobacco smuggling, VAT and customs fraud, online fraud and migrant smuggling. They operate mainly in Czechia, Poland, Slovakia, Spain and Ukraine.
  - ◇ Criminal networks built around Polish key members often cooperate internally with a diverse group of more than 40 different nationalities, most prominently Czech, Dutch, German, Slovak and Ukrainian nationals. Their main activities include trafficking of cannabis, cocaine and precursors, tobacco smuggling and VAT fraud. They operate mainly in Belgium, Germany the Netherlands, Poland, Slovakia, Spain and the United Kingdom.
- ◇ **Eastern European networks with criminal nationals from Baltic States (Estonia, Latvia and Lithuania) show a strong connection with each other and with Russian nationals.** Within these networks, the leadership may be taken up by any of these nationalities. The networks are mostly active in drug trafficking (cocaine, cannabis and synthetic drugs), money laundering, tobacco smuggling and trafficking in human beings (THB) for labour exploitation. Their main countries of activity are Estonia, France, Germany, Latvia, Lithuania, the Netherlands, Poland, Spain, Russia and the United Kingdom.

### Cohesion based on nationality

The nationality of the members of the criminal network is often the first lead for law enforcement to chart out closely tied criminal networks. How often do the same nationalities work together within a criminal network? How relevant is nationality as a factor in network cohesion?

Overall, serious and organised crime remains truly international in nature. The most threatening criminal networks affecting the EU are composed of 112 different nationalities. All EU Member States are represented in the most threatening criminal networks, as are citizens of no less than 85 non-EU countries.

Below we explore whether nationality is a key factor for cohesion of the most threatening criminal networks. The data show that it is for some, but not for all. The majority of the most threatening criminal networks have a mixed composition with internal cooperation between multiple nationalities towards a common objective.

***The analysis is based on data on the 821 identified most threatening criminal networks affecting the EU, contributed by Member States and third countries.***

<sup>13</sup> Dominant nationality refers to the most represented nationality(-ies) of the criminal network members in terms of frequency.

32 % of the most threatening criminal networks are composed of one nationality. Such homogenous groups are most often composed of one EU nationality, and in fewer cases made up of one non-EU nationality.

The homogenous criminal networks made up of members of one EU country are mostly Italian, but also French, Polish and Romanian, among others.

- ◇ Italian mafia-style criminal networks are often centred solely around Italian key members. Yet, with activities in more than 45 countries, they have a very broad reach in the EU (besides Italy mainly in Belgium, Germany, the Netherlands, Malta, Romania and Spain) and beyond (in Colombia, Switzerland and the United States of America). Their main activities are drug trafficking (including cocaine, cannabis and heroin), extortion and racketeering, waste trafficking, tobacco excise fraud and money laundering.
- ◇ Romanian homogenous networks are typically active in organised property crime (burglary, motor vehicle crime and robberies), subsidy and VAT frauds, and THB for sexual exploitation. Almost all their criminal activities take place in Europe. They operate mainly in Austria, Belgium, Czechia, France, Germany, the Netherlands, Spain, Sweden, Switzerland, Romania and the United Kingdom.
- ◇ Polish homogenous networks are mainly active in trafficking of cannabis and synthetic drugs, tobacco smuggling and motor vehicle crime. They operate primarily in Czechia, Germany, the Netherlands, Poland and Spain.
- ◇ Criminal networks composed of solely French members are mostly active in trafficking of cocaine and cannabis. They also engage in extortion and racketeering and THB for sexual exploitation. They operate primarily in France, but also have connections to more than 15 other countries including Belgium, the Netherlands, Portugal and Spain in the EU, and the United Arab Emirates outside the EU.

### Case example

#### **'NDRANGHETA INVOLVED IN VARIOUS CRIMINAL ACTIVITIES**

Several powerful 'Ndrangheta families lead a mafia-style criminal network engaged in various criminal activities such as drug trafficking, firearms trafficking and tax fraud. The main activity of the network is drug trafficking from South America to Europe, as well as Australia. They work in partnership with the Colombian 'Gulf clan' and another network operating in Ecuador and multiple European countries. They also provide weapons to the notorious PCC (Primeiro Comando da Capital) in exchange for cocaine. Criminal proceeds are invested in various European and South American countries, mainly in real estate, restaurants, supermarkets, hotels and other commercial activities.<sup>14</sup>

<sup>14</sup> Europol, 03 May 2023, 132 'Ndrangheta mafia members arrested after investigation by Belgium, Italy and Germany, available at <https://www.europol.europa.eu/media-press/newsroom/news/132-ndrangheta-mafia-members-arrested-after-investigation-belgium-italy-and-germany>

Criminal networks composed of one non-EU nationality originate mostly from Albania, Bosnia and Herzegovina, China, Georgia, Iceland, Nigeria, Serbia, Türkiye, the United Kingdom and Ukraine.

- ◇ Homogenous Ukrainian criminal networks are mostly active in THB and online frauds. They operate mostly in Poland and Ukraine.
- ◇ Criminal networks centred solely around Albanian key members are mainly active in cocaine, heroin and cannabis trafficking, mainly in Belgium, France, Germany, Italy, the Netherlands and Spain. Outside the EU they mainly operate in Brazil, Colombia, Ecuador and their home country Albania.
- ◇ Georgian homogenous criminal networks are active in organised property crime (burglaries and robberies), mainly in Greece, Italy, Malta, Poland, Portugal and Spain.

#### Case example

##### **ALBANIAN DRUG TRAFFICKING NETWORK**

A criminal network active in heroin and cocaine trafficking and money laundering across Europe was taken down by law enforcement. The network has a family-like structure tied together by common nationality, composed mainly of Albanian and dual Albanian nationals. The criminal network smuggles drugs in containers into Belgium. The drugs are then moved to Germany in vehicles equipped with sophisticated hidden compartments, and from there distributed throughout Europe.<sup>15</sup>

#### Cohesion based on a common non-EU background

Among the groups composed of multiple nationalities, various groups are bound by common origin. These groups often operate within EU Member States while maintaining close links to their regions of origin outside the EU. They are bound together by a common culture, language and history.

- ◇ These networks often combine membership from various Western Balkan countries and are often centred around Serbian nationals. They include Albanian, Belgian, Bosnian, Croatian, Dutch, German, Montenegrin, Slovenian and Turkish nationals. Their main criminal activity is drug trafficking, primarily cocaine and cannabis, and to a lesser extent synthetic drugs and heroin. They also engage in organised property crime, tobacco smuggling and THB for sexual exploitation. They primarily operate in Belgium, Colombia, Croatia, France, Germany, the Netherlands and Western Balkan countries. For some criminal networks, there are no distinct patterns in terms of nationality composition.

<sup>15</sup> Europol, 26 May 2023, 17 arrested in Belgium and Germany in takedown of clan-based drug trafficking network, available at <https://www.europol.europa.eu/media-press/newsroom/news/17-arrested-in-belgium-and-germany-in-takedown-of-clan-based-drug-trafficking-network-0>

- ◇ Albanian-centred criminal networks are composed either solely of Albanian nationals, or of Albanians combined with nationalities such as Belgian, Dutch, French, Greek, Italian and Serbian. In over half of these criminal networks, Albanians are the dominant nationality. They are active in drug trafficking, firearms trafficking, robberies and migrant smuggling. They operate in a large number of EU Member States and third countries such as Norway, Switzerland, the United Kingdom and Latin American countries.

### Case example

#### **CRIMINAL NETWORKS WITH LINKS TO THE WESTERN BALKAN REGION**

Several different criminal networks, composed of members originating from the former Yugoslav republics of Slovenia, Croatia, Bosnia and Herzegovina, Serbia and Montenegro, are involved in the large-scale trafficking, including financing and distribution, of cocaine from South America to various European destinations, and beyond. They are characterised by a powerful presence throughout the EU and in the Western Balkan region. They have also established very strong presence in Latin America by exploiting corruption opportunities in and around key ports and in shipping companies. They thus exercise end-to-end control over the supply of cocaine. Some of these groups are also specialised and/or heavily involved in excessive violence, professional kidnappings and executions, corruption, money laundering, trafficking of weapons and explosives and forged documents. Violence is mainly used as retaliation for lost or un-finalised drug shipments, but also to gain dominance over the territory or the supply chain.<sup>16</sup>

- ◇ Turkish key members often form the core of criminal networks with Belgian, Dutch and German criminals. These networks engage mainly in drug trafficking (cocaine and cannabis) and money laundering. Main countries of activity include Belgium, Colombia, Ecuador, France, Germany, the Netherlands, Spain, Sweden, Switzerland and Türkiye.
- ◇ All criminal networks with Moroccan key members consist of multiple nationalities. They often cooperate with Belgian, Dutch and Spanish criminals, and keep close ties to Morocco. These criminal networks engage in drug trafficking, mainly cocaine and cannabis. They operate primarily in Belgium, Colombia, Costa Rica, Ecuador, France, Italy, Morocco, the Netherlands, Spain and the United Arab Emirates.

<sup>16</sup> Europol, 1 September 2023, Balkan cartel sinks as Spain seizes 2.7 tonnes of cocaine on board large vessel, accessible at <https://www.europol.europa.eu/media-press/newsroom/news/balkan-cartel-sinks-spain-seizes-27-tonnes-of-cocaine-board-large-vessel>; Europol, 23 October 2023, One of Europe's most wanted drug traffickers behind bars and 16 arrested in Brazil, available at <https://www.europol.europa.eu/media-press/newsroom/news/one-of-europes-most-wanted-drug-traffickers-behind-bars-and-16-arrested-in-brazil>; Europol, 23 November 2023, Croatian narco boss arrested in Istanbul, accessible at <https://www.europol.europa.eu/media-press/newsroom/news/croatian-narco-boss-arrested-in-istanbul>



## Other factors for cohesion

A range of other factors may be (part of) the foundation for cohesion within the most threatening criminal networks. One such factor is family ties, as family members form a tightly knit and trusted group sharing the same values, beliefs and objectives. People identifying with specific sub-cultures, ranging from street gangs to outlaw motor cycle gangs, can also be drawn to join in a common criminal objective based on a shared vision and the desire to form part of a larger entity.

