

EU-SOCTA 2025

EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT



EUROPOL



The changing DNA of serious and organised crime

EXECUTIVE SUMMARY



The EU-SOCTA serves as Europol's flagship threat assessment, offering in-depth insights into the future threats posed by serious and organised crime within the EU. Europol plays a pivotal role in providing national law enforcement agencies and partners with critical intelligence on emerging threats, enabling stakeholders to better anticipate and prepare for future challenges. This strengthens law enforcement's ability to respond effectively to the evolving risks associated with organised crime.

Building upon previous editions of the EU-SOCTA—produced in 2013, 2017, and 2021—this fourth edition continues to build on the foundation of collaborative, intelligence-led approaches to combatting serious and organised crime. However, this edition of the EU-SOCTA stands as the most comprehensive, forward-looking analysis to date. It is underpinned by intelligence gathered from thousands of law enforcement investigations supported by Europol each year, complemented by strategic insights from law enforcement experts, contributions from other EU agencies and international organisations, private-sector data from Europol's Advisory Groups, and reflections from our Academic Advisory Group. This integration of diverse sources of information makes this report unique in its ability to provide a thorough forward-looking threat assessment of organised crime in the EU.

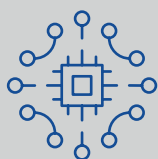
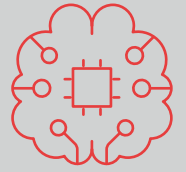
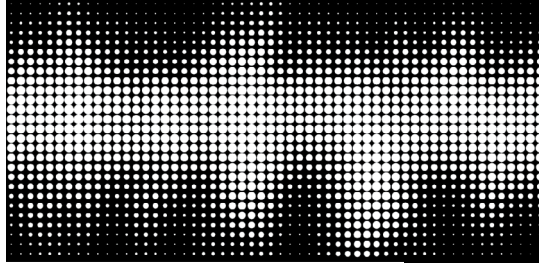
The EU-SOCTA re-emphasises that the threat of serious and organised crime to the EU and its Member States is pervasive, serious, and changing in fundamental ways. All criminal phenomena represent a threat to the EU, but some stand out as key threats, due to various features that make them more threatening. It is Europol's role, through the EU-SOCTA, to identify those key threats.

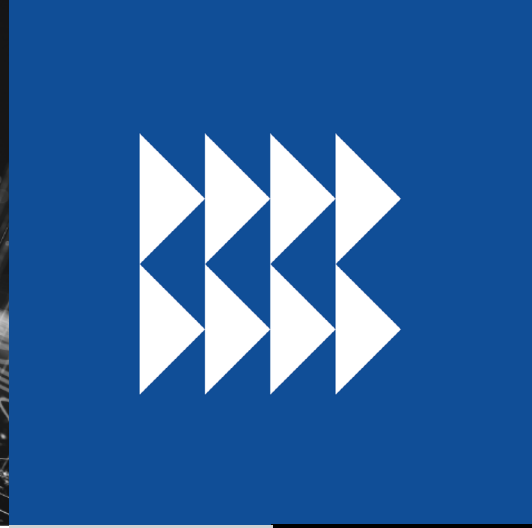


A FUNDAMENTAL SHIFT IN THE BLUEPRINT OF SERIOUS AND ORGANISED CRIME

The key crime areas that represent the highest threat level to the EU will be further exacerbated by the changing DNA of serious and organised crime. What stands out today, and will take even more prominence tomorrow, is how serious and organised crime is progressively destabilising, increasingly nurtured online, and strongly accelerated by Artificial Intelligence (AI) and other new technologies. A future-proof fight against serious and organised crime must consider this changing blueprint.

