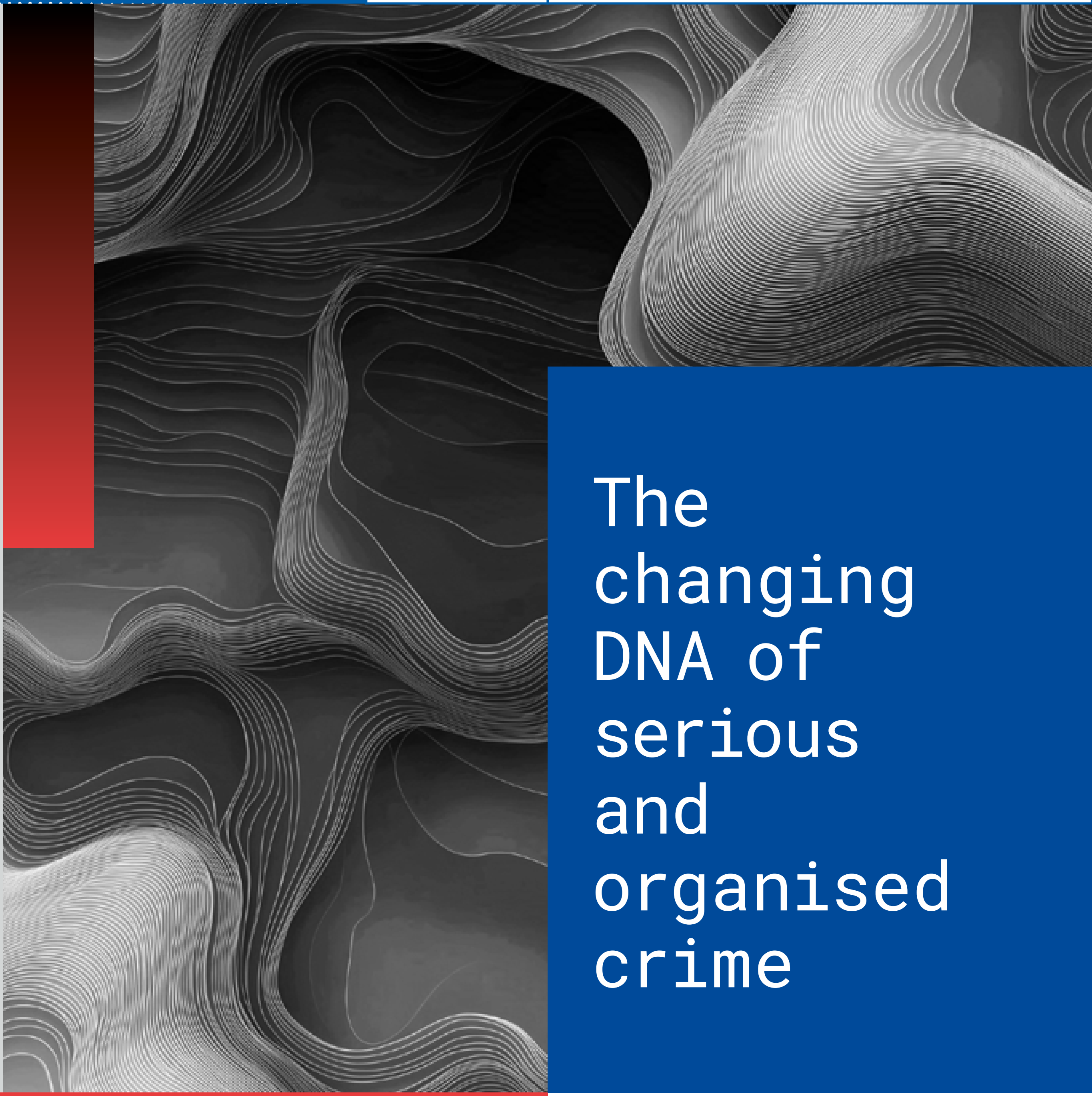


The changing DNA of serious and organised crime

2025

EUROPEAN UNION
SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT
THE CHANGING DNA OF SERIOUS AND ORGANISED CRIME

PDF Web | ISBN 978-92-9414-000-5 | DOI: 10.2813/0758057 | QL-01-25-005-EN-N

PDF/X | ISBN 978-92-95236-99-8 | DOI: 10.2813/5473714 | QL-01-25-005-EN-C

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, 2025

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.

The European Union Law Enforcement Cooperation does not own the copyright in relation to the following elements:
Page 7 © Nicolas Peeters

Europol would like to express its gratitude to EU Member States, Europol partner countries, EU agencies and institutions, international organisations, the members of the private sector of the Europol Advisory Groups, and the Academic Advisory Group for their valuable contributions and input.

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

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

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.

Contents

Foreword

Serious and organised crime is one of the greatest security threats facing the European Union today. It is a powerful, corrosive force that is evolving at an unprecedented pace, exploiting new technologies, digital platforms, and geopolitical instability to expand its reach and deepen its impact. The very DNA of organised crime is changing rapidly, adapting to a world in flux. The 2025 EU Serious and Organised Crime Threat Assessment (EU-SOCTA) provides the most comprehensive, intelligence-driven analysis of these threats to date, serving as both a stark warning and a call to action.

Crime has a twofold destabilising effect on our society. The findings of the EU-SOCTA 2025 make clear that serious and organised crime undermines the very foundations of political, economic and social cohesion and stability through illicit proceeds, the perpetuation of violence and the extension of corruption. Criminal networks are increasingly intertwined with hybrid threats originating externally, encompassing a wide range of criminal activities and tactics, often executed through criminal proxies. While the financial gains remain the primary motivation for these networks, their actions also serve – directly or indirectly – the geopolitical interests of those orchestrating hybrid threats.

Serious and organised crime is increasingly nurtured online. The online domain has become an essential, omnipresent aspect of daily life, and its role in facilitating organised crime will continue to grow. It serves as a powerful tool for enabling, amplifying and concealing various forms of criminal activity, while also becoming a prime target for criminal infiltration and data theft. Meanwhile, the online space is increasingly becoming the main ecosystem for committing certain crimes, with minimal involvement in the offline world, thus transforming the digital environment into the primary theatre for criminal operations.

Emerging technologies, such as artificial intelligence, accelerate crime and provide criminal networks with entirely new capabilities. These innovations expand the speed, scale, and sophistication of organised crime, creating an even more complex and rapidly evolving threat landscape for law enforcement.

Alongside the previous EU-SOCTA reports of 2013, 2017 and 2021, this edition continues to build on the EU-wide collaborative, intelligence-led response to combating serious and organised crime. However, the EU-SOCTA 2025 constitutes the most comprehensive, forward-looking analysis to date. It is based on intelligence gathered from thousands of law enforcement investigations supported by Europol each year, enriched by the strategic insights from law enforcement experts, other EU agencies and international organisations, the private-sector, Europol's expert groups, and reflections from our Academic Advisory Group.

Our response to these challenges must be equally dynamic. The growing intersection of cutting-edge technology and organised crime demands a proactive response to effectively address the evolving threats posed by these advancements. Europol plays a central role in providing national law enforcement agencies and partners with critical intelligence on current and emerging threats, enabling stakeholders to better anticipate and prepare for future challenges. The EU-SOCTA directly informs the multi-annual cycle of the European Multidisciplinary Platform Against Criminal Threats (EMPACT), ensuring that national law enforcement agencies, EU institutions and key partners are aligned in the fight against organised crime.

Tackling serious and organised crime also means prioritising victim protection. Intelligence-led operations are critical, but law enforcement must remain committed to supporting victims—amplifying their voices and addressing their needs. This focus not only alleviates the immediate harm inflicted on individuals, but also plays a crucial role in dismantling criminal networks in the long term. By addressing crime at its roots, we empower victims to break free from cycles of exploitation. Ultimately, securing justice for victims strengthens the trust between police and the communities we serve, helping to build a more resilient and cohesive society.

At this pivotal moment in time, complacency is not an option. The threats we face demand continuous innovation, deeper cooperation and an unrelenting commitment to safeguarding our societies. Since the last EU-SOCTA report in 2021, Europol's support to Member States' law enforcement agencies has evolved towards a more targeted, effective operational focus, consolidating a more integrated EU police cooperation model. Today, the Agency is involved in the most complex and ambitious criminal investigations that are undertaken at European level, prioritising actions against High Value Targets in the framework of Operational Task Forces. As we look towards the next five years, we rise to the challenge of taking Europol a step further to the new level of ambition reflected in the Political Guidelines issued by the Commission in July 2024. Our aim is to provide an even more comprehensive response to internal security threats, to reinforce Europol's role as a centre of excellence and knowledge, to boost dedicated operational teams in those crime areas of most concern to the EU Member States, and to continue to develop our capacity for innovation for law enforcement purposes.

The insights provided by the EU-SOCTA 2025 will shape strategic decision-making, operational priorities, and legislative developments to strengthen the EU resilience against serious and organised crime. Addressing this evolving threat landscape demands continuous innovation, enhanced collaboration, and long-term engagement. Together, through intelligence-sharing, strategic and technological adaptation and decisive joint action, we can turn the tide against serious and organised crime.

Catherine De Bolle
Executive Director of Europol

This year's edition of the EU-SOCTA comes at a pivotal moment for Europe. The geopolitical instability continues to shape a totally new global landscape. We are witnessing the emergence of a genuinely multi-polar world. To respond, the forthcoming new Internal Security Strategy will need to provide a significantly more integrated look at the challenges we are facing together and to provide a joint up view on how to address them.