Finally, some criminal networks may join forces purely for opportunistic reasons. Some of the most threatening criminal networks indeed do not show any clear distinct patterns in nationality composition, and are composed of members with a variety of nationalities that cooperate on a joint criminal project.

- ◇ Almost all criminal networks with Spanish key members are comprised of multiple nationalities. They cooperate and share key positions within the networks with 48 different nationalities represented. They engage mainly in drug trafficking (cocaine and cannabis), environmental crime, fraud against the public interests of the EU<sup>17</sup> and money laundering. They operate in almost 50 countries, most commonly in Belgium, China, Colombia, France, Germany, Italy, Morocco, the Netherlands, Portugal and Spain.
- ◇ Several criminal networks include German members. The key members of these networks include a wide range of 48 nationalities, mainly Dutch, Italian, Polish Russian and Turkish. German members are often dominant in the networks they form part of, or the network may be dominated also by nationals from Albania, Italy, Poland, Switzerland and Türkiye. They engage mainly in drug trafficking (cannabis and cocaine) but also carry out online frauds and frauds against the public interests of the EU.
- ◇ The number of criminal networks with a Latin American national is limited despite the high occurrence of drug trafficking networks. Only 1 out of 10 criminal networks include a national of a Latin American country. Their main activity is cocaine trafficking and the main countries of activity are Belgium, Colombia, the Netherlands, Portugal and Spain. The main nationalities are Brazilian and Colombian, along with a handful of nationals from Argentina, Bolivia, Costa Rica, the Dominican Republic, Ecuador, Guinea, Guyana, Haiti, Mexico, Panama, Paraguay, Peru, Suriname and Venezuela. These networks are often led by key members from Albania, Belgium, Italy, the Netherlands, Portugal and Spain. Cocaine trafficking brings these members together, with shared language and history as additional uniting factors for Latin American, Portuguese and Spanish nationals. The low number of criminal networks with key members from Latin America and the Caribbean indicates that criminals from these regions currently do not exert significant influence on EU criminal markets.
- ◇ Although the dataset included a limited number of heterogenous criminal networks with Chinese nationals, they play a dominant role in their networks. Chinese criminals mainly cooperate with key members of French, Spanish and Vietnamese nationality. They are active in trafficking of cannabis and synthetic drugs, customs import fraud, wildlife trafficking and money laundering. Countries of activity include Belgium, China, France, Poland, Portugal and Spain.

<sup>17</sup> Such as VAT fraud and subsidy fraud.

## Leadership

Leadership has been identified as a role of critical importance within the most threatening criminal networks. These leaders are high-level decision makers who manage criminal operations, assign tasks to members and sometimes also supervise the finances of the network. The importance of this role correlates with the finding that most criminal networks are hierarchically structured with strong leadership, or centred around a core group of key members. Decentralised criminal networks can also have a clear leadership style. Strong leadership, no matter the exact structure, is an important characteristic of the most threatening criminal networks.

Leadership is in most cases considered irreplaceable, while middle-management is considered easier to replace. This is also corroborated by the finding that most leaders either operate from the country of main activity or their country of origin (see more in *Their international reach with regional focus*).

Leaders distance themselves physically from criminal operations in exceptional cases, either as a countermeasure against detection or because of detention. In both scenarios, they are able to keep lines of communication and delegation open, and continue to coordinate their criminal business remotely. (see also: *The spectrum of leadership: proximity and beyond*).

Some hierarchically structured criminal networks, such as certain OMCGs and Italian mafia, consider the leader important but replaceable. This may be because strategies to ensure strong, continued leadership are 'institutionally' embedded in the network. Examples include succession within the criminal family and 'recurrent election' of leaders. A re-structuring or split in different branches, coupled with a re-division of leadership and tasks is another strategy to ensure continued leadership.

Detention and conviction of leadership or other high-value targets do not necessarily halt the networks' criminal business. Leaders often continue to coordinate criminal operations from prison, even over extended periods of time, allowing the network to maintain its dominance. Some networks also demonstrate a high degree of resilience and agility with multiple key network members imprisoned.

## Criminal activities

### Main vs supporting criminal activities and poly-criminality

The majority of the most threatening criminal networks (82 %) focus on one main criminal activity, such as drug trafficking or organised property crime. The remaining 18 % are truly poly-criminal networks active in multiple main crime areas.<sup>18</sup>

Overall, drug trafficking stands out as (one of the) main activities<sup>19</sup> of the most threatening criminal networks, with about half of the reported networks involved in this crime area. Other prominent criminal markets include frauds (including online fraud schemes, excise, VAT-fraud), property crime, migrant smuggling and THB. Networks involved in environmental crime and counterfeit goods are less reported than other crime areas. In this dataset, criminal networks active in cyber-attacks and online child sexual exploitation are less reported as most threatening.

The vast majority of poly-criminal networks combine drug trafficking activities with other criminal activities, such as extortion and racketeering. The criminal infrastructure already in place for the main criminal activities may make it easy to carry out additional activities. Examples of such parallel criminal activities of drug trafficking networks include migrant smuggling, illicit tobacco smuggling and firearms trafficking. Other examples of poly-criminality combinations include migrant smuggling and THB, and organised property crime and THB (forced criminality).

The large majority of the most threatening criminal networks, whether they are engaged in one or multiple criminal activities, often commit other types of crime in support of their main criminal business (supporting activity), or as a smaller side-activity (subsidiary activity).<sup>20</sup> For example, some criminal networks combine their main activities in drug trafficking with firearms trafficking as subsidiary activity, and use crime infrastructure (money laundering, corruption, document and identity fraud, and violence) as supporting activities.

Violent crimes such as murder, inflicting physical harm and kidnapping are never reported as standalone criminal activities. These crimes are often used by criminal networks involved in drug trafficking, extortion and racketeering and firearms trafficking. Another example is document and identity fraud, often as a supporting activity for their core business, which is migrant smuggling, THB, online fraud and environmental crime. Some criminal networks were reported to only be engaged in document and identity fraud. Other elements of crime infrastructure such as infiltration of legal business structure, the use of countermeasures, corruption, and money laundering, are discussed in the next chapter.

***In what follows, the focus will be on those most threatening criminal networks that specialise in one type of criminal activity, such as frauds or drug trafficking.***

<sup>18</sup> And excluding supporting or subsidiary criminal activities, including criminal activities part of the crime infrastructure such as money laundering, corruption, infiltration legal business structures, violence, and corruption). A criminal network active in trafficking cocaine and cannabis as main activities is not considered poly-criminal.

<sup>19</sup> For poly-criminal networks and networks with one sole main activity combined.

<sup>20</sup> Supporting activities are criminal activities that are committed to facilitate the criminal network's main criminal activity. Supporting activities provide the criminal infrastructure in which the criminal business can be committed. They provide support to the criminal process or to a specific modus operandi in order to make the main criminal activity possible, easier to commit, or for it to remain undetected. See also European Council, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) 2025 – Revised methodology, 14642/23 REV 2, 21 November 2023. Subsidiary activities are criminal activities that are not the main focus of the criminal business, but that are committed as a (profitable) side business.

## Drug trafficking

Half of the most threatening criminal networks are involved in drug trafficking as the main criminal activity (solely focusing on drug trafficking or in combination with another main crime area).

Most threatening criminal networks engaging in drug trafficking activities have been reported by almost all EU Member States. Drug trafficking operations are most often located in Belgium, Germany, Italy, the Netherlands and Spain; and outside the EU in Albania, Brazil, Colombia, Ecuador and the United Kingdom.

Most of the drug trafficking networks (113) specialise in cocaine trafficking, with an equal share engaging in polydrug trafficking (111), dealing with various types of drugs. They mostly combine cocaine and cannabis trafficking or cocaine, cannabis and synthetic drugs trafficking. Cannabis trafficking is the sole main activity for 44 of the most threatening criminal networks. The number of most threatening criminal networks specialising in other types of drugs (synthetics, heroin, precursors) is fairly limited: 9 networks specialise in synthetic drugs trafficking, 6 in heroin trafficking and 12 in other drug-related substances (mainly precursors or essential chemicals for drug production).

Networks trafficking only cocaine are mainly active in EU Member States such as Belgium, Germany, Italy, the Netherlands and Spain. The presence of important ports in these countries, often with direct connections to drug-producing countries, plays a major role in their prominence. Many of the reported networks operate in and around these ports in these countries. Criminal networks that combine various types of drug trafficking are predominantly active in France, Germany, the Netherlands, Spain and the United Kingdom.

Most represented nationalities in cocaine trafficking networks are Albanian, Belgian, Dutch, Italian and Spanish. Top nationalities in cannabis trafficking networks are Albanian, Belgian, Dutch, German, Spanish, and Turkish.

Drug – and particularly cocaine – trafficking networks are very flexible and operate using various modi operandi or at multiple locations. For example, they hide the drugs in the physical structure of containers, using the rip on / rip off method to later extract the illicit commodity, or hide the drugs in various types of legal goods. They organise drug transports from various points of departure to different ports of arrival. Next to maritime transport, they also use air or road transport to move drugs.

Synthetic drug production and trafficking has expanded from the traditional production region in Western Europe (countries such as Belgium and the Netherlands) to the East (some Baltic States, Eastern European countries and countries bordering the EU such as Ukraine).

Legal business structures (LBS) in the import/export, port logistics and transport sector play an important role in the drug trafficking process, and are often set up or infiltrated by criminal networks. They provide cover to hide drugs, facilitate transport, extract and store trafficked drugs with a legal front. LBS are also used for the laundering of criminal profits, using companies in the construction, real estate, retail and catering and hospitality sectors.