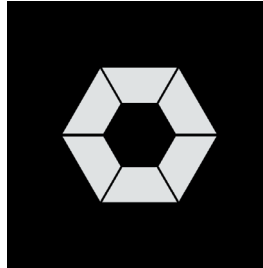
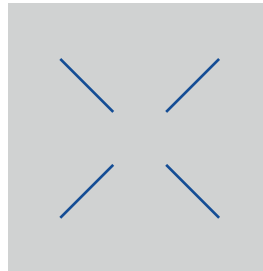
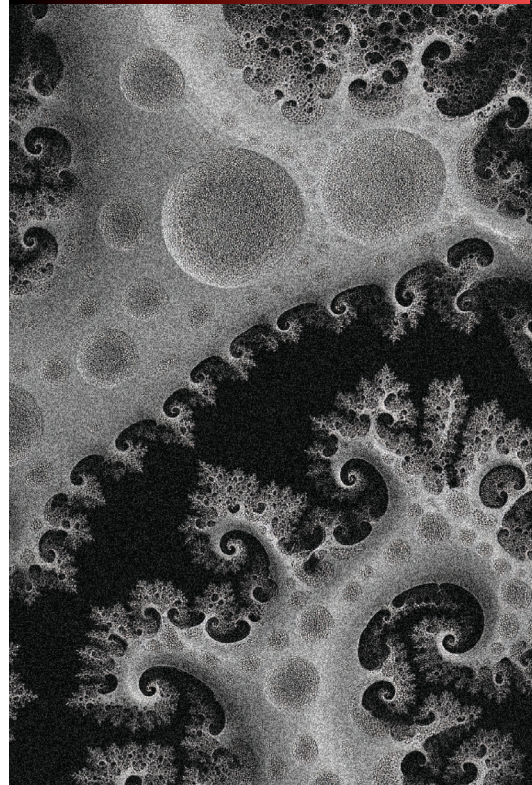
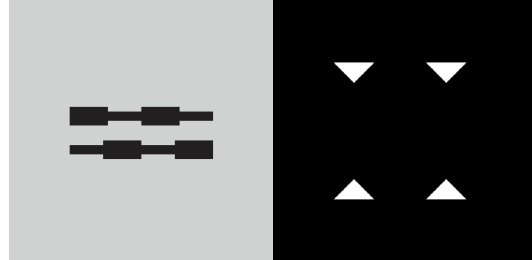
Destabilising: Serious and organised crime has a double destabilising effect on the EU. It undermines the EU's economy, rule of law and society by generating illicit proceeds, spreading violence, and normalising corruption. In a concerning development, serious and organised crime also increasingly destabilises the EU through collaboration between criminal networks and hybrid threat actors, leveraging each other's resources, expertise, and protection, to each achieve their objectives. The line between profit and state-aligned or ideological motivations is blurring.

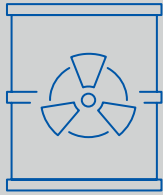




Nurtured online: Crime is increasingly nurtured online, more specifically by criminal networks' exploitation of digital and online infrastructure. More criminal activities are taking place to a larger extent online, with an increased volume and a wider reach. The digital space functions as a tool that enables organised crime, scales up its volume, or disguises it. Some digital tools, such as dedicated encrypted communication platforms, are designed by criminals for other criminals, while other criminal networks abuse over-the-top communication applications as a shield against law enforcement.

Accelerated by AI and other new technologies: AI and other new technologies such as blockchain or quantum computing will accelerate serious and organised crime in line with their rapid development. They are a catalyst for crime, and drive criminal operations' efficiency by amplifying their speed, reach, and sophistication.





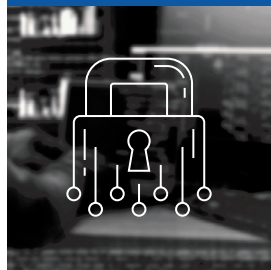
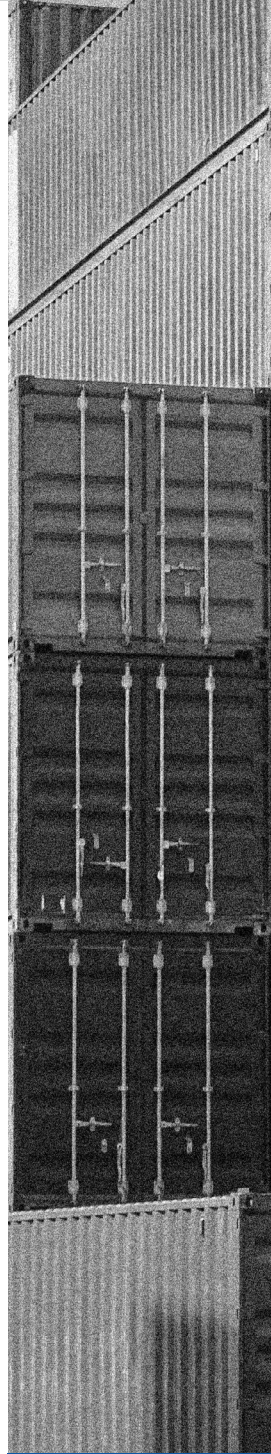
IDENTIFYING KEY THREATS