Organised crime is exploiting this evolving landscape and proliferating exponentially. It benefits from advanced technologies, is active across multiple jurisdictions, and has strong connections beyond EU borders.

It has also ingrained itself in our societies, economies, and unfortunately even in the daily lives of people in the EU. It is evident in the frequent shootings and explosions occurring in major European cities and the drug trade that has spread to far too many street corners.

Security has consequently become a real concern. People in the EU want to move around without fear, whether on the streets, in public places, at events, in metro stations, or on the internet. When asked about the future, a majority of EU citizens in 2024 was concerned about the security of the European Union. The same is true for businesses: mis- and disinformation, crime and illicit activity and cyber espionage are all among the top ten risks they identified in the World Economic Forum Global Risks Report 2025.

To maintain a secure and prosperous EU in a volatile world, and to reassure people and businesses, we must strengthen our common response. Both in our internal policies and external affairs, we must become a Union of shared vision and joint action. We must build an EU that plays a strong and active role in the world.

Internally, we must reinforce cooperation between law enforcement authorities in all relevant areas. In this, the role of Europol can hardly be overstated. It is the nerve center of the EU's internal security architecture, and we will strengthen it to ensure an even stronger response. We will enhance access to data for law enforcement for efficient prevention and successful investigations and convictions.

Externally, we will continue to cooperate with our international partners to limit the influence organised crime, or other hostile actors, have on our internal security. We will expand our network of bilateral international agreements to allow Europol to engage in enhanced cooperation with law enforcement from partner countries across the world.

Above all, we will tackle organised crime in the measured, methodical way that defines not only good policymaking, but also effective law enforcement. Operational cooperation between national authorities, the EU agencies and key third partners based on joint priorities and operational action under EMPACT (European Multidisciplinary Platform Against Criminal Threats) is a key achievement. The process starts with a good understanding of the lay of the land - through a thorough analysis of the relevant threats based on information from the Member States and numerous other partners. In other words, it all starts with the EU-SOCTA.

Magnus Brunner
European Commissioner for
Internal Affairs and Migration

Poland took over the presidency of the Council of the European Union at a time of uncertainty and concern. We are witnessing increasing geopolitical tensions, the erosion of the rules-based international order and attacks targeting European democracy and security. Our motto "Security Europe!" is more accurate than ever.

Responsibility for the future is the key. Therefore, it is absolutely crucial to have reliable tools which will help us to provide Europeans with a sense of security and prospects for development.

The new EU Serious and Organised Crime Threat Assessment (EU-SOCTA) is one of the instruments which help the European Union to protect itself and its citizens and to take care of its immediate neighbourhood. EU-SOCTA is a pivotal instrument for understanding and responding to the evolving landscape of serious and organised crime in Europe. SOCTA provides us a detailed, intelligence-sourced assessment of criminal threats, empowering us to prioritise actions and allocate resources effectively in the fight against these complex and ever-changing challenges. As these threats continue to evolve, so too must our strategies and responses. These responses are essential in our ongoing efforts to safeguard the security and well-being of our citizens.

The threat posed by serious and organised crime remains one of the most significant challenges facing our countries today. Criminal groups are growing increasingly sophisticated. They are exploiting technology and global networks, infiltrating legal structures, and recruiting minors to engage in a wide range of illicit activities—from drug trafficking and production to cybercrime, migrant smuggling, trafficking in human beings and all kinds of financial frauds.

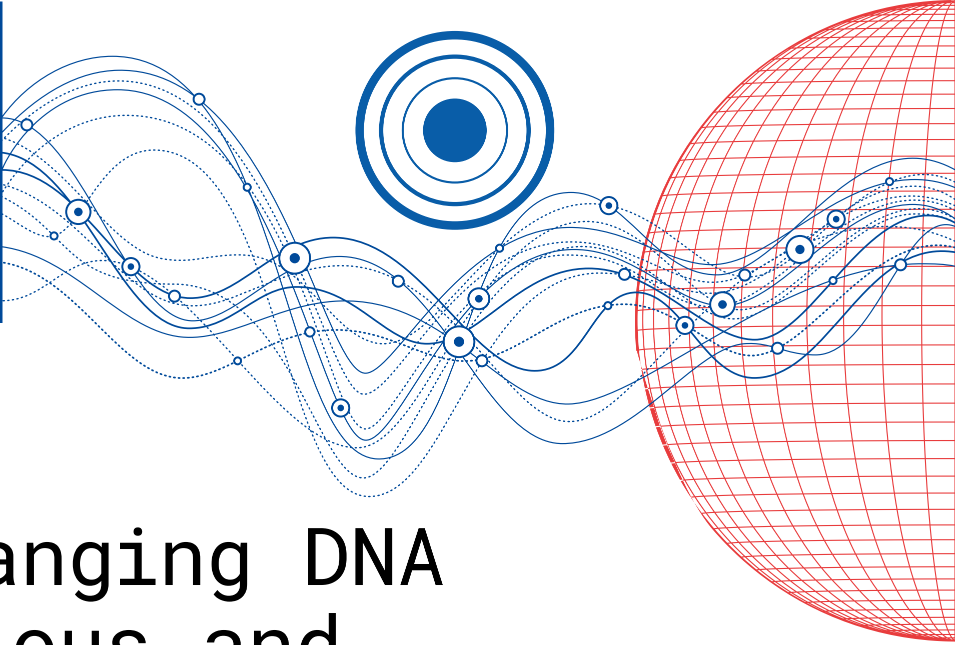
The ongoing armed conflict in Ukraine is a source of ever new threats to our internal security. Aware of this fact, we must identify and monitor these threats on an ongoing basis, reacting quickly and adequately. We must also be ready for new challenges after the end of this war, such as an increase in the smuggling of weapons and ammunition from Ukraine. To effectively counter these threats, we must continuously enhance our resilience and capabilities. Efficient international cooperation, the rapid exchange of information and a detailed intelligence picture are the key factors here.

As we look to the future, it is imperative that we remain vigilant and adaptable to cooperate and coordinate our efforts. We must continue to reinforce our collective work to combat serious and organised crime at local, national, and European level. This is a responsibility shared by the EU, national governments, national law enforcement agencies and Europol. However, to meet these challenges effectively, we must also ensure that we allocate sufficient resources to support these vital efforts and strengthen our capacity to act decisively and swiftly.

It is our duty to keep investing in the fight against serious and organised crime, strengthening cooperation, and staying one step ahead in order to ensure a safer and more secure Europe. Therefore, we must strive to make optimal use of existing and proven tools in the field of operations, such as EMPACT, by taking appropriate steps to optimally adapt these tools to the current challenges and geopolitical conditions. That is why it is so important today, in the face of unprecedented challenges and threats in the area of internal security, to have an appropriately focused debate on a political level about the right direction for the further development of Europol.

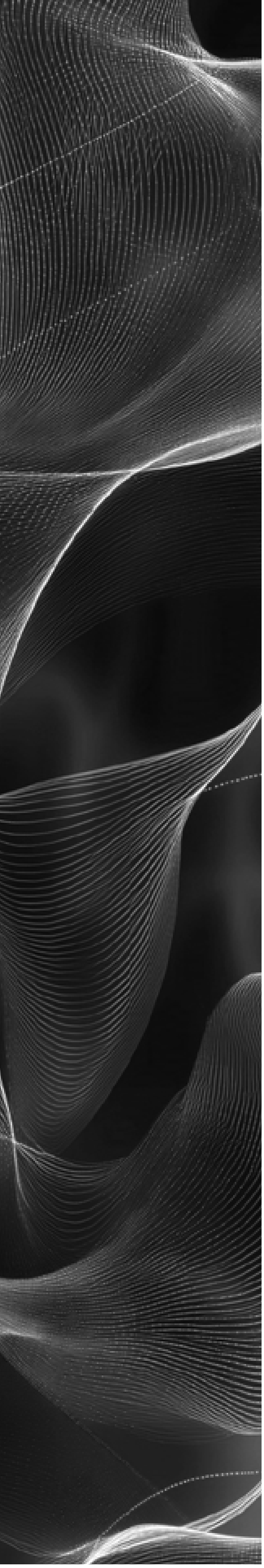
Tomasz Siemoniak
Minister of the Interior
and Administration of
the Republic of Poland

1



The changing DNA of serious and organised crime

The DNA of serious and organised crime in the EU is changing against the backdrop of today's - and tomorrow's - multi-faceted and rapid transformations in our world. Just as DNA serves as the blueprint for life, we are seeing a fundamental shift in the 'blueprint' of crime – the underlying tools, tactics, and structures employed by criminal networks. In the same way that DNA is composed of four basic building blocks that combine in countless ways to create genetic instructions, the changing blueprint of crime is defined by three interconnected dynamics that are increasing the threat of criminal activities to varying degrees: crime is progressively **Destabilising society**, increasingly **Nurtured online**, and strongly **Accelerated by AI and other new technologies**.



↘ **Serious and organised crime has a double destabilising effect on the EU and its Member States.** It undermines and reduces trust in the EU's economy, rule of law, and society as a whole by generating illicit proceeds, spreading violence, and normalising corruption. It is also progressively driven by hybrid threats, directed externally, that encompass a broad range of criminal activities and tactics operated via criminal proxies. While criminal networks are in it for the financial profits, their activities contribute to the political goals of the hybrid threat actor they support.

↘ **The online domain is an omnipresent facet of everyday life, and will gain an even more crucial prominence in nurturing organised crime.** It functions as a tool to enable, scale up or disguise any form of criminal activity, and is a target for criminal infiltration and data theft. Even more so, it is increasingly becoming the theatre where certain crimes are committed from start to finish with very limited presence in the offline world.