While most networks have full control over the criminal process, some engage in only one or a few stages. For instance, certain groups cultivate cannabis, whilst others take care of the distribution. Similarly, there are networks specialising in the extraction of cocaine from containers in ports and transportation of drugs, providing their services to multiple networks. Networks that cover only part of the criminal process tend to be active for fewer years than ones that have end-to-end control.

Criminal networks engaged in drug trafficking often cooperate with other criminal networks for supply and distribution, money laundering, or logistical tasks such as exchanging vehicles and providing storage. Various networks sometimes jointly purchase drugs and divide the load on arrival in the EU to negotiate attractive prices at the source and cut transport costs.

Critical roles in drug producing and trafficking networks are accommodation providers (for cannabis cultivation), concealment specialists, corrupted actors and leadership. Chemists are also critical in certain networks.

The leadership of these networks is usually based in the country which contributed their information to the dataset. In a few cases, leadership is based in the country of the dominant nationality in the network or in the United Arab Emirates.

## Cocaine trafficking

**113**

most threatening criminal networks identified

Main nationalities

Albanian, Belgian, Dutch, Italian, Spanish

Main countries of activity

Belgium, Germany, Italy, Netherlands, Spain

**25**

reporting countries

## Cannabis trafficking

**44**

most threatening criminal networks identified

Main nationalities

Albanian, Belgian, Dutch, German, Spanish, Turkish

Main countries of activity

Belgium, Germany, Netherlands, Portugal, Spain

**15**

reporting countries

## Synthetic drugs trafficking

**9**

most threatening criminal networks identified

Main nationalities

Armenian, Dutch, Latvian, Lithuanian, Slovak

Main countries of activity

Czechia, Estonia, Latvia, Netherlands, Russia

**5**

reporting countries

## Poly-drug trafficking

**111**

most threatening criminal networks identified

Main nationalities

Dutch, French, German, Spanish, Turkish

Main countries of activity

France, Germany, Netherlands, Spain, United Kingdom

**33**

reporting countries

*Number of most threatening criminal networks involved in the different types of drug trafficking as a sole main activity, main nationalities, countries of activity, reporting countries (Note: Poly-drug trafficking includes the number of networks involved in trafficking various types of drugs)*

Source: Data provided on 821 most threatening criminal networks

## Frauds

Fraud schemes affect millions of people in the EU, and harm the financial interests of the EU and its Member States.<sup>21</sup> This is the second most common activity of the most threatening criminal networks. One-fifth of these networks engage in fraud as their main criminal activity, sometimes strategically engaging in other crime areas.<sup>22</sup>

Criminal networks lure victims into various types of online fraud schemes, mainly investment and romance fraud. Such fraud schemes are the speciality of 50 of the most threatening criminal networks. The main countries of activity of such networks include Belgium, Germany, the Netherlands, Poland and Portugal. Call centres play an important role in these schemes, targeting specific categories of victims such as elderly people. Operators are often located outside of the EU, such as India, Israel, Türkiye and the United Kingdom, but also sometimes in the EU. While certain call centre operators limit their activity to making the fraudulent calls, others take charge of the whole process, including tasking individuals, recruiting new personnel and regulating the distribution of individual remuneration. Annual profits from online fraud schemes vary depending on the type of scam. Investment fraud scams can lead to networks obtaining hundreds of millions in a short period of time. A wide variety of nationalities are involved in online fraud scams, including Belgian, French, German, Italian and Portuguese as well as Albanian, British, Israeli and Ukrainian from outside the EU.

Excise fraud is the sole main activity of 34 of the most threatening criminal networks. Tobacco excise fraud in particular is often a core activity, mainly for networks composed of Polish, Slovak and/or Ukrainian nationals. They operate in Poland, Slovakia, Spain and the United Kingdom. Half of the networks engaging in tobacco excise fraud have end-to-end control, the other half control particular stages such as the acquisition of tobacco for production of illegal cigarettes, transportation and distribution. Most networks involved in tobacco excise fraud limit themselves to this criminal activity. However, some combine the production and trafficking of illicit cigarettes with drug trafficking activities or with other types of fraud (oil excise fraud or customs import fraud).

Eighteen of the most threatening criminal networks specialise in VAT fraud – including carousel fraud. They usually have end-to-end control over the criminal process. The most represented nationalities in these networks are Czech, Polish, Portuguese and Spanish. Poland, Portugal and Spain are most affected by this type of fraud.

---

21 Europol, 2023, European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime, Publications Office of the European Union, Luxembourg, accessible at <https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf>

22 30 % of the most threatening criminal networks engaging in fraud schemes as their core business combine this with other main activities such as counterfeiting or property crime. The latter are not taken into consideration in this section.

<b>Online fraud schemes</b>	<b>50</b> most threatening criminal networks identified	Main nationalities German, Italian, Portuguese, Ukrainian	Main countries of activity Belgium, Germany, Netherlands, Poland, Portugal	<b>16</b> reporting countries
<b>Excise fraud</b>	<b>34</b> most threatening criminal networks identified	Main nationalities Dutch, Latvian, Polish, Slovak, Spanish, Ukrainian	Main countries of activity Latvia, Poland, Slovakia, Spain, United Kingdom	<b>9</b> reporting countries
<b>VAT fraud – including MTIC fraud</b>	<b>18</b> most threatening criminal networks identified	Main nationalities Czech, Polish, Portuguese, Spanish	Main countries of activity Poland, Portugal, Spain	<b>6</b> reporting countries
<b>Other frauds &amp; multiple frauds</b>	<b>23</b> most threatening criminal networks identified	Main nationalities Chinese, Italian, Polish, Portuguese, Spanish	Main countries of activity China, Germany, Portugal, Spain, Türkiye	<b>11</b> reporting countries

*Number of most threatening criminal networks involved in the different types of frauds as a sole main activity, main nationalities, countries of activity, reporting countries*

Source: Data provided on 821 most threatening criminal networks

Other types of fraud, such as subsidy fraud and customs import fraud, are the sole main activity for 15 of the most threatening criminal networks and 8 networks combine various types of fraud. Poland and Portugal are the main countries reporting on subsidy or customs import fraud. The most represented nationalities in these networks are Brazilian, Chinese, Polish, Portuguese, Spanish and Vietnamese. China and Portugal are the most affected countries.

## Organised property crime

73 of the most threatening criminal networks engage in organised property crime, mainly in burglaries and thefts (33) and motor vehicle crime (19), as their sole main activity. Three networks engage in cultural goods trafficking and five engage primarily in robberies. Three networks engage in various types of organised property crime. 10 networks also engage in THB (forced criminality) or drug trafficking as part of their core criminal portfolio.<sup>23</sup>

The countries most affected by networks committing burglaries and thefts are France, Italy, Malta, Portugal and Spain. The most represented nationalities in these networks are Croatian, Georgian, Italian and Romanian. The networks are described as either clan/family based mobile organised crime groups (MOCGs), or as Thieves in Law. They usually have full control over the criminal process. Some are also active in other types of property crime, in forcing victims into criminality (THB) or in drug trafficking. Alongside the leader, the role of scouter is considered critical in many of these networks.

The countries most affected by motor vehicle crime networks are Germany, Poland, Portugal and Serbia. In particular, Serbia appears to be a hub for the modification of stolen vehicles to give them a new identity and sell them further on. These networks are often composed of nationals from Germany, Italy, Romania, Serbia and Ukraine. The networks are usually hierarchical with a clear division of tasks and end-to-end control over the criminal process. Alongside the leader, the roles of document and identity forgers, technical experts and fencers are considered critical in these networks.

### Organised burglaries and thefts

**33**

most threatening criminal networks identified

Main nationalities

Croatian, Georgian, Italian, Romanian

Main countries of activity

France, Italy, Malta, Portugal, Spain

**9**

reporting countries

### Motor vehicle crime

**19**

most threatening criminal networks identified

Main nationalities

German, Italian, Romanian, Serbian, Ukrainian

Main countries of activity

Germany, Poland, Portugal, Serbia

**12**

reporting countries

### Other property crime & multiple property crimes

**11**

most threatening criminal networks identified

Main nationalities

Dutch, French, German

Main countries of activity

Albania, France, Germany, Switzerland

**5**

reporting countries

*Number of most threatening criminal networks involved in different types of organised property crime as a sole main activity, main nationalities, countries of activity, reporting countries*

Source: Data provided on 821 most threatening criminal networks

<sup>23</sup> The latter are not taken into consideration in this section.



## Migrant smuggling

57 of the reported most threatening criminal networks engage in migrant smuggling. 48 are solely active in this area, while the remaining 9 also engage in other criminal activities, mainly drug trafficking and THB (labour and sexual exploitation, forced criminality).<sup>24</sup>

### Migrant smuggling

**48**

most threatening criminal networks identified

Main nationalities

Iraqi, Moldovan, Romanian, Syrian, Turkish, Ukrainian

Main countries of activity

Belgium, France, Germany, Italy, Netherlands, Türkiye, Ukraine

**19**

reporting countries

*Number of most threatening criminal networks involved in migrant smuggling as a sole main activity, main nationalities, countries of activity, reporting countries*

Source: Data provided on 821 most threatening criminal networks

The most threatening criminal networks facilitate illicit entry in the EU, secondary movements within the EU, and the legalisation of stay (via sham marriages or the provision of residence permits, for example). Some provide services to other smuggling networks, such as the supply of nautical equipment or fraudulent documents. In some cases, networks smuggle migrants with a view to exploiting them, mainly in the form of labour exploitation.

Compared to criminal networks engaging in other crime areas, migrant smuggling networks are less likely to exert end-to-end control on their activities.

A wide variety of nationalities are involved in migrant smuggling activities, with Iraqi, Moldovan, Romanian, Syrian, Turkish and Ukrainian being the most common. A broad range of countries are affected, including origin, transit and destination countries.

<sup>24</sup> The latter are not taken into consideration in this section.