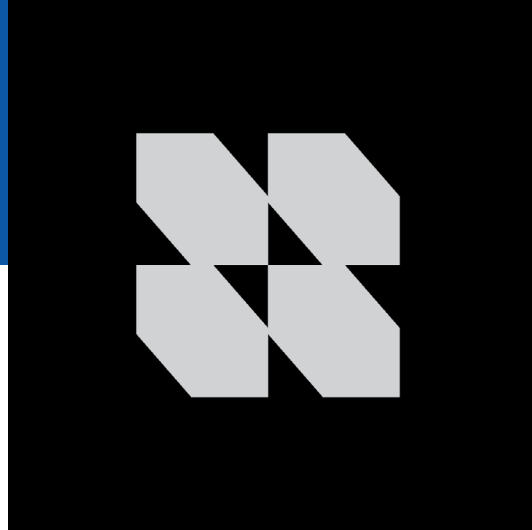
The key threats to the EU's internal security are infused with this changing DNA in varying ways. They stand out because of the threat they pose and the impact they have on the EU and its Member States today, and the way they are expected to evolve tomorrow.

The key threats include crime areas which predominantly take place in the digital and online realm, but also more traditional crime areas entailing physical trafficking and illicit cross-border activity. With their point of gravity mostly in the physical world, parts of these criminal activities' processes are shifting more to the online domain, particularly when it comes to recruitment, communication, marketing or retail activities. Relevant use cases of AI are also on the horizon.

The key threats identified on the basis of the EU-SOCTA methodology include the following seven crime areas: cyber-attacks, online fraud schemes, (online) child sexual exploitation, migrant smuggling, drug trafficking, firearms trafficking, and waste crime.

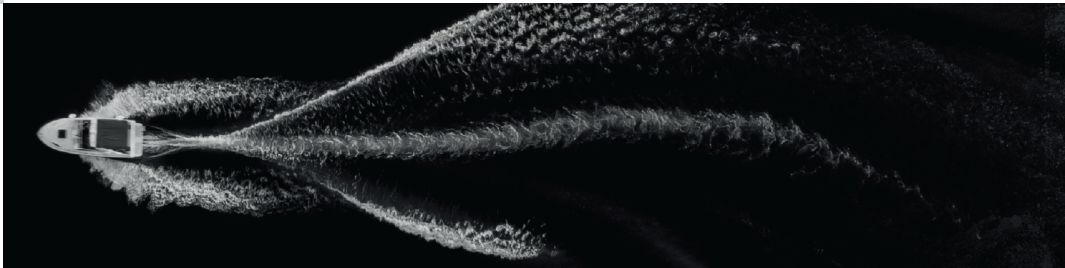
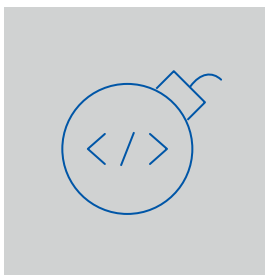
- ↳ **Cyber-attacks** targeting critical infrastructure, governments, businesses, and citizens are further proliferating. They exploit digital infrastructure vulnerabilities, leverage data for system access and target data for profit. These attacks showcase a combination of motives of profit and destabilisation, as they are increasingly state-aligned and ideologically motivated. Progress in AI will further refine cyber-attacks' modi operandi and target identification.
- ↳ An **online fraud** epidemic affects EU citizens, businesses, and public institutions alike. The scale, variety, sophistication and reach of online fraud schemes is unprecedented. Accelerated by AI aiding social engineering and access to data, it is expected to outpace other types of serious and organised crime.
- ↳ **(Online) child sexual exploitation** is transforming, with generative AI used to produce child sexual abuse material, highly secured online communities of offenders, and to facilitate the expanding online grooming of children.