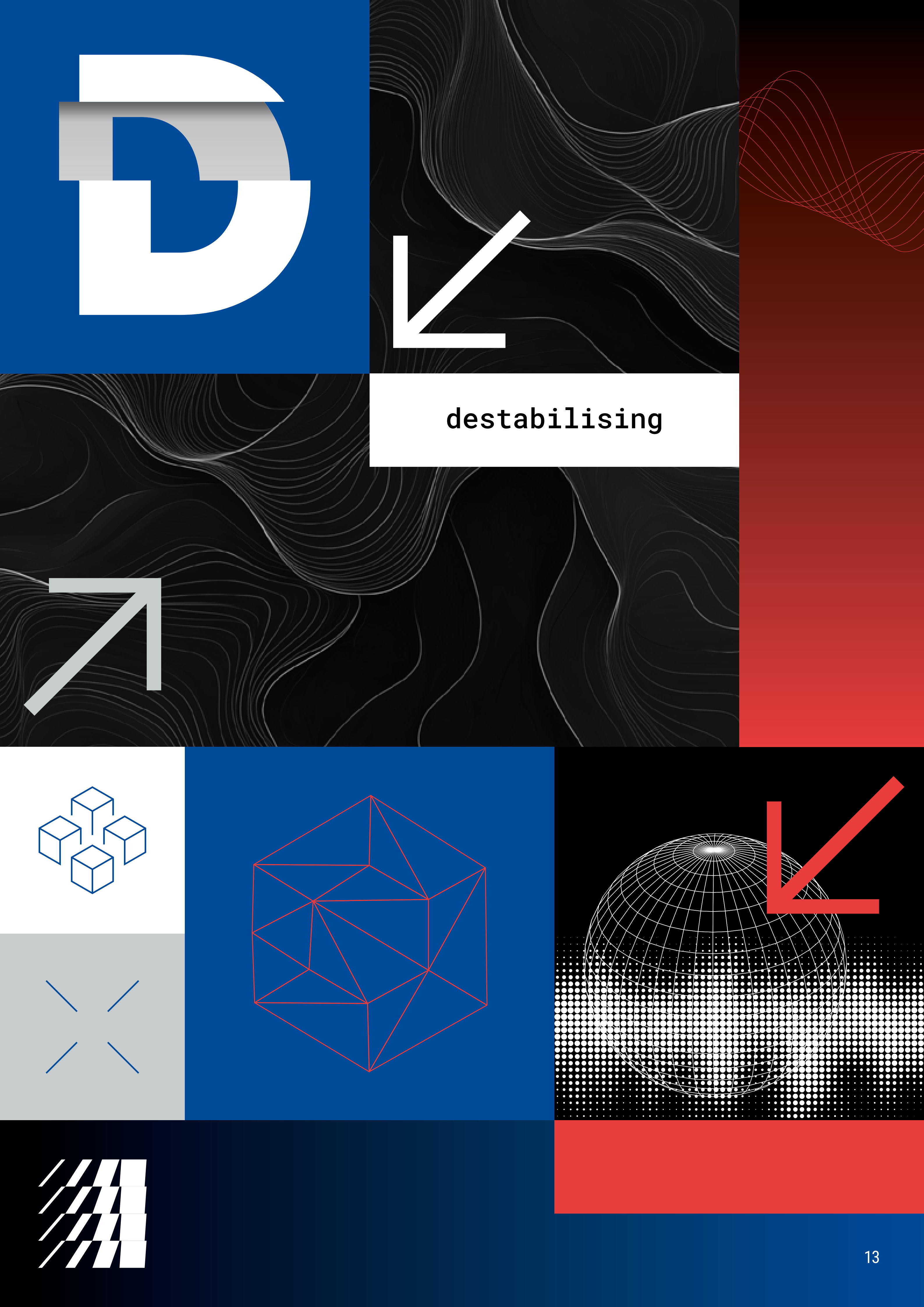
↘ **Artificial intelligence and other new technologies such as blockchain or quantum computing will accelerate serious and organised crime in line with their rapid development.** They are a catalyst for crime, and drive criminal operations' efficiency by amplifying their speed, reach, and sophistication.

Serious and organised crime is in the grip of a profound transformation. Geopolitical tensions have created a window for hybrid threat actors to exploit criminal networks as tools of interference, while rapid technological advancements – especially in artificial intelligence (AI) – are reshaping how crime is organised, executed, and concealed. These shifts are making organised crime more dangerous, posing an unprecedented challenge to security across the EU and its Member States.

Serious and organised crime is Destabilising society

Serious and organised crime is not just a threat to public safety; it impacts the very foundations of the EU and its society. Criminal networks fuel their operations through corruption and money laundering, creating a hidden financial system that weakens economies and erodes trust in governance structures. But the threat does not stop there: increasingly, criminal networks serve as proxies for hybrid threat actors, exploiting vulnerabilities to destabilise the EU and its Member States from within.

The destabilising properties and effects of serious and organised crime have a double dimension. It is destabilising because it is significantly undermining our economy and society. Furthermore, it is destabilising because it is increasingly directed externally.


destabilising

Destabilisation through economic and social undermining

At its core, serious and organised crime is a profit-driven activity. Criminal networks operate like businesses, creating an intricate web of parallel economies that entire communities rely on for income, goods or services. This dependence fosters a sense of normalcy around illicit activities and erodes the willingness to report crimes or cooperate with authorities, making it challenging to disrupt cycles of crime.

Criminal networks seek to weaken governance to enable and expand their illegal activities. In doing so, they use corruption as a key tactic to enable or conceal all types of criminal activity, to secure illicit proceeds or even to obstruct law enforcement activity. While grounded in well-known mechanisms, corruption is adapting to digitalisation as it increasingly serves to access systems, and to the crime-as-a-service model with the emergence of corruption brokers.

> *The profit-driven nature of serious and organised crime destabilises our economy and reduces trust in our institutions, as high amounts of illicit proceeds are laundered and/or re-invested to reinforce criminal networks' illicit business.*

The profit-driven nature of criminal networks is similarly reflected in its proficiency in money laundering - an indispensable part of the criminal process. Criminal networks rely on laundering profits to fund and grow their operations, bridging the gap between the licit and illicit worlds. It undermines our society – not only by infiltrating the legal economy, but also because it allows criminal networks to grow more resilient. The most lucrative criminal markets generate billions of illicit proceeds on an annual basis. They virtually all depend on money laundering to conceal the sources of illegally obtained funds, so that they can re-invest them and further expand their illicit undertakings. This opaque financial ecosystem undermines trust in institutions, destabilises economies and societies, and poses a grave threat to the internal security of the European Union.

The scale and profit potential of some crime areas particularly stand out, and therefore also their undermining effect. High demand for illicit drugs generates immense criminal profits that are laundered and reinvested in various sectors, increasing criminal networks' hold in the legal world. The reach of various online frauds is exponentialising, exposing all EU citizens and businesses repeatedly to financial risks while strengthening criminal networks. The trade in illegal firearms and explosives fuels violent crime, instilling fear in society and exploiting young perpetrators in committing violence for a fee.

Cutting off criminal networks' resources is an effective strategy for law enforcement, but recovering assets remains a challenge. Despite substantial investments in resources and legislative frameworks, the confiscation of criminal proceeds has stagnated at around an estimated 2 % of illicit proceeds. Challenges in asset recovery are further exacerbated by the increasing criminal exploitation of digital assets.

The additional factor: Increasing destabilisation through collaboration between criminal networks and hybrid threat actors

The risk of destabilisation becomes exponential if criminal networks also become proxies for hybrid threat actors. Among the many forms of serious and organised crime, for some there is reason to believe that they are intended to destabilise the functioning of the EU and its Member States. This intent to destabilise may focus on democratic processes, social coherence within societies, the sense of security or the rule of law. In some cases, it may also affect the financial stability and prosperity of the economy.

Hybrid threats encompass a range of criminal activities and tactics, such as sabotage of critical infrastructure through digital or physical means, information theft, disinformation campaigns, cyber-attacks, migrant smuggling, certain types of drugs trafficking and other forms of crime. Such threats are increasingly potent in today's volatile geopolitical landscape, where multiple crises – ranging from the aftermath of the COVID-19 pandemic to the Russian war of aggression against Ukraine and the ongoing conflicts in the Middle East, but also economic and political tensions (China, Iran, North Korea) – are deepening instability and vulnerability. These tensions provide opportunities for hybrid threat actors to exploit divisions, spread disinformation, and manipulate public perception.

Shadow alliances: Why do hybrid threat actors co-operate with criminal networks?

Hybrid threat actors cooperate with criminal actors for mutual benefit, leveraging each other's resources, expertise, and protection to achieve their objectives. Financial gain is one of the primary motivations for criminals cooperating with hybrid threat actors, but the relationship is more complex and extends beyond just financial profit.

Some states provide safe havens for criminals in exchange for their services, allowing them to operate freely without fear of prosecution. It also allows these states to deny direct involvement by outsourcing certain crimes such as cyber-attacks, disinformation campaigns or even money laundering to criminal networks, making attribution difficult. The outsourcing to multiple networks or actors might also be cost effective for state actors as criminal networks already have infrastructure in place and often have a global reach.

For criminals, cooperation with hybrid threat actors might give them access to cutting-edge tools that criminal networks can use later.