### Case example

#### **CRIMINAL NETWORK CHARGING UP TO EUR 20 000 PER MIGRANT**

A criminal network facilitates the entry and secondary movements of irregular migrants in the EU. Migrants pay enormous sums to the smugglers to enter the EU clandestinely and move on to further destinations within its borders. The entire journey from the country of origin to the EU costs between EUR 15 000 and 20 000. The criminals advertise their illicit activities on various social media platforms to lure migrants, also by posting videos of successful transports. Migrants are moved along two main routes, either from Croatia via Slovenia to Italy, or from Serbia via Hungary to Austria.<sup>25</sup>

Various roles are important within migrant smuggling networks, such as recruiters (of migrants and drivers), accommodation providers (for temporary stay of migrants or drivers along the trafficking routes), cash collectors, document and identity forgers, equipment suppliers and drivers who transport migrants. Alongside the leadership, middle management<sup>26</sup> plays an important role in handling the logistics of the criminal business.

In some cases, extreme violence – including kidnapping, torture and sexual assault – is used against irregular migrants.

<sup>25</sup> Europol, 16 February 2023, 13 criminals arrested for smuggling at least 212 people, available at <https://www.europol.europa.eu/media-press/newsroom/news/13-criminals-arrested-for-smuggling-least-212-people>

<sup>26</sup> Definition middle management: members of the network that receive orders from the leader and give orders themselves to the executive level.

## Trafficking in human beings (THB)

### THB for sexual exploitation

**18**

most threatening criminal networks identified

Main nationalities

Bulgarian, Romanian, Serbian, Ukrainian

Main countries of activity

France, Germany

**12**

reporting countries

### THB for labour exploitation

**13**

most threatening criminal networks identified

Main nationalities

Georgian, Romanian, Russian, Ukrainian, Uzbek

Main countries of activity

Germany, Netherlands, Poland, Ukraine

**11**

reporting countries

*Number of most threatening criminal networks involved in THB for sexual or labour exploitation as a sole main activity, main nationalities, countries of activity, reporting countries*

Source: Data provided on 821 most threatening criminal networks

55 of the reported most threatening criminal networks engage in THB as (one of) their main activity(-ies). THB for sexual exploitation is the sole core business for 18 criminal networks, THB for labour exploitation for 13 networks and 5 networks specialise in other forms of THB. 19 criminal networks combine THB with other crime areas, such as drug trafficking, organised property crime and migrant smuggling. Document and identity fraud often facilitates THB activities.<sup>27</sup>

The countries most affected by THB for sexual exploitation are France and Germany. The nationalities most represented in networks engaging in this form of THB are Bulgarian, Romanian, Serbian and Ukrainian. These criminal networks tend to have end-to-end control over the criminal business.

Criminal networks active in THB for labour exploitation mainly operate in Germany, the Netherlands, Poland and Ukraine. The most represented nationalities within networks engaging in this form of THB are Georgian, Romanian, Russian, Ukrainian and Uzbek. Labour exploitation most often takes place in restaurants, construction and agriculture. Here too, end-to-end control is the general rule.

## Counterfeiting

Among the reported most threatening criminal networks, 31 engage in counterfeiting activities. For most of them, this is not their sole activity, but part of a broader criminal portfolio. Counterfeiting goods is often associated with excise fraud, for example.

Criminal networks engaging in counterfeiting as their sole criminal activity typically counterfeit goods (5) or money (5). Two networks specialise in

<sup>27</sup> The latter are not taken into consideration in this section.

counterfeiting pharmaceuticals and one in digital content piracy.

The countries most affected by counterfeiting are Belgium and France. These groups are composed mainly of nationals from Greece and Moldova.

## Cyber-attacks

### Cyber-attacks

9

most threatening criminal networks identified

Main nationalities

Russian, Ukrainian

Main countries of activity

France, Germany, Switzerland, USA

6

reporting countries

*Number of most threatening criminal networks involved in cyber-attacks as a sole main activity, main nationalities, countries of activity, reporting countries*

Source: Data provided on 821 most threatening criminal networks

Nine of the most threatening criminal networks specialise in cyber-attacks as their main activity. A handful of others engage in this area to support their fraud and money laundering activities. Russians and Ukrainians are the most represented nationalities within these networks.

These criminal networks operate on an affiliate business model. In some cases, the number of members exceeds 100, with a smaller core group managing operations. The core group makes ransomware available to its affiliates, who then carry out the cyber-attack. The core group manages the negotiations and payment of ransom, often in cryptocurrency. It hands over, for example, 80 % of the sum to its affiliates. Technical members, who develop malware represent a critical role in the functioning of these networks. Leadership tends to be replaceable.

### Case example

#### **DISRUPTION OF LOCKBIT RANSOMWARE GROUP**

The LockBit ransomware group has been recently targeted by law enforcement, damaging its capabilities. LockBit is one of the most harmful pieces of ransomware known. The group behind LockBit is a 'ransomware-as-a-service' network, meaning that a core group of the network creates malware and licenses out the code to affiliates who launch attacks. LockBit's attack presence has been seen globally, with hundreds of affiliates recruited to conduct ransomware operations using LockBit tools and infrastructure. Ransom payments are divided between the core group and the affiliates, who receive on average three quarters of the ransom payments collected.<sup>28</sup>

<sup>28</sup> Europol, 20 February 2024, Law enforcement disrupt world's biggest ransomware operation, accessible at <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>

## Environmental crime

Four criminal networks specialising in waste and pollution crimes<sup>29</sup> and three engaging in wildlife crimes as their sole criminal activity have been reported in the most threatening criminal networks. Additionally, 12 networks engage in environmental crime as part of their wider criminal portfolio, mainly alongside drug trafficking.

The networks involved in wildlife crimes have been contributed by France, Portugal and Spain and relate to illicit glass eel trafficking. The criminals involved in this area are mainly Chinese, French and Spanish nationals.

Most of the criminal networks engaging in waste and pollution crimes as (one of) their main activities have been contributed by Italy. It usually involves poly-criminal mafia-type criminal networks, operating in Italy, the Netherlands and Spain.

## Extortion and racketeering

Five most threatening criminal networks engage in extortion and racketeering activities as their sole criminal business. These networks have been contributed by Cyprus, France and Italy.

Extortion and racketeering are more often linked to main criminal activities, such as drug trafficking and fraud. In some cases, there are also links with violent crimes such as murders, kidnappings and robberies. The main nationalities represented in these networks are Cypriot, Italian and Swedish, and these are also the countries that have reported the networks with extortion and racketeering in their criminal portfolio.

## Firearms trafficking

Five most threatening criminal networks engage in firearms trafficking as their sole criminal business. More often, it is linked to main criminal activities such as drug trafficking.

The availability of firearms also supports a range of other serious and organised crime activities. Illicit firearms, explosives and pyrotechnics trafficked in the EU enable and reinforce serious and organised crime-related violence, a phenomenon that has become a daily reality in some Member States. The availability of firearms on the black market also heightens security risks to the safety of citizens, such as through public shootings.

According to available intelligence, most illegal firearms in circulation in the EU originate from within the region. They are diverted from legal supply, smuggled in from (past) conflicts in neighbouring regions (for example the Western Balkans), reactivated or converted from non-lethal firearms or manufactured in clandestine workshops.

The broadening range of trafficked firearms and explosives has come

<sup>29</sup> The illegal trafficking and/or disposal of several types of waste, both hazardous and non-hazardous. Some of the most common types of substances unlawfully disposed are chemical waste, construction and demolition waste, plastic waste, waste of electronic and electric equipment (WEEE), end-of-life vehicles and car parts and scrap metals.

to the forefront in the past few years. Illegal privately manufactured firearms appear to have become more commonly trafficked in the EU. Such firearms are assembled from parts that are sourced legally and then combined with illegally obtained polymer frames or fake components. Investigations reveal that privately manufactured firearms have been used in violent incidents in the EU. Seizures of bigger volumes of completely non-original, counterfeit firearms in the EU have also become common. These fake firearms are believed to be manufactured outside of the EU, often in Türkiye, and then trafficked to EU Member States by Turkish criminal networks.

The threat posed by 3D-printed weapons and weapons parts is also increasing, with more printing workshops being dismantled by law enforcement authorities. However, it remains limited in comparison to the other sources of firearms, and the interest of the most threatening criminal networks remains in real, converted or counterfeit firearms.

Three types of entities are involved in firearms trafficking. The first are criminal networks that specialise in dealing with firearms as their main activity. These networks often originate from the Balkan region.

The second are large-scale poly-criminal networks, mainly drug trafficking (cocaine and cannabis) and extortion and racketeering networks that engage in weapons trafficking as a subsidiary activity. Some criminal groups likely enter this business by tapping into existing criminal contacts, crime infrastructure and smuggling routes used for other illegal commodities. However, it is not always clear where and how these networks source the weapons they traffic and whether part of the network specialises in firearms trafficking. It is possible that the surplus of weapons purchased from specialised firearms traffickers for the networks' own use are sold further for additional profit, or that criminal networks that specialise in other criminal activities have access to weapon stocks through their network.

The third type of entity involved in firearms trafficking are individuals selling firearms to different criminal networks and people with violent extremist or terrorist affiliations.

Law enforcement continues to face challenges from the fragmented intelligence picture on weapon seizures in the EU. Tracing illicit firearms used in organised crime activities remains challenging, as often, the only forensic evidence left at the crime scene is the ammunition discharged, which receives less attention from investigators than the primary offence committed. Even when firearms are seized, they are difficult to trace as most are unregistered, diverted or stolen or have had their identification markings altered or removed, hampering investigations.

# WHAT MAKES CRIMINAL NETWORKS MOST THREATENING?

From their agility (A) to their destructive nature (D), specific characteristics of criminal networks are essential for their functioning and serve as pointers to better understand the threats these criminal networks pose. This chapter considers the relevance of such threat indicators<sup>30</sup> and explains why these make some networks more threatening than others. Once we understand what determines the threat of criminal networks, we are better equipped to design measures to counter them.