- ↳ In **migrant smuggling**, criminal networks smuggle irregular migrants to, via or out of the EU, charging disproportionate fees. Hybrid threat actors instrumentalising migration flows create additional opportunities for migrant smuggling criminal networks. These networks are known to adapt flexibly in their methods and routes and have a total disregard for human dignity. Migrant smuggling networks increasingly rely on online platforms for marketing, recruitment and money transfers.
- ↳ **Drug trafficking** is a dynamic crime threat with high destabilising potential for the EU as a society, given its association with violence, corruption, infiltration in the legal economy, and worldwide interconnections. It is highly lucrative yet competitive. The trafficking of cocaine and synthetic is particularly dynamic, with often shifting routes, new modi operandi and product varieties, and a potential displacement of violence across the EU.
- ↳ **Firearms trafficking** is shaped by a complex supply and demand interplay, and contributes to the regional expansion of drug-related violence. Sources of illicit firearms shift and further expand under the influence of developments in technology, AI, and the online sphere. The availability of weapons in (post) crisis and war zones in countries in the EU neighbourhood and beyond also contributes to this expansion.
- ↳ The **illicit trafficking of waste** is a financially driven crime that intersects closely with the legitimate waste sector, and that employs experts from the sector. It has a detrimental impact on the natural environment, on the economy, and on the health and safety of EU citizens.

Other crime areas such as; trafficking in human beings, wildlife crime, organised property crime, intellectual property crime, currency counterfeiting, fraud schemes against the financial interest of the EU and Member States, and sanctions evasion, remain persistent.



CONFRONTING CRIMINAL NETWORKS' CROSS-CUTTING TACTICS

The identified key threats have a number of elements in common, which sustain and boost them in varying ways. Law enforcement must also integrate these cross-cutting elements when designing approaches to fight key criminal threats.

The DNA of serious and organised crime is strongly embedded in criminal networks' ways of working. Criminal networks find opportunities to operate as proxies for hybrid threat actors in the online realm, and turn AI and technology into tools for their criminal use. In addition, criminal networks integrate a range of beneficial tactics in their operations.

The nature of **money laundering and criminal finances** continues to evolve. Criminal networks increasingly invest illicit proceeds into a parallel financial system designed to protect and grow their wealth acquired from illegal activities. It is shielded by a digital cloak of online platforms and emerging technologies such as blockchain, resulting in a new era of money laundering.

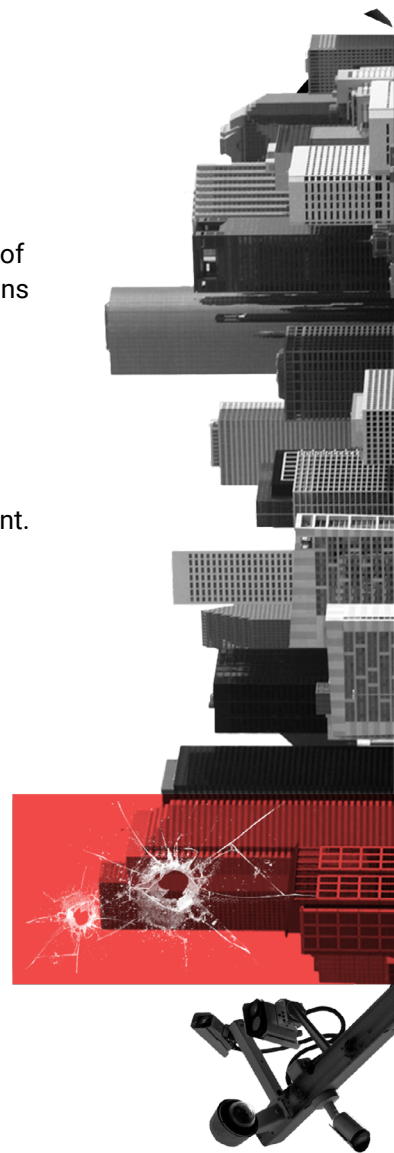
The **infiltration of legal business structures** allows organised crime to grow in power and influence. It supports, disguises, or facilitates any criminal activity and the laundering of its proceeds. Legal businesses in various sectors are misused throughout the criminal process, and insider threats in particular are of concern.

Corruption is among the strongest undermining powers, as it is a crime that facilitates all other types of organised crime. It has adapted to the digital environment, with more targeting of individuals with access to digital systems.

Organised crime-related violence is intensifying in several Member States and spills over into society. This violence moves and intensifies with criminal markets that are prone to competition and conflict. It is catalysed by online and encrypted communication solutions that support borderless recruitment, communication, extortion, and coordination.

The **criminal exploitation of young perpetrators** not only damages the fabric of society, but also shields the higher echelons in criminal networks from identification.