> *Hybrid threat actors and criminal actors cooperate for mutual benefit, leveraging each other's resources, expertise, and protection to achieve their objectives.*

Activities of criminal networks for hybrid threat actors

Hybrid threats manifest in a number of crime areas that are already highly threatening today, and are expected to further amplify. Criminal actors in cyber-attacks were early adopters of the crime-as-a-service business model. Cyber-attacks are now carried out against payment in service of external threat actors, being increasingly state-aligned and ideologically motivated.

Criminal networks play a pivotal role in advancing the objectives of hybrid threat actors by leveraging their expertise in cybercrime. One of the most significant ways they contribute is through ransomware attacks on critical infrastructure, businesses, and government agencies. These attacks not only generate financial revenue—often through cryptocurrency payments—but also serve to disrupt and weaken opponents by immobilising essential services, creating chaos, and undermining public trust in institutions.

Beyond ransomware, criminal networks can steal data on behalf of hybrid threat actors. By infiltrating secure systems, they might steal data of strategic importance for governance or business and provide hybrid threat actors with invaluable information that can be used for espionage, economic advantage, or even coercion. By cooperating with criminal networks, hybrid threat actors can obscure their direct involvement, as the attacks appear to be carried out by criminal networks rather than hybrid threat actors.

Additionally, these networks are instrumental for propaganda campaigns aimed at spreading disinformation and influencing political systems. These campaigns often involve fake social media accounts, coordinated troll operations, and manipulated news content, which serve the strategic interests of hybrid threat actors by weakening opponents from within.

The instrumentalisation of irregular migrant flows by hybrid threat actors serve the interests of migrant smuggling criminal networks, who see demand for their services and their profits spike. Also statements of certain state actors to flood the EU and its Member States with illicit drugs serves criminal networks producing drugs and might create social instability.

The evasion of sanctions not only contributes to economic destabilisation; it also indirectly fuels hybrid threats by strengthening sanctioned economies and foreign powers.

Criminal networks may also play a role in providing weapons to proxy military groups. By leveraging weapons trafficking from criminal networks, hybrid threat actors can circumvent legal restrictions and maintain also here deniability while ensuring that weapons reach their intended recipients.

The woodpecker modus operandi

Incidents are often originally assessed as single incidents, such as sabotage of critical infrastructure (water or energy supply, for example), arson, intimidation, kidnappings. However, there is the possibility that they are also executed by criminal networks on behalf of hybrid threat actors. Such incidents may be part of a larger strategic objective of destabilisation, involving persistent, targeted, and cumulative disruptions rather than a single, overwhelming attack.

> *Much like a woodpecker weakens a tree over time through repeated strikes, hybrid threat actors engage in ongoing, seemingly minor actions that collectively erode stability, security, and trust in institutions.*

The evolution of online tools has drastically amplified the reach of hybrid threats and their impact on our society. Hybrid threat actors now have enhanced capabilities to recruit supporters to commit criminal acts, in particular via online and closed platforms.

The blurring of lines between state and non-state actors has created a complex and evolving threat landscape. Hybrid threat actors exploit criminal networks for deniability and political or economic gain, while criminals benefit from protection, advanced tools and financial gain.

Serious and organised crime is Nurtured online

In our interconnected world, the online domain is an indispensable facet of everyday life. However, this dependency extends beyond legitimate use, permeating the realms of serious and organised crime. Today, nearly all forms of serious and organised crime have a digital footprint. From cyber fraud and ransomware attacks to drug trafficking and money laundering, the internet is no longer just a platform – it is the pillar of a criminal enterprise.

Criminal networks are increasingly abusing digital infrastructure to carry out their activities with increased efficiency and scope in multiple ways: as an enabler, as a countermeasure, and as a target.

nurtured online

Digital infrastructure as an enabling tool to drive criminal operations

The dark web, social media and e-commerce platforms allow criminal networks to operate with high degrees of efficiency, anonymity, and security, and to scale their activities with minimal physical contact. A broad range of criminal activities take place solely or predominantly in the online realm, as in the case of cyber-attacks, online fraud schemes, or the distribution of child sexual abuse material.

Also criminal businesses with their centre of gravity in the physical world and a focus on trafficking or production, increasingly benefit from shifts to the online world. They exploit available digital infrastructure for recruitment, marketing, trade and financial transactions. With a high degree of organisation, criminals advertise illicit goods and services, identify targets, use encrypted and coded messaging to communicate and recruit individuals – including minors – on these platforms. Criminal networks often work with technical specialists to carry out these activities.

> *Criminal networks exploit digital infrastructure to its fullest, leveraging technology and online systems to facilitate illegal activities, evade law enforcement, and maximise their profits.*

Victims of sexual exploitation are targeted online, their services advertised, managed and paid online, all remotely. Alongside the use of online mapping and booking applications to organise journeys, criminal networks promote migrant smuggling services on social media, and use successful crossings as advertisements. Criminal networks that traffic drugs benefit from digital infrastructure for communication, or for fraudulently obtaining relevant information (through intrusion of digital systems or corruption of their users) on shipments where their drugloads are concealed.

Digital infrastructure as a shield against law enforcement detection

Criminal networks increasingly exploit digital infrastructure to shield their activities from law enforcement. Encrypted communication technologies, originally designed to enhance privacy and cybersecurity, have become critical tools for criminal networks, enabling them to coordinate operations, evade detection, and expand their illicit enterprises. This misuse of digital tools manifests in two ways:

Criminals for criminals

Some criminal networks develop or rely on dedicated encrypted communication platforms designed for illicit activities. Platforms such as EncroChat, Sky ECC, Ghost and others provided a communication environment for serious and organised crime. Such systems are designed to provide an end-to-end encryption that prevents external interception. Additionally, bespoke security features, such as remote wiping and anonymity mechanisms, may hinder the timely retrieval of relevant digital information during investigations.

Abuse of mainstream (communication) tools

Criminals abuse end-to-end encrypted communication services, which are legally designed to protect users' privacy. These over-the-top communication applications provide legitimate encryption, large user bases that allow criminals to blend in with ordinary users. Unlike the first category, these platforms or tools are not built for criminals, making it necessary for law enforcement to engage with private companies, navigate legal frameworks to investigate and disrupt criminal networks operating within them.

Data as a target of criminal activity

Digital infrastructure and the data it holds is in itself a target of criminal activity. Criminal networks use ransomware, Distributed Denial of Service (DDoS) attacks, business email compromise fraud, and phishing, to infiltrate systems, steal data and extort payments. At the same time, Internet of Things (IoT) devices and contactless payment systems have increasingly become targets for criminals, while the rise of botnets and vulnerabilities in emerging technologies such as the metaverse is a sign of new challenges to come.

Data is the new currency of power; stolen, traded and exploited by criminal actors. But it is also a crucial tool for law enforcement to track illicit activities, identify perpetrators, and dismantle criminal networks.

Data has become a central commodity, and will be increasingly stolen, traded and exploited by criminal networks or hybrid threat actors. It is a commodity that is high in demand, as it opens doors to a myriad of criminal activities, including cyber-attacks, online frauds, online child sexual exploitation, extortion, and others. With data being such a sought-after and valuable commodity, its illicit trade is expected to take further prominence in crime-as-a-service business models. The sale of stolen sensitive information will be even more common on criminal marketplaces.

A critical aspect of this threat is that stolen data is not always used immediately or just once. In many cases, criminals exploit it within a few years, and multiple times over several years, with victims targeted repeatedly.

Serious and organised crime is Accelerated by AI and other new technologies

Criminal networks have demonstrated the ability to rapidly adapt to new technological solutions. This includes artificial intelligence (AI), a solution that has transformed the modern world with unprecedented speed and impact. Indeed, the very qualities that make AI revolutionary – accessibility, versatility, and sophistication – have made it an attractive tool for criminals.

accelerated by AI
A

AI and other new technologies are fundamentally reshaping the serious and organised crime landscape in two main ways: as a catalyst for crime, and as a driver for criminal efficiency.

AI and other new technologies as a catalyst for crime

As AI-driven systems (large language models (LLM), generative AI (GenAI)) become more advanced and user-friendly, criminal networks are increasingly leveraging their capabilities across a wide spectrum of crimes. GenAI models, for instance, have drastically reduced the barriers to entry for digital crimes. Criminals can now craft messages in multiple languages, target victims with precision on a global scale, create sophisticated malware, and even produce child sexual abuse material (CSAM).

By creating highly realistic synthetic media, criminals are able to deceive victims, impersonate individuals and discredit or blackmail targets. The addition of AI-powered voice cloning and live video deepfakes amplifies the threat, enabling new forms of fraud, extortion, and identity theft. These tools are easily accessible and do not require specific technical skills. The accessibility of AI tools has multiplied the volume of CSAM available online, creating challenges in the analysis of imagery and identification of offenders.

In the financial realm, the emergence of blockchain technology and cryptocurrencies has been leveraged to facilitate payments and launder proceeds, supported by decentralised systems and unregulated exchanges. The criminal exploitation of cryptocurrency as a payment method now has moved beyond the scope of cybercrime, and is encountered increasingly in more traditional crime areas such as drug trafficking or migrant smuggling. In addition, various modi operandi have emerged which aim to steal cryptocurrency, non-fungible tokens (NFT) or appropriate infrastructure and resources in order to mine cryptocurrency (cryptojacking).

AI and other new technologies as a driver for criminal efficiency

AI's automation capabilities are transforming the efficiency of criminal operations. From automating phishing campaigns to executing large-scale cyber-attacks, AI enables criminals to achieve more – reach more victims, be more targeted in their approach, and expand their global reach – with fewer resources. Cybercriminals leverage AI for attack automation, social engineering, and bypassing security measures, making cyber-attacks more scalable and efficient. Furthermore, the emergence of fully autonomous AI could pave the way for entirely AI-controlled criminal networks, marking a new era in organised crime.

As existing technologies continue to improve and key emerging technologies mature, criminal networks will have access to a broad range of increasingly powerful capabilities. Today's criminals have turned tools such as CCTV surveillance, chips, drones, GPS, and 3D printing to their advantage. With developments in quantum computing, the metaverse, 6G, unmanned systems, and brain-computer interfaces on the horizon, the high levels of anonymity, speed, and sophistication currently demonstrated by criminal networks will only likely increase over the coming years.

With the expectation that decryption technology or computational power — such as quantum computing — will advance sufficiently in the future to compromise current encryption methods, criminal networks (sometimes on behalf of hybrid threat actors) employ a strategic approach known as "store now, decrypt later". This tactic involves the collection and storage of encrypted data with the intent of decrypting it once more advanced computing capabilities become available. Such practices pose a considerable risk to sensitive information of governments, businesses and citizens, particularly as the development of quantum computing threatens to render existing encryption standards obsolete.

To counter the growing threat of AI-enabled crime, policymakers, law enforcement agencies and the technology sector must collaborate to develop robust safeguards, consistent regulations, and advanced detection tools. The rapid pace of AI and other innovation demands a proactive approach to ensure that its benefits are not overshadowed by its potential for harm.

2

Tactics of serious and organised crime

Criminal networks employ a range of tactics that facilitate their illicit enterprises across the criminal landscape. These tactics enable them to further develop their criminal business, increase their profits, and augment their resilience. Of growing relevance and concern are criminal finances and the proficiency to launder money, the widespread corruption, the regional peaks of organised crime-related violence, the criminal exploitation of young perpetrators, as well as the consistent intertwining with the legal business world. These cross-cutting catalysts contribute to the destabilising impact of organised crime, are nurtured in the online sphere, and will be further leveraged by technology and AI.

- Criminal networks have adopted the practice to move illicit proceeds to parallel financial systems designed to protect and grow their wealth stemming from their illegal activities. This goes together with the obfuscation of financial flows.

- The infiltration of legal business structures by criminal networks allows organised crime to grow in power and influence, creating a self-sustaining cycle that threatens the foundation of society. Legal businesses in various sectors are misused throughout the criminal process, from committing and concealing crimes to laundering profits.

- Corruption is instrumental for organised crime, and among the strongest undermining powers for the rule of law and citizens' trust in democratic institutions. Corruption has adapted to the broader trends toward digitalisation and a crime-as-a-service model, with several threats becoming increasingly visible: targeting of individuals with access to digital systems in public and private entities, the use of digital recruitment tactics, and the elevated role of corruption brokers.

- Organised crime-related violence is intensifying in several Member States, spilling over into public spaces, harming citizens and instilling fear in society. Violence both enables criminal networks' activities, and results from them. It involves professional actors operating without borders under a violence-as-a-service model.

- The criminal exploitation of young perpetrators has increasingly become a tactic used by criminal networks to avoid detection, capture, prosecution, and punishment. Recruitment methods evolve, including tailored language and online channels fitting with youth culture. As these young recruits often lack knowledge of the broader criminal network and have reduced legal exposure, they serve as low-risk assets for criminal networks.

Criminal finances and money laundering

As the criminal landscape continues to evolve, so does the intricate nature of money laundering and criminal finances. Criminal networks increasingly invest in creating a parallel financial system tailored to expanding their illicit operations and accumulating wealth generated from illegal activities. This threat is escalating as parallel financial systems are increasingly facilitated by digital platforms and enhanced by emerging technologies.

Money laundering plays a crucial role in enabling criminals to profit from illegal activities; it is the backbone of organised crime. It allows criminals to convert criminal money into seemingly legal assets, ensuring a continuous flow of funds to finance further criminal operations, expand their influence or to add to their personal wealth.

Traditionally, the process was often conceptualised in three primary stages. The first stage, placement, involves introducing illicit funds into the legitimate financial system. The second stage, layering, consists of multiple transactions designed to obscure the origin of the funds through a series of transfers, conversions, or purchases. Finally, in the integration stage, the laundered funds are reintroduced into the formal economy, often through investments in real estate, luxury goods, or legitimate business ventures.

However, in practice, money laundering is far more sophisticated, with criminal networks employing a diverse array of methods to legitimise their illicit profits. The complexity of the threat increases as it is also increasingly nurtured online and enabled by new technologies. Additionally, modi operandi often involve multiple transactions across various non-EU jurisdictions, exploiting regulatory disparities and creating a labyrinthine trail that challenges financial investigations.

From the simple use of cash intensive businesses to complex layering techniques via shell companies, from informal value transfer systems to the exploitation of cryptocurrencies, all these techniques serve as crucial components of a parallel financial criminal underworld. This ecosystem enables the movement of criminal money while remaining increasingly undetectable.

Money laundering is the backbone of organised crime. It allows criminals to legitimise the proceeds of their illegal activities and integrate illicit funds into our legitimate economy.

Emerging technologies as a digital cloak: a new era of money laundering

Cash still features prominently in money laundering schemes today. Criminals often use cash-intensive businesses—such as restaurants, hotels, car washes—to mix illicit funds with the businesses' legitimate income. When illicit proceeds are moved physically across borders, cash is often transported via cash couriers. Increasingly, young and vulnerable people are recruited, often via social media and gaming platforms, to act as money mules.

The increasing digitalisation of financial systems, coupled with emerging technologies, has significantly heightened the threat of money laundering. Cryptocurrencies, decentralised finance (DeFi) platforms, and AI-driven automation facilitate greater anonymity, enabling criminals to obscure illicit transactions more effectively and obfuscating the beneficial owners of illicit financial flows. Additionally, the proliferation of non-fungible tokens (NFTs) and dark web marketplaces further complicate the detection and regulation of illicit financial activities.

> *Virtual currencies are increasingly used to launder money as they offer possibilities for borderless, instant, global transactions when layered through privacy enhancing technologies. While cash remains central to traditional schemes, the rise of cryptocurrencies, DeFi platforms, and AI-driven automation has transformed illicit finance. These technologies are being used as a digital cloak to hide money laundering.*

Virtual currencies provide criminals with opportunities to obfuscate financial flows. The pseudonymous nature of several cryptocurrencies, coupled with the use of mixing services and privacy-focused coins, present challenges in tracing illicit transactions. Complex schemes are set up to increase the opacity of transactions.

CASE EXAMPLE – Cryptocurrency laundromat washed out[1]

ChipMixer, an unlicensed cryptocurrency mixer, was taken down in March 2023, for its alleged involvement in money laundering activities. Deposited funds would be turned into "chips" (small tokens with equivalent value), which were then mixed together - thereby anonymising all trails to where the initial funds originated. The investigation into the criminal service suggests that the platform may have facilitated the laundering of 152 000 Bitcoins (worth roughly EUR 2.73 billion in current estimations) in crypto assets. A large share of this is connected to darkweb markets, ransomware groups, illicit goods trafficking, procurement of child sexual exploitation material, and stolen crypto assets. Information obtained after the takedown of the Hydra Market darkweb platform uncovered transactions in the equivalent of millions of euros.

Chain hopping, for example, involves the switching between different cryptocurrencies to obscure the origin of funds. Crypto-swapping services facilitate a quick conversion of one coin into another by placing orders on behalf of users. They allow instant trade of one cryptocurrency for another and they are becoming more widely used for money laundering. These transactions are difficult to trace when well-known coins are exchanged into less known ones or privacy coins like Monero, enhancing anonymity. Many of these services are registered in jurisdictions with loose anti-money-laundering regulations and often use lenient or non-existent know-your-customer procedures. In some cases, they even advertise their non-compliance.

Decentralised finance (DeFi) is another important element in the cryptocurrency market. DeFi protocols, built on blockchain platforms, provide financial services without intermediaries like banks. These protocols use cryptocurrencies to facilitate decentralised lending, borrowing, trading, and more. Whereas traditional exchanges are focussed on turning fiat currencies into cryptocurrencies, decentralised exchanges are focussed on turning cryptocurrencies into other coins and currencies.

International trade is increasingly exploited for crimes, particularly money laundering and illicit financial transfers. Criminal networks leverage strategic trade partnerships — including free trade zones (FTZs), shell companies, trade misinvoicing, and opaque supply chains — to launder money, evade sanctions, and finance illicit activities.

Criminal actors

Money laundering can be conducted either by those directly involved in the predicate offence or by specialised professional money launderers and brokers. In the former case, the laundering process varies depending on factors such as the nature of the predicate crime, the volume and frequency of transactions, and the geographic distribution of the criminal network. In the latter case, professional launderers or money brokers select the most effective laundering methods based not only on the amount of money involved but also on their financial expertise, available resources and parallel financial infrastructure.

Professional money launderers, increasingly with specialised knowledge in digital asset trading, have developed parallel, underground financial systems that operate outside the regulatory frameworks governing legal financial institutions. Some high-level money brokers occupy pivotal positions within criminal networks, offering extensive, unregulated financial services to multiple criminal networks. Their activities facilitate large-scale money laundering while evading financial oversight mechanisms, thereby reinforcing the resilience and reach of criminal networks.

Asset recovery

Money laundering serves as a critical enabler for criminal enterprises, allowing them to integrate their illegal gains into the legitimate economy. Asset recovery, the process of locating and reclaiming assets derived from illicit activities, presents several significant challenges. The challenge to recover criminal assets allows criminal networks to expand their illicit activities, and increasingly infiltrate the legal economy. Infiltration into the legal system is what makes crime pervasive and destructive.

Asset recovery is a powerful deterrent and an effective tool to tackle serious and organised crime. It deprives criminals of their criminal assets and prevents them from reinvesting them in other crimes or integrating them into the mainstream economy.

The low rate of asset recovery in the European Union remains a significant challenge in combating organised and financial crime. Despite substantial investments in resources and robust legislative frameworks, the confiscation of criminal proceeds remains at an alarmingly modest level of approximately 2 %.

Criminal exploitation of legal business structures

The infiltration of the legitimate business world is a key enabling tactic in the strategies of criminal networks. The abuse of legal business structures (LBS) is a multi-functional tool to support, disguise, or facilitate any form of criminal activity and to launder its proceeds. All business sectors are at risk, to varying degrees, in all crime areas.

LBS as multifunctional tools for serious and organised crime

LBS are a key instrument in criminal networks' toolboxes, supporting their operations in various ways, from committing and covering up crimes to laundering criminal proceeds.

While the abuse of LBS is optional in some areas of crime, certain criminal activities simply cannot be carried out without them. LBS misuse is particularly prevalent in economic and financial crime, and in all criminal activities carried out through commercial operations in the legal economy. All types of fraud schemes targeting individuals, private companies, and public institutions, but also intellectual property crimes and environmental crimes are perpetrated behind the façade of legitimate businesses. 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.

Varying degrees of criminal exploitation and infiltration of LBS

Criminal networks can seek to exert varying degrees of influence and control over LBS. Most subtly, an existing LBS may be used by a criminal network without their knowledge. In this instance, the criminal network does not exert any direct control over the LBS but merely uses its name, infrastructure, or services. Taking a step further, a criminal network can directly infiltrate an LBS at a low level, by colluding with or coercing its employees. Further still, a criminal network can infiltrate an LBS at a high level, coercing key high-level individuals within the structure, or set up its own LBS which it fully controls.

CASE EXAMPLE – Counterfeiting criminal network owns courier companies[2]

In June 2022, the Greek authorities conducted investigations into a criminal network involved in trading counterfeit luxury goods through a website and 13 social media profiles. The criminal network had managed to distribute over 364 000 parcels to customers and obtain more than EUR 18 million in illicit profits, laundered via other business companies owned by the network. The network supposedly also owned two courier companies that would exchange goods and money multiple times to avoid detection and conceal their criminal activities.

A large majority of the reported criminal networks abuse LBS to some degree. Many of them do so at the highest threat level – setting up their own LBS, infiltrating an existing LBS at a high level, or colluding with or coercing key high-level individuals within an LBS to gain access or control.

The greatest concern lies in insider threats—high-level infiltration or criminal ownership of the LBS—enabling criminals to tailor the system to their needs and maintain full control.

The infiltration and abuse of LBS can be systematic and long-term, or temporary. When abuse is systematic, it becomes a functional part of the process without which the criminal activity cannot be carried out. Some LBS are abused throughout the criminal process, others only in one or a few stages.

All business sectors at risk

All business sectors are potentially at risk of criminal exploitation, each presenting different types of opportunities for abuse by criminal elements. LBS are infiltrated or abused by criminal networks across almost all sectors, in all crime areas. Three types of businesses are particularly affected by criminal infiltration or abuse: construction and real estate, cash-intensive businesses (particularly hospitality), and logistics (i.e. transport and import/export companies).

Corruption

Corruption is embedded in the very DNA of crime. It acts as a key enabler and catalyst for criminal activities, and contributes to destabilising society. It is instrumental to most forms of organised crime and this to evade law enforcement, gain economic or political influence, facilitate criminal operations or weaken the trust in public sector or law enforcement. While grounded in well-known mechanisms, corruption has adapted to the broader trends toward digitalisation and a crime-as-a-service model. Several issues become increasingly visible: the targeting of individuals with access to digital systems in public and private entities, the use of digital recruitment tactics, and the elevated role of corruption brokers.

Corruption as a tool to facilitate all crime areas and expand criminal influence

Corruption serves as a critical enabler of organised crime, allowing criminal networks to infiltrate institutions, evade law enforcement, and expand their influence across political, economic, and social domains. It undermines the rule of law, weakens governance structures, and distorts economic systems, creating an environment conducive to illicit activities. The intersection of corruption and crime presents several significant threats to societal stability and security.

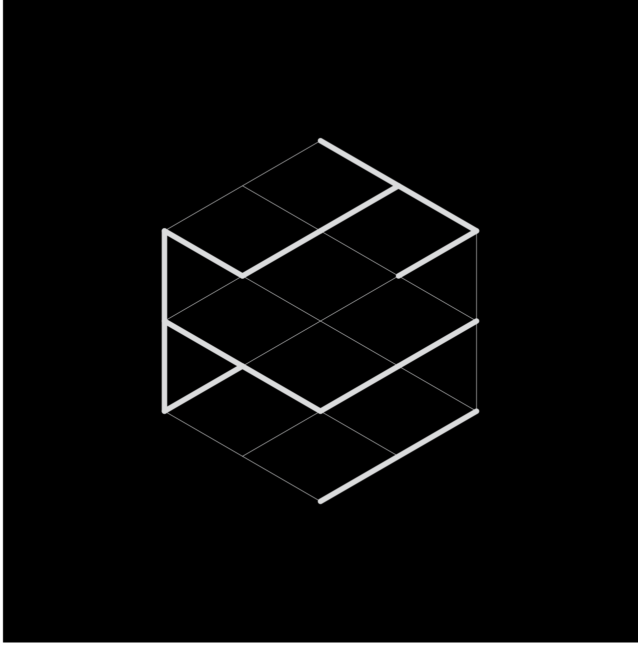
One of the most immediate consequences is the erosion of law enforcement and judicial integrity. Criminal networks exploit corruption to secure protection from prosecution by trying to bribe law enforcement and the judiciary. This enables them to avoid arrests, obstruct investigations, and manipulate legal proceedings in their favour. Additionally, corrupt officials may provide criminals with classified information regarding operations, allowing them to evade detection and continue their activities with impunity.

Beyond law enforcement and judiciary, public institutions are highly susceptible to infiltration by criminal networks[3]. Corrupt officials can facilitate organised crime by granting access to government contracts, procurement processes, and financial systems. This not only enables fraudulent activities, such as money laundering, but also allows criminal networks to exert influence over policymaking and regulatory frameworks. In some cases, this may result in situations where criminals systematically manipulate political and administrative structures to serve their interests.

Corruption also plays a pivotal role in facilitating the illicit trade in itself. Bribery of border security staff, law enforcement and customs officials, and financial regulators may facilitate the uninterrupted flow of illegal goods and services across borders. Furthermore, corrupt staff in financial institutions may enable money laundering by disregarding regulatory compliance, allowing criminal profits to be integrated into the formal economy. Such activities not only fuel organised crime but also pose serious risks to financial stability and security.

From an economic perspective, corruption linked to organised crime distorts market dynamics and undermines legitimate business activities. The infiltration of criminal networks into economic sectors disrupts fair competition, discourages investment, and fosters an environment of economic inefficiency.

Corruption is embedded in the very DNA of crime – as a criminal act in itself, but also as a facilitator for all types of serious and organised crime. It undermines the rule of law and threatens citizens' trust in democratic institutions, affecting citizens, businesses and society as a whole.



An enduring catalyst of criminal threats, under-reported yet ever-adapting

Corruption is set to further digitalise. Recruitment of, and communication with corruptees takes place online. Bribes are transferred by criminally exploiting cryptocurrencies or fintech. In addition, individuals with access to digital systems become key targets for corruption as they can provide access to information relevant to the criminal enterprise.

> *As technology and AI advance, individuals with access to digital infrastructure/solutions in both public and private spheres have become prime targets for manipulation and exploitation.*

The largest threat of corruption within organised crime is its impact on public trust and societal stability. When institutions are perceived as compromised, citizens lose confidence in governance structures, law enforcement, and the judicial system. This erosion of trust creates a power vacuum in which criminal organisations may position themselves as alternative authorities, providing illicit services, financial assistance, and even social order in areas. Over time, this may weaken democratic structures and reinforce criminal governance.

Corruption sometimes manifests as foreign influence, as demonstrated by the involvement of public officials in some major corruption cases[4]. This is why corruption is part of the core DNA of crime, destabilising the internal security of the EU by undermining our economy and society.

While Member States continue to strengthen their regulatory frameworks alongside EU and national legislative developments and law enforcement efforts, corruption remains underreported, further amplifying the threat it poses.

Corruption is not merely an ancillary component of organised crime but a fundamental mechanism through which criminal networks consolidate power, evade justice, and expand their operations.

Violence

Organised crime-related violence has intensified in some Member States, particularly in port cities and urban drug markets. With diversification of drug routes and entry points, also a further displacement of violence throughout the EU is expected. Violence is encroaching upon public spaces, instilling fear and eroding trust in authorities. Score-settling between and within criminal networks is the most common trigger. Online and encrypted communication solutions enable criminals to recruit hitmen – including young perpetrators – and coordinate violent actions all over the world. Violence is provided as a service and made possible by the availability of trafficked weapons.

The use of violence in organised crime: widespread, heterogenous, facilitated by weapons trafficking

The use of violence is a common feature, with two-thirds of the criminal networks engaging in forms of violence ranging from psychological violence, such as intimidation and threats, to the infliction of physical harm, including assaults, kidnapping, torture, and homicide.

Hotspots of violence often coincide with key locations for organised crime, with a particular increase in drug trafficking hotspots. Violence is associated with both the import of drugs at key ports and distribution in major cities, although drug-related violence is also spilling over into smaller cities. In line with a diversification of entry points of cocaine, the violence may further spread to other locations in the EU.

Distance and boundaries are irrelevant when it comes to the use of violence by criminal networks. Enabled by online platforms, social media and encrypted communications, violent criminal networks have a long reach. This enables them to set up violent actions remotely, in all corners of the world – from private homes to public institutions such as prisons. Perpetrators incarcerated are easily approached, sometimes with the help of ex-convicts, to harm a fellow inmate for intimidation or retaliation.

Online platforms and encrypted communications are a major catalyst for violence, for recruitment, communication, extortion, or remote coordination. They also facilitate the reach of young and vulnerable perpetrators.

Violence, intimidation, and threats are intrinsic features of many forms of organised crime. Extortion and racketeering, kidnapping for ransom, aggravated robberies, home invasions, tiger kidnappings and car-jackings, trafficking in human beings (THB), and child sexual exploitation are inherently violent crimes, with direct impact on their victims. Extortion-related violence increasingly takes place online with intimidation tactics, including the threat of releasing sensitive data, divulging personal data, personal conversations, or images, blocking cyber services and computer systems, cyberbullying, and verbal intimidation over the phone. It is also seen in child sexual exploitation, where grooming and psychological violence enable criminals to obtain child sexual abuse material.

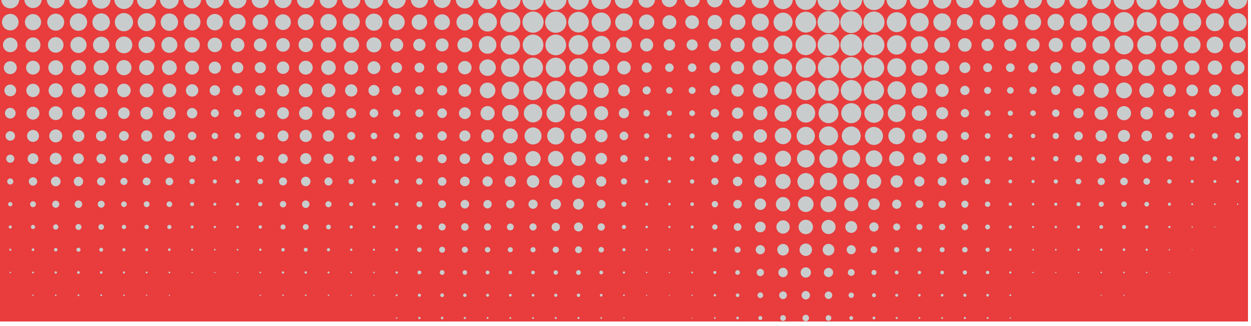
Violence is also used as a tool by criminal networks to establish and maintain power over a criminal market, territory, route, key location, critical infrastructures, transportation and distribution networks. Removal of competitors and elimination of rivals is often a fast track to gaining dominance. Violence is also a tool to conceal and enable criminal activities. It is used to evade authorities – including by silencing and coercing people into participating in the criminal process. As such, violence is occasionally used by criminal networks to secure their infiltration into legal business structures, going hand-in-hand with corruption and ensuring corrupt actors remain compliant.

Settling business conflicts and score-settling between and within criminal groups is the most common trigger for violence. Within criminal networks, any member of the network, regardless of rank, as well as their close acquaintances, can become a target when disputes arise. Between criminal networks, criminal partnerships are fleeting and volatile, and competition between criminal actors is fierce, particularly among drug networks. Once a conflict starts, it can escalate into an endless circle of retaliation, interpersonal conflicts, and vendettas.

Score-settling following disputes, transgressions, thefts and betrayal between and within criminal networks are the most common triggers for violence. High stakes, high distrust and fleeting criminal partnerships contribute to creating a high-tension atmosphere, further enabled by the availability of illicit firearms and explosives.

While violence concerns many crime areas, it is most commonly associated with drug trafficking and, to a lesser extent, migrant smuggling. In crime areas such as burglaries and organised theft, violence is mostly reactive and for defensive reasons.

Weapons trafficking often does not lead directly to violence, but firearms trafficking to and within the EU, and the availability of weapons in general, are major enablers for organised crime-related violence. The use of explosives and firearms is becoming more frequent, relying on intermediaries and weapons dealers. Heavy pyrotechnics or improvised explosive devices containing considerable amounts of flash powder are used as weapons, most notably in the context of retaliation in drug trafficking, but also in THB, thefts and robberies.



Violence-as-a-service: who does what and how does it work?

Various actors play a role in planning and executing violent acts, with distinct responsibilities. In many cases, there is a distance between those commissioning or ordering the act of violence and those executing it.

There seems to be a ready supply of individuals willing to be recruited to commit violent acts. Within criminal networks, low-ranking members commonly act as perpetrators, but violence is also outsourced to young perpetrators, assorted criminals, and professional hitmen or hit squads offering violence-as-a-service. They are contacted directly through a network of personal contacts, in prisons, or via intermediary contacts. Encrypted communications and online platforms are instrumental in finding and recruiting these executors.

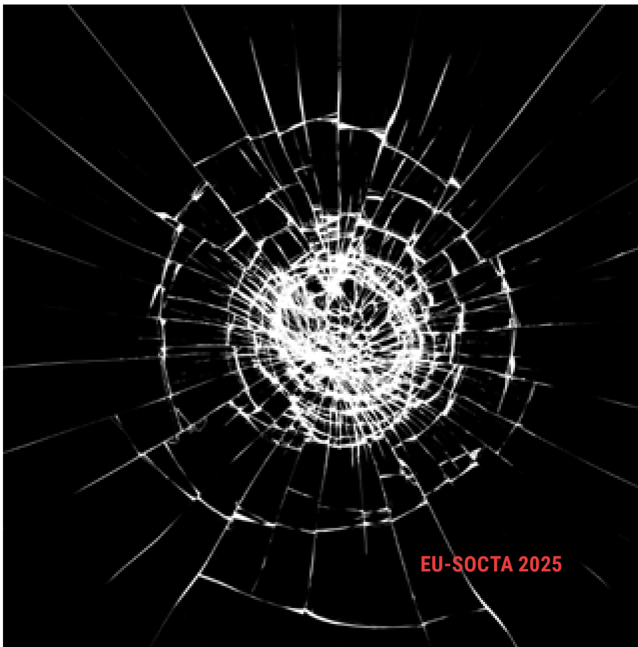
Violence can be highly premeditated and prepared, as seen in typical score-settling hits. A small number of criminal networks are known to use and/or provide violence-as-a-service. These services include professionally planned and organised contract killings, as well as violence used as a means of debt collection, extortion or to settle criminal conflicts.

Increasingly, executors of violence appear to have little knowledge of the intended victims and their physical surroundings prior to a hit or assassination. Facilitators are sometimes also recruited ad hoc in online group chats for specific tasks such as surveillance and logistics. This leads to shorter time frames to set up the violence. Badly informed and inexperienced perpetrators increase the threat of causing collateral damage to unintended victims.

CASE EXAMPLE – Violence-as-a-service: criminals hire criminals[5]

After a dispute in the illegal drug trade, a criminal network was hired to carry out violent retaliation attacks in Germany. They orchestrated a series of attacks with the use of explosives, as well as kidnappings. An action day in January 2025 resulted in the arrest of three persons and the seizure of various criminal assets, such as EUR 20 000 in cash, a converted firearm and powerful explosive pyrotechnics.

Of particular concern is the involvement of young perpetrators in violent crimes. Their involvement is seen in street robberies, extortion and racketeering, child sexual abuse and trafficking in human beings, and has become particularly visible in drug trafficking. The violence is carried out by violent youth groups and street gangs, but also by young people groomed and recruited for this purpose via social media and messaging applications.



Criminal exploitation of young perpetrators

Young perpetrators used as a tactic in various types of serious and organised crime

The recruitment of young perpetrators, including young adolescents and children, into serious and organised crime and terrorism is not a new phenomenon. However, it has increasingly become a means used by criminal networks to remain out of reach of law enforcement and the judiciary.

Young perpetrators are frequently exploited in several criminal markets and in several roles. In cyber-attacks, script kiddies[6] are influenced to conduct specific cyber-activities for a fee. In drug trafficking, young people are recruited in roles like dealers or couriers but also warehouse operators, and drug extractors from shipping containers. Young people are used as money mules, receiving and transferring illicit funds through their bank accounts, often in exchange for a small share of the money. In (online) frauds, young perpetrators may be asked to recruit others, share posts, or create online profiles to drive interest, often in return for commissions or rewards. Young perpetrators have also found to be involved in migrant smuggling or organised property crime.

This trend has expanded across more countries, with recruitment methods evolving and young perpetrators also being tasked with violent acts such as extortion and killings.

Recruitment of young perpetrators primarily takes place on social media and messaging apps, taking advantage of the anonymity and encryption they offer and using communication strategies that speak to young people.

The young perpetrators are recruited through social media platforms and messaging applications, exploiting the anonymity and encryption they offer. Criminals use tactics to lure young people, including tailored language, coded communication, and gamification strategies. By glorifying a luxurious and violent lifestyle, they convince vulnerable young people to join their ranks.

Investigations show that there is a demand from the criminal realm for young perpetrators, but also that there is a supply of such perpetrators willing and looking for assignments to participate in violent acts. In several cases, violent attacks committed by young perpetrators are orchestrated remotely by a criminal service provider.

Extremely violent online communities manipulate children and young people

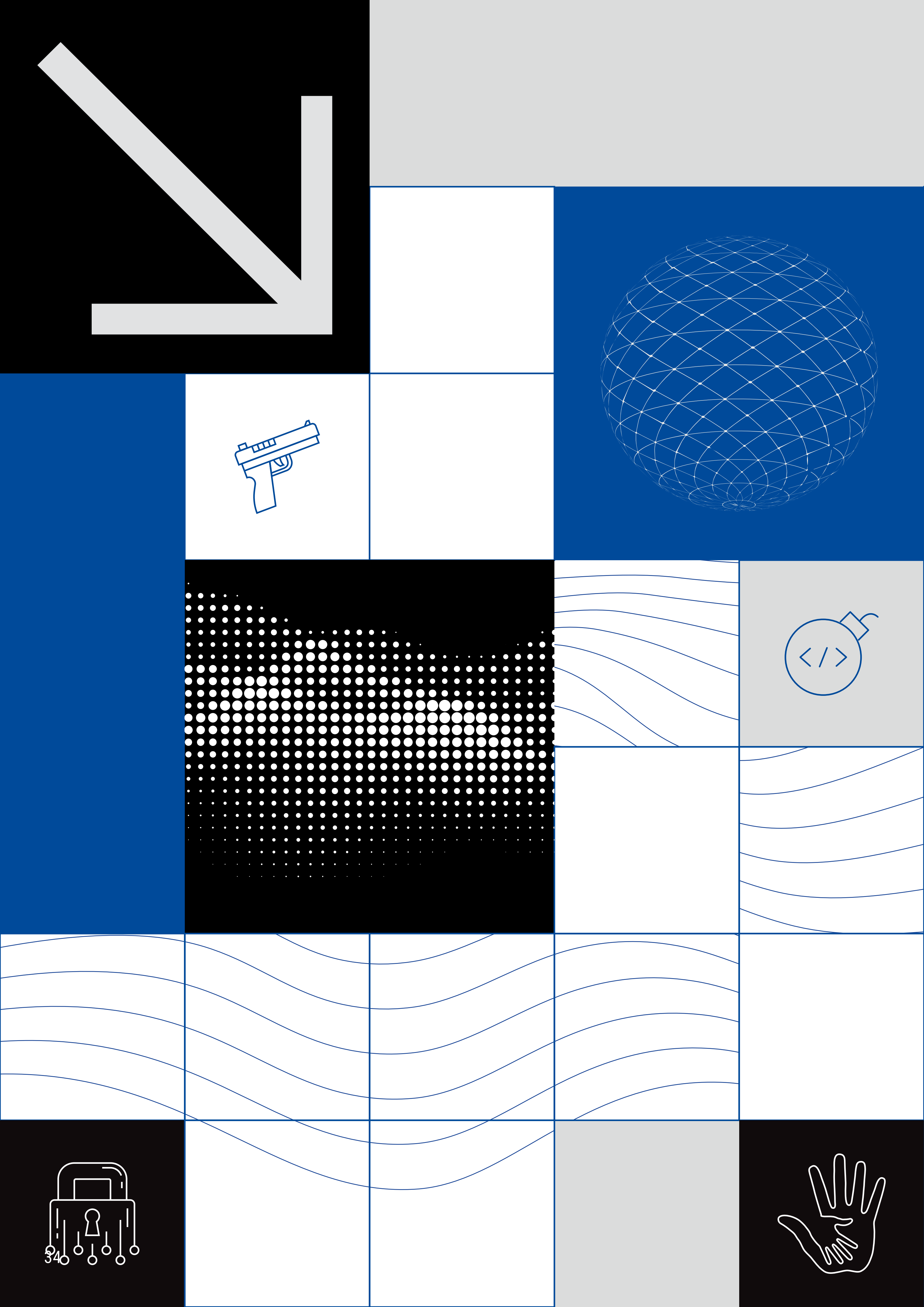
At the intersection of serious and organised crime and violent extremism, several online groups have emerged that have a common purpose of destroying civilised society through the corruption of young people. Based on their extreme ideological views, criminal actors groom and victimise children, coercing them to commit violent acts, including sexual abuse, acts of cruelty, torture and murders.

These violent online groups are targeting and manipulating vulnerable children and young people across widely accessible online platforms, including social media and gaming platforms. The predators in these networks influence children or young people into conducting acts that increasingly shame, incriminate, or isolate them, and this in turn makes them more vulnerable to further exploitation. In many cases, there is a correlation between victimhood and perpetration of abuse, with abusers who were themselves victims of abuse, thus perpetuating a cycle of harm[7].

CASE EXAMPLE – Online group "CVLT"[8]

In January 2025, two individuals were arrested for participating in a violent extremist child exploitation ring named "CVLT" that groomed and then coerced minors to produce child sexual abuse material and images of self-harm. The group allegedly abused at least 16 minors around the world. The leaders and administrator of this violent online abuse community hosted and ran CVLT online servers, and controlled membership for the group.

CVLT members' coercion escalated to pressuring victims to kill themselves via video livestream. They blackmailed the victims to submit and remain silent, threatening to distribute already-obtained compromising photos and videos to their family and friends. CVLT would sometimes go through with their threats against victims who tried to escape their grip. CVLT is part of a larger network of violent extremists and child abusers active within similar online communities.



3

The EU criminal landscape: **a shifting blueprint**

All organised crime activity presents a threat to the EU and its Member States to some degree, while certain crime areas come to the fore as more threatening because of their current threat level, impact on society, and expected future evolution. The criminal landscape is very heterogenous with many various types of crime committed by a plethora of criminal actors affecting Member States in different ways. For this reason, it is important to identify the most threatening crime areas so as to prioritise the EU's fight against serious and organised crime in the years to come.

A range of criminal threats thrive predominantly in the online sphere, and they are fast-tracking in terms of volume, reach to victims, sophistication of modi operandi. This is due to the general online presence of citizens and businesses, and the acceleration of enabling technologies, particularly AI. In some cases, these digital crimes are executed in support of hybrid threat actors' ideologically motivated objectives.

↘ 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, and combine motives of profit and destabilisation. Expertise is shared in the cybercrime underworld in a crime-as-a-service model, expanding the pool of cyber-offenders, within a landscape that is already fragmented in response to law enforcement intervention. The crime-as-a-service model also supports external actors, as in today's global context, the motivations for cyber-attacks do not only include profit, but are also increasingly state-aligned.

↘ A widespread fraud epidemic is affecting numerous EU citizens, businesses, and public institutions alike. The scale, diversity and sophistication of fraudulent activities are previously unseen, driven by advancements in automation and AI. These schemes leverage AI to create highly realistic narratives that incorporate trending societal topics, making them increasingly convincing. Crytocurrency holds a central role, both as a payment method and as a vehicle for investment fraud. Impact on victims is both financial and psychological, and many are targeted multiple times.

↘ Child sexual exploitation and the production and distribution of child sexual abuse material is transforming. Production is nurtured by the ever-expanding victim base online, and accelerated by the accessibility of AI tools to manipulate images and videos and to groom minors convincingly. Material is distributed in high volumes within online communities of offenders who also use new tools as countermeasures against detection.

Some criminal businesses that are fundamentally physical, cross-border crimes entailing the trafficking of goods or persons, persist as key threats to the EU's internal security. As more traditional crime areas, they stand out because of their extensive ramifications on society, the agility and resilience of the criminal actors involved in them, and the high demand for the involved illicit goods or services. At the same time, key parts of these illicit businesses move online, gain from innovation, or even serve the objectives of hybrid threat actors.

↘ Migrant smuggling remains a thriving criminal enterprise, adapting routes and modi operandi in response to demand, emerging opportunities, or imposed obstacles. This global market with the EU as major destination and transit, is sustained by ongoing conflicts, economic hardships and environmental challenges. The manipulation of irregular migration flows by hybrid threat actors at the EU's external borders has amplified opportunities for the provision of migrant smuggling services. Despite its point of gravity in the physical world, migrant smuggling is increasingly shaped by advancements in digital and technological tools.

↘ Drug trafficking is a pervasive crime threat across the EU and with a multitude of global interconnections. It represents a highly lucrative yet competitive criminal enterprise. It has a high potential to destabilise EU society, given its association with violence, corruption, and infiltration in the legal economy. Cocaine and synthetic drugs trafficking are particularly dynamic, with often shifting routings, modi operandi, and a variety of criminal actors, as exemplified by the waterbed effect currently seen in cocaine trafficking. Further innovation in chemical processes and new – potentially dangerous - variants are expected, further exacerbating the already layered impact drug trafficking has.

↘ Firearms trafficking is a critical issue in the EU shaped by a complex supply and demand interplay. Patterns in the market for illicit firearms are shifting, driven by heightened levels of violence involving firearms and explosives in organised crime and terrorism, criminals seeking alternative sources of weapons, and technological as well as geopolitical developments that facilitate illicit production and trafficking. Technological advancements such as online sales points, 3D printing, and AI lower access barriers and increase sophistication. Weapons available in (post war) Ukraine will further exacerbate this threat.

↘ Environmental crime, particularly waste crime, has a detrimental impact on the natural environment and economy, and on the health and safety of EU citizens. Waste trafficking is closely interconnected with the licit waste sector, and involves criminal actors benefiting from extensive expertise.