## **Their infiltration in the legal business world for facilitation of criminal activities, as a countermeasure, or for money laundering**

A critical characteristic of the most threatening criminal networks is their capability to misuse the infrastructure available through businesses and companies to facilitate their criminal objectives. There is almost no actor in the serious and organised crime landscape who is not linked, in one way or another, to a sector of the legal economy, whether to commit the criminal activity, to disguise the criminal activity, or to launder their criminal profits. This is what makes the most threatening criminal networks agile.

### **Criminally owned or infiltrated LBS**

86 % of the most threatening criminal networks make use of LBS. A large part does this in a way that represents the highest threat level: setting up its own LBS, infiltrating existing LBS at a high level or colluding with or coercing key high-level individuals within a LBS to gain access to or control over the LBS.

---

<sup>30</sup> Any statistics on the threatening aspects of criminal networks are based on those criminal networks for which information on the particular threat indicator is available.

### Case example

#### **LBS USED FOR COCAINE TRAFFICKING AND MONEY LAUNDERING**

The leader of a criminal network, an Italian businessman of Argentinian origin residing in Marbella, uses his companies to conceal both drug trafficking and money laundering activities. He manages several companies, including one importing bananas from Ecuador to the EU. He also owns sports centres in Marbella, commercial centres in Granada and multiple bars and restaurants. An Albanian accomplice, based in Ecuador, takes care of the import of cocaine from Colombia to Ecuador and the subsequent distribution to the EU. Ecuadorian fruit companies are used as a front for these criminal activities.<sup>31</sup>

The misuse of LBS can be an inherent part of the crime area in which criminal networks are active. For instance, in the case of frauds against the national financial interest of EU Member States, such as the misuse of public funding, VAT fraud and Missing Trader Intra Community (MTIC) fraud. For other crime areas, even though LBS are not an intrinsic part of the modus operandi, they may be important facilitators of criminal activities. For example, front or shell companies may be used to facilitate the movement of illicit or stolen goods or to enable money laundering activities. Companies are set up to provide official work for members of the criminal networks. Shell companies are set up to conceal and facilitate a wide range of criminal activities, from investment fraud and match-fixing to recruitment of victims for THB, and beyond.

Infiltration and misuse of LBS can be systematic and long-term, or temporary. Criminal networks set up new companies or infiltrate existing business structures to take advantage of the façade of legitimacy, as existing companies with an established and healthy financial and tax record often attract less attention from tax authorities and law enforcement. Criminal networks abuse the names of bona fide existing companies to facilitate their criminal activities while those abused are unaware of it. They sometimes also set up companies with similar names to existing companies.

LBS are registered in the name of the leaders, core members or low-ranking members of criminal networks. Strawmen without criminal records, often relatives or friends of network members, are also used to register the LBS or the accounts linked to the real or bogus legal business entity.

LBS used or abused by criminal networks for their criminal enterprise are situated in almost 80 countries across different continents (see also: *Global links and reach overall*).

<sup>31</sup> Europol, 16 February 2024, Properties worth EUR 48 million frozen after cocaine sweep in Ecuador and Spain, available at <https://www.europol.europa.eu/media-press/newsroom/news/properties-worth-eur-48-million-frozen-after-cocaine-sweep-in-ecuador-and-spain>



## Some sectors particularly at risk; all sectors potentially affected

The data show clearly that LBS are infiltrated or misused by criminal networks across almost all sectors, including tourism, recycling, wellness and sports, retail and cultural associations.

Three sectors are particularly affected by criminal infiltration or abuse: construction, hospitality and logistics (i.e. transport and import/export companies). The companies are used in all crime areas with the exception of cyber-attacks.

In the construction sector, LBS are used to facilitate criminal activities and money laundering in almost all crime areas: drug trafficking, extortion and racketeering, frauds against the public interest of the EU or Member States and online fraud, migrant smuggling, organised property crime, waste trafficking and weapons trafficking. Construction companies can be used to invest laundered criminal proceeds or can be set up as a cover for renting warehouses to conduct illicit activities.

LBS in the hospitality sector, including nightclubs, are often exploited for the purposes of drug trafficking, extortion and racketeering, frauds against the public interest (including VAT, MTIC and excise fraud), migrant smuggling, organised property crime and weapons trafficking. However, the sector is not reported in connection with criminal networks active in commodity counterfeiting goods, cyber-attacks, environmental crime and online frauds. Establishments operated by this sector are convenient as meeting places for criminal partners, as selling points for drugs or as a front for money laundering schemes.

LBS in the logistics sector (transport and import/export) are mainly used in drug and waste trafficking, but also in almost all other crime areas – counterfeiting of goods, extortion and racketeering, frauds against the public interest of the EU or Member States (including VAT, MTIC and excise fraud) and online frauds, migrant smuggling, organised property crime (for example, stolen vehicles), waste and wildlife trafficking, and weapons trafficking. Besides the common facilitation of illicit goods overseas and the transport throughout the EU by haulage companies, this can also include the abuse of taxi companies to move money, for example.

The sectors and types of LBS that a criminal network may infiltrate, and the motivations behind these choices, can vary considerably. Examples include infiltration of the construction, catering and real estate sector for money laundering, the retail sector for VAT fraud, and the car industry for vehicle trafficking. To support the criminal activity while increasing resilience against law enforcement intervention, the LBS can be spread over a number of countries.

## Their money laundering capabilities

Money laundering, criminal finances and corruption are as pervasive and disruptive for society as they are indispensable for criminal actors. Almost all of the most threatening criminal networks make use of at least basic money laundering techniques. Their far-reaching tentacles corrode the rule of law, grind down people's trust in the justice system and its institutions, and weaken societal and economic growth. The lines between the illegal and legal worlds become increasingly blurred; criminal finances and investments are tangled with legal ones.

The most threatening criminal networks in the EU use real estate as one of the main industries to launder their illicit profits (41 %). When laundering through investments in real estate, some criminal networks launder their profits through the purchase of physical and financial assets often linked to private companies, or by financial and legal experts (i.e. lawyers and accountants) who are sometimes unaware of the criminal origin of the assets. Ownership of these assets is exchanged between companies when necessary, either as a means of payment for other criminal activities and/or as an investment. This blending of illicit profits with legal assets and the fact that there are no financial transactions involved during the transferral of assets makes it challenging for investigators to link the movement of assets to a criminal venture.<sup>32</sup>

Other common money laundering techniques include investments in high-value goods such as gold and luxury items (27 %), the use of cash-intensive businesses, for example in the hospitality sector (20 %), and the use of cryptocurrencies (10 %). Creating a complex web of companies, often without real activity, with strawmen as administrators and located in various countries, is another technique used for money laundering purposes. False contracts and invoices make it possible to transfer large amounts of money via the bank accounts of these companies. Other techniques include identifying companies on the brink of bankruptcy (which are then bought out), placing money in offshore companies and bank accounts of third parties, fraudulent bookkeeping, and the issue and use of invoices for non-existent business activities.

### Case example

#### **MONEY LAUNDERING NETWORK OFFERING TRADE-BASED MONEY LAUNDERING SERVICES**

A specialised criminal service provider network, composed of Italian, Albanian, Colombian, Moroccan, and Syrian nationals, has built up an international network of companies to launder illicit proceeds. The criminal network offers professional services to hide the origin of proceeds generated from illegal drug trafficking in South America. In order to launder drug profits, the network offers a service of trade-based money laundering. The drug producers would provide drugs to Italian buyers as a form of credit. The profits generated from the sale of the drugs in Europe are then picked up by brokers, introduced into companies, and used for ordering goods such as mobile phones from China. These goods are then shipped to the United States and further transported to Colombia, where they are offered on the market. Upon being sold, the cartels receive the cash and thus their veiled payment for the drugs provided to European sellers.<sup>33</sup>

<sup>32</sup> Ibid.

<sup>33</sup> Europol, 16 February 2024, Properties worth EUR 48 million frozen after cocaine sweep in Ecuador and Spain, available at <https://www.europol.europa.eu/media-press/newsroom/news/properties-worth-eur-48-million-frozen-after-cocaine-sweep-in-ecuador-and-spain>

Money laundering activities take place in more than 80 countries (see also: *Global links and reach overall*).

Dedicated expertise is indispensable when it comes to money laundering, and experts are often considered critical and irreplaceable in the criminal process. The availability of such expertise for criminal networks is linked to a higher threat, as it allows them to bring criminal money into the legal economy and gain more power in society.

The experts needed for money laundering range from professionals with deep technical expertise to those skilled in more executive tasks. More technical profiles include financial experts, legal experts and real estate experts. Profiles relevant for executive tasks in money laundering include cash collectors, money couriers and money mules. Experts are generally located in the reporting country.

The importance of money laundering as part of the crime infrastructure, coupled with the profit-oriented nature of serious and organised crime, means that it is often regarded as the main activity of criminal networks, even if it supports their actual core business, and these expert roles are actually embedded in the criminal network. In exceptional cases, expertise is available outside of the network under the 'crime-as-a-service' concept.

The most threatening criminal networks include (a small number of) specialised criminal service-providers, which are only involved in the provision of money laundering services to other criminal networks, without being active in other crime areas. Money laundering techniques used by these networks vary, including trade-based money laundering through legal business structures, investment in real estate and cash-based money laundering techniques. In these networks, in addition to the role of the money launderer on which the activities of the criminal networks rest, financial and legal advisors, document forgers and brokers also play an important role. Frequently, some of the money laundering activities take place in the country where the launderer is based. However, these activities are not exclusively limited to the country of location of the launderer.

## Their international reach with regional focus

The most threatening criminal networks are active in all 27 EU Member States and have nationals of all 27 Member States among their members. In addition, they work with many other nationals and have a reach that spreads across the globe. Serious and organised crime is truly international and borderless.