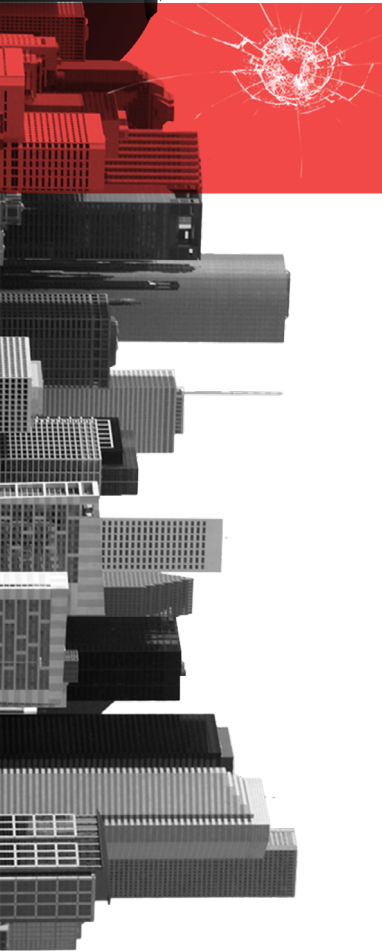
These tactics contribute to criminal networks' ability to develop and grow their criminal businesses across borders, increase their profits, and augment their resilience, creating a cycle of reinforcement.





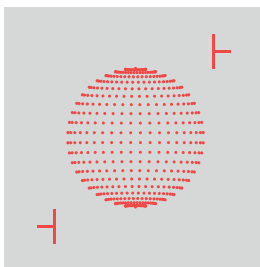
THE GEOGRAPHY OF CRIMINAL NETWORKS

Criminal networks and their activities are unhindered by borders, be it within the EU or between the EU and the rest of the world. For this reason, it is also of utmost importance to monitor major developments, particularly in the EU neighbourhood but beyond it as well, as these may present pressing implications for criminal networks' operations and for the internal security of the EU. As the Russian war of aggression against Ukraine resulted in some changes, a future post-war situation may in turn also cause relevant shifts in the EU criminal landscape.



INTELLIGENCE-LED PRIORITY SETTING FOR THE FIGHT AGAINST SERIOUS AND ORGANISED CRIME

Further changes to the DNA of serious and organised crime – its tools, tactics, and structures – will continue to shape the criminal landscape. These transformations, driven by broader societal developments, will present new opportunities and challenges for both criminal networks and law enforcement alike. The EU-SOCTA serves as a vital tool in identifying these key threats, enabling the EU to take a proactive and targeted approach to combatting serious and organised crime. By understanding the shifting blueprint of crime, law enforcement can anticipate future threats, refine their strategies, and stay ahead in the ongoing fight against serious and organised crime.





**THE CHANGING DNA OF SERIOUS AND ORGANISED CRIME
- EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT
ASSESSMENT, 2025 - EXECUTIVE SUMMARY**

PDF | ISBN 978-92-9414-008-1 | DOI-10.2813/8524220 | QL-01-25-008-EN-N

© European Union Agency for Law Enforcement Cooperation, 2025

This executive summary has been translated for convenience purposes.
Please note that the English version serves as the official reference.

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.

Cite this publication: Europol, *The changing DNA of serious and organised crime -
European Union Serious and Organised Crime Threat Assessment 2025,*
- Executive summary, Publications Office of the European Union,
Luxembourg, 2025.

The full report can be accessed on the Europol website:

www.europol.europa.eu

Europol is the EU's law enforcement agency, supporting the 27 EU Member States in their fight against serious international crime and terrorism. Europol also works closely with non-EU partner countries, other EU agencies and international organisations, strengthening global security through intelligence-sharing and operational cooperation. Europol is at the heart of the European security architecture and offers a unique range of services. It acts as an expert centre for law enforcement operations, a hub for information on criminal activities, and a centre of law enforcement expertise. Analysis is at the core of Europol's activities, with the agency producing regular assessments that offer comprehensive, forward-looking insights into serious and organised crime and terrorism in the EU.

The European Union Serious and Organised Crime Threat Assessment (EU-SOCTA) is the most detailed and forward-looking study of its kind and a product of systematic and comprehensive analysis of law enforcement information on serious and organised crime affecting the EU. The EU-SOCTA is designed to assist decision-makers in the prioritisation of serious and organised crime threats for the upcoming years. It has been produced by Europol, drawing on data from investigations Europol is supporting and extensive contributions from all partners.



Your feedback matters.

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

Your input will help us further improve our products.

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