EUROPOL

The
changing
DNA of
serious
and
organised
crime

2025

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**.
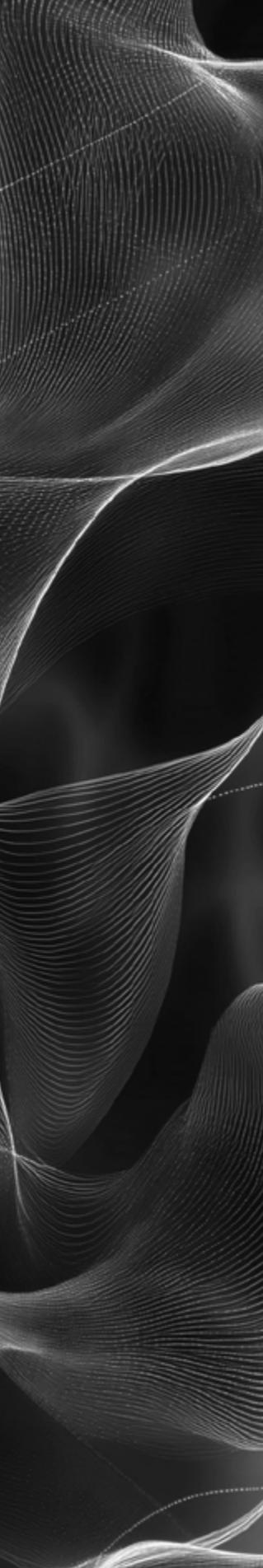
↘ **Serious and organised crime has a double destabilising effect on the EU and its Member States.** It undermines and reduces trust in the EU's economy, rule of law, and society as a whole by generating illicit proceeds, spreading violence, and normalising corruption. It is also progressively driven 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
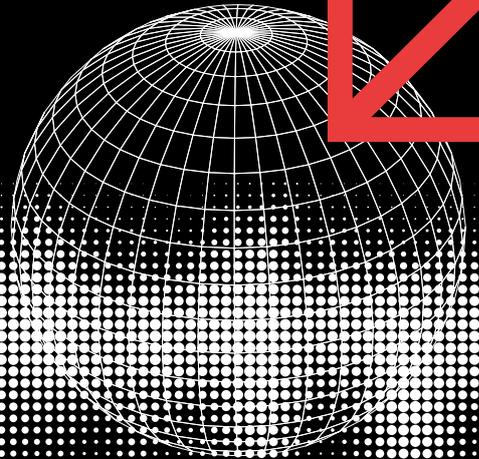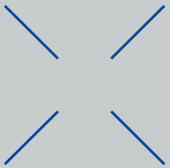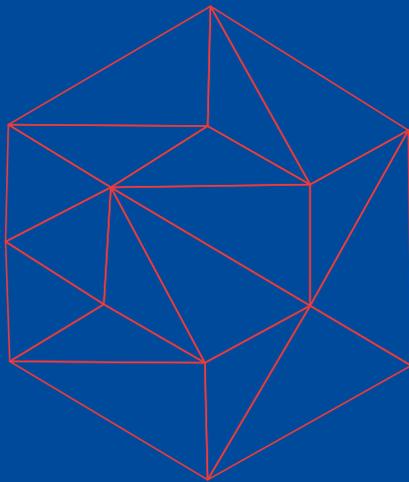
Destabilisation through economic and social undermining

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 cooperate 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.
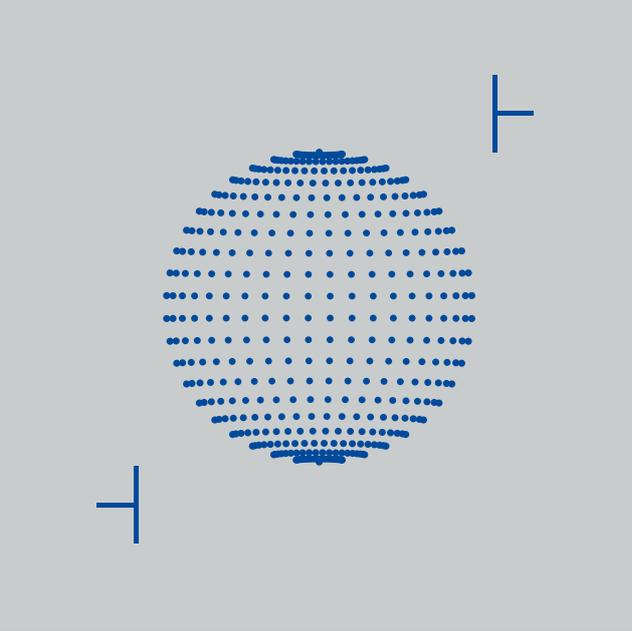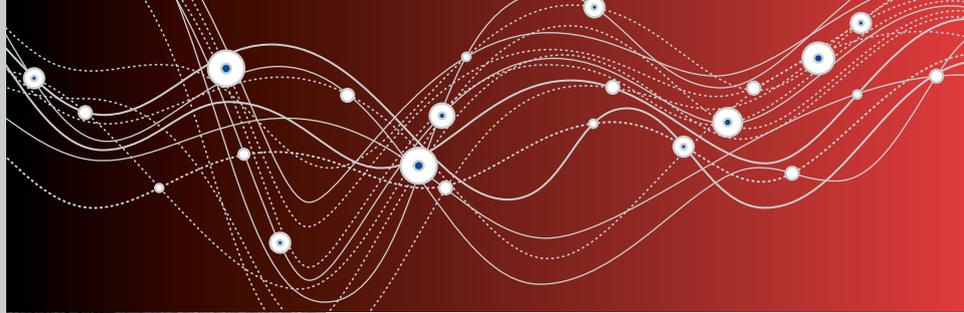
nurtured online
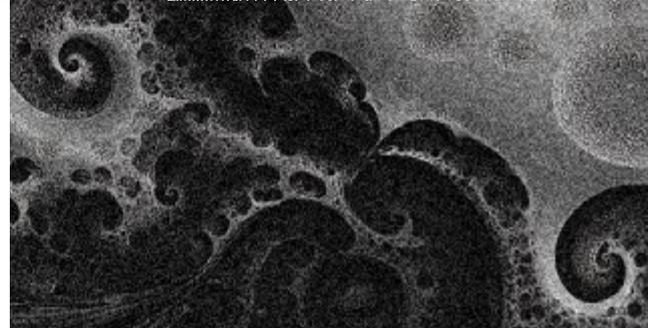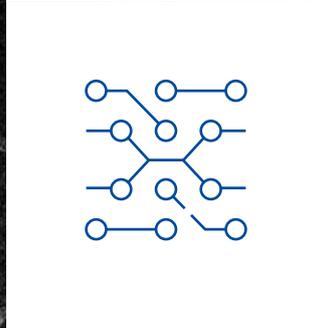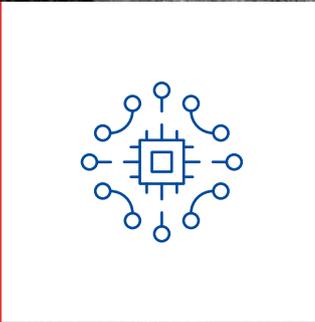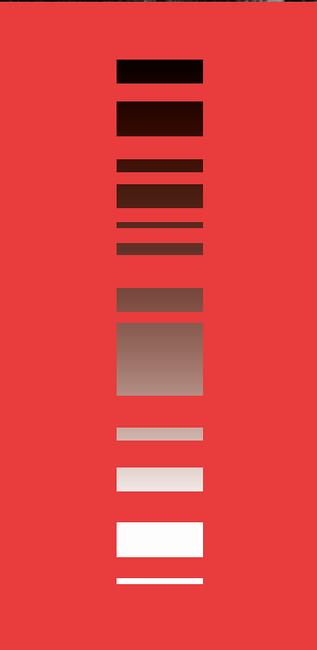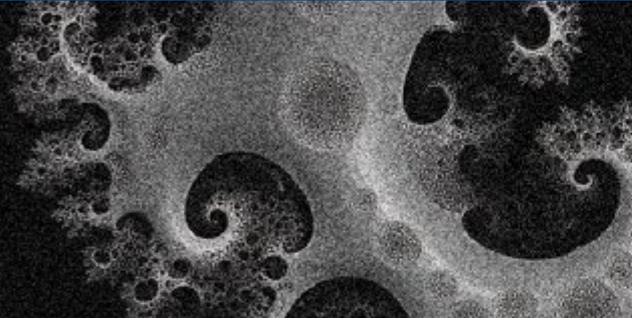
Digital infrastructure as an enabling tool to drive criminal operations

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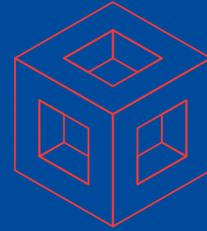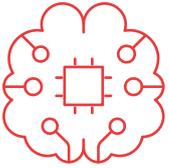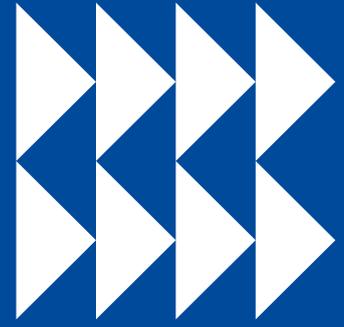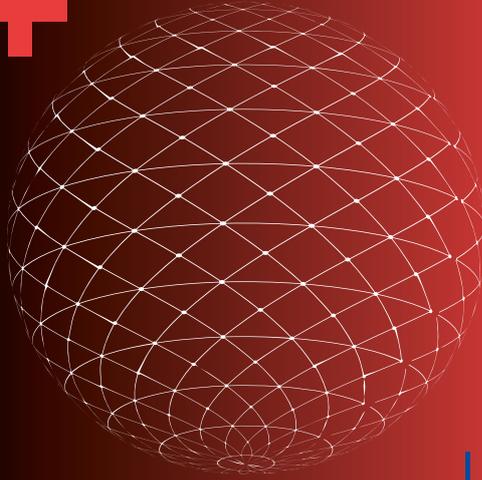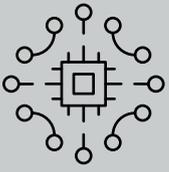
accelerated by AI
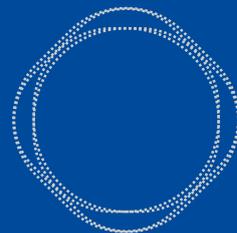
AI and other new technologies are fundamentally reshaping the serious and organised crime landscape in two main ways: as a catalyst for crime, and as a driver for criminal efficiency.

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.

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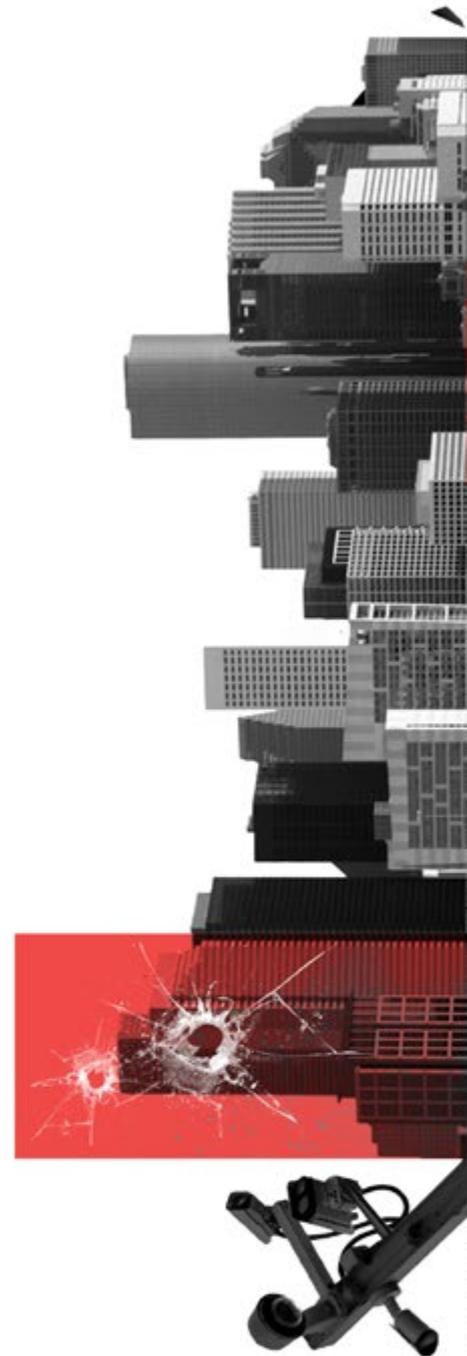
↘ Criminal networks have adopted the practice to move illicit proceeds to parallel financial systems designed to protect and grow their wealth stemming from their illegal activities. This goes together with the obfuscation of financial flows.

↘ 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
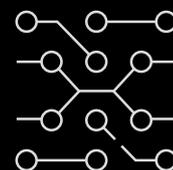
As the criminal landscape continues to evolve, so does the intricate nature of money laundering and criminal finances. Criminal networks increasingly invest in creating a parallel financial system tailored to expanding their illicit operations and accumulating wealth generated from illegal activities. 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 focused on turning fiat currencies into cryptocurrencies, decentralised exchanges are focused 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 the 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.
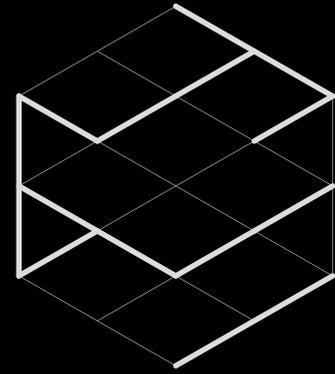
An enduring catalyst of criminal threats, under-reported yet ever-adapting

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 under-reported, 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.
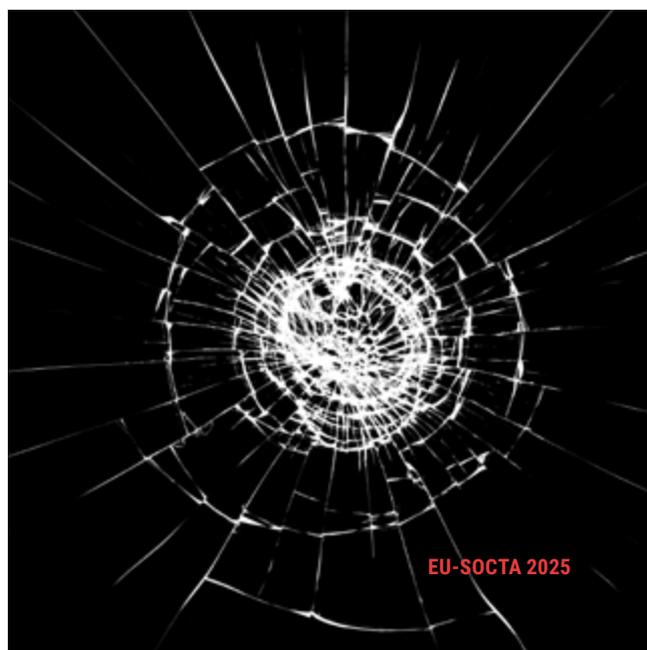
Criminal exploitation of young perpetrators

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.
```
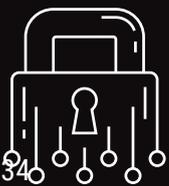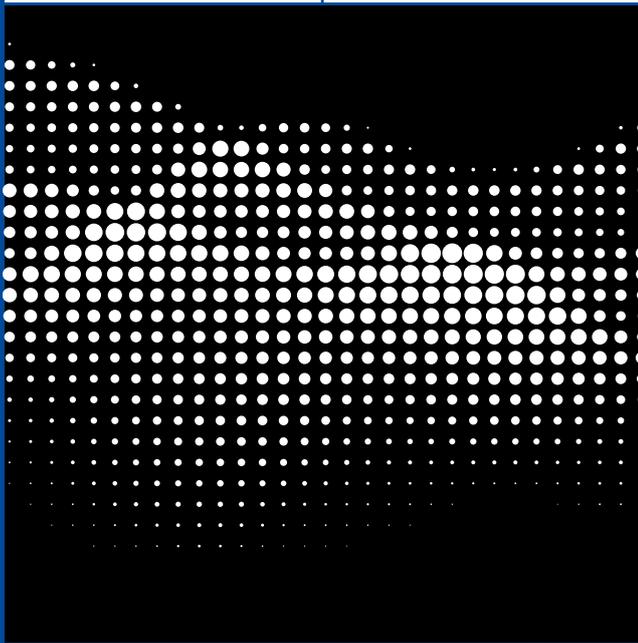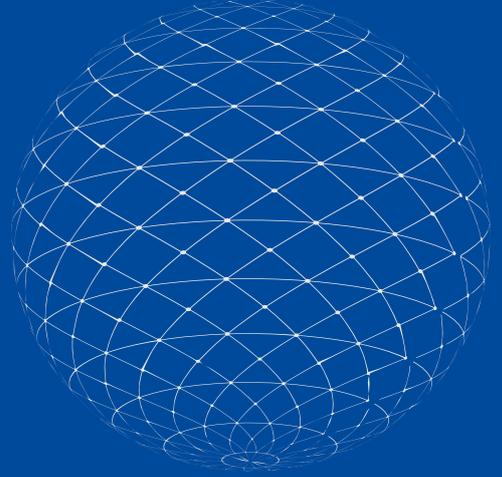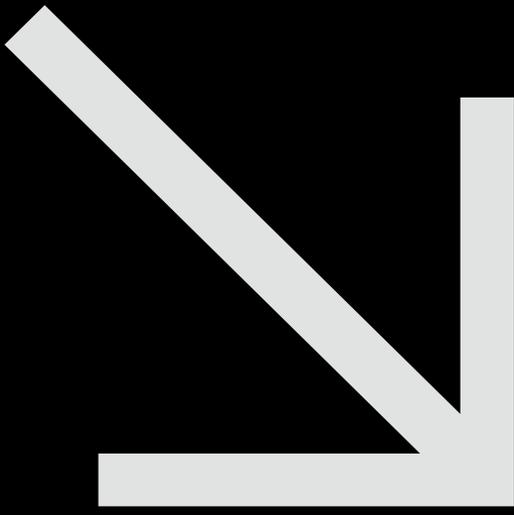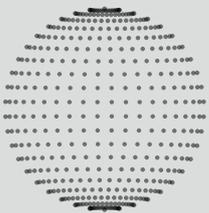
3

The EU criminal landscape: a shifting blueprint
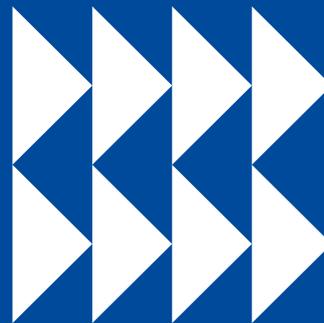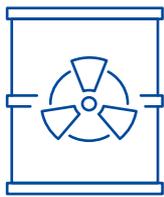
All organised crime activity presents a threat to the EU and its Member States to some degree, while certain crime areas come to the fore as more threatening because of their current threat level, impact on society, and expected future evolution. The criminal landscape is very heterogenous with many 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.
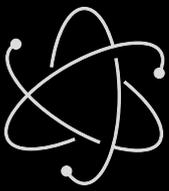
Cyber-attacks

Cyber-attacks targeting critical infrastructure, governments, businesses and private citizens are highly threatening and impactful due to a broadening attack-surface, and data theft acquiring a central role. Lines are further blurring between profit-oriented and ideologically-motivated cyber-attacks, and the cybercrime landscape is further fragmenting. AI will continue to leverage more sophisticated and scalable cyber-attacks that will even more target data than is already the case today. Cyber-attacks have a wide impact spectrum, including financial consequences, loss of personal data and eroding sense of security.
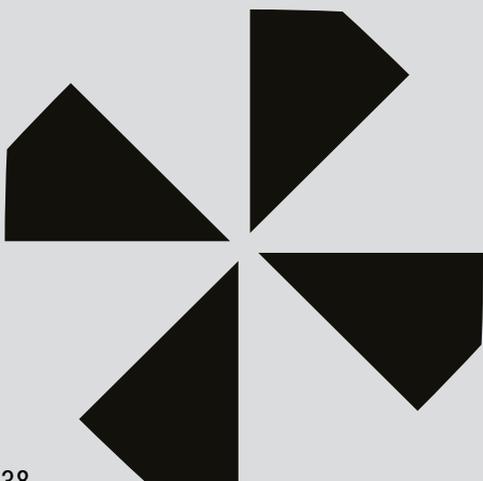
Broadening attack-surface in which data are key, further enhanced by AI technologies

Crime is nurtured online. The number of cyber-attacks against public and private entities has increased[9], and this trend is expected to continue in the future. The rapid digitalisation of everyday life has resulted in the increased complexity of most digital infrastructures. Combined with the speed of transition and the insufficient digital literacy of the broader user base, this has left more systems exposed and vulnerable to cyber-attacks. The increase in cyber-attacks is further driven by the development of more sophisticated tools and techniques available in the Cybercrime-as-a-Service (CaaS) market.

In today's complex digital infrastructures, cyber-attacks increasingly exploit their vulnerabilities.

There is an increase in politically motivated cyber-attacks against critical infrastructure and public institutions, originating from Russia and countries in its sphere of influence.

Politically motivated cyber-attacks demonstrate precisely how the three elements of the DNA of crime work in tandem, completely changing the criminal landscape. Cyber-attacks are increasingly directed by networks and agents based outside EU external borders. Digital platforms and tools provide the perfect breeding ground for illicit activities. Cutting-edge technologies are making attacks faster, smarter, and more devastating than ever.
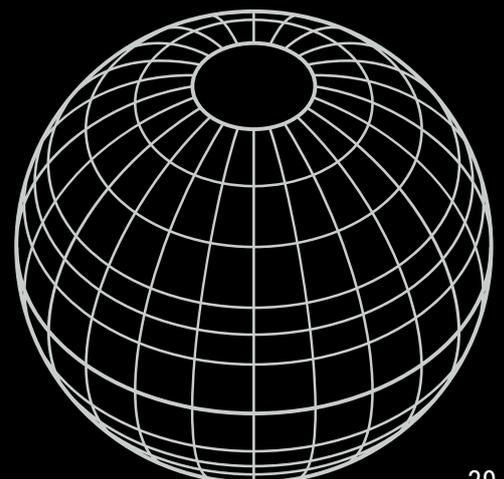
In order to gain entry to systems, criminal actors exploit zero-day vulnerabilities[10], Common Vulnerability Exposures[11], misconfigurations in public-facing infrastructure and leverage vulnerabilities that have been disclosed but not patched. The growing reliance on different digital service providers (e.g. virtual privacy networks (VPN), cloud, e-mail, and software service providers) increases the risk of supply-chain attacks, where a victim's system is breached by compromising a trusted third party. Social engineering methods and phishing kits[12] are widely available on the dark web. Criminals also use phishing-as-a-service to distribute emails containing malicious macros and files to steal login credentials.