Yet, the collected data also show that criminal networks are at their most threatening when their geographic sphere of activity and influence remains relatively contained. Most of them contain their presence and activities in three to seven countries. Only a minority of the most threatening criminal networks are present and active in more than seven countries.

Overall, the data show that while most threatening criminal networks are active across (EU and non-EU) borders, they do often maintain a certain regional focus. A wide geographical reach may also increase the risk of detection.

### Global links and reach overall

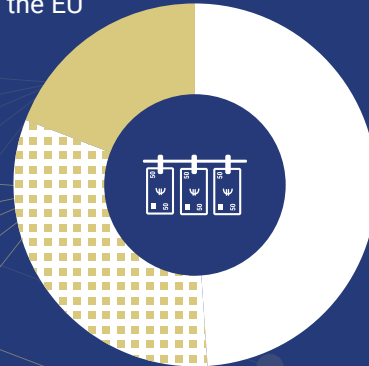
Overall, the most threatening criminal networks affecting the EU link to all of the 27 EU Member States, all Schengen-associated countries, all countries bordering the EU and all global regions. Serious and organised crime at its most threatening level concerns every single EU Member State. And it reaches outside the EU – for the origin of criminal goods, the recruitment of victims, for partnerships and infrastructure that enables criminal endeavours.

Crime is borderless – the majority (68 %) of the most threatening criminal networks have activities and presence in both EU and non-EU countries. Countries outside the EU with most activity are Albania, Brazil, Colombia, Switzerland, Türkiye, United Arab Emirates and the United Kingdom. One-third of the most threatening criminal networks focus their activities on EU Member States only.

Money laundering activities take place in more than 80 countries. Zooming into the geographic scope of these networks' money laundering operations, 49 % of the most threatening criminal networks launder money only in the EU, 32 % launder money both in and outside the EU, and 19 % launder money only outside the EU.

**19%**

only outside  
the EU



**49%**

only in the EU

**32%**

both in and  
outside the EU

**MONEY LAUNDERING**

**10%**

only outside  
the EU



**20%**

both in and  
outside the EU

**70%**

only in the EU

**MISUSE OF LEGAL BUSINESS STRUCTURES**

Criminally infiltrated LBS are situated in almost 80 countries across different continents. 70 % of the most threatening criminal networks misuse LBS only in the EU, 20 % both in and outside the EU, and 10 % only outside the EU.

The true international nature of the most threatening criminal networks is not only reflected in their area of activity, but also in their composition. Members of the most threatening criminal networks represent 112 nationalities, including all 27 Member States and 85 non-EU countries from all regions of the world (see also: *Internal organisation and composition*), mostly in the form of combined membership of both EU and non-EU nationals.

While the nationalities cooperating within a network may indicate how international its reach is, there are other ways to establish connections to certain regions. Criminal networks with activities overseas do not necessarily have members from that region. For example, only 36 % of the criminal networks operating in Latin America have related nationalities among their members. In cases where criminal networks operate in an overseas region without having a member originating from there, it may be the case that the activities are facilitated by brokers and other criminal service providers with ties to that specific area (see also: *Their criminal cooperation model*).

### The spectrum of leadership: proximity and beyond

Most threatening criminal networks' leadership is in the majority of cases settled in the reporting country and, by extension, in the country where the criminal network is (partially) active. Alternatively, the leadership is settled in the same country as the network members' dominant nationality – likely also the leader's country of origin. Settling in a country of activity may be a strategic choice for high-level members of criminal networks to more effectively manage criminal operations and their contacts. Having the leadership located and operating remotely from an outpost in another country of activity may be also used as a countermeasure against law enforcement detection.

For 18 % of the most threatening criminal networks, the leadership is based in a country that is different to the reporting country or the country of origin, either in or outside the EU. Some 6 % have remote leadership settled outside the EU; the most common locations are the United Arab Emirates and to a lesser extent Türkiye and the United Kingdom.

Previous investigations into encrypted communications used by criminal elements revealed that Dubai (United Arab Emirates) has emerged as a remote coordination hub where high-level members and other criminal actors, such as brokers and organisers, reside to coordinate the activities of criminal networks and hinder law enforcement detection. However, when looking at the geographical locations of leaders of high-risk criminal networks, Dubai does not appear to stand out as a secluded safe haven for leaders. In most cases, those networks whose leaders are settled in Dubai also conduct either their main, supporting or subsidiary activities in the United Arab Emirates. It is only in two cases in which the leadership is completely remotely settled in the United Arab Emirates with no apparent links to the country in terms of their criminal activities (see also: *Leadership*).



## Key locations of criminal networks

When analysing the geographic dimension of criminal networks, some countries are more visible than others, as locations for criminal activity, origins of criminal network members, settlement for leadership or locations of exploited legal business or money laundering infrastructure. There are several reasons why these locations stand out, including the availability of logistical infrastructure (e.g. harbours misused for large-scale trafficking activities, road infrastructure connecting to the hinterland), urban areas with high demand for illicit goods, production of illicit goods close to the distribution as a countermeasure against detection of the international trafficking process, the proximity of borders, or a combination of these factors.

## Their survival strategies: adaptive problem solving and countermeasures

The most threatening criminal networks are often long-lasting ones, that have already been active for multiple years and have managed to resist dismantlement. They continue their criminal business despite – or thanks to – changes in their environment and law enforcement attention.

## Resilience and continuity over time

The amount of time a criminal network is active for highlights its effectiveness and efficiency and its capacity to withstand disruption. The majority of the criminal networks reported have been active for a long period, and one-third have even been active for 10 years or more.

Good cohesion (see also: *What glues networks together? Cohesion and leadership*) also leads to high levels of continuity and resilience in networks. It enables criminal networks to withstand disruption, investigations and arrests of core members, and adapt to changes in the environment.

The majority of the most threatening criminal networks are able to continue their activities and withhold their organisation over time, while also maintaining their influence and power. Two-thirds are described as being in a stable and settled situation in terms of scope of criminal activities, dominance of criminal markets, profits and infiltration of legal economies. Emerging, up-and-coming criminal networks are less common among the most threatening ones – they represent one in five.

This means that law enforcement attention should remain focused on long-standing, known criminal networks, even if they are under law enforcement scrutiny and even if action has already been taken against them. After being convicted, members of networks are able to continue their criminal business from prison, in sight of law enforcement, by reorganising and delegating to trusted fellow members.

## Case example

### **CRIMINAL NETWORK COORDINATED FROM PRISON**

The leader of a criminal network with links to the Western Balkan region continues to orchestrate criminal activities from his prison cell in Italy. From there, he is believed to regularly give orders and instructions to his subordinates on matters related to the trafficking of drugs and firearms. The criminal network is active in Belgium, the Netherlands, Italy, Germany, Croatia, Slovenia and Bosnia and Herzegovina.<sup>34</sup>

## Flexibility and adaptability

The ability of a criminal network to adapt its criminal activities or working processes to changes in the macro-environment in which it operates is another key indicator of its threat. Most criminal networks are able to adapt proactively and even innovatively.

## Countermeasures

The majority of the most threatening criminal networks have a good understanding of law enforcement techniques and use countermeasures strategically to avoid detection, investigation or prosecution by law enforcement.

The criminal networks that use countermeasures against law enforcement strategically as part of their day-to-day operations mostly use technologies such as encrypted applications or devices (EncroChat or SkyECC) on which they use code language to communicate. The use of artificial intelligence may further facilitate criminals' use of countermeasures in the future. Other networks avoid communicating on any device and hold face-to-face meetings to leave no trace of their activities.

A recurring element in avoiding detection and prosecution is the counter-observation and infiltration of law enforcement, including the identification of informants and undercover agents. This often goes hand-in-hand with investing in countering prosecution through collusion with lawyers who provide access to confidential information and engage in excessive appeal procedures and witness tampering. In some cases, lawyers even advise criminal networks on how to minimise detection and liability before the criminal act is committed.

<sup>34</sup> Europol, 25 May 2023, 37 arrested as violent Balkan criminal cell is taken down, available at <https://www.europol.europa.eu/media-press/newsroom/news/37-arrested-violent-balkan-criminal-cell-taken-down>



## Case example

### **SECURITY MEASURES EMPLOYED BY CRIMINAL NETWORK TO PROTECT THIEF IN LAW CHIEF**

A criminal network of 'Thieves in Law' (Vory V Zakone) is involved in the theft and sale of stolen merchandise, smuggling of tobacco and the laundering of criminal assets. They employ a set of countermeasures in order to shield the leader. This includes the use of different vehicles registered in the name of members of the organisation, and a house rented under a different name. The vehicles used by the leader are regularly examined at the organisation's workshops to detect electronic tracking devices that might have been installed by the police.<sup>35</sup>

Countermeasures are usually used against law enforcement authorities, including police, customs and the judiciary. Countermeasures and corruption are closely linked, as one of the common objectives of corruption is to obtain information about law enforcement investigations and to obstruct the course of justice. In this context, other actors in the judicial system such as lawyers and witnesses are liable to being approached by criminal networks for corruption (see also: *Corruption and influence*).

### Recruitment of minors

Vulnerable minors and young individuals are often abused by some of the most threatening criminal networks. They recruit minors for on-the-ground execution, such as the distribution of drugs or the commission of violent attacks to intimidate non-collaborative actors. This has come to the front more explicitly over the past years, with various youngsters having been linked to drug-related crimes. Minors are also (ab)used for other criminal activities, such as forced begging or thefts. This is particularly the case within certain MOCGs.

Criminal networks' abuse of minors is a countermeasure as it increases the distance between the criminal activity and the network's core members or leaders, hampering identification. From the perspective of criminal networks, the impunity granted to minors may make them attractive recruits. Such practices victimise minors as they may become entrapped in a criminal lifestyle, making it difficult to remove themselves from such an environment.

<sup>35</sup> Europol, 28 June 2023, 28 arrests as France and Spain hit chief 'Thief in Law', available at <https://www.europol.europa.eu/media-press/newsroom/news/28-arrests-france-and-spain-hit-chief-%E2%80%98thief-in-law%E2%80%99>

## Their criminal cooperation model

The most threatening criminal networks can profit from their independence or from opportunistic and equal partnerships to reach their criminal objectives. This allows them to maintain a high degree of control over the criminal business or at least over their part of the criminal process. Where they are in need of technical expertise or low-level executors, the networks delegate parts of the criminal process to external service providers. This further adds to their threat, as any capability or function can be obtained in exchange for payment.

### Independence, or equal partnerships

About one-third of the most threatening criminal networks do not engage in cooperative partnerships with other criminal networks. They operate independently and manage all relevant functions of the criminal process in a self-reliant manner.

For those who choose to cooperate, collaboration is characterised by relational dynamics primarily centred around equal partnerships. This is a more relevant qualifier for a threatening criminal network, than being on the dominant side of the cooperation – or, logically, on the inferior side.

However, these equal cooperations can also blur our understanding of the functioning of criminal networks. Boundaries can become unclear when a criminal network consists of different cells working together and cooperating closely with other criminal networks, with brokers acting as a bridge between networks.

### End-to-end control over criminal operations

This form of cooperation model likely increases efficiency and allows for a high degree of independence in controlling the full criminal business process, from start to finish. More than half of the reported criminal networks tend to have end-to-end control over the majority of their activities, especially when it comes to their main criminal activities. Supporting activities are also often kept in-house. For their subsidiary activities, criminal networks are more likely to delegate certain stages of the criminal operations.

Criminal networks tend to exert strong end-to-end control over their activities when inter-personal deceit or influence plays a central role in the crime, for example, in the case of extortion and racketeering, online frauds, match-fixing and THB for sexual or labour exploitation. End-to-end control also seems prominent in different forms of organised property crime and goods counterfeiting. Criminal networks tend to delegate specific stages of criminal operations to other networks when activities involve physical long-distance trafficking with multiple stages (for example migrant smuggling, drug trafficking and firearms trafficking) or require deep expertise (for example, VAT, customs and excise fraud).

To exert end-to-end control over their criminal activities, criminal networks build reliable contacts all over the world. These contacts can be part of the networks themselves posted in strategic locations or part of

another network with whom they cooperate in a regular, established way. Alternatively, these contacts may take the form of external partners from the private or public sectors.

### Service provision for niche or low-level criminal activities

Crime as a service constitutes the provision of a criminal activity or part of the criminal process, as a service and against payment, to one or multiple criminal actors.

It often revolves around a niche activity that requires technical specialisation (see also *Expertise by people and tools*), or a low-level activity that is outsourced as a countermeasure. The top 10 roles most commonly performed by external actors who are not members of the criminal network and act as external crime-as-a-service providers include strawmen, technical experts, transport service providers, corrupt actors, financial advisors/experts, document and identity forgers, street dealers and couriers (except for money).

A few of the most threatening criminal networks offer or use violence-as-a-service, including professional contract killings, or violence used to support criminal business or settle conflicts (see also: *Widespread use of violence and intimidation*). Similarly, professional broker networks offer money laundering as a service (see also: *Their money laundering capabilities*).

## Their – often combined – use of violence and corruption

Not all of the most threatening criminal networks use corruption or violence. However, a key portion use violence and/or corruption as part of their criminal process and strategy. This is what makes them destructive and damaging to the EU's internal security and the rule of law.

### Widespread use of violence and intimidation

About one-third of the most threatening criminal networks do not use violence. A further one-third use violence reactively or to support their criminal activities, while the remaining one-third use violence or extreme violence in an offensive, planned, premeditated and systematic way.

Criminal networks engaging in violence and intimidation are mainly involved in extortion and racketeering as an inherent feature of their modus operandi. The majority of criminal networks involved in drug trafficking, environmental crime, firearms trafficking and THB engage in some form of violence or intimidation. Criminal networks involved in firearms trafficking and drug trafficking use more extreme violence, while for those active in environmental crime and trafficking of human beings, violence is less extreme and more reactive. Drug trafficking networks often engage in extortion and racketeering activities. In this way, they gain access to and control over local entrepreneurs and traders, which often include cash-intensive businesses such as restaurants or nightclubs. If

intimidation fails to work, they resort to (threats of) violence, including physical violence or destruction of premises, to achieve their goal. As such, they strongly infiltrate the legal economy in certain territories.

One-third of the criminal networks do not use violence or intimidation. These criminal networks are mainly involved in cyber-attacks, online frauds and counterfeiting.

Many use extreme violence in an offensive, planned, premeditated and systematic way, both towards group members and their family and friends, and towards rival criminal networks and other external targets. Criminal networks engaging in drug-related crime, extortion or racketeering activities exhibit a particularly high degree of violence.

Internal violence takes the form of direct or indirect threats, throwing explosives or shooting at houses or cars, kidnappings, torture and even murder. There are several motives for this form of violence including maintaining discipline, punishing members for betrayal, financial damage (e.g. lost drug loads) or actions that deviate from the network's policy, pressurising individuals who want to leave the criminal network and preventing individuals from providing information to the police or rival networks.

External violence is predominantly directed towards rival criminal networks for revenge, retaliation for another crime, a fight over territory or to settle outstanding debts.

The private sector is also a regular target of violence or intimidation. This often takes place in the framework of extortion and racketeering or drug trafficking activities.

Violence against police, customs, judiciary and other public officials does not appear to be an explicit strategy of criminal networks.

Victims of THB or customers of migrant smuggling services may also suffer violence or intimidation from the criminal networks exploiting them. The same applies to witnesses of crimes. Violence or intimidation may be used against them to prevent them from making statements to the police.

Instances of extreme external violence include the kidnapping and torture (cutting of fingers, pouring boiling water over body parts, stabbing, etc.) of rival group members or former business partners, as well as contract killings. The use of explosives and firearms – sometimes in populated public places – is not uncommon.

A small number of criminal networks are known to use and/or provide violence as a service (see also: *Their criminal cooperation model*). Most of the groups involved are hierarchical and poly-criminal. These services include professionally planned and organised contract killings, as well as violence used as a means of debt collection and extortion or to settle criminal conflicts.

## Corruption and influence

71 % of the most threatening criminal networks use some form of corruption, including 28 % that use it proactively and systematically.

The data reveal how criminals use bribery, actively and passively, to further their criminal enterprises. Bribes are the most common modus operandi, together with the donation of gifts and other benefits in kind such as holidays, facilitation of sexual services or meals. The exploitation of family, loyalty and friendship is also common. Trusted members who are part of the inner circle of strategic and high-level actors are targeted to exert influence and make these actors support criminal activity, either knowingly or unknowingly.

Criminal networks use corruption to facilitate their activities in drug trafficking (heroin, cannabis, cocaine), VAT, MTIC and subsidy fraud, extortion and racketeering, match fixing, environmental crime (waste and wildlife trafficking) and firearms trafficking. Investigations into Sky ECC have shown how corruption is deeply rooted in many countries in and outside of the EU. Member States are not immune to this reality.

Although corruption varies in nature and extent from one country to another, it affects all Member States in which criminal actors carry out their business.<sup>36</sup>

Corruption targets both the private and public sectors. Some criminal networks have access to corrupted individuals in multiple organisations and hubs, often via multiple channels. Strategically placed along routes and criminal processes, these corrupted individuals become part of the network. Corruption does not appear to be provided as a service to multiple networks; rather, corrupted actors are embedded within the criminal networks themselves.

### Case example

#### **CORRUPT PORT EMPLOYEES FACILITATE DRUG EXTRACTION**

A family-structured criminal network, based in Antwerp, engages in cannabis and cocaine trafficking. Most of the suspects have both Belgian and Albanian nationalities. This network has close contacts with a second criminal network, engaged in the importation of hashish from Spain and the extraction of cocaine shipments from Antwerp harbour. They have access to several corrupt employees working around the port.<sup>37</sup>

Police, customs and justice departments are obvious targets for corruption. Corruption is used to obtain an extensive range of services, with a focus on obtaining information or obstructing interventions of law enforcement and justice. They are approached to provide information, for example, on ongoing investigations or operational actions, or to intervene directly by falsifying or destroying official documents, through witness-tampering, perjury, covering up illegal actors and influencing sentencing. Within this framework, other actors in the judicial system such as lawyers and witnesses are also prone to approaches by criminal networks for corruption purposes.

<sup>36</sup> Kantar, 2020, Special Eurobarometer 502 "Corruption", Survey requested by the European Commission, Directorate-General for Migration and Home Affairs and coordinated by the Directorate-General for Communication

<sup>37</sup> Europol, 11 May 2023, Underworld 'co-working' space shut down in Antwerp, available at <https://www.europol.europa.eu/media-press/newsroom/news/underworld-co-working-space-shut-down-in-antwerp>

The data show that other public officials are also a highly targeted group for corruption, including civil servants, employees in public and local administrations, financial and other inspectors, tax collectors, and administrators. Criminal networks try to influence public administration, including employment, migration and tax agencies, economic inspection and municipal administration, to commit welfare fraud, vehicle and population registration offences, receive building permissions, and influence public procurement, land allocation, land development and public contracts (for example, in the waste sector) and grants to associations.<sup>38</sup> This influence is exerted through infiltration, threats, violence and corruption. Corrupted individuals in public administration are also key assets for networks involved in fraud schemes and money laundering, as they facilitate the acquisition of public tenders and contracts and turn a blind eye to the management of illicit businesses used for money laundering purposes.

Private sector workers are also regularly targeted for corruption as the logistical processes for transporting illicit commodities through ports depend on the support of a variety of actors. Typical targets include employees of port-related companies. These corrupted personnel members facilitate unrestricted access to ports and port systems and provide logistical support and information. They include port workers and shipping company personnel, freight forwarders and shipping agents, importers, transport companies, terminals, security companies, maintenance companies and semi-public authorities with access to the port data systems. Bribery payments can reach hundreds of thousands of euros. The highest fees are paid to essential links in the extraction chain, who often include straddle carrier drivers, crane operators, planners or employees providing access to information via IT systems.<sup>39</sup> Networks also infiltrate the private sector to invest criminal proceeds.

### How violence and corruption go together

From an outside perspective, highly violent – and therefore more directly visible or at risk of detection – networks, appear to be very different from highly corruptive criminal networks which infiltrate the public and private worlds to strengthen their criminal operations. However, the data on the most threatening criminal networks highlight that violence and corruption often go hand-in-hand. As many as one in five of the most threatening criminal networks use both corruption and violence in a proactive, planned manner, as critical parts of their business process.

Corrupt practices are often closely linked with violence and accompanied by intimidation through threats, physical assaults, vehicle arson and the use of explosives. When compromised personnel want to step out of a corrupt network or, more rarely, criminals need to force unwilling individuals to serve them, criminal networks turn to intimidation, blackmail and violence.<sup>40</sup>

38 Carina Gunnarson, SNS, Center for Business and Policy Studies Sweden, 2023, The Vulnerable State: A Research Review on How Organized Crime Influences the State and Municipalities available at <https://www.sns.se/en/articles/the-vulnerable-state-a-research-review-on-how-organized-crime-influences-the-state-and-municipalities/>

39 Europol and Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam, 2023, Criminal networks in EU ports: Risk and challenges for law enforcement – Focus on the misappropriation of container reference codes in the ports of Antwerp, Hamburg and Rotterdam, Joint report, accessible at [https://www.europol.europa.eu/cms/sites/default/files/documents/Europol\\_Joint-report\\_Criminal%20networks%20in%20EU%20ports\\_Public\\_version.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint-report_Criminal%20networks%20in%20EU%20ports_Public_version.pdf)

40 Ibid.

Yet, corruption and violence are not a prerequisite for a criminal network to feature among the most threatening ones. About 1 in 10 of the most threatening networks do not use violence or corruption.

## **Their resources – from money to expertise**

The most threatening criminal networks affecting the EU are also characterised by the specific resources that they have obtained or are able to deploy. They are at their strongest and most effective when they already have or can easily find abundant financial resources, as well as materials, information and communication tools for their criminal activities. This characteristic often goes hand-in-hand with extensive criminal profits.

In addition to material resources, a key characteristic of the most threatening criminal networks is that they are able to use people with specific skills and knowledge, such as high-level experts that are part of the criminal network, or service providers that can deliver a specific expertise or service needed for the criminal process. Most threatening criminal networks also tend to employ expert-level digital or technological tools.

### **Financial resources and criminal profits**

---

The largest share (56 %) of the most threatening criminal networks have or are able to obtain abundant financial resources to support their criminal undertakings.

The availability of sufficient funds is closely linked with the potential for profit-making – a key objective for most actors in serious and organised crime. Many networks are able to generate more than EUR 1 million per year.

Generally, the estimated yearly criminal proceeds range from several millions to tens of millions of euros. Some criminal networks are even thought to generate hundreds of millions in illicit funds, with a handful reaching up to a billion euros.

While information is often missing about how other resources, such as materials, information, or communication tools are used for criminal objectives, it is clear that having access to other necessary resources heightens the threat of criminal networks. Examples of essential resources include the availability of precursors, means of transportation, (ware)houses and companies, devices used for secure communications and weapons. Social capital – relationships with police and public administrations – is a crucial asset for many of the most threatening criminal networks.

## Expertise through people and tools

Criminal networks often need experts with particular skills or know-how. These can be low-level or highly specialised experts and may be used periodically or on a continuous basis. This includes professional facilitators (notaries, solicitors and lawyers, accountants and tax specialists), and specialised experts (hackers, technicians, chemists, document forgers, recruiters, etc.), but also pilots, drivers, couriers and guides.

There is often a lack of information on the extent to which criminal networks make use of people with specific knowledge or skills. However, the largest share of criminal networks make use of high-level experts or provide a hard-to-find criminal service.

Dedicated experts are often considered to be among the most critical roles in the functioning of criminal networks. These include financial experts (money launderers, cash collectors, financial advisors), document counterfeiters, cyber-service and technological solution providers, and producers. These roles are critical for criminal networks whose main activities are drug trafficking, extortion, racketeering, criminal finances and money laundering.

Of the five most critical roles identified in the most threatening criminal networks, three are linked to money laundering (see also: *Their money laundering capabilities*). All the critical financial roles may be attributed to the final stages of the criminal process associated with the movement, laundering and repatriation of the illicit proceeds generated.

Cyber-service and technological solution providers offer critical support to networks involved in fraud schemes. Specifically, they devise mass mailing and phishing campaigns, create fake websites, advertisements and social media accounts, and support other cyber-based processes related to investment frauds and online fraud schemes. Networks involved in cyber-attacks play a critical role in programming malware, ransomware and hosting botnets. These individuals also occupy a crucial position in networks engaged in drug trafficking, extortion and racketeering and money laundering. They support the networks by advising them on online means for the movement of money and cryptocurrency payments. The simplest roles to replace are field operators (individuals tasked with low-level tasks), drivers, skippers and pilots, street dealers, couriers, money couriers and mules, accommodation providers, distributors, scouts and extractors.



## Case example

### **CYBERCRIME AS A SERVICE**

Genesis Market, one of the biggest criminal facilitators selling stolen account credentials to hackers worldwide, is taken down. This marketplace offers for sale so called 'bots' that infect victims' devices through malware or account takeover attacks. Such a bot provides criminals access to all the data stored on the devices, such as logins and passwords. The price per bot ranges from USD 0.70 to several hundreds of dollars depending on the amount and nature of the stolen data. The most expensive ones contain financial information that give access to online banking accounts.<sup>41</sup>

Several critical roles may also be outsourced under the crime-as-a-service model (see also *Their criminal cooperation model*).

In addition to human expertise, specific tools and technologies offer significant potential in facilitating criminal businesses.

In today's digitally accelerated world, the use of online platforms by organised crime seems obvious. However, 22 % of the most threatening criminal networks rarely use online platforms to support their criminal activities.

<sup>41</sup> Europol, 5 April, Takedown of notorious hacker marketplace selling your identity to criminals, available at <https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals>

# CONCLUSION

This report is a significant step forward in deepening our understanding of the key characteristics of the criminal networks that represent the highest threat to the EU's internal security. It is the first in-depth assessment at EU level from the criminal actor perspective and builds on an extensive amount of recent data submitted by EU Member States and third countries.

Each of the 821 identified most threatening criminal networks is unique. They vary significantly in terms of composition, structure, criminal activity, territorial control, longevity, types of cooperation and a range of other dimensions. But what makes one criminal network more threatening than another?

Some key capabilities stand out as determining characteristics of the most threatening criminal networks, summed up by the ABCD model:

## Agile

- ◇ The most threatening criminal networks are able to extensively infiltrate and misuse LBS. This helps their criminal business thrive, allows them to launder their criminal profits and shields them from detection.
- ◇ They implement strategies that allow them to persist over long periods of time. They respond swiftly to new opportunities and challenges, including those posed by law enforcement.

## Borderless

- ◇ Crime is borderless. The most threatening criminal networks have an international, and often global reach, yet they contain their criminal activity to a region or a limited number of countries.
- ◇ The composition of networks is very international, with nationals from all EU Member States and many other countries around the world cooperating within networks.

## Controlling

- ◇ The most threatening criminal networks tend to specialise in one main criminal business and operate with a large degree of independence.
- ◇ They are characterised by a strong leadership that is often close to operations but can also keep command remotely from global locations.

## Destructive

- ◇ Half of the most threatening criminal networks are involved in drug trafficking as their main activity. Other crime areas include fraud, property crime, migrant smuggling and trafficking in human beings (THB). These criminal activities have a severe impact on the EU and its citizens.
- ◇ Not all criminal networks use violence and corruption to support their businesses, but when they do, it heightens their threat level. These tools mutually reinforce each other and damage the fabric of our society.

Some other characteristics help us better understand how criminal networks function, but do not necessarily increase their threat level:

- ◇ **Structure:** While the majority of the most threatening criminal networks are organised in a hierarchical way, more horizontal and fluid networks can be equally threatening. Although strong leadership is of critical importance, it is not necessarily linked to specific individuals, and is in some cases replaceable (by inheritance, delegation or reorganisation) and continues even after conviction.
- ◇ **Member nationalities:** There is a large variety in the composition of criminal networks. Most are made up of members of different nationalities, and patterns of cohesion based on nationality are not always distinguishable. Alongside the common criminal objective, criminal networks form and persist due to strong social cohesion. This may also play a key role in attracting young people to organised crime.

This analysis can help law enforcement set out priorities on how best to combat the most threatening criminal networks.

Investigations should mirror the agility and resilience of criminal networks by employing proactive and all-encompassing approaches. They should look at not just main criminal activities, but also supporting and subsidiary activities that enable and support criminal networks to thrive for long periods of time.

To counter the strong borderless aspect of criminal networks, international and interregional cooperation is needed. This can be augmented by dedicated cooperation structures and partnerships, both within the EU and with global partners.

Finally, to tackle the destructive and threatening nature of criminal networks, law enforcement should join forces with partners to build pathways that fight organised crime at its very roots and cut off criminal businesses from the fabric of our society.

The collection and analysis of this comprehensive dataset of the 821 most threatening criminal networks affecting the EU is an extraordinary feat. It has provided valuable insights into the foundation of criminal networks and their threat level. Further developing the intelligence picture is a fundamental next step and goes hand-in-hand with sustained and timely information exchange.



**Your feedback matters.**

By clicking on the following link or 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](https://ec.europa.eu/eusurvey/runner/eus_strategic_reports)