```
CASE EXAMPLE – Notorious ransomware group
dismantled[13]

In February 2024, law enforcement from 10
countries disrupted the LockBit ransomware,
causing billions of euros worth of damage.
It first emerged at the end of 2019, and in
2022 it became the most deployed ransomware
variant across the world. The group is a
'ransomware-as-a-service' operation, meaning
that a core team creates its malware and
runs its website, while licensing out its
code to affiliates who launch attacks.
LockBit's attack presence is seen globally,
with hundreds of affiliates recruited to
conduct ransomware operations using
LockBit tools and infrastructure. Ransom
payments were divided between the LockBit
core team and the affiliates, who received
on average three-quarters of the ransom
payments collected.

The ransomware group is also infamous
for experimenting with new methods for
pressuring their victims into paying
ransoms. Triple extortion is one such method
which includes the traditional methods of
encrypting the victim's data and threatening
to leak it, but also incorporates
Distributed Denial-of-Service (DDoS) attacks
as an additional layer of pressure.
```

Droppers are similarly used to allow criminals to evade and deactivate security measures and deploy additional harmful programs. They have become more effective over the past few years with the newer variants being able to evade dynamic detection, and deploy sophisticated obfuscation methods[14]. Droppers are most commonly spread through phishing campaigns.

Access to compromised systems has become a commodity in the CaaS economy, with access to compromised systems sold in bulk or auctioned on dark web forums. Compromised victims can be subjected to several simultaneous or consecutive cyber-attacks.

The crime-as-a-service economy enables different forms of cyber-attacks, including dark web market forums selling stolen data, intrusion services as well as criminal hosting and proxy providers.

Malware-based cyber-attacks[15], especially ransomware[16] and info-stealers[17], continue to be a prominent threat with data acquiring a central role[18]. Stolen credentials can be used to gain unauthorised access to digital assets, including sensitive information, that can be stolen and held for ransom. Data stolen with the use of info-stealers can be used for various cyber-attacks and online fraud schemes.

Data is a central commodity in the malware threat landscape — used for carrying out attacks, as target, and as by-product of attacks.

Within ransomware attacks, the tactic of threatening to publish exfiltrated sensitive information has become a key coercion method. There has been a shift from mass distribution of ransomware (e.g. through phishing campaigns) to more targeted attacks against private industries, critical infrastructure, healthcare, and other public institutions[19]. In recent years, targeted ransomware attacks against small and medium-sized businesses have also become more common. There has been a growing number of supply chain attacks[20]. Leaks of source codes, combined with rapidly improving AI tools, have also accelerated the development of new ransomware variants.

Crime is accelerated by technology and AI. As AI technologies improve, they will start playing an increasingly important role in criminals' tactics, techniques and procedures. They can be used for hyper-realistic social engineering attacks using deepfakes or voice alteration, or can be taught to impersonate the mannerisms, writing style and background knowledge of a person. AI can also be used to improve and automate criminal processes like finding new exploitable vulnerabilities, triaging stolen information or automating ransom negotiations or different forms of online fraud schemes, increasing the scale of attacks. Data theft will play an increasingly central role in different forms of cyber-attacks, given its importance in AI-driven attacks.

Hybrid and traditional cybercrime actors will increasingly be intertwined, with state-sponsored actors masking themselves as cybercriminals to conceal their origin and real disruption motives. Overall, it is expected that ransomware, data theft extortion and multifaceted extortion — employing complex, multi-layered tactics to maximise pressure on victims and increase the likelihood of payment — will become the most disruptive crime globally, both in volume and impact. An increased availability of CaaS, with the support of generative AI technologies, will lead to more attacks and potentially increase their efficiency. An increased use of automated tools has also been observed, for instance, to distribute malware on a large scale and adapt payloads to bypass traditional security measures. AI-generated content is also being used in phishing campaigns.

Cyber-attacks leveraged by hybrid threat actors may take further prominence against the backdrop of a shifting global geo-political balance.

Criminal engagement driven by financial, ideological, and service provision motives

Financial motivation remains the primary driver for most cyber-attacks. Ideological motivations or service provision to hybrid threat actors in the context of hybrid threats are also common. Criminal networks engaged in cyber-attacks are present and active in a number of different countries, both in terms of the physical location of their members and the jurisdictions where they carry out their activities. Cybercriminals continuously improve their intrusion and attack techniques and countermeasures to stay ahead of evolving security solutions.

Independent ransomware groups or malware-as-a-service providers often function with a core group surrounded by a network of individuals (e.g. affiliates, other service providers). The threat actors behind these groups are technically advanced and capable of carrying out sophisticated, wide-scale attacks. The ransomware landscape has become more fragmented due to international law enforcement actions and internal disputes, forcing ransomware operations to disperse or rename themselves to cover their tracks.

The cybercrime landscape has become more fragmented, with shorter life-spans, for and splintering of, markets and ransomware groups, making attribution of threat actors more challenging.

Economic recession, geopolitical instability and widening global inequality have increased incentives for individuals to engage in financially motivated cybercrime. Tech-savvy adolescents and young adults are especially susceptible to recruitment by criminal networks.

Advancements in AI will be further deployed for various aspects of cyber-attacks: for attack automation, social engineering, finding new vulnerabilities and by-passing security solutions. This will increase both the scale and efficiency of cyber-attacks.
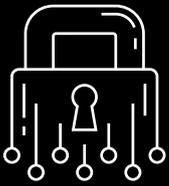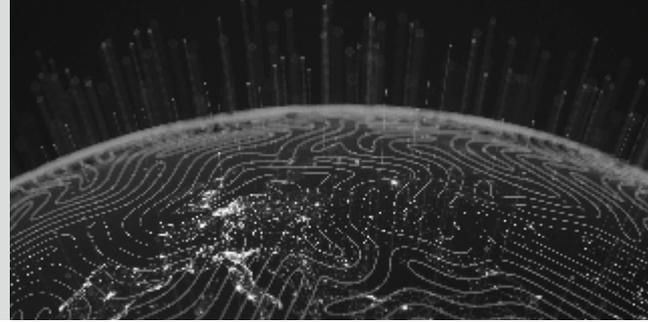
Online fraud schemes

Fraud schemes constitute the most rapidly expanding sector in organised crime, targeting a broad spectrum of victims, including individuals, public and private sector organisations, and their data, and generating large profits. The scale of online fraud, driven by advancements in automation and AI, has reached an unprecendented magnitude and is projected to continue growing. Narratives are extremely realistic, crafted with the help of AI, and incorporating trending societal topics. Cryptocurrency features prominently as a payment method and as an investment fraud product. The many victims of fraud suffer serious financial and psychological harm, and are often subject to re-victimisation. Investment fraud and business email compromise remain the most prolific online fraud schemes.
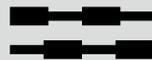
Many victims of fraud are subject to re-victimisation.

Investment fraud

Increasing threat driven by technology and AI

Investment fraud is one of the most common and growing types of online fraud, nurtured through the use of digital tools and accelerated by new technologies. The main types are Ponzi schemes[21], pyramid schemes[22], and advance fee frauds[23]. Cryptocurrencies remain the most significant investment fraud product in the EU. While fraudsters mostly target individuals, companies are also occasionally targeted. Criminal networks have been adapting the modus operandi to the availability of digital and AI tools and to exploit new and developing markets. The criminal threat is likely to further accelerate through the use and credibility of deepfakes, as well as the use of AI, machine learning, and automation.

> CASE EXAMPLE — JuicyFields large scale Ponzi scheme[24]
>
> In the "JuicyFields" investment fraud case, suspects lured victims into fraudulent crowdsourcing investments in the cultivation and distribution of cannabis for medicinal purposes. Upon the purchase of a cannabis plant, with a minimum investment of EUR 50, investors could collect high profits from the sale of marijuana to authorised buyers. The platform was not only present in the digital world, but upheld the image of a trustworthy legal business structure with physical offices, staff and representation at cannabis events. Initially, the 500 000 "e-growers", or digital growers, were receiving their investment returns.
>
> In July 2022, the criminals behind the scheme abruptly removed company profiles from social media and stopped users from logging in to their accounts, thus freezing cash withdrawals. The scheme impacted a very high number of victims throughout the EU, with a total of reported damages of around EUR 645 million, but they could be significantly higher. The criminal network had a strong cross-border dimension, led by Russian masterminds, with strawmen in Germany and money laundering activities in Cyprus.

Internet-enabled investment fraud is becoming more prominent than unsolicited contacts, like cold calling. Online advertisements, including social media platforms, news sites and sponsored search engine results are the main advertisement channels used by criminal networks to attract victims.

Online frauds, including investment frauds, are often elaborate, long-lasting, and well-crafted, creating a convincing air of legitimacy. AI and automation will further accelerate this criminal activity in the coming years.

Criminal networks perpetrating investment fraud display a high level of adaptability to socio-economic trends, new markets, media, and public interest, shifting their focus to attractive emerging products.

Investment fraudsters are extremely adaptive, adjusting their narratives to socio-economic trends and shifting their focus to attractive emerging products, ranging from cryptocurrency to cannabis.

Business email compromise

Prolific online fraud schemes expected to further increase

In business email compromise (BEC) cases, fraudsters gain unauthorised access to the mailbox of an employee to intercept and analyse information contained in official correspondence. Once email accounts are taken over, spoofed or new versions are created. Fraudsters request payment, misleading victims[25] by closely resembling corporate communication style and accompanying their request with well-crafted, identical falsified documents such as invoices containing modified bank accounts[26]. Identity theft and identity fraud are an intrinsic part of the sophisticated and targeted scheme crafted around the victim.

AI, including large language models (LLMs) and deepfakes, is creating new opportunities and capabilities for criminals active in BEC. As the rapid pace of technological development continues, BEC fraud is also expected to increase. Convincing fraud emails can be easily generated with the support of LLMs, while deepfake technologies, an emerging type of impersonation replicating people's voices, images, and videos, are now being used in CEO fraud, in which fraudsters seek to trick an organisation's employees by impersonating their CEO[27].

AI, including LLMs and deepfakes, lowers the threshold for entry in the criminal market, and drives new opportunities for BEC fraud and other online frauds. This is set to continue alongside rapid technological development.

Romance fraud

Lucrative online fraud scheme relying on profiling and social engineering techniques with enhanced realism foreseen

Criminal actors from around the globe are actively involved in romance fraud. Victims seeking companionship are approached on social media or dating sites by fraudsters, who impersonate individuals using fake accounts and profiles.

Criminals often adapt their fraudulent requests to the changing geopolitical situation, for instance, requesting money under the pretext of being victims of current conflicts or humanitarian crises. Unsuspecting victims are defrauded by being persuaded to provide financial and personal information, or to directly transfer money based on false pretexts. Targeted individuals may even be manipulated into acting as money mules. Identity theft and sexual extortion are also linked in some cases.

Romance fraud remains a lucrative online scheme, and is perpetrated mostly on dating sites, social media, and communication platforms. Criminal networks and fraudsters employ profiling and social engineering techniques to create a rapport with victims and increase profits.

Romance scams are expected to increase in the future, accelerated by AI tools. Voice cloning technology, deepfakes, LLM-generated scripts, and AI-driven translation will all continue to enhance fraudulent schemes, creating new fake scenarios and social engineering techniques.

Fraud against payment systems

High level of expertise, variation and continuous development of techniques with the future threat driven by adaptability

While physical skimming on bank and credit cards is rapidly diminishing in the EU, digital skimming through specific malware became more widespread[28]. Compromised card details are sold and purchased, often several times, on websites and dark web marketplaces. These are then used, for instance, in card-not-present (CNP) fraud performed by bots carrying out parallel automated purchases. There has been a major shift in digital skimming from targeting the front-end systems (such as webpages and browsers) to infecting the back-end infrastructure (server) with malware. Criminals use SIM swapping to overcome customer authentication methods.

The theft of personal data from payment systems is the main concern. Data is exploited directly or sold to other criminal actors, resulting in repeated victimisation of targets.

The fast and ongoing digitalisation of payment systems, resulting in novel payment gateways, will present new opportunities to criminal networks and require constant updates in security systems and relevant regulatory measures[29].

The modi operandi of criminal actors to defraud payment systems will continue to evolve based on further digitalisation of payment systems and fin tech developments.

Criminal actors involved in the perpetration of fraud against payment systems display high levels of expertise as it requires the development of specific malware, up-to-date knowledge of payment systems and their vulnerabilities, and the production of complex technical devices. In some cases, criminal actors who compromise payment systems also carry out cyber-attacks on other networks.
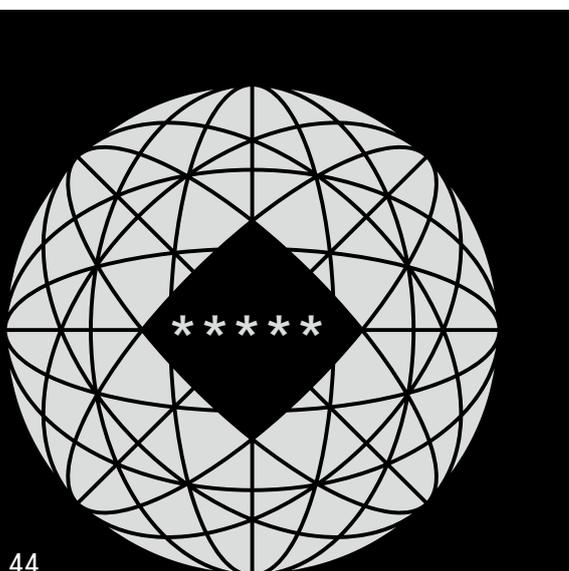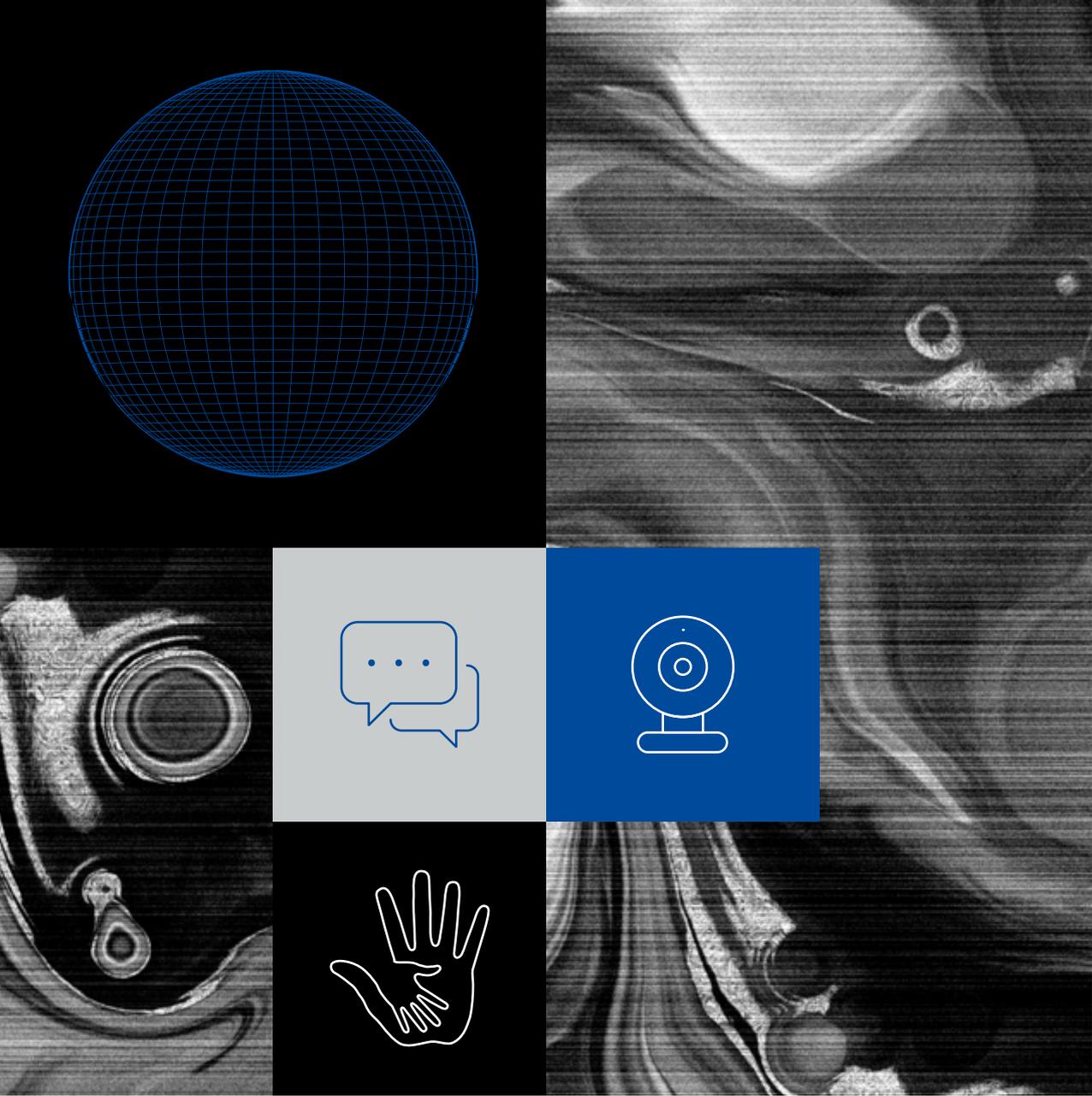
(Online) child sexual exploitation

Child sexual exploitation is a severe and impactful crime as it involves physical and psychological violence on children, heavily impacting their health and development. It is nurtured online, with online platforms providing offenders with an ever-expanding victim base to carry out sexually explicit interactions or exchange imagery within communities of offenders. It is and will be further accelerated by AI, expediting the generation of material and stepping up the scale.
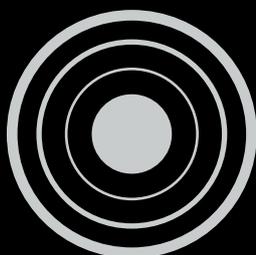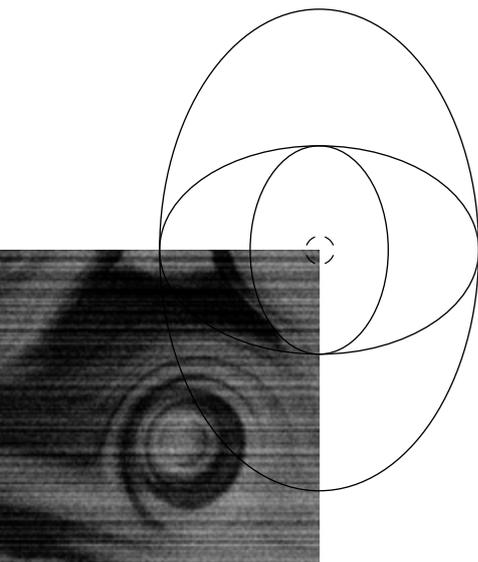
Rapid evolution driven by advancements in digital technology and generative AI

Online child sexual exploitation (CSE) offences have increased in recent years, with a significant rise in the volume of child sexual abuse material (CSAM) detected online, as well as referrals and investigations. The production and distribution of CSAM is expected to grow in the future.

The exchange of CSAM appears to be much more frequent than in the past, likely due to the ease of use and large storage space in mobile phones, which have become the main device for the production, acquisition, and storage of CSAM. It is also increasing in severity, both in terms of the nature of the abuse and the age of victims.

The increase in online CSE has been driven by rapid advancements in digital technologies. Most children, even very young ones, use social media and communication applications, offering ample opportunity for predators to approach their victims. The use of social media in an age characterised by self-discovery and experimentation, combined with the normalisation of online sexual behaviours (such as sexting), has contributed to the proliferation of self-generated sexual material. Sexual extortion is another ever-increasing threat.

The digital acceleration has triggered a rapid evolution in online CSE. It has provided borderless platforms for offenders to create, store and exchange CSAM, and to contact and groom victims. The increased online presence of children will impact further on offenders' approaches to, and grooming and exploitation of, children.

End-to-end encrypted communication applications have created cross-border networking possibilities for offenders, both for smaller networks such as transnational child sex offenders (TCSOs)[30] and large online communities.

Generative AI has emerged as a new means to produce CSAM, leading to growing concerns. It can support the editing of existing CSAM and the creation of new content. Explicit pictures of adults can be manipulated to make the individual look younger or applications can 'nudify' non-explicit images. Text-to-video models have emerged, following the rapid development of text-to-image models. Given their pace of advancement, text-to-video technology is likely to evolve just as quickly[31]. In one of the first cases of its kind, a suspect was recently arrested for running an online platform with AI generated CSAM which he produced and shared around the world[32].
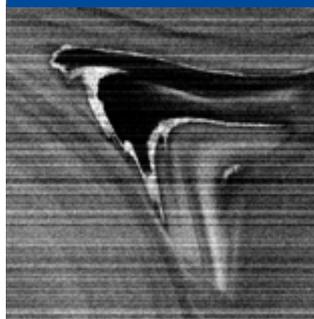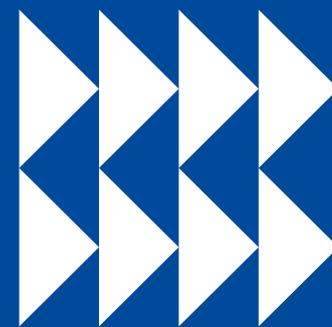
Synthetic AI-generated child sexual abuse material (CSAM) multiplies the volume of such material online.

SEVERE VIOLENCE INFLICTING SERIOUS HARM, AND RE-VICTIMISATION

```
CASE EXAMPLE — Symbolic monthly subscription to fully AI-generated CSAM[33]

In one of the first cases involving fully AI-generated child sexual abuse material, in February
2025, 25 arrests were made worldwide. The main suspect, a Danish national, ran an online
platform where he distributed the AI-generated material he produced. Following a symbolic online
payment, users from around the world were able to obtain a password to access the platform and
the high-quality AI-generated CSAM. He was posting non-explicit AI-generated images of children
on social media, including a link to his surface website where there would be teasers of
CSAM material. The membership also gave access to exclusive communities of AI offenders. This
community had around 1 500 subscribing members who were exchanging tips on how to best exploit
technology to obtain CSAM and how to avoid detection.
```

The accessibility of AI tools has transformed the CSE landscape. Synthetic AI-generated CSAM multiplies the volume of such material online, creating additional challenges in the analysis of imagery for victims and offenders identification.

Criminal actors

Given the large spectrum of offences constituting CSE, a wide range of offenders — with diverse profiles and different motivations — are involved in this criminal activity. Hands-on abusers, producers, distributors, and consumers of CSAM are mostly motivated by their sexual interest towards children. Criminal actors involved in financial sexual extortion and professional production of CSAM for commercialisation often show no sexual interest in children and are motivated solely by financial gain.

A variety of groups leverage digital platforms to normalise acts of extreme cruelty, extort victims, share CSAM, and radicalise individuals into violent extremism.

CSE offenders are becoming increasingly tech-savvy, highly aware of the security measures they can apply to protect their identities and able to rapidly adapt to changes. Most of them have the skills to develop very sophisticated countermeasures to avoid or deceive law enforcement investigations.

IT solutions for encrypted communication, streaming, file exchange as well as AI tools will enhance offenders' countermeasures and shift CSAM production methods.

The majority of offenders take part in online communities on the dark web and clear web, including forums, groups, and chatrooms. They discuss abuse, fantasies, how to acquire original CSAM, techniques to groom children and tips related to operational security. Offenders also use online means other than chatrooms for one-on-one interactions, with different levels of encryption and data transfer methods. Closed online groups on end-to-end encrypted communication applications are often international, with some having a large and long-term membership base.

Offenders who engage in direct abuse vary in profiles, ranging from middle-to-late-age perpetrators with direct access to children — either by profession or family ties — to offenders who are underage themselves. Many exhibit little to no understanding of the harm they are causing to their victims. In many cases, they describe their relationship with victims as one of love and care and do not perceive themselves as a threat to the child. Hands-on abusers are characterised by an extremely high level of recidivism.

The use of physical and psychological violence, including torture, for a prolonged duration heavily impacts the health and development of victims.
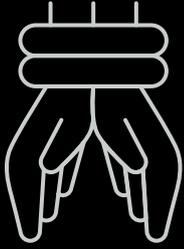
Trafficking in human beings

Trafficking in human beings (THB), for sexual or labour exploitation in particular, remains a substantial criminal market within the EU and its Member States. It is a phenomenon with global interconnections and increasingly nurtured by the online domain. It usually takes place within closed communities or environments. Criminal networks tailor modi operandi to evade law enforcement detection while increasing profits, and victims are manipulated so that they seldom consider themselves to be a victim. Yet, trafficking in human beings profoundly impacts the physical and mental health of numerous victims.

Driven into the shadows by the online domain and criminal networks' manipulation tactics

In a crime area where individuals are exploited as a commodity, criminal networks target and deceive people who are in a vulnerable position because of their security, economic or personal situation. Economic hardship and geopolitical conflict and instability drive the supply side of THB. Economic inequalities cause many victims to fall prey to traffickers' deceptive promises of better jobs and living conditions. Poverty and a lack of employment opportunities heighten this vulnerability, which is further exacerbated by geopolitical crises that may push people to seek opportunities outside their countries of origin. Combined with sustained demand for cheap labour, sexual services or other exploitative circumstances, THB is, and is expected to remain, a persistent phenomenon.

The online dimension and technological developments are central to orchestrating different forms of THB and driving them into the shadows of the criminal world. Criminal networks remotely identify and recruit their victims over the internet and social media, reach out to a wide customer base, avoid physical contact with victims and clients, and exchange their criminal earnings electronically, including using cryptocurrencies. The online space, including social media platforms, encrypted messaging services and online services, is also used for circulating pictures of travel and identity documents and the personal data of possible victims of trafficking to be inserted in a future forged/counterfeited document. Document and identity fraud remains a relevant part of the modus operandi of criminal networks involved in THB.

Criminal networks tailor their modi operandi to remain invisible and manipulate victims so that they do not consider themselves as victims.

Victims often endure forced labour, sexual exploitation, and other forms of exploitation and abuse, leading to long-term trauma. Criminal networks use psychological intimidation and manipulation to coerce victims into exploitation; the use of physical violence is less common. The so-called lover boy method — often used by young traffickers — along with debt bondage, abusing the victims' fears, and framing the exploitation as a form of assistance, are all examples of psychological manipulation. Such tactics bind victims to their traffickers and make it hard to prove the exploitation. These are often combined with the dispossession of identity documents and phones.

Trafficking in human beings is being further driven into the shadows, as traffickers increasingly use modi operandi that evade attention and that create the appearance of legitimacy. They deceive victims by encouraging them to voluntarily enter into an alleged business agreement, according to which the profits are divided between the victims and the traffickers. In this way, the criminals try to give the victims the feeling to not perceive themselves as victims of a crime. In some cases, the victims are presented with contracts that create the appearance of legitimacy for the criminals themselves and for the services the victims ultimately deliver.

The online dimension has become crucial in the organisation of the criminal process of trafficking in human beings.

Legal business structures are misused frequently for the exploitation of victims of THB. Victims of sexual exploitation are exploited in short stay accommodations, hotels, massage parlours, night clubs. Victims of labour exploitation are exploited in nail salons, shops, hospitality, construction, agriculture, etc.[34]. These businesses are sometimes owned by members of the criminal networks. Criminal networks cooperate with employment agencies and sub-contracting companies to provide a façade of legality and provide contracts and paperwork including victims' work visas and other immigration documents.

Global inequalities will continue to be a driver for criminal networks seeking to make profit. Both demand and supply of sexual services, cheap labour and other forms of THB will remain high. Ongoing conflicts in the EU's neighbourhood and beyond continue to offer favourable environments for recruiting victims. Similarly, unaccompanied minors travelling to and through the EU and its Member States will remain vulnerable to criminal exploitation in whatever form.

Criminal networks

Adaptability is a key characteristic of criminal networks involved in THB. Examples are the shift of sexual exploitation to private facilities since the pandemic and the movement of victims between various cities and countries to avoid detection and prosecution. Social media platforms, some specific for certain communities, are used to recruit victims and to coordinate the criminal business. Criminal networks are running several groups at the same time to communicate with victims, clients, and associates separately. Victims also exchange information, experiences, and the possibility to work in other countries on social media groups administered by criminal networks.

Criminal networks continue to distance themselves from the actual exploitation, managing and coordinating the criminal business, including the transfer of criminal proceeds, remotely.

Both criminal actors and victims of THB originate from within and outside the EU. There is often a link between the nationality of criminal network members and the victims.

```
CASE EXAMPLE – Chinese criminal network
involved in THB for sexual exploitation[35]

A Chinese criminal network recruited Chinese
victims using online platforms and instant
messaging apps promising them a legitimate
job and the possibility to rapidly earn a
lot. After the recruitment, victims were
trafficked to Europe using fraudulent EU
identity and travel documents. In Europe,
members of the criminal network advertised
the sexual services of the victims online
and exploited them in hotels across Europe,
rotating the victims between many countries,
to elude law enforcement detection and meet
the growing demand for sexual services. The
criminal network had various branches in
several EU Member States that coordinated
the exploitation of the victims on instant
messaging apps. Some members were dedicated
to the recruitment and trafficking of
victims while others managed their actual
sexual exploitation.
```
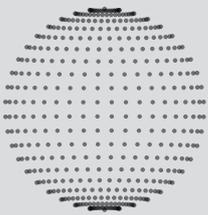
The instrumentalisation of irregular migrants' vulnerable situation for geopolitical motives may provide additional peaks in opportunities for migrant smuggling services.
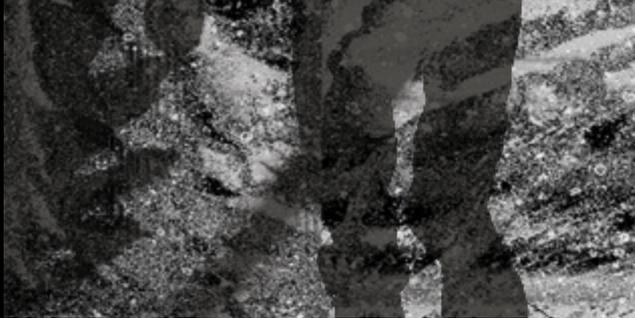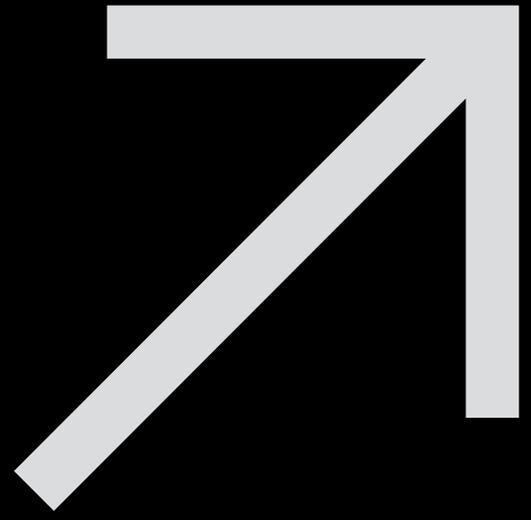
Migrant smuggling

Migrant smuggling persists as an attractive and profitable criminal business. It is subject to multiple global push and pull factors, and affects all Member States either as entry point, transit, and/or destination. Migrant smugglers respond quickly to changes in the environment, leading to re-routings or changes in modus operandi. The DNA of serious and organised crime shows strongly in migrant smuggling — the presence of hybrid threats in this crime area has the strong potential to destabilise societies, and it is being nurtured through digital tools driving operations.

The loss of life related to migrant smuggling is high. Violence and recklessness increasingly characterise migrant smuggling.
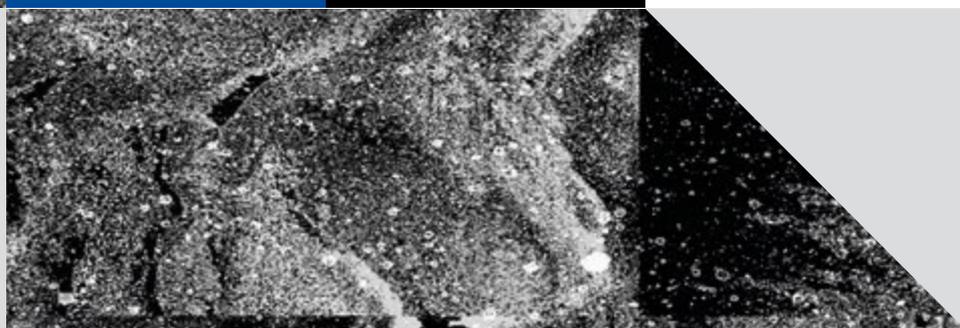
Persisting and fluctuating flows

Migrant smuggling continues at a large scale. This criminal business is incessant and moves geographically according to demand, opportunities and/or obstacles. It involves a large number of criminal networks that facilitate the irregular migration or stay of a large number of customers who are treated with little regard for human dignity.

Migrant smuggling affects the EU as a whole as it involves facilitation of entry, secondary movements, exit, and legalisation of stay.

Criminal networks facilitate irregular migrants' entry into, secondary movements within, and/or exit out of the EU, and this by land, sea, air, or a combination. It may also entail the fraudulent legalisation of irregular migrants' residence status.

While routes and modi operandi show ad hoc shifts in response to changes in demand and supply, they remain largely the same over time. For entry into the EU, migrant smuggling criminal networks are active along the Central, Eastern, Western Mediterranean and Western African routes by sea.

Migrant smuggling services into the EU by land concentrate along the Eastern Mediterranean land routes and onwards via the Western Balkan routes, and with fluctuating peaks along the Eastern land routes. Members of criminal networks either act as guides while crossing the green borders or provide instructions remotely. Irregular migrants are smuggled in passenger vehicles including in rental vehicles, busses, small commercial vehicles, and in lorries (hidden among commodities, but also in fuel tanks, between the cabin and the trailer, or on the trailer).

Facilitated secondary movements within the EU remain a key criminal business, either departing from irregular migrants' first countries of arrival or from Member States where they were temporarily residing, and are overall multi-directional throughout the EU. Facilitated secondary movements may entail land and/or air transport, and along the route, irregular migrants may be held in safehouses.

The EU also serves as a departure point towards other destinations. Criminal networks organise the exit of the EU towards the United Kingdom, predominantly through crossings of the English Channel in small boats. Some criminal networks have specialised in the provision of nautical equipment for these crossings. The EU also functions as a transit for migrant smuggling by air, mostly to North America.

In addition to facilitating the entry, transit or exit of irregular migrants, an important component of migrant smuggling entails the facilitation of irregular migrants' fraudulent legalisation of stay. Common modi operandi include the misuse of visa, marriages of convenience, the use of fraudulent breeder documents (including fraudulent invitation letters) to obtain genuine documents, false declarations of paternity, and the misuse of applications for international protection. Document fraud is a key enabler in this context, as it is for migrant smuggling by air.

Hybrid threat link and digitalisation

Migrant smuggling services are shaped by the interplay of a broad range of push and pull factors[36]. The instrumentalisation of migration has become a highly visible new factor at play today and is expected to further expand in the future. This is a further consequence of the Russian war of aggression against Ukraine and its implications for the regional and global geopolitical situation. Hybrid threat actors misuse the migratory situation to destabilise the EU and its Member States, thereby also providing additional business opportunities to criminal players in the field.

While migrant smuggling is, for a large part, inherently a physical cross-border crime, it is and will be further accelerated by digital and technological developments. As well as its reliance on online platforms for marketing, recruitment, communication and money transfers, specific to migrant smuggling is also the misuse of online applications to organise journeys (such as booking accommodation or mapping out routes to provide to the irregular migrants). The advertising strategies of migrant smuggling criminal networks are increasingly professional, showcasing successful crossings — across multiple social media platforms in parallel — to promote their services to potential migrants.

Against the backdrop of today's volatile and uncertain global context, migrant smuggling is expected to remain a profit-making criminal business. Demand is likely to remain high as migratory flows — due to economic, geopolitical, conflict, environmental or other reasons — will continue to be directed towards or via the EU. The migrant smuggling landscape may become even more volatile, unpredictable or large-scale if irregular migrants continue to be instrumentalised by hybrid threat actors to destabilise society. Current conflicts may continue in the long term or may spread to larger regions, triggering additional displacements in the Middle East, Africa or the EU's eastern neighbourhood.

The instrumentalisation of irregular migrants' vulnerable situation for geopolitical motives may provide additional peaks in opportunities for migrant smuggling services.

```
CASE EXAMPLE — Migrant smuggling via Russia
and Belarus to the EU[37]

A criminal network smuggled irregular
migrants from Iraq via Türkiye, Russia and
Belarus to northern European countries
with onwards facilitated secondary
movements towards Germany and the United
Kingdom, the main destination countries.
The criminal network adapted the modus
operandi and smuggling route quickly,
depending on different factors such as visa
regulations, natural conditions on the route
and taking advantage of the geopolitical
situation. The smuggling activities were
coordinated among different parts of the
criminal network operating along the route.
Irregular migrants paid between EUR 3 000
and EUR 5 000 per person, depending on
the provided services, directly to hawala
offices, also in cryptocurrencies.
```

The threat of migrant smuggling is particularly exacerbated by the high degree of adaptability and opportunism that has long characterised criminal networks active in this illicit business. The supply of migrant smuggling services is constantly adapting to the dynamics of irregular migration flows or the response thereto. Such adaptability also contributes to the resilience of criminal networks against law enforcement or criminal competition.

Criminal networks continuously respond to opportunities and challenges by shifting routes, modi operandi, and offering crime as-a-service.

Significant security, economic and social implications

Migrant smuggling has a high impact on the EU and its Member States, as it is a complex challenge that combines security threats with social implications. The vast migration flows, in which organised crime facilitation plays a key role, place a huge strain on border management systems and require significant investments from law enforcement and other authorities. Particularly for journeys over sea and land, criminal networks consider their clients as commodities, lacking human dignity. Testament to this is the overcrowding of sea vessels entering and exiting the EU and of vehicles entering or transporting irregular migrants through the region.

The loss of life related to migrant smuggling is high. Violence and recklessness increasingly characterise migrant smuggling. Violence targets competing criminal actors, law enforcement officials, and irregular migrants.
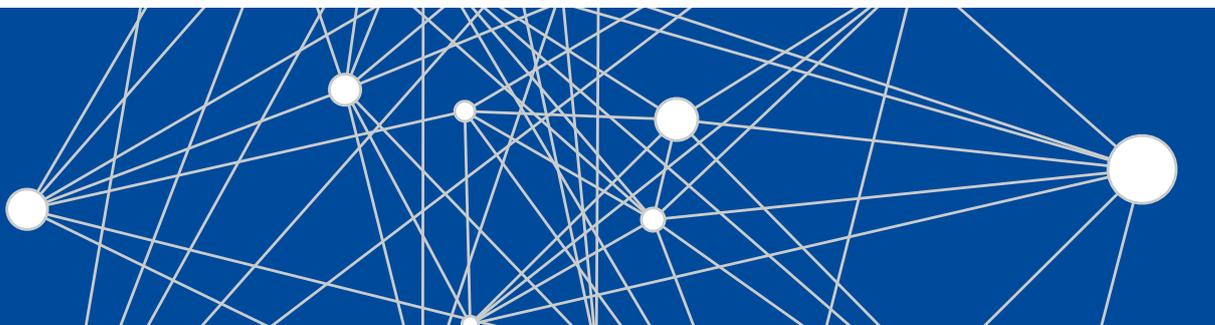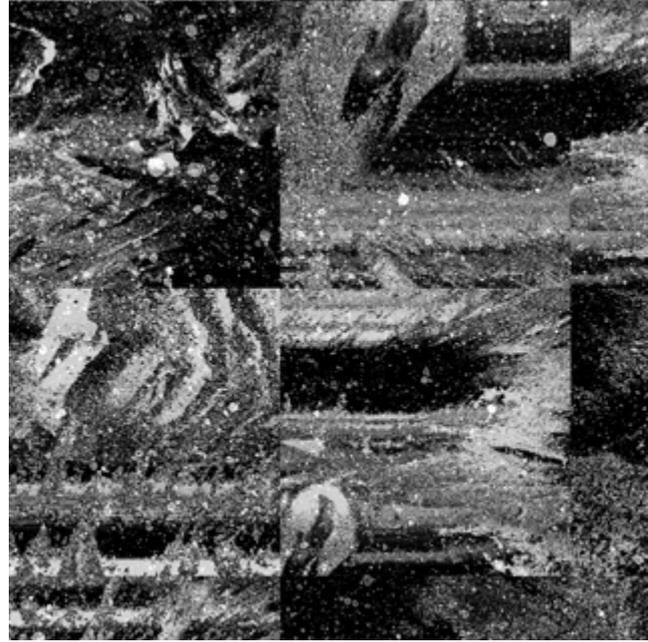
The EU holds a multifaceted position, with combined roles of import, production, processing, distribution, transit, and export of illicit drugs.

The trade in illicit drugs

Drug trafficking is a dynamic global criminal business, affecting all Member States. The threat posed by drug trafficking networks has increased and will continue to do so. Both demand and supply of most types of drugs are high, as are the illicit profits criminal networks can make. The impact of drug production and trafficking — in particular on health and the environment — is substantial. Using tools such as corruption, violence, and money laundering, drug trafficking networks destabilise society and undermine legal economies and trust in institutions.

The possible further spread of dangerous synthetic opioids is a concern and must be closely monitored.

Recent fluctuations in cocaine seizures reflect a waterbed effect, leading to alternative routes and modi operandi. This could further spread drug-related violence.

Dynamic criminal market with high demand and supply and a multitude of actors

The European illicit drug market is characterised by the widespread availability of a broad range of drugs, with substances often available at high potency or purity in new forms, mixtures or combinations[38]. The drug market is constantly developing. Chemical innovations lead to the production of novel drugs or new ways of chemically concealing drugs. The application of technological and digital innovation conceals communications and broadens drug retail channels.

Drug trafficking affects the whole of the EU. It is highly profitable and attractive, but also competitive. Drug trafficking criminal networks demonstrate the most threatening characteristics, such as the misuse of trade infrastructure and legal businesses, the use of (technological) countermeasures, and the willingness to engage in corruption and violence[39].

The illicit drug market is a global and dynamic criminal market, with continuously adapting routes and modi operandi.

The EU is a source, transit and destination region for various types of drugs. Cannabis herb and synthetic drugs are produced on a large scale within the EU, for local markets and for export abroad. Other drugs, such as cocaine, are imported into the EU, sometimes as intermediate products, with final processing within the EU before local distribution or export to non-EU markets.

The EU holds a multifaceted position in the drugs landscape, with combined roles of import, production, processing, distribution, transit or export.

Drug trafficking to, from and within the EU is expected to remain a key threat to the region's internal security in the coming years, as criminal networks continue to be driven by the large profits in the drug trade. The agile and sophisticated use of new production methods, technologies, legal business structures, online tools, and trafficking modus operandi will likely continue to drive both supply and demand.

Drug trafficking is closely interwoven with the abuse of legal businesses, for transportation, for concealment among legitimate loads, and for obtaining the necessary precursors/chemicals.
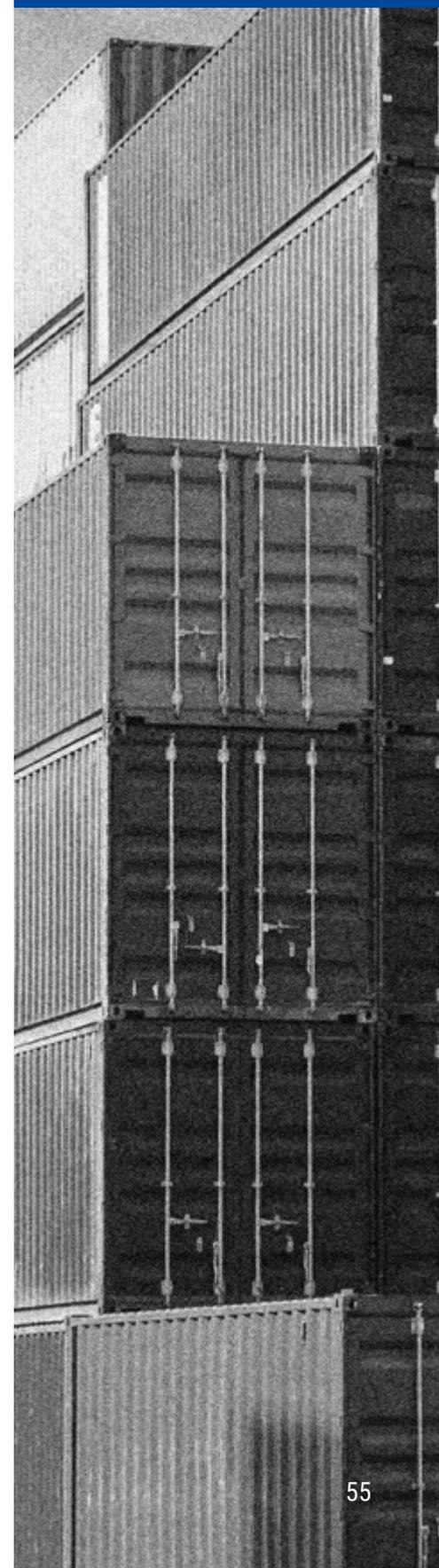
Far reaching impact with risks for citizens and opportunities for criminals

The impact of drug trafficking is far-reaching. Risks for users have increased as there is widespread availability of a broader range of drugs, often of high potency or purity, some of which have a high risk of life-threatening poisoning[40]. Additionally, drug related violence not only targets subjects in the criminal world, but also harms various other groups in society, including public officials and innocent bystanders. Violence spilling over into the public space fuels feelings of insecurity and instils fear in citizens. Drug trafficking activities also have major financial implications. With retail value running into several billion euros, drug trafficking represents a major income source for criminal networks, further strengthening their position[41]. Drug production has a significant impact on the environment as it creates large amounts of hazardous waste and damages fauna and flora.

Cocaine

Changing routes and modus operandi in a competitive and violent market

The surge in cocaine production in Latin American source countries has reached unprecedented levels, supplying the EU and its Member States with substantial quantities of the drug. This increase in production aligns with the growing demand within the EU[42] ensuring a steady influx of cocaine into European markets. This stable market equilibrium ensures that cocaine trafficking remains a highly profitable activity, making the cocaine market an attractive prospect for criminal networks.

Cocaine trafficking to the EU has become increasingly diversified in terms of transportation methods, concealment techniques, and trafficking routes.

While there was a drop in maritime seizures in some major entry points in the EU in 2024, the volume of cocaine entering the EU has likely not decreased. Instead, trafficking routes and modi operandi are further diversifying. In Latin America, departure and transit points are shifting. Ports in various countries may further emerge as key transit points for cocaine destined for the EU. On the EU side, higher amounts were seized in some other large ports in the EU, as well as in smaller, secondary EU ports. Such a waterbed effect and further variation and displacement of drug entry points in the EU, may also bring along consequences for criminal networks' operations and their competition, potentially bringing along violent activity in more locations throughout the EU, with possible involvement of young perpetrators.

Maritime trafficking using containers remains the dominant modus operandi, especially for the transport of multi-tonne shipments of cocaine bricks. Various other types of vessels, such as sailing boats, are used too. At-sea drop offs have become a more prominent modus operandi. It is further likely that some criminal networks have shifted to trafficking smaller amounts, via multiple entry points and containers, instead of multi-ton loads in one go, spreading the risk of interception. Cocaine is also trafficked to the EU by air, both as air cargo and in person.

Cocaine trafficking to the EU has diversified in transport, concealment methods, and routes. Recent fluctuations in seizures reflect a waterbed effect, leading to alternative routings and modi operandi. This could further spread drug-related violence and drive the recruitment of young perpetrators across the EU.

Criminal networks use a variety of modi operandi to traffic cocaine to the EU. In most cases, the end product — hydrochloride salt ('cocaine powder') — is trafficked in bricks. The intermediate product, cocaine base, is also exported. The final processing then takes place in the EU. To reduce risks and optimise profits, cocaine is incorporated in various materials. It is then taken out through specific chemical procedures. Laboratories for the processing and/or extraction of cocaine are mainly found in western and southern European countries. There are indications of a further spread of cocaine extraction activities in laboratories in the EU.

```
CASE EXAMPLE — Cocaine injected in cardboard
boxes[43]

A criminal network, made up of mainly
Colombian and Spanish suspects, trafficked
cocaine, using a sophisticated method to
avoid detection. They injected cardboard
boxes containing legal cargo (such as fruit)
with cocaine base. Once successfully shipped
in maritime containers from Colombia to
Málaga (Spain), the criminal network would
extract the cocaine base from the cardboard
and process it into the final consumable
product, ready for distribution.
```

Criminal networks

The immense profits associated with cocaine trafficking present significant financial incentives, attracting numerous criminal networks—often in direct competition with one another. This competition fosters not only illicit practices but also a heightened propensity for violence and corruption, as criminal networks fight for control over profitable trafficking routes and market dominance.

Cocaine trafficking networks are often resilient — many of them have been active for more than 10 years. The most threatening ones control the entire criminal process. They either have cells in source countries or cooperate with networks based there. Networks cooperate to share resources, facilitate contacts, and coordinate steps of the criminal process. Investment groups are created to fund and share the risk of importing large quantities of cocaine. Brokers play a key role in organising large combined shipments. Latin American and European criminal networks also partner in cocaine production activities in Europe.

The profits to be made in cocaine trafficking are huge and provide incentives for many — often competing — criminal networks to engage in this business, and to commit violence and use corruption.

Cocaine trafficking networks tend to use violence more frequently and resort to more extreme forms than networks trading other types of drugs. Violence is mainly used internally, within the criminal network, to guarantee discipline and cooperation, maintain control and punish associates for deals that went wrong. Violence is also used against competitors in the market to establish and stay in power. Explosives and heavy pyrotechnics are regularly used in certain Member States, most notably to intimidate network members or carry out retaliation attacks within or between drug trafficking criminal networks. The involvement of underage perpetrators in such attacks, some as young as 13, is not uncommon.

Cocaine trafficking networks often have a global reach, allowing them to simultaneously traffic from and to different locations. Networks trafficking large volumes of cocaine via containers into ports regularly resort to corruption, paying large bribes to various key actors, to safeguard the drugs[44].

The threat posed by cocaine trafficking is likely to remain high. The huge profits will continue to attract criminals. Networks will search for more sophisticated ways to conceal cocaine, new routes to circumvent enhanced security measures in major entry ports (e.g. using smaller ports) and apply new countermeasures.

Both supply and demand are expected to remain high, attracting criminal actors from within and outside the EU, competing for a share of the profitable market.

Cannabis

Massive supply and demand generate huge profits

Cannabis remains the most commonly consumed illicit drug in Europe[45]. Cannabis trafficking has increased over the past years and it is expected to be sustained at a high level in the upcoming years.

Cannabis trafficking is expected to be sustained at a high level.

Legal and illegal markets might become increasingly intertwined.

A large variety of products is available on the illicit cannabis market in the EU, either produced locally or smuggled from other regions. Examples include cannabis oil, other high-potency extracts, edibles and vaping products. In addition, semi-synthetic cannabinoids are emerging in EU markets. Some of these products are highly potent, posing higher risks to users' health[46].

Cannabis is likely to remain the most commonly used drug in the EU, with criminal networks either focused solely on cannabis or on polydrug crime. Criminal networks will continue to diversify their trafficking routes into the EU, increasingly using a variety of entry points in the Mediterranean for smuggling cannabis resin. Taking advantage of markets where herbal cannabis has been decriminalised in various forms, it is likely that trafficking of herbal cannabis from outside the EU will increase as criminal networks seek to exploit new opportunities.

Herbal cannabis is grown in most Member States, usually indoors, albeit at different scales. Technological improvements in cannabis cultivation, such as automation or remote control, air humidity monitoring and computer-guided cultivation are a general trend.

Herbal cannabis production in the EU — both indoor and outdoor — is widespread and often large-scale. Some cannabis resin manufacturing facilities have been detected in the EU too.

There is an increase in the trafficking of herbal cannabis from countries in North America and Asia. Cannabis resin is also trafficked to the EU.

CASE EXAMPLE — Cannabis trafficked by helicopter from Morocco to Spain[47]

A criminal network used modified helicopters to traffic cannabis from Morocco to the South of Spain. Once in Spain, the drugs were trafficked to France by falsely registered vehicles of heavy good trucks. Multiple false identities were used as countermeasures and the network used shell companies to launder the profits from the illicit trafficking and trade. Profits were subsequently used to grow and advance their business, including improving and expanding the trafficking system.

Criminal networks

Criminal networks involved in cannabis cultivation regularly engage specialists for certain tasks, such as installing and managing electricity at the cultivation sites, arranging transport, and building sophisticated hidden compartments in vehicles. Some criminal networks even engage experts in the genetic manipulation of cannabis. Services for waste dumping are also sourced. The tactics of criminal networks involved in cannabis production, trafficking and distribution also include violence. The pursuit of strategic dominance and the protection of key vending points are important motives for violent clashes among competing networks.

Synthetic drugs and new psychoactive substances (NPS)

EU as global production centre and expansion within the EU

The production and trafficking of synthetic drugs have increased over the past years, and this threat is expected to further increase. Both the demand and supply of synthetic drugs are high. The misuse of legal business structures for the sourcing of necessary chemicals and equipment is a common practice. This is often done via legitimate pharmaceutical companies in the EU, without them being aware of it.

The EU is central in the global synthetic drugs landscape, with EU-based production serving both the EU and international markets.

The EU is a major source of synthetic drugs distributed on a global level. The production of synthetic drugs within the region is characterised by continuous innovation and expansion.

Production has spread to more Member States. It is often industrial scale, while there is also a proliferation of small labs.

In addition to amphetamine, methamphetamine and MDMA, the production within the EU of other types of synthetic drugs has been identified: synthetic cathinones[48] (i.e. mephedrone and alpha-PVP, also known as Flakka), synthetic cannabinoids[49] and synthetic opioids (i.e. methadone). Some of these substances are controlled throughout the EU, others are forbidden in some Member States or remain entirely uncontrolled within the EU (the so-called new psychoactive substances, or NPS).

> CASE EXAMPLE – Production of synthetic opioids and cathinones in the EU[50]
>
> In August 2024, several production sites of synthetic opioids and cathinones were dismantled in Poland and Ukraine. Amongst the detected facilities was the largest laboratory of synthetic opioids ever found in Poland, used to produce methadone in crystalline form. Additionally, 8 multi-laboratories, used for the production of synthetic cathinones (mephedrone, Alpha-PVP) and methadone, were dismantled in Poland and Ukraine. Next to the arrest of 7 members of the criminal network, 195 kilograms of methadone and 153 kilograms of Alpha-PVP were seized, together with large quantities of drug precursors and chemicals necessary for the production of synthetic opioids and cathinones.

Although the number of NPS appearing for the first time on the market has slowed down, the appearance of very potent synthetic opioids (such as nitazenes and diverted or counterfeit prescription opioids) on the EU drug market is a serious reason for concern. These substances are often sold as other products, such as heroin, or mixed with medicines. Users are not always aware of the contents of the substance they buy and use. There is an increase in reported poisonings, including deaths, involving nitazenes in various European countries[51].

The further spread of dangerous synthetic opioids, such as nitazenes or potentially fentanyl, must be closely monitored.

As it stands, reporting on the presence of fentanyl within the EU is limited. Close monitoring of this substance and other synthetic opioids remains important.

Next to synthetic opioids, other synthetic drugs such as synthetic cathinones and ketamine are also increasingly appearing on the EU drug market, generating substantial illicit profits and causing serious health risks.

Criminal networks

Synthetic drug producing criminal networks based in the EU control multiple production units throughout the EU and beyond. Some criminal networks facilitate the import of (pre)precursors from Asia and divert chemicals from legal trade to illicit drug production facilities, misusing existing legal business structures and mislabelling chemicals.

Further innovation in chemical processes and new variants of synthetic drugs are expected, driven by new technologies and use of chemical/lab experts. A further spread of production facilities throughout the EU is highly likely.

Criminal networks will continue to look for new production methods and chemicals to circumvent controls. New variants of precursors will appear on the market, and shortages of hardware may lead to other, potentially more dangerous, production methods. The variability of synthetic substances will further increase, and their production will likely continue to spread throughout the EU.

Overdoses and dangerous production methods

Synthetic drug production has a negative environmental impact as large amounts of chemical waste are generated, leading to water and soil pollution[52]. Chemical reactions and fumes can also cause air pollution, while the production and use of synthetic drugs cause serious health issues. Dangers associated with the chemical processes may kill the cooks involved and cause fires and explosions, impacting innocent neighbours. Additionally, some European countries note a high and increasing number of synthetic drug-related deaths, mainly associated with the use of synthetic opioids, and nitazenes in particular.

Heroin

Sustained demand with shifts in supply and suppliers, as well as to other illicit drugs

The heroin trafficking market has been subject to a shifting context. Both demand and supply are sustained at a low level in most Member States, but the impact on health is high. Heroin is the most frequently used illicit opioid in the EU and the drug causing the highest levels of dependence, health issues, and mortality[53].

The long-term impact of the Taliban's April 2022 poppy cultivation ban on heroin availability in the EU remains uncertain. Should the poppy ban in Afghanistan remain in force, there will likely be an increase in heroin produced in other countries being trafficked to the EU. It is also possible that dangerous synthetic opioids, such as nitazines, will spread in the EU, as a replacement for heroin.

The heroin trafficking criminal business is shifting in light of the uncertainties on the effect of the Afghan opium ban and consequent uncertainties with regard to supply.

Occasionally, the final steps of the heroin production process (the conversion of morphine into heroin, cutting and packaging) take place within the EU, mainly in western European countries.

Criminal networks

Heroin trafficking criminal networks are typically rather small, hierarchically structured or relatively tightly organised, and centred around families or clans. The use of violence is less common than in other drug trafficking networks. This may be because heroin trafficking is controlled by fewer and more homogeneous groups, reducing the risk of conflicts.

Heroin and other opioids have the highest levels of dependence, health problems and mortality.

The trade in illegal firearms and explosives

Firearms and explosives trafficking poses a critical threat to the internal security of the EU, with recent trends indicating changing black market dynamics. Illicit firearms and explosives enable other forms of serious and organised crime and reinforce related violence. Concerns of Ukraine emerging as a significant source of illicit firearms persist. Privately manufactured firearms and the large-scale production of counterfeit weapons feature prominently. AI technologies are expected to make weapon production more accessible and precise.

Firearms trafficking is a security threat on its own, but even more so due to its enabling role in other criminal activities.
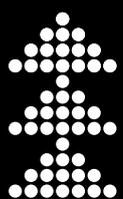
The Western Balkan region continues to be a key source of illicit firearms trafficked into the EU; however, other conflict zones, such as Ukraine, may similarly emerge as significant sources of firearms trafficking.

Changing illicit market dynamics with further increase driven by changes in sourcing and technology

Activities related to firearms and explosives trafficking remain a critical issue in the EU. There are indications of changing black market dynamics, manifested by criminals tapping into alternative sources of illicit firearms. The severity of violence caused by illicit firearms and explosives has increased, and so has the frequency of shootings and bombings in the criminal milieu. Technological as well as geopolitical developments also impact and facilitate the illicit production and trafficking of weapons in and to the EU. These factors suggest an evolving landscape of firearms trafficking, posing increased security risks across the EU.

Both demand and supply of trafficked firearms and explosives remain high. Demand for firearms persists because they enable serious and organised crime-related violence and other forms of serious and organised crime, such as drug trafficking, extortion and racketeering, armed robberies, migrant smuggling and street gang activities.

Firearms trafficking is a security threat on its own, and it also enables other criminal activities, such as drug trafficking, extortion and racketeering.

Geopolitical instabilities will continue to significantly influence firearms trafficking. While large-scale detections of weapons smuggled from Ukraine remain limited since the escalation of the Russian war of aggression against Ukraine, concerns persist about Ukraine becoming a significant source of illicit firearms and ammunition (including also the drones developed in this context) in the short to medium-term. This risk is exacerbated by legacy weapon stocks from past conflicts and established criminal networks capable of exploiting such resources. The Western Balkans for example remain a crucial source region for illicit firearms trafficking into the EU. Similarly, the geopolitical instability in the Middle East may facilitate the trafficking of weapons from the region.

AI will enhance access to and the precision of weapon designs for 3D printed weapons, facilitate the production of homemade metal firearm parts and explosives, and make knowledge of weapon conversion and modification more readily available. The use of online trade for the trafficking of firearms, components, ammunition, and explosives, both on the surface and the dark web, is expected to become more significant.

Advancing technologies are likely to further scale up the volume of 3D printed and counterfeit firearms.

EU-SOCTA 2025
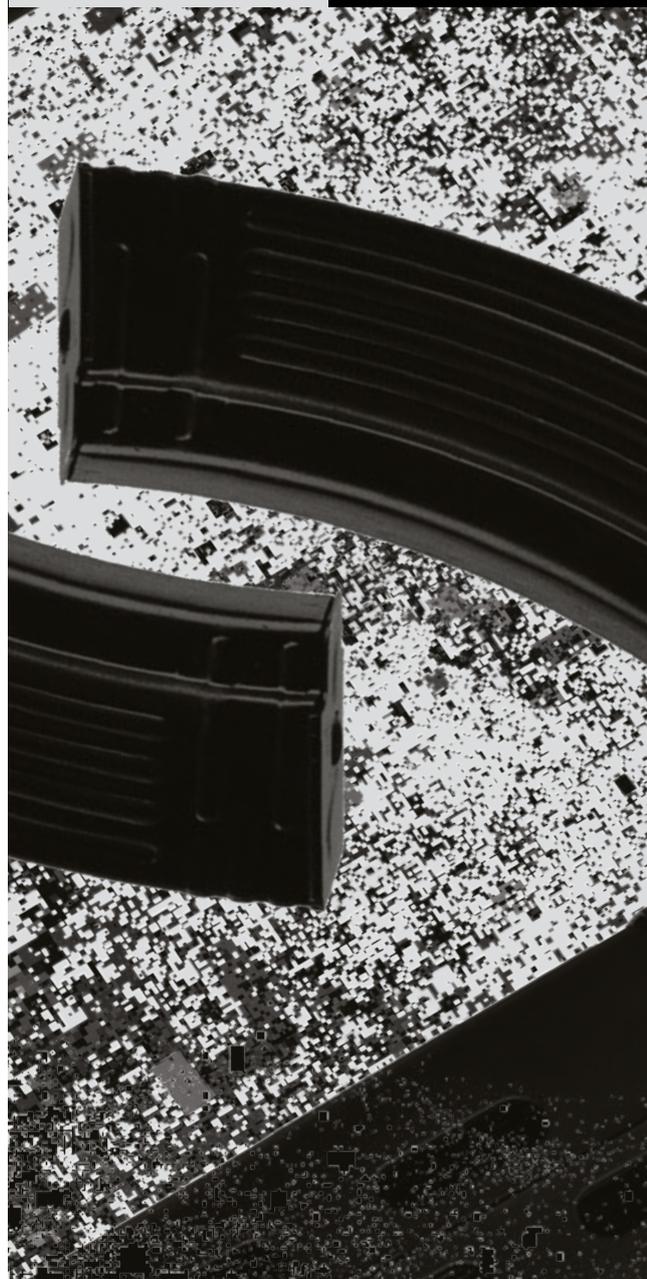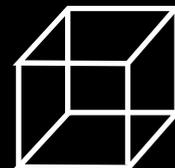
Advancing technologies are likely to further scale up the volume and sophistication of 3D printed and counterfeit firearms and components.

Air/gas and alarm/signal weapons converted into live-firing ones in and outside of the EU, and firearms trafficked from weapon stockpiles from the vicinity of the EU remain significant sources of illicit firearms trafficked to the EU.

Likely linked to the more restricted availability of Flobert-type weapons, firearm traffickers have tapped into alternative sources of illegal firearms. This includes privately manufactured firearms. Firearms traffickers assemble weapons from components, such as slides, barrels, receivers/frames, that are freely available without a licence in certain Member States and outside of the EU, and can be often freely purchased online.

The range of sources and types of illicit firearms circulating on the EU black market has broadened, highlighting the adaptability of firearms traffickers. More frequently emerging illicit firearms include privately manufactured firearms (assembled combining legal with fake or fraudulently sourced components as well as 3D printed firearms), and counterfeit or falsely branded firearms.

In the context of privately manufactured firearms, the phenomenon of 3D printed firearms and components appears to have intensified, exacerbated by the ease of access to printing machines and computer-aided design plans freely circulating on the internet.

Counterfeit firearms — illegally manufactured on a large, likely industrial scale — have become another significant source of illicitly circulating firearms in the EU.

Illicitly sourced heavy pyrotechnics appear to have become a preferred choice for criminal networks to use as explosives and as components in explosive devices. Trafficking in heavy pyrotechnics facilitates ATM attacks and serious and organised crime-related violence. Heavy pyrotechnics have been used in incidents related to violent extremism and featured in terrorism-related propaganda and plots.

Trafficked heavy pyrotechnics enable multiple forms of serious and organised crime, and terrorism and violent extremism. Trafficked firearms enable violence among and within criminal networks. Spill-over of organised crime related violence into public spaces mentally and physically harms EU citizens and instils fear in society.

```
CASE EXAMPLE — Assembled firearms sold to
contract killers[54]

In 2024, a man was arrested in Poland while
transporting weapon kits he had purchased in
Austria. The suspect assembled and completed
the weapons with missing parts in Poland,
before selling them to criminal networks
operating across the EU. He sold dozens of
illegal weapons, including automatic guns
and pistols. A violent gang allegedly used
weapons sold by the suspect to carry out
contract killings in Sweden.
```

Environmental crime

Environmental crime, particularly waste and pollution crimes, poses a critical threat to our natural environment and economies. Waste trafficking is intensifying with a projected further growth in scale and sophistication. The illicit market of trafficked wildlife remains largely stable with a potential shift foreseen in trafficked specimens and growing online trade.

EU-SOCTA 2025
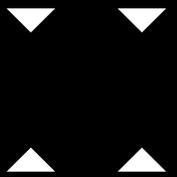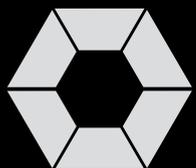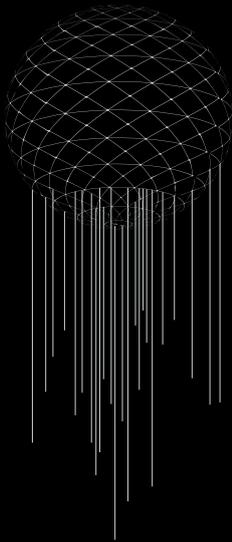
Waste and pollution crime

Intensifying waste trafficking and pollution crimes

Waste trafficking is sustained by the immense amounts of waste generated on a global basis. It is expected to increase further in the coming years. Law enforcement authorities in and outside the EU have observed a growing number of violations related to waste trafficking procedures and pollution crime in recent years. Although more stringent rules and regulations are being introduced to protect our environment, waste and pollution crimes are expected to grow in scale and sophistication.

> CASE EXAMPLE — Illegal disposal of hazardous waste[55]
>
> A criminal network orchestrated the illegal import of hazardous waste from Italy, Slovenia and Germany to Croatia. Instead of being properly treated and disposed of, the waste was simply buried or dumped in at least three locations. By disposing of medical or hazardous waste in Croatia without having treated it in any way, the criminal network saved the costs associated with this procedure and pocketed the difference. It is estimated that at least 35 000 tonnes of waste were illegally disposed of in this manner, generating a profit of at least EUR 4 million for the criminals.

As countries increasingly adopt circular economy principles and promote resource recovery, criminals may exploit loopholes in recycling and waste recovery systems to divert materials for illegal purposes. Common types of trafficked waste include Waste Electrical and Electronic Equipment, plastics and vehicle parts. End-of-life electric vehicle batteries may be trafficked to illicitly extract valuable components.

Waste trafficking is increasingly committed from within the waste management sector, blurring the lines between licit and illicit operations.

Criminal networks involved in fluorinated gas (F-gas) fraud may also take advantage of the steep reduction in the amounts of hydrofluorocarbons that importers and producers may place on the EU-market. Prevailing high demand for these products may motivate criminal networks to find new avenues to enable their illicit trade.

Waste and pollution crimes are nurtured online. Digital infrastructure such as websites, online platforms, and marketplaces are used to advertise illicit products or services. Certain websites are used by management companies or brokers based in the EU to contact their counterparts outside of the region, who also post advertisements on the kind of waste and the quantities they wish to receive.

Criminal actors involved in waste trafficking: opportunistic legal business owners and operators

Criminal networks involved in waste trafficking comprise a variety of nationalities. In the past, waste crimes were mainly perpetrated by criminal networks dumping waste on behalf of legal operators. Today many of them are opportunistic legal business owners and operators who complement their legal activities with illicit ones.

Criminal actors active in the waste management sector possess a high level of expertise as they are aware of waste regulations and the different ways of modifying waste codes and accompanying documents. Operating from the legal waste management sector allows criminal networks to set up new trafficking companies when needed, taking control of the entire waste management chain. Corruption and document fraud are significant enablers of these illicit operations.

Waste brokers have come to occupy a crucial role in the waste trafficking process, connecting producers of waste with final disposers. They facilitate the acquisition of fraudulent authorisations and documents, often inflating the price of waste, taking a cut, or completely misdescribing it.

Trafficked and improperly treated and/or dumped waste pollutes land, water and air, causing lasting damage to the natural environment.

Wildlife crime

Stable market — potential shift in illicitly traded species and growing online trade

Wildlife crimes have remained largely stable, with wildlife trafficking activities sustaining through the continuous demand and supply, both in the EU and overseas consumer markets.

Wildlife traffickers trade a variety of protected fauna and flora specimens. This includes non-CITES-listed wildlife, which traffickers have been increasingly turning to, to avoid law enforcement attention. In addition to endangered species, traffickers unlawfully smuggle pets without proper documentation and veterinary approval, advertising them online. Criminal actors also engage in the illegal trade of horses of dubious origin to illegally introduce them into the food chain.

Wildlife traffickers trade in a variety of endangered and protected species, turning increasingly to non-CITES-listed specimens to avoid attention from law enforcement.

The trafficking of glass eels remains one of the most substantial and lucrative illegal trades of protected species across the globe, with illegal profits estimated to be up to EUR 3 billion in peak years.

One of the most harmful forms of illegal, unreported, and unregulated crimes is related to the fishing of bluefin tuna in the Mediterranean Sea. The illegal fishing of mollusc species also generates profits of several million euros per year.

Wildlife is trafficked from, to and through the EU. Wildlife originating from other geographical locations, such as Africa, the Americas, and the Middle East, is also targeted and traded to European buyers.

The EU is a source, destination and transit hub for endemic wildlife trafficking.

Due to increasing awareness of biodiversity loss and environmental conservation, consumer preferences may shift and traffickers may adapt accordingly. Traffickers may target lesser-known species or products with high commercial value. The use of digital platforms, particularly social media and e-commerce, will continue to grow as a marketplace for wildlife trafficking.

Criminal actors possessing high levels of expertise

Criminal networks active in wildlife crime are characterised by high levels of expertise, with specialists in veterinary science, chemistry, and biology either part of networks or offering their knowledge on a crime-as-a-service basis. This knowledge is combined with a strong understanding of the market, access to a relevant network of buyers and sellers, and awareness of the regulations and market dynamics.

For the trafficking of some wildlife specimens to Asia through the EU, EU-based criminal networks work closely with Asian criminal networks, especially for the illegal trade in glass eels.

Organised property crime

Most forms of organised property crime have remained relatively stable in recent years, with minor adaptations in target selection and modus operandi, largely as a result of enhanced security measures. However, advancements in security technologies may prompt shifts in intrusion techniques employed in burglaries, thefts, and robberies, as criminal networks adapt to evolving protective measures. Additionally, a growth of the digital asset market may lead to a shift from physical to online property crimes.

As in many crime areas, the effects of digitalisation and technological advancement have become apparent in organised property crime. In some cases, car thieves have been reported to use more technically advanced intrusion techniques. Online platforms are increasingly used for the sale of stolen goods but also new types of theft, such as the theft of digital assets (virtual currencies and non-fungible tokens (NFT)), are becoming visible.

Organised burglaries and thefts (including motor vehicle crime)

No significant changes so far, but the evolving digitalisation of security measures could alter this

Organised burglaries and thefts have remained at relatively low levels and are expected to remain stable. No significant changes in modi operandi have been observed. However, some Member States reported an increase in the use of solid explosives in ATM attacks. As modern vehicles and their security systems become increasingly digitalised, criminal networks primarily exploit electronic vulnerabilities to steal them, employing various technological methods. Relay attacks, which exploit keyless entry systems, continue to be prevalent, alongside cases of motor vehicle embezzlement, including lease and rental fraud.

With the evolving digitalisation of security measures of homes, business premises, and vehicles, criminals are likely to incorporate cyber intrusion methods into their modi operandi.

While the effects are not yet being felt, changes in home safety technologies, such as electronic locks, might also influence criminals' modi operandi in the long term, for example by prompting burglars to adapt to using more electronic intrusion methods. As the automotive industry rapidly evolves with the market proliferation of hybrid, electric, and keyless vehicles, so will the intrusion techniques and technologies employed by criminal networks. This includes the use of digital software and targeted cyber-attacks to compromise 'connected' vehicles, allowing them to infiltrate and remotely modify or disable security systems. Although motor vehicle theft facilitated by cyber intrusion is not yet widespread, its use has been observed and might become more common.

Mobile organised crime groups

The criminal networks involved in organised burglaries and thefts are mostly mobile organised crime groups (MOCGs) that travel from country to country to perpetrate criminal offences and maximise profits. Individuals from the same community or with the same nationality typically facilitate the network's travel and stay in the target countries. They are able to shift from one form of theft to another, adapting their targets, stolen goods, tactics or geographical locations depending on the season or market circumstances.

Criminal networks active in organised burglaries and thefts use young people for some auxiliary activities, such as surveillance, and also for carrying out criminal activities, including shoplifting, theft by trickery, metal thefts, pickpocketing (of high value goods) or vehicle theft. Young perpetrators are recruited by offenders who take advantage of their relative impunity. In some cases, they are used for practical considerations, such as ease of entry through narrow passages.

Organised robberies

With the gradual development of cashless societies, robbers mainly target luxury goods at high-end stores, or gold, diamonds or cash in transit.

Criminal networks engaged in organised robberies travel across borders to carry out strategically planned offences.

Some criminal networks are using cybercrime techniques such as manipulating security networks before carrying out physical robberies. Sometimes robberies also involve corrupt staff or security personnel.

The illegal trade in cultural goods

The continuously expanding role of online sales channels and the impact of ongoing conflicts in the Middle East and the eastern flank of Europe may result in increased trafficking of cultural goods. The instability in Ukraine due to the ongoing Russian war of aggression has already impacted cultural goods trafficking, with some Member States reporting an increase in cultural items being trafficked from the country.

The Russian war of aggression against Ukraine already resulted in cultural goods being stolen in Ukraine and trafficked to the EU. The instability in the Middle East will likely also result in a surge of cultural objects trafficked to the European art market.
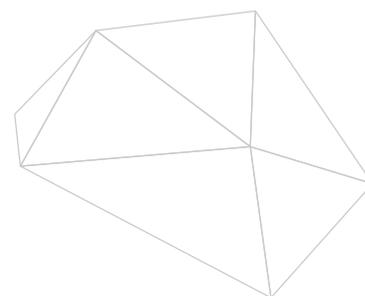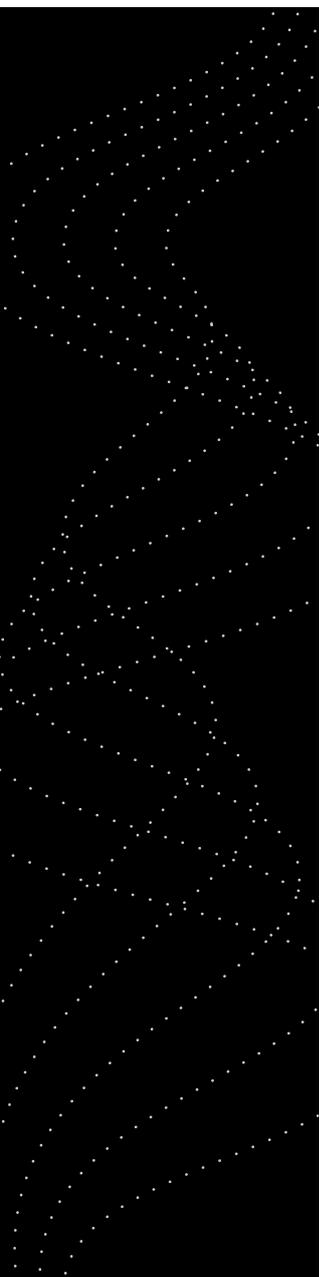
Digital art is increasingly traded through non-fungible tokens (NFTs), presenting new opportunities for criminal exploitation. The transition to art trading in the digital realm through NFTs facilitates crime due to flexibility, anonymity, and a lack of deterrence. Criminals likely exploit the public's limited knowledge of blockchains to defraud them of money or tokens.

Illegal excavations and looting in countries where locals struggle to secure a livelihood are likely sustained by international economic uncertainty. At the same time, the relatively stable value of artwork and cultural goods may attract more investment in this sector, including for money laundering purposes, which may also indirectly contribute to the intensification of trafficking activities in cultural goods.

Criminal actors have considerable expert knowledge

Cultural goods trafficking is a highly specialised criminal market. The criminals range from specialised criminal networks to corrupt dealers or expert dark web traders. Criminal networks and actors active in the area of cultural goods trafficking are characterised by a high degree of expertise and specialised knowledge. They possess considerable knowledge of archaeology and history in order to recognise, authenticate, and determine the value of illicitly acquired cultural goods, also being aware of the demand and dynamics of the art market.

Theft of digital assets

The rising adoption of digital assets and the rise of virtual economies, coupled with vulnerabilities in blockchain-based systems, will increase the threat of digital asset theft such as cryptocurrency or NFT theft. Due to the decentralised and pseudonymous nature of digital assets, recovering stolen assets presents significant challenges, making them a highly attractive target for cybercriminals.

(Online) Fencing

Criminal networks active in organised property crime inherently rely on fencing to make financial gains from the items they steal. Stolen goods, some of which are untraceable by nature, often find their way into the legitimate market and to unsuspecting customers, generally with no possibility of tracing them back and identifying the fencing process behind them.

The expansion of virtual economies will lead to an increase of digital asset thefts and online fencing.

Some criminal networks arrange the sale of stolen goods themselves while others outsource it to specialised fences, finding the right individual fences or fencing networks through contact with other criminal networks. Or they have established connections to legal business structures dealing with stolen products while others may be owners or staff themselves of legal business structures.

Stolen goods are sold on the black market or end up in the legitimate market, such as second-hand shops, pawnshops, goldsmiths, car dealers or retail shops.

With the growth of virtual economies and the increase of digital thefts, fencing of digital goods will also further increase.
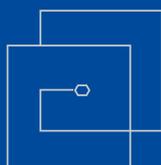
Intellectual property crime and trafficking of substandard goods

Intellectual property crime remains a lucrative criminal business, particularly for some specific counterfeit goods and pharmaceuticals. Marketing and distribution has shifted largely to online platforms and particularly via social commerce. Demand is likely to sustain or decrease depending on the type of product or service. All types of intellectual property crime and trafficking of substandard goods have a broad range of negative implications.
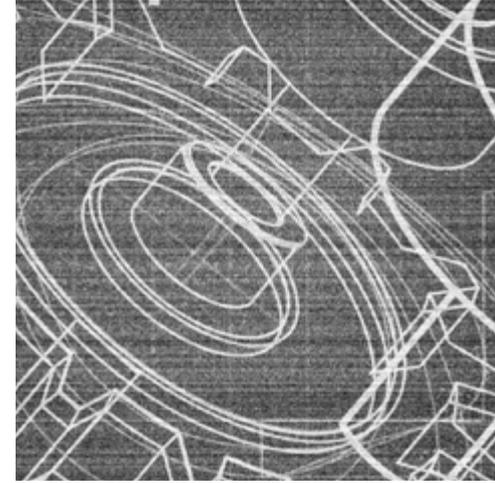
Digital content piracy

Shift to online realm and potential drop in demand

Mobile and web-based applications have become the main channel for delivering pirated content and services, driven by the continuous expansion of online streaming and the consolidation of over-the-top services as the preferred choice for entertainment[56]. The current cost-of-living crisis as well as the fragmentation of content across multiple legal streaming platforms prompt consumers to seek more cost-effective and unified packages regardless of their illegality. Yet, due to improved access to legal platforms, and enforcement scrutiny in some Member States, a further drop in users for illicit platforms[57] is anticipated.

Criminal networks offering digital piracy services will be facing a drop in demand.

Digital content piracy increasingly overlaps with cybercrime, as criminals use various technical means to breach both intellectual property and data security. The expansion and improvement of internet bandwidth in countries outside the EU will likely lead to a further outsourcing of dedicated servers that host and offer video and live streaming content, thus, creating jurisdictional challenges.

Criminal actors involved in digital content piracy: professional expertise and anonymity

Criminal networks often lease servers from legitimate hosting provider companies to ensure the anonymity and scalability of their operations. Others establish their own servers which may be outsourced to other criminal networks as a service. The increased use of anonymisation tools such as VPNs to avoid server blocks ordered by judicial or law enforcement authorities will continue to be a default modus operandi. Criminal actors also rely on a variety of professional expertise, mainly associated to information technology (IT) services such as technicians who build, operate and optimise the software and digital infrastructure for illegal streaming[58].. Digital pirates may steal or purchase login credentials from legitimate subscribers — often sourced via phishing scams or data breaches — and then repackage multiple over-the-top libraries into a single, unauthorized service. They often use specialised software or devices to intercept and record live or on-demand streams, relaying the pirated content through internet protocol television (IPTV) servers or file-sharing platforms.

Product counterfeiting

Lucrative criminal business with sustained demand and technological developments as enablers

Criminal networks continue to profit from high demand for low-priced goods, fuelled by the current cost-of-living crisis, and from consumers' lack of awareness of the dangers of counterfeit goods on the economy, health, and environment. Counterfeit goods are typically manufactured outside the EU. Small, seemingly legitimate manufacturing facilities and assembly points are also set up within the EU. Growing concerns are observed for the trade in counterfeit and illicit pesticides, and the trade in counterfeit automotive parts — particularly airbags — also considering these product categories are among those posing the highest health, safety and environmental risks. Automotive parts and ingredients used in pesticides are largely produced in and imported from Asia to the EU, but recent investigations highlight EU-based production networks with advanced equipment operating within the EU too[59].

Criminal networks continue to profit from high demand for low-priced goods, with particular lucrative criminal businesses in counterfeit pesticides and counterfeit automotive parts.

Digital acceleration has shifted the distribution of counterfeit goods online, drastically reducing the number of physical retailers. Social commerce (the integration of e-commerce with social media) is emerging as a key driving force used by counterfeiters to attract consumers.

The abuse of tools such as 3D printing and AI is also expected to grow in the near future, as they are set to enhance counterfeiting techniques even further, reducing the risk of human error and facilitating automated production.

The criminal actors behind the counterfeiting of goods

Criminal networks trading in counterfeit products often mirror legitimate business operations, using crime-as-a-service models, outsourcing vital functions (including finances), and infiltrating the supply chain at every step — from manufacturing and importing to distributing and selling.

Criminal and corrupted actors act within a structured ecosystem, with a decision-making hub and multiple levels, utilising intermediaries or subcontractors for specific tasks[60].

The illicit production and sale of counterfeit products generates significant losses in terms of business profits and tax revenues. The health and safety of consumers is directly at risk.

Pharma crime

Broad range of pharmaceuticals counterfeited or diverted, wide availability online

Benefitting from digitalisation, the circulation and promotion of counterfeit, falsified, substandard or fraudulently obtained legitimate medicines is enabled by their widespread availability on online platforms, often paid with cryptocurrencies, and their ease of delivery facilitated by postal and parcel services.

All types of pharmaceutical products can be concerned, with particularly rising concerns regarding antidiabetic, weight loss and hormonal substances. In addition, pharma crime is used as an enabler for drug crime, by diverting and using legal pharmaceuticals as precursors for the production of synthetic drugs. Other medicines contain substances that are classified as narcotic in certain countries, but not in others. Such legal differences create opportunities for criminal actors.

Criminal networks divert legally manufactured pharmaceutical products from their legitimate distribution channels to illicit markets, infiltrating pharmaceutical laboratories and pharmacies. Theft of medicines may occur anywhere throughout the supply chain, at the manufacturing site, during transit, at distribution centres, in warehouses, at pharmacies, or even in hospitals. Criminal actors also illicitly manufacture pharmaceuticals. EU-based clandestine laboratories are often small scale, and require relatively limited human resources and equipment, making them harder to detect.

Demand for fraudulent pharmaceuticals and other counterfeit products will be sustained against the backdrop of widespread online marketing, including by influencers, and with strained purchasing power of individuals.

A steady yet increasing demand for fraudulent pharmaceuticals is anticipated, sustained by the expanding role of social commerce, online influencers and individuals' decreased purchasing power to afford genuine medicines. AI and technological advancements, including 3D printing, will continue to be leveraged by criminal networks to manufacture tablets.

Pharmaceutical crime has a direct impact on public health and safety, undermines brand credibility, generates significant losses, and its production harms the environment.

Food fraud

Fewer seizures offset by more sophisticated production methods and sustained opportunities

Food fraud remains attractive for criminal actors due to the potential high profit margins. Although the volume of counterfeit foodstuffs seizures in the EU has decreased, food fraudsters are using increasingly sophisticated production methods to target high-value products or products with geographical indications, such as wine, olive oil, honey, and spices[62]. The fraudulent supply of food products such as fruits and meats, and fast-moving consumer goods such as soft drinks and confectionery, remains in demand. The growth of e-commerce has provided counterfeiters with new avenues to distribute fraudulent food items.
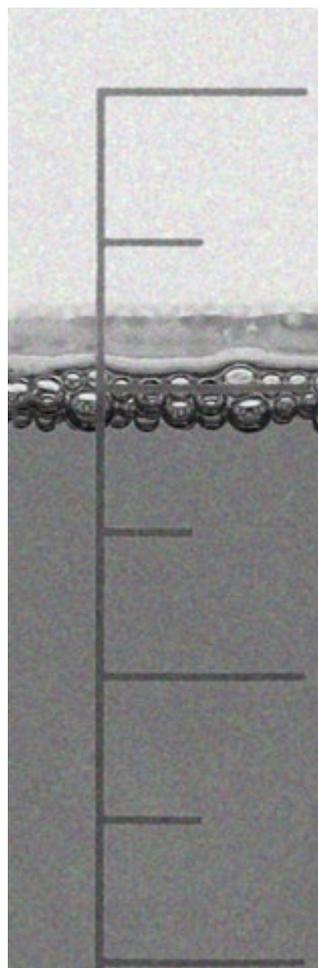
Currency counterfeiting

The threat of currency counterfeiting remains stable. Non-compliant altered-design banknotes are particularly favoured by currency counterfeiting criminals. The increasing use of cashless payment methods and the introduction of a digital euro may result in a decrease in currency counterfeiting activities. The production and circulation of counterfeit euro banknotes and coins causes financial and economic damage to the EU and its Member States.

Altered-design banknotes and production in and outside the EU with future demand surpassed by cashless payment methods

Counterfeiters in and outside the EU continue to produce counterfeit euros and other EU or non-EU currencies. Some raw materials sourced in Asia, are purchased via e-commerce platforms and shipped in parcels to the EU for production[63].

> CASE EXAMPLE — Sophisticated euro banknote print shop detected in Italy[64]
>
> After arresting buyers of large quantities of fake banknotes in Italy and France, a print shop was dismantled in June 2024, which was used to produce these counterfeits of various denominations (EUR 5, 10, 20 and 50). The forgers produced highly convincing counterfeit euro banknotes, which they offered for sale via a popular encrypted messenger service. The producers accepted payment in cryptocurrencies and sent the fake banknotes via post.

Social media and the surface web are gaining an increasingly prominent role in counterfeit currency distribution. Courier or postal services facilitate the dispatching of counterfeit currency and the sourcing of non-compliant, altered-design banknotes.

The use of social media platforms continues to provide a wider audience and exposure to currency counterfeiting. Courier or postal services remain a key factor in distribution.

In parallel with counterfeit banknotes and coins in circulation, there has been an increased availability of non-compliant altered-design banknotes detected in the EU, representing approximately 30 % of counterfeit banknotes seized during the past four years[65]. Criminal networks purchase ready-made non-compliant altered-design banknotes for circulation — both in the licit and the underground economy — but also as basis for counterfeit banknotes. Non-compliant altered-design banknotes are likely to consolidate their prevalence, rendering traditional illegal banknote printshops located in the EU redundant.

Non-compliant altered-design banknotes will remain popular in the currency counterfeiting criminal business.

Any potential economic instability may also lead to more currency counterfeiting. However, if cashless payment methods continue to become more mainstream and a digital euro is introduced, currency counterfeiting may become less appealing on the criminal market.

The increasing use of cashless payment methods and virtual currencies may serve as a deterrent to criminal actors involved in this criminal activity.

Criminal networks show a high level of technical expertise and internal organisation, with different affiliates in charge of supplying equipment, production, printing, and distribution.

Currency counterfeiting undermines trust in the currency.

Fraud schemes against the financial interest of the EU and Member States

Subsidy fraud, customs import fraud, VAT fraud and excise fraud all target state or Union funds, depriving legitimate beneficiaries of funding, and contributing to the destabilisation of national and EU economies. While differing in sophistication, these fraud schemes all continually adjust their methods, including the exploitation of online platforms and AI and fast-growing sectors, and are expected to continue so in the future.

Subsidy fraud, including benefit fraud

EU and national subsidies and benefit schemes remain at risk for fraud

EU and national subsidies and benefit schemes have long been attractive targets for fraudsters, while new funds that become available are also at risk of being defrauded. This was the case for the relief funds and interest free loans that were made available to support EU citizens, the private and the public sector in the aftermath of the COVID-19 pandemic. The Next Generation EU (NGEU) recovery fund has become a target of subsidy and benefit fraud schemes, with criminals implementing corrupt practices throughout the funds allocation cycle: application, implementation, closure and evaluation[66].

With the EU focused on developing a more sustainable, digital, and resilient economy, subsidy fraudsters are set to focus on sectors such as renewable energy, research programmes, and the agricultural sector — some of the 'pillars' of the 2021-2027 Multiannual Financial Framework and NextGenerationEU. In several countries, the application process for subsidies and social benefits has moved online rather than being conducted through a more traditional paper and face-to-face assessment process. This relative reduction in human oversight offers new and sometimes easier opportunities for abuse.

Criminal networks will seek to take advantage of any crises that emerge for which companies or individuals are eligible for funding, such as natural disasters or health emergencies. In addition, developments in AI will provide new text and image generation tools which may be misused to quickly and cheaply create fake identities or convincing false documentation.

Digitalisation and AI will accelerate the commission of subsidy and benefit fraud, as application procedures and manipulation of supporting documents become more accessible.

Benefit fraud combines, in some cases, with trafficking in human beings, during which victims' identity is used to fraudulently claim social benefits.

Subsidy and benefit fraud impacts the EU and its Member States financially and deprives legitimate recipients of funding opportunities.

Customs import fraud

Decrease in imports vs increase in e-commerce and postal items

Customs import fraud has remained stable, partly due to a decrease in imports across the EU's Eastern border as a result of the Russian war of aggression against Ukraine, counterbalanced by an increase in e-commerce and volume of postal items dispatched. In the future, additional anti-dumping duties, continued increase of e-commerce, and AI used for false documentation may open up new incentives or opportunities for fraudsters.

Criminals use various methods, including undervaluation, misclassification of the category (tariff classification fraud) and false declaration of the origin of goods. Document fraud and the misuse of legal business structures are common denominators for customs import fraud schemes across these different modi operandi.

Goods at higher risk of being undervalued include textiles, food, medicines, electronics, vehicles, sugar, shoes, and toys.

Customs import fraudsters

Customs import fraudsters easily adapt their operations to different entry points for the goods to avoid customs checks and swiftly exploit legal loopholes in other countries. Criminals make use of limited liability companies, individual entrepreneurs, and shell companies, which they quickly establish and dissolve. Legally operating customs brokers work with fraudsters to lend their specialist knowledge.

Value-added tax (VAT) and missing trader intra-community (MTIC) fraud

Persistent threat reliant on the legitimate economy

The threat posed by VAT fraud, and MTIC fraud in particular, to the EU's and its Member States' financial integrity persists, with a high level of sophistication. Electronic products, particularly mobile phones, are among the most widely reported commodities involved in VAT fraud schemes.

```
CASE EXAMPLE — 400 companies involved in a
EUR 297 million VAT fraud network[67]

A complex VAT fraud scheme, involving
the trade of popular electronic goods,
resulted in an estimated VAT loss of EUR 297
million. The suspects established multiple
companies in 15 Member States, which acted
as legitimate suppliers of electronic goods.
They sold over EUR 1.48 billion worth of
popular electronic devices via online
marketplaces to end customers in the EU.
Although the end customers paid VAT on their
purchases, the selling companies avoided
paying the amounts owed to the respective
national tax authorities. Other companies
in the fraudulent chain would subsequently
claim VAT reimbursement from these national
tax authorities. The proceeds of this
criminal activity were then transferred to
offshore accounts.
```

MTIC fraud is the most common modus operandi in VAT fraud. It refers to schemes where a trader imports goods VAT-free from another EU country and sells them domestically, charging VAT to the buyer but failing to remit this tax to the authorities. The trader then disappears, hence the term "missing trader". Carousel fraud is the most common form of MTIC fraud and involves a circular trading scheme where the same goods are repeatedly imported and exported across multiple Member States, with VAT refunds being claimed for taxes that were never paid. IT goods and accessories are frequently targeted, as are high-demand food and beverage products and luxury second-hand cars, due to the challenges associated with tracking their movement through supply chains. Precious metals, including gold, are an emerging commodity in VAT fraud schemes through misdeclaration[68]. The contra-trading scheme is the most complex and emerging scheme of MTIC carousel fraud, in which criminal networks add an extra layer of companies to create a second trading circuit or carousel.

Fraud schemes against the financial interest of Member States and the EU differ in sophistication. MTIC fraud in particular inherently relies on complex networks of companies to obscure participant connections, a level of complexity culminating in contra-trading schemes.

The systematic misuse of legal business structures is a critical component of VAT and MTIC fraud. Shell or buffer companies, whether infiltrated or set-up, facilitate the exploitation of cross-border VAT systems and VAT refund processes.

Fraudsters are expected to diversify their tactics, targeting emerging markets and leveraging digital platforms. A notable concern is the potential exploitation of digital content transactions, where goods produced within the EU are sold to entities outside the Union and subsequently resold to EU consumers, circumventing VAT obligations.

Criminal actors with expert knowledge

VAT fraud is committed by professionals with extensive knowledge of the VAT system, legislation, and tax administration procedures, often the product of professional expertise in areas such as accounting, finance, tax, technology, and law. They respond quickly to changes in legislation and market dynamics, as well as after law enforcement action.

The economic impact of VAT fraud is significant, with several tens of billion euros lost annually.

Excise fraud

Excise fraud particularly visible for tobacco products

Excise duties are indirect taxes on the sale and use of specific products, and countries that apply high excise and VAT rates are more vulnerable to the illicit sale of excise products[69]. Significant price differences between different Member States, and between the Member States and neighbouring non-EU countries, are the main incentive, and increased duties in various countries create opportunities for criminal networks. Excisable goods are smuggled across the EU using excise duty suspension schemes, abusing the Excise Movement and Control System (EMCS)[70]. Excise fraud particularly stands out for tobacco products and, to a lesser extent, for designer fuels. Excise fraud concerning alcohol products has become less visible.

As for other physical trafficking activities, the Russian war of aggression against Ukraine has caused disruptions in global supply chains and in the provision of services. This has opened up opportunities for fraud and led to a diversion of smuggling routes or changes in modus operandi. Frauds with Russian-origin-sanctioned products may enable the evasion of restrictive trade sanctions, for example, for Russian vodka or Russian oil products.

Demand for cheap versions of highly taxed goods remains high. Nearly a quarter of the EU's population smokes[71], maintaining a retail market for cheaper products. Criminal networks involved in excise fraud are likely to shift their operations to a broader range of excise products. The partial shift from smoking to vaping may cause criminal networks to add counterfeit vapes and/or e-cigarettes to their portfolio. And as the biofuel market grows, criminal networks may extend their involvement in this market.

The illicit production of counterfeit tobacco products in the EU has grown. Illicit production facilities have been discovered in almost all Member States. This increase has been driven by a combination of factors, including the disruption of supply chains by crisis situations, improved security in the trade of original branded cigarettes, high and rising excise duties and taxes, and the increased capacity of illicit factories due to the availability of multiple production lines in one location.

Tobacco products are illicitly produced in large-scale facilities, in more Member States than before. Criminal networks split up the production process in multiple facilities, and locate them in border regions.

Known illicit designer fuel production experienced a significant drop in 2022, mainly due to the disruption of raw material (gas oil) supply from Russia and law enforcement measures. However, a resurgence in illicit production has been observed since.

Criminal networks rely on experienced technicians

Criminal networks involved in the production and smuggling of illicit tobacco products operate with ample resources and through adaptable modi operandi[72]. These groups are highly resilient, with some actors and multiple networks that have been active for more than 10 years. Members have specific roles, and the tasks are clearly divided and controlled. Skilled and experienced technicians set up and maintain the machinery.

Criminal networks tailor their operations, producing specific brands for targeted end-markets and counterfeiting other popular tobacco and nicotine categories, such as water pipe tobacco, tobacco/nicotine pouches, or rolling tobacco.

Fuel fraud is a complex criminal process typically carried out by individual criminals or groups that manage the entire supply chain and retail[73]. Criminals involved in fuel fraud rely on the expertise of professionals, such as chemists and/or workers operating in the oil industry. Document fraud, such as the misdeclaration of transported goods, is well-established.

Sanctions evasion

Despite increased enforcement efforts, the intelligence picture of sanctions evasion remains fragmented and centred on trade control. Yet, while it is committed by economic actors in order to continue trade despite sanctions, it also strengthens sanctioned economies and states, and may therefore also entail a manifestation of foreign influence.

Multi-layered combination of economic crime and hybrid threat

Since the start of the Russian war of aggression against Ukraine in 2022, the EU has significantly reinforced its sanctions framework, and Member States have stepped up their sanctions enforcement efforts. Yet, the intelligence picture on sanctions evasion remains fragmented, and is primarily focused on trade control outcomes, while the investigations into related criminal finances and connections to hybrid threats remain limited. Sanctions evasion enables sanctioned economies to maintain their economic influence on EU markets. Moreover, sanctions evasion may serve broader agendas, including destabilisation — particularly through the proliferation of strategic goods, fuelling military threats. This threat is significant and inherently hybrid.

```
CASE EXAMPLE — Sanctions evasion fuelling strategic goods
proliferation and military threats[74]

In early 2024, Dutch authorities arrested three individuals
for allegedly exporting military-grade goods to Russia, in
violation of European Union sanctions. The investigation,
initiated in late 2022, coordinated among Dutch, German,
Latvian and Lithuanian authorities with Europol's support,
uncovered that the suspects had shipped aircraft parts and
other military equipment to Russian entities. These illicit
exports were allegedly facilitated through front companies
and falsified documentation to circumvent trade restrictions.
```

Criminals active in sanctions evasion will continue exploiting cooperation gaps, taking advantage of the complexity of sanctions enforcement arising from the wide range of criminal activities and actors it involves.

It is likely that criminal networks increasingly leverage tools such as encrypted communications, anonymised financial transactions, cryptocurrencies and blockchain technologies, and cyber-enabled trade-based money laundering. Also, more sophisticated methods of money laundering associated with sanctions evasion, based on complex ownership structures, will likely become mainstream.

As sanctions further tighten, modi operandi to evade them may become more advanced, including the extended leveraging of digital and AI tools.

In addition, while the demand for strategic goods from sanctioned entities increases (particularly for armaments), the procurement of strategic goods increasingly takes place in third countries serving as transit hubs today, particularly in West and Central Asia.
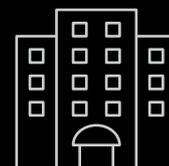
Criminal actors: a crime-as-a-service model

Sanctions evasion relies heavily on a crime-as-a-service model, with criminal enablers playing a central role throughout the supply chain of goods and assets trafficked or illegally transferred to circumvent sanctions. This often involves a division of roles across the criminal actors located in various countries to handle procurement, shipment, document fraud, and financial transactions. This demonstrates the adaptability and transnational nature of sanctions evasion networks and their ability to tailor their operations to specific trades and routes and establish criminal business contacts internationally.

Trade-based sanctions evasion relies heavily on a crime-as-a-service model combined with infiltration into legitimate businesses to handle the supply chain. Sanctioned actors maintain beneficial ownership of corporate structures and influence across Member States and sectors.

The geographical dimension of sanctions evasion varies with the focus of sanctions regimes. However, the current geopolitical context has driven cases of exports of strategic goods and assets to Russia and Belarus. Countries from the Eurasian Economic Union and the Caucasus play a central role in transhipment. Legal businesses are infiltrated, and front companies are set up in retail, import-export, transport, or the financial sector for the procurement and shipment of goods or assets.

This infiltration into legitimate businesses highlights the deeply embedded nature of sanctions evasion within established trade structures. This integration not only enables evasion but also incentivises corruption, undermining the integrity of national economies.

Sanctions evasion leads to economic destabilisation as it implies illicit trade flows, and strengthens sanctioned foreign powers in their economy, potentially fuelling hybrid threat actors.

The organised crime-terrorism nexus

Within the EU and its Member States, collaboration between criminal networks and terrorists is rare, limited to sporadic and opportunistic affiliations, while outside the region, certain links exist within shared or overlapping territories.

On EU territory, connections between terrorism and organised crime remain mainly unstructured and unsystematic. Links between criminal networks and terrorists typically emerge for opportunistic reasons, such as the joint use of criminal services or a common recruitment pool. Criminal networks benefit financially from providing services to terrorists. Likewise, terrorists engage with criminal networks for financial gain (e.g., funding from drug trafficking), as well as benefitting from logistical support (e.g., smuggling routes) and expertise (e.g., money laundering services). Geographical overlap of criminal actors and terrorists in the EU territory occurs either in prisons (through links formed between incarcerated individuals) or through terrorist organisations involved in criminal activities.

Links between organised crime and terrorism are unsystematic, mostly characterised by sporadic and opportunistic affiliations based on the use of crime-as-a-service by terrorists and on common recruitment pools.

Outside the EU, certain routes — used to smuggle migrants, drugs, and firearms — are shared by criminal and terrorist actors. In some countries, particular terrorist organisations exert control over sites where illicit activities are carried out by local criminal networks; for instance, in locations dedicated to cocaine production or cannabis crop cultivation and firearms trafficking.

The laundering of organised crime proceeds via terrorist financing links the two milieus, along with criminal services provided to terrorists, such as the provision of illicit firearms and explosives and of fraudulent identity documents.

Money laundering constitutes the strongest link between these milieus, as several cases of laundering of organised crime proceeds have been associated with the financing of terrorism. Criminal networks attempt to obfuscate the origin of their funds, whereas terrorists aim to conceal the purposes for which funds are used. The same professional money laundering service providers often operate as connectors between the worlds.

Cases of procurement and trafficking of firearms and explosives between criminal and terrorist actors, both outside and within the EU, have been reported. Criminal actors also provide fraudulent documents to terrorist actors, who use them to enter the EU under false identities or for secondary movements.

The geography of criminal networks
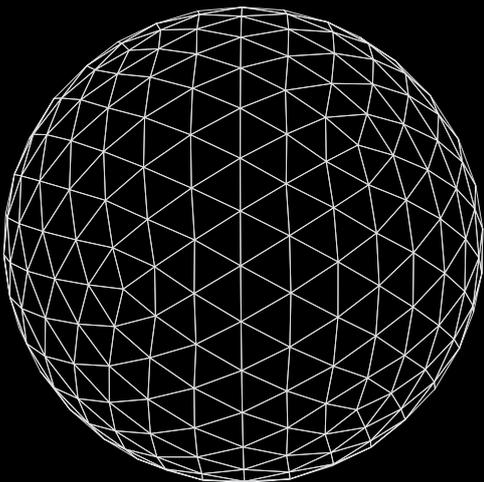
The DNA of serious and organised crime is strongly embedded in criminal networks' ways of working. Highly agile, they capitalise on developments in the online environment to adapt their modus operandi and expand their portfolio. Criminal networks are able to sustain their criminal activities over a long lifespan, resilient amid changes in the criminal landscape, violent disputes with criminal rivals, law enforcement pressure, and imprisonment. Their use of corruption, violence, money laundering activities, and legal business structures undermines economies and the rule of law, and has a destabilising effect on the fabric of society.

Criminal networks and their activities are unhindered by borders, be it within the EU or between the EU and the rest of the world. The EU has a central location in the global criminal landscape, being closely connected with all continents, and serving as a source, transit and destination region for illicit goods and services. Online interactions accentuate and facilitate these global interconnections even more. Yet, local and regional characteristics also influence how and where criminal operations and cooperations take place. As much as serious and organised crime in the EU cannot be assessed without considering the global context, it also needs to take into consideration regional similarities and differences.

A potential settlement of the Russian war of aggression against Ukraine may bring along shifting opportunities for criminal networks. These may include more activity in firearms trafficking; a growing recruitment pool for members of criminal networks; frauds related to recovery funds; a further blurring of lines between licit and illicit structures; and a potential change in cyber-attacks and online fraud schemes.

Criminal networks

Criminal networks exhibit remarkable agility, combining flexibility in their activities with resilience against disruption. They are adept at turning challenges and geopolitical crises into opportunities. A large majority makes use of legal business structures as a facilitator to commit their crimes, as a front to disguise them, or as a vehicle for laundering criminal profits. The sectors most vulnerable to infiltration by organised crime include logistics, hospitality, and construction. Criminal networks easily adopt developments in the online environment. Some capitalise on social, economic, and technological changes, including deepfake techniques, to set up fraud schemes, for example.

Criminal networks turn challenges into opportunities and maintain power and influence over long periods of time. The abuse of legal business structures is a key factor in their resilience.

Through the combined use of criminal finances, countermeasures, and corruption, which shield them against law enforcement disruption, many criminal networks are able to maintain their power and influence over very long periods of time. Members who are imprisoned or killed are easily replaced and leaders continue their coordination from prison. A large number of criminal networks have been active for more than a decade.

The resilience and agility of criminal networks are underpinned by strong cohesion between network members. Criminal networks come together around a common criminal enterprise and are often bound by a common regional area of activity, a common nationality, a shared origin or cultural background, a common language, family ties, or belonging to a subculture or organisation. These connections are exemplified by references to clans, cartels, mafia, confraternity, street gangs, Thieves in Law, or Outlaw Motorcycle Gangs (OMCGs). Common connections strengthen cohesion, make criminal networks resilient, and allow them to have an extensive geographical reach.

The organisational set-up of criminal networks ranges from vertical to horizontal and from small to large. The boundaries of criminal networks and membership are sometimes difficult to assess, particularly for criminals operating in the periphery of the criminal networks such as low-level recruits, wannabees, straw men, intermediaries, and crime-as-a-service providers.

Criminal networks have an international and often global reach and multinational membership.

The majority of the criminal networks have a reach that extends beyond the EU and its Member States, particularly to neighbouring countries, but also more distant locations. They deploy activities in more than 150 countries across the Americas, Africa, Asia, and even the South Pacific. This global reach is also reflected in the composition of these criminal networks, with over 100 nationalities represented. Multinational criminal networks are often composed of nationalities from neighbouring countries or of nationalities with large diaspora communities present in the country of activity.

Criminal networks tend to exert strong control and focus over their criminal operations. They are often specialised and led by strong leadership who overlook the full criminal process. The leadership is mainly settled either in the main country of activity or in the country of origin of the key members. A limited number have a leadership settled outside the EU. Another form of remote coordination involves criminal leaders directing operations from prison — orchestrating illicit activities across the globe, including violent actions.
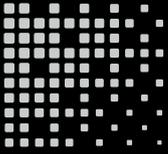
Criminal networks tend to specialise in one main criminal business, keeping strong control over it. Leadership is often close to operations. Cooperation with other criminal networks is usually based on equal partnership.

Cooperation mostly occurs in balanced, equal partnerships or under the crime-as-a-service framework. Criminal networks tend to have end-to-end control over the main part of the criminal process, including essential support activities such as the laundering of illicit proceeds. The vast majority deal in one main criminal activity. Truly poly-criminal networks active in very distinct crime areas, such as drug trafficking and online fraud, are rare.

A number of criminal networks specialise in crime-as-a-service, which allows other criminal actors to delegate specific tasks — such as complex money laundering, transport, and violence — gain outside expertise, and distance themselves from criminal activities.

The criminal activities, corruptive practices, and indiscriminate violence committed by criminal networks inflict significant damage to the fabric of society, the EU's internal security, the rule of law, and the economy. With their corruption of legal business structures, public institutions and other entities, and investments in the legal world to launder their criminal proceeds, criminal networks distort the local economy and local communities. They engage in corruption to facilitate criminal activity or obstruct law enforcement or judicial proceedings. Corruption plays a major role in information collection and is often crucial in identity and document fraud.

Criminal networks have a destructive and destabilising impact on the EU's and Member States' internal security, economy and rule of law. They often use corruption or resort to violence and intimidation.

Two-thirds of the criminal networks use intimidation and violence as an inherent feature of their modus operandi. The remaining one-third are not engaged in violence. The use of violence seen in the public domain is often related to drug trafficking and has become more visible and severe across a number of Member States.

Geographic dimension of serious and organised crime

The EU's positioning in the global criminal landscape

The EU is a region of destination, transit and origin for illicit commodities and services, and is interconnected in various ways with all continents[75]. Due to their proximity and the borderless nature of serious and organised crime, regions bordering the EU are of key relevance. The Western Balkan region remains a key transit cone for drugs and other illicit commodities to and from the EU. Eastern European countries are sources and destinations for illicit trade flows of a broad range of commodities, including illicit tobacco products, firearms, and also sanctioned goods. It is a source region for trafficking in human beings for sexual and labour exploitation. The Russian war of aggression against Ukraine has resulted in displacements of flows.

The EU is and will continue to be deeply interconnected with the global criminal landscape, with illicit goods and services flowing in, out, and through its external borders. Criminal networks adapt and operate or are facilitated by actors and businesses outside the EU.

To the west, Latin America is the main cocaine cultivation and production region, and its ports starting points for onward transport to the EU. It is also a source of people trafficked for sexual and, to a lesser extent, labour exploitation, and of irregular migrants smuggled by air to the EU. North America is a source region for cannabis and weapons trafficked to the EU.

To the south, Africa functions as a region of origin, transit and destination of illicit flows affecting the EU. Cannabis resin enters the EU market from major production regions in North Africa. Flows of irregular migrants smuggled, and victims of THB trafficked to the EU originate in diverse African regions. West Africa has further emerged as a significant hub for various criminal activities. The region presents favourable conditions for criminal operations due to its geographical positioning, limited law enforcement capacity, and high levels of corruption. The region plays a significant role in cocaine trafficking as a transit location between Latin America and the EU, and as a centre of gravity for fraudulent schemes targeting EU victims.

To the east, the Middle East and Asia are major sources of synthetic drugs (NPS and pre-precursors), heroin, counterfeit goods, and illicit tobacco products. They are also origin regions of victims of THB trafficked to the EU for sexual and labour exploitation, and of irregular migrants purchasing migrant smuggling services to reach the EU. Specific locations in the Middle East and Asia function as global hubs for money laundering. Asia and the South Pacific are destination regions for EU-produced synthetic drugs.

The global reach of organised crime and the multi-sided position of the EU as a sender or receiver of criminal activity is even more prominent in organised crime activity that takes place largely in the online realm. Perpetrators of child sexual exploitation operate in a virtually borderless environment, as do many money launderers, online fraudsters, and cyber-attackers. Hybrid threats, including disinformation campaigns orchestrated from outside, have an impact on the internal security of the EU. Sometimes also terrorist or violent extremist organisations cooperate with or are used by hybrid threat actors to reach their goal. All of these threats undermine our economies, destabilise societies and have a negative impact on the security of the EU's citizens.

Criminal networks operating in the EU also look for enabling opportunities on the global horizon. They launder their illicit proceeds and infiltrate legal businesses around the world. Money laundering very often takes place within the EU, but locations outside the EU are regularly reported too. In a similar manner, misused legal business structures are most commonly located in Member States, but in the majority of crime areas, businesses located outside the EU are also in focus. Violence, another important tool for criminal networks, can be commanded and controlled from remote coordination hubs.

While the EU functions as a base of operations and leadership in many cases, there are also many international links. Many of the criminal networks active in the EU do not only commit illicit activities within the EU. They often also operate outside the EU, in the EU's neighbourhood and beyond. A similar picture emerges for the location of leaders. Most criminal networks' leaders are settled in the country where the criminal network is (partially) active. This may be a strategic choice for high-level members of criminal networks to more effectively control criminal operations and manage their contacts. However, in some cases the leadership is settled abroad, in the same country as the network members' dominant nationality, potentially also a strategic choice to avoid apprehension.
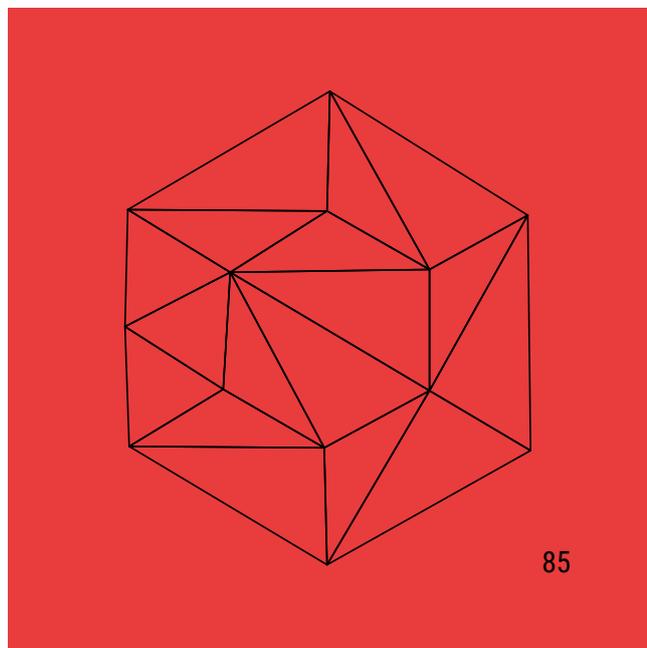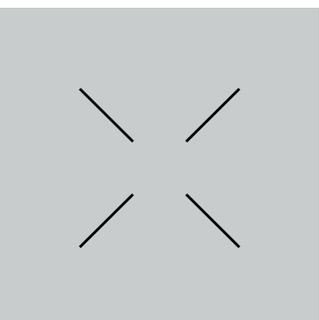
Regional dynamics within the EU

Variations in the EU between Member States and regions create differing opportunities and challenges for criminal businesses and cooperations.

Criminal networks' internal collaboration patterns are often based on regional similarities. Many criminal networks are composed of multiple nationalities, often from neighbouring countries or nationalities with large diaspora communities present in Member States. They join forces on criminal projects in order to capitalise on regional opportunities.

A common regional origin contributes to cohesion between members of these networks. While operating within Member States, they often maintain close links with their regions of origin outside the EU — as is the case for various criminal networks with roots in Western Balkan countries, for example.

The availability of commercial, logistic, and digital infrastructure, and the proximity to channels of supply and demand, influence in a dynamic way the vulnerability of regions to certain types of serious and organised crime.

Certain types of physical locations provide opportunities for criminal networks to implement their operations. Criminal networks make efficient use of transportation and trade infrastructure, such as ports and airports, both for inbound and outbound movements of illicit commodities. Planned expansions and new routes amplify criminal opportunities. Law enforcement activity affects smuggling routes and modi operandi, as criminal networks redirect their operations or look for other ways to reach their goals and circumvent the actions of law enforcement.

Free trade zones, usually located near transport hubs such as ports, offer exemptions from national import and export duties on goods that are re-exported. They become attractive for criminals involved in the trade in illicit goods and financial crime.

When operating in border regions, criminals take advantage of the close proximity to multiple markets, as well as the natural delineations between individual law enforcement jurisdictions, which offer opportunities to evade law enforcement.

The presence of certain types of key locations contributes to influencing how Member States and regions within the EU are affected by organised crime. Certain Member States serve as large-scale points of entry for illicit flows. Large maritime ports, as well as large airports, offer connectivity to international locations to facilitate the entry and onward transit of all types of illicit goods. These regional characteristics evolve in a dynamic way and do not remain static.

Russian war of aggression against Ukraine: Potential post-war implications on EU's internal security

While the Russian war of aggression against Ukraine has triggered some implications for the EU's internal security, any future settlement will also bring shifts that impact the EU and its Member States. The end of the Russian war of aggression against Ukraine will reshape some parts of the criminal landscape. While peace would bring stability and economic recovery, it may also create new opportunities for criminal networks to exploit vulnerabilities.

The war has facilitated the widespread distribution of weapons, which will persist even after an agreement. The demobilisation of military forces will lead to the diversion of surplus arms into the black market, exacerbating security challenges across Europe and beyond.

The reintegration of ex-military into the normal civilian life might pose challenges. Many former soldiers, particularly those facing economic hardship, may turn to organised crime, may be offered criminal jobs by established criminal networks, or may seek to establish private military organisations. This phenomenon has been observed in other post-conflict societies where demobilised fighters have been absorbed into criminal or para-military networks. Russian criminal networks may use the post-war environment to expand their operations. The lifting of economic sanctions on Russia, should it accompany a peace settlement, could also allow Russian criminal networks to enhance their financial networks through money laundering, and criminal finances across Europe or beyond.

Recovery funds could provide fertile ground for criminal networks to thrive. As both countries might undertake large-scale reconstruction efforts with potential foreign aid and investment, there is a heightened risk of corruption and financial crimes. Criminal networks may seek to infiltrate reconstruction projects, for example, through fraudulent contracts, money laundering, and embezzlement of public funds. Furthermore, oligarchs may leverage their influence to secure control over key sectors such as energy, infrastructure, and agriculture, further embedding criminal networks into legitimate economic structures.

If the end of the war or a peace resolution would result in unresolved territorial disputes, these regions might become safe havens for criminal actors. The future of the Thieves in Law (Vory v Zakone) will also depend on how the war in Ukraine ends and how power shifts within Russia, Ukraine, and the broader criminal underworld.

Throughout the conflict, both Russia and Ukraine have been engaged in cybercrime. In a post-war setting, cybercriminals, directed by hybrid threat actors, may redirect their expertise to pure financial cybercrime and continue targeting public institutions, businesses and individuals. With both nations having established cybercriminal ecosystems, there is potential for increased cooperation or competition between Russian and Ukrainian cybercriminal groups in activities such as ransomware, financial fraud, and digital extortion, leading to increased levels of threat.

While a changing situation between Russia and Ukraine would bring an end to a conflict, criminal networks are likely to adapt by exploiting post-war vulnerabilities in economic recovery and demilitarisation.

Conclusion: Identifying key threats in serious and organised crime

EU-SOCTA: the cornerstone of an intelligence-led approach for EU law enforcement

The EU-SOCTA is one of the most thorough and forward-looking analyses conducted on threats by serious and organised crime to the EU's internal security. It is also of key importance as an intelligence-led input to setting the EU's priorities in the fight against serious and organised crime, and to targeting law enforcement approaches to the most threatening challenges in the vast criminal landscape.

This in-depth examination 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, because of 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 **D**estabilises society in two ways: it undermines the EU through the generation of illicit proceeds and parallel economies, and additionally, it destabilises the EU because criminal networks increasingly operate as proxies in service of hybrid threat actors, a cooperation that is mutually reinforcing. In addition, serious and organised crime is increasingly **N**urtured online, with more, and very impactful criminal activities happening largely in the digital space. And it is **A**ccelerated by AI and other new technologies, making serious and organised crime more accessible and automated, increasing its scale and reach, and enhancing its capabilities. A future-proof fight against serious and organised crime must consider this changing DNA.

5

Identifying key threats

The key threats to 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 are predominantly taking place in the digital and online realm, but also more traditional crime areas entailing physical trafficking and illicit cross-border activity. The key threats identified on the basis of the EU-SOCTA methodology include the following crime areas: **cyber-attacks, online fraud schemes, (online) child sexual exploitation, migrant smuggling, drug trafficking, firearms trafficking, and waste crime.**

In the online realm, the objectives with which criminal networks execute **cyber-attacks** are to an increasing extent state-aligned. Alongside individuals and businesses, they target critical infrastructure and government structures, with a destabilising effect. 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 being used to produce child sexual abuse material, highly secured online communities of offenders, and expanding online grooming of children.

Another range of key threats concern physical cross-border crime areas, for which parts of the criminal process also progressively showcase aspects of the changing DNA. In **migrant smuggling**, criminal networks smuggle irregular migrants to, via or out of the EU, charging disproportionate fees while disregarding human dignity. Hybrid threat actors instrumentalising migration flows create additional opportunities to migrant smuggling criminal networks, known to adapt flexibly in their methods and routes. **Drug trafficking** as a key criminal market and threat has a high destabilising potential due to the parallel system it creates with its high profits and embedded violence, corruption, and abuse of legal businesses. Its continuous diversification in modi operandi, products and routings contributes to a fast pace and certain degree of unpredictability, which further enhances its threat. Contributing also to the regional expansion of drug-related violence, is the critical issue of **firearms trafficking**. Sources of illicit firearms shift and further expand under the influence of developments in technology, AI, and the online sphere, and of the availability of weapons in (post) crisis zones in countries in the EU neighbourhood and beyond. The **illicit trafficking of waste** is a financially driven crime harming the natural environment that intersects closely with the legitimate waste sector, and that employs experts from it. 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, and relevant use cases of AI are on the horizon.

Confronting criminal actors' cross-cutting tactics

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

The DNA of serious and organised crime is strongly embedded in criminal networks' ways of working, as they find opportunities as proxies for hybrid threat actors, in the online realm, and turn AI and technology to their criminal use. In addition, criminal networks operate unhindered by borders or by imprisonment, and integrate beneficial tactics in their operating procedures. The nature of **money laundering and criminal finances** is evolving, with criminal networks investing illicit proceeds in a parallel financial system designed to protect and grow their wealth stemming from illegal activities. It is shielded by a digital cloak of digital platforms and emerging technologies such as blockchain, resulting in a new era of money laundering. The **infiltration of legal business structures** supports, disguises, or facilitates any criminal activity, and the laundering of its proceeds. **Corruption** is a catalysing and widely used destabilising tactic, and is also gaining an online component. Intensifying organised crime-related violence in some Member States exacerbates feelings of insecurity and risks further diversifying in line with changing dynamics in drugs trafficking or other key criminal threats. The **criminal exploitation of young perpetrators** not only damages the social fabric of society, but also shields the higher echelons from identification.

These tactics contribute to criminal networks' ability to develop and grow their criminal business, increase their profits, and augment their resilience, creating a cycle of reinforcement. Therefore, it is essential to also integrate approaches towards confronting these reinforcing tactics.
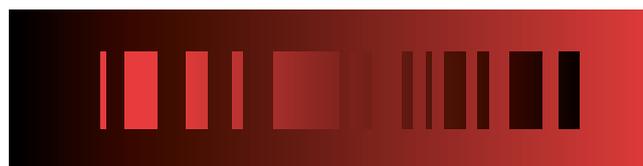
The geography of criminal networks

In addition to the tactics that facilitate criminal networks' operations, the DNA of serious and organised crime is strongly embedded in criminal networks' ways of working. Highly agile, they capitalise on developments in the online environment to adapt their modus operandi and expand their portfolio. Criminal networks are able to sustain their criminal activities over a long lifespan, resilient amid changes in the criminal landscape, violent disputes with criminal rivals, law enforcement pressure, and imprisonment.

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 also beyond, as these may present pressing implications for criminal networks' operations and for the EU internal security. As the Russian war of aggression against Ukraine resulted in some changes, a future post-war situation may in its turn also cause relevant shifts in the EU criminal landscape.

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.
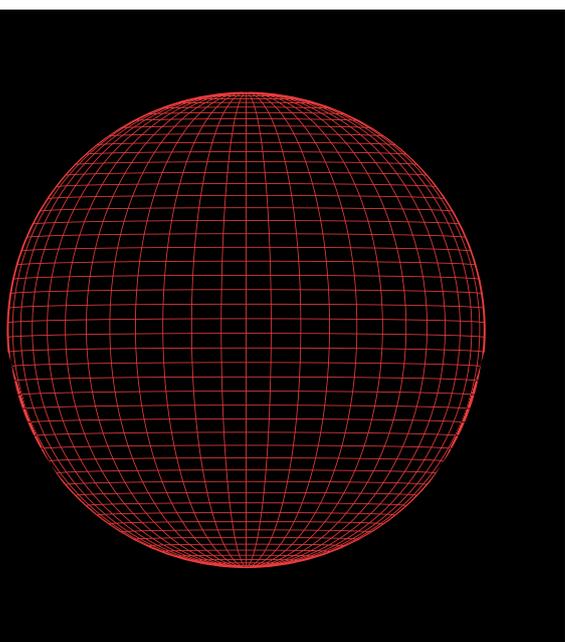
Reflection by the Academic Advisory Group

The 2025 EU Serious and Organised Crime Threat Assessment (EU-SOCTA) is a major undertaking by Europol, providing policymakers, Member States' law enforcement agencies, and other stakeholders with a structured, data-driven analysis of organised crime trends, manifestations, and impacts within the EU and beyond.

Previous EU-SOCTAs have contributed to a shared understanding of the organised crime threats facing the EU collectively. This edition is based on an extensive data collection by national law enforcement agencies, following a standardised protocol defined by Europol. Subsequently, Europol analysts integrate and analyse these data alongside information from various sources, including police intelligence, open-source reports, academic research, and case studies that illuminate key issues. By building on past experiences, lessons learned and insights gained from previous assessments, Europol aims to refine its methodology, enhance data collection and strengthen strategic foresight with each edition.

Leveraging Europol's intelligence and collaboration with Member States, EU-SOCTA 2025 offers an intelligence- and information based assessment of the evolving criminal landscape, including both current and emerging threats posed by criminal networks. It covers key cross-cutting themes such as criminal finances, the role of Artificial Intelligence and other technologies, the abuse of legal business structures, and the use of corruption and violence. More than just an analytical report, EU-SOCTA 2025 serves as a critical resource for understanding and informing decision-making on the complex security challenges facing the EU and its Member States.

The Value of the EU-SOCTA

EU-SOCTA 2025 enhances strategic planning by translating intelligence into actionable insights, enabling law enforcement to anticipate crime trends, allocate resources more effectively, and track long-term developments. By identifying criminal actors, recruitment methods, and financial crimes, it provides both operational and tactical benefits. These insights can help disrupt supply chains, prevent youth involvement in organised crime, and recover illicit funds.

Additionally, the report strengthens cross-border law enforcement and judicial cooperation by facilitating intelligence sharing across the EU and supporting joint efforts against all forms of serious and organised crime. It also aids policymakers in updating legislation and improving regulatory oversight. At its core, EU-SOCTA 2025 highlights salient risks, encouraging crime reduction efforts by the public, business, governments and non-profit organisations.

The Criminal Landscape

A significant portion of the report provides an in-depth review of major criminal markets and activities, offering a structured and detailed understanding of criminal dynamics across the EU. EU-SOCTA 2025 is highlighting the key criminal phenomena as an input to priority setting in tackling serious and organised crime.

Findings indicate that an increasing number of contemporary crimes are business and cyber-enabled. These crimes, along with related corruption, directly harm European citizens, businesses and governments, both economically and socially. This underscores the necessity of fostering public-private partnerships against serious and organised crime — an approach that has gained traction since the previous EU-SOCTA was released.

The in-depth review of the main criminal markets and activities is preceded by an innovative discussion of upcoming challenges for EU security. The Academic Advisory Group particularly appreciates the chapter on hybrid threats: attempts of state and/or non-state actors to exploit the vulnerabilities of the EU to their own advantage by using a mixture of measures (i.e. diplomatic, military, economic, technological) in a coordinated way, while remaining below the threshold of formal warfare. Ranging from information manipulation to cyber-attacks, from interference in electoral processes to politically instrumentalised migration, these serious threats to EU and Member States' security often involve unorthodox alliances between representatives of rival and/or 'rogue' states and organised crime actors.

The Academic Advisory Group is encouraged to observe some focus on regional elements in the EU-SOCTA 2025. By incorporating a regional breakdown, EU-SOCTA allows Member States to better contextualise threats within their own national frameworks and develop tailored policy

responses. Regional differentiation also makes it more likely that strategic and operational responses are aligned with overarching EU frameworks and priorities, and that they are also tailored to the daily realities of crimes occurring both 'on the ground' (sometimes on the cross-border grounds) and in cyberspace.

Focus on Enablers

The report also examines factors that knowingly or implicitly facilitate organised crime, such as corruption and the abuse of legal business structures by professionals from various sectors. Identifying these enablers and facilitating mechanisms helps policymakers and enforcement agencies target systemic vulnerabilities.

Forward-Looking Perspective

The EU-SOCTA anticipates future challenges, providing stakeholders with strategic insights into how criminal networks and groups may evolve and what measures can mitigate threats. These challenges are not only cross-border but also cultural, legal, and organisational. For instance, they include digital professionalisation of police and criminal justice, upstream crime disruption, and increased engagement with corporate entities that may act as "precursors" to various crimes.

The Role of the Academic and Scientific Community in the EU-SOCTA Process

As members of the academic and scientific community, we appreciate Europol's commitment to integrating scientific expertise throughout the data analysis process and commend its openness to feedback and growing engagement with academic research.

At a time when some political decisions may be influenced by intuition rather than empirical evidence, it is crucial to ensure that validated resources — based on both police intelligence and scientific research — are systematically incorporated. Robust scientific methodologies have further strengthened the credibility of EU-SOCTA findings, supporting intelligence-led policymaking.

While the current approach provides significant added value to policymakers and law enforcement agencies, the inclusion of even more peer-reviewed research, established theoretical frameworks, and interdisciplinary expertise would further enhance EU-SOCTA's analytical depth and academic rigor.

The Academic Advisory Group welcomes Europol's decision to involve the academic community in refining the methodology for the next edition. A well-structured and methodologically sound data collection and reporting process — with clear and consistent definitions — is essential to maintaining analytical integrity and ensuring that future assessments remain both accurate and policy-relevant. We look forward to continuing this productive collaboration.

Concluding remarks

EU-SOCTA 2025 is a strategic asset for law enforcement, policymakers, and other stakeholders. By employing an accepted methodology, addressing key serious and organised crime threats, and providing forward-looking insights, it provides law enforcement agencies and policymakers with some of the intelligence required to reduce serious and organised crime. As the landscape of crime continues to evolve, with regional variations rather than homogeneously within Europe and beyond, this report continues to function as an even more central reference point for reflective policymakers and practitioners, enabling them to improve serious and organised crime prevention and to innovate future policing across the EU.

Prof. Dr. Babak Akhgar OBE, Director of Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research - CENTRIC

Prof. Dr. Charlotte Colman, Professor Drug Policy & Criminology, National Drug Coordinator - President of the General Drug Policy Cell

Prof. Dr. Monica den Boer, Professor by special appointment of Police Studies at the Institute of Security and Global Affairs, Leiden University

Prof. Dr. Michael Levi FAcSS FLSW, Cardiff University

Dr. Joery Matthys, Assistant Professor, Institute of Security and Global Affairs, Leiden University

Prof. Dr. Letizia Paoli, Chair of the Department of Criminal Law and Criminology, Faculty of Law and Criminology, KU Leuven

Prof. Dr. Michele Riccardi, Deputy Director, Transcrime - Università Cattolica del Sacro Cuore

Annexes

Annex I — List of abbreviations

AI	Artificial Intelligence
ATM	Automated Teller Machine
BEC	Business Email Compromise
CaaS	C(yberc)rime-as-a-Service
CEO	Chief Executive Officer
CSAM	Child Sexual Abuse Material
CSE	Child Sexual Exploitation
EU-SOCTA	European Union Serious and Organised Crime Threat Assessment
EMCS	Excise Movement and Control System
GenAI	Generative AI
LBS	Legal Business Structures
LLM	Large Language Model
MTIC	Missing Trader Intra-Community
NFTs	Non-Fungible Tokens
NPS	New Psychoactive Substances
THB	Trafficking in Human Beings
VAT	Value-Added Tax
VPNs	Virtual Private Networks

Annex II — The EU-SOCTA Methodology

The EU-SOCTA methodology was developed by Europol in cooperation with the EU-SOCTA Advisory Group composed of representatives of the Member States, relevant Justice and Home Affairs agencies, third partner international organisations and the European Commission DG Home. Since the first issue of the EU-SOCTA in 2013, the methodology is reviewed on a continuous basis. For this 2025 issue, new customer requirements were agreed and endorsed in June 2023. Based on these, an improved methodology was agreed in November 2023, and implemented.

Aim and scope of the EU-SOCTA

The aim of the EU-SOCTA is to assess the key threats of serious and organised crime in the EU in a consistent way. The EU-SOCTA methodology is structured along the following aspects: the focus, the tools (indicators), the analysis and prioritisation, and the results.

The EU-SOCTA is focused on the following areas:

- Serious and organised crime areas
- Criminal networks and other criminal actors
- Crime infrastructure
- Geographical aspects
- Drivers for serious and organised crime
- Impact of serious and organised crime

Data sources

The EU-SOCTA 2025 data collection is three-layered:

- Data already available at Europol for the purpose of analysis, information exchange or cross-checking.

- External data collected from Member States, third countries, and other relevant partners. Member States and third countries contributed via dedicated questionnaires for criminal networks and crime areas. Third countries were requested to report on links to the EU or criminal activity at EU level. As multidisciplinary input is crucial to achieve an integrated and integral approach, contributors were encouraged to collect data from all available sources, including from relevant non-law enforcement authorities. For the first time in the series of EU-SOCTA reports, partners in the private sector were invited, via relevant Europol Advisory Groups, to contribute.

- Open-source information was used as a complementary data source. It includes research, reports, official statistical data, case examples, or contextual information from academic institutions, research networks, think tanks, global institutions, national authorities and other centres of expertise. The use of open sources was verified and approved as part of the review process. Members of the EU-SOCTA Academic Advisory Group contributed research on drivers, impact and outlook on organised crime, as well as methodological advice.

Indicators

In order to assess the threats of serious and organised crime, sets of indicators are used for serious and organised crime areas, criminal networks, impact, crime infrastructure and environment. A balanced combination of these features and the likelihood of change is crucial to reach conclusions and produce recommendations

Indicators can be either descriptive (D) or threat (T) indicators. Descriptive indicators are merely used to analyse and describe the threat. Threat indicators are used to assess and prioritise the threat.

Overview indicators

Indicators for SOC areas: modus operandi (D), resource availability (T), demand and supply (T), evolution (T), geographical distribution (T), links to other crime areas (D), number of criminal networks active in the crime area (D), nationalities of network members active in the crime area (D), sophistication of expertise (T), cooperation between criminal networks active in the crime area (T), adaptability of criminal networks active in the crime area (T)

Indicators for criminal networks: structure (D), crime areas in which they operate (D), nationality (D), size (D), modus operandi (D), roles (D), geographical dimension and mobility (T), continuity and resilience (T), financial resources (T), criminal profits (T), other resources (T), level of skills of experts (T), level of sophistication of tools used (T), cooperation with other networks (T), adaptability and flexibility (T)

Crime infrastructure indicators: use of legal business structures (T), level of sophistication of money laundering and criminal finances (T), identity/document fraud (T), corruption/influence (T), violence/intimidation (T), countermeasures (T), use of logistical infrastructure (D), use of technological and digital infrastructure (D)

Indicators for geographical dimension: geographical dimension and mobility of criminal networks (T), location where leadership is settled (D), geographical scope of cooperation with other criminal networks (D), countries where criminal money is laundered (D), countries where criminal networks misuse legal business structures (D), countries where external violence is used (D)

Impact indicators: financial/economic impact (T), social impact (T), health impact (T), security impact (T), political impact (T), impact on the physical environment (T)

Environment indicators: economic situation (D), sociological situation (D), geopolitical situation (D), transport and trade infrastructure (D), innovation and new technologies (D), legislation (D), national strategies (D), law enforcement activity (D), future evolution (T)

Analysis and prioritisation

The aim of the analysis is to develop the most precise and valid inferences from all the information collected, with a view to identify key threats and to provide substantiated recommendations for priority setting.

Key threats are those threats that rank highest based on the agreed prioritisation mechanism. The prioritisation comprises three elements. The first is the current threat, which is based on threat indicators of the crime area, the criminal actors, crime infrastructure, and geographical dimension. The second element is the future evolution of the crime area, based on expected changes in the broader environment. The impact of the crime area is the third element.

Results

The EU-SOCTA develops recommendations for priority setting in the fight against serious and organised crime for the EU policy level. It describes and assesses threats regarding all crime areas under Europol's mandate, the criminal actors, crime infrastructure, and geographical dimension, taking into account the drivers for and impact of SOC. In addition, it identifies those that are key threats to address as an EU priority in the fight against SOC for the next four years in the context of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

Member States were given the possibility to review the EU-SOCTA report and provide comments and propose amendments to ensure accurate interpretation of their contributions. Prior to publication, a quality assessment of the EU-SOCTA was conducted internally, according to the standard review criteria: consistency, completeness, clarity and compliance.

Endnotes

1   Europol, 15 March 2023, One of the darkweb's largest cryptocurrency laundromats washed out, accessible at https://www.europol.europa.eu/media-press/newsroom/news/one-of-darkwebs-largest-cryptocurrency-laundromats-washed-out

2   Information contributed to EMPACT IPCCGC OA 1.3; EUIPO and Europol, 2024, Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact, accessible at https://www.europol.europa.eu/publications-events/publications/uncovering-ecosystem-of-intellectual-property-crime

3   Eurojust, 2022, Eurojust Casework on Corruption: 2016-2021 Insights, accessible at https://www.eurojust.europa.eu/publication/eurojust-casework-corruption-2016-2021-insights

4   Europol, 8 December 2023, EUR 5.5 million frozen in anti-corruption investigations across Europe, accessible at https://www.europol.europa.eu/media-press/newsroom/news/eur-55-million-frozen-in-anti-corruption-investigations-across-europe

5   Europol, 23 January 2025, Violence as a service: criminals hire criminals, accessible at https://www.europol.europa.eu/media-press/newsroom/news/violence-service-criminals-hire-criminals

6   Script kiddies are young people gathering on forums and social media platforms to discuss hacking. As they lack advanced programming skills and expertise, they use existing scripts and tools to carry out cyber-attacks.

7   Europol, 20 February 2025, Intelligence Notification: Violent online communities threaten children, accessible at https://www.europol.europa.eu/media-press/newsroom/news/intelligence-notification-violent-online-communities-threaten-children

8   Europol, 5 February 2025, Law enforcement targets online cult communities dedicated to extremely violent child abuse, accessible at https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-targets-online-cult-communities-dedicated-to-extremely-violent-child-abuse

9   European Union Agency for Cybersecurity, 2024, ENISA Threat Landscape 2024, accessible at https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

10 Zero-day refers to a vulnerability in a software or hardware that is unknown to the vendor and for which no patch or other fix is available.

11 Common Vulnerabilities and Exposures (CVE) program is a catalogue of known cybersecurity vulnerabilities, where one CVE ID is specific to one software flaw.

12 Phishing kits allow attackers to easily generate an imitation of a legitimate website to steal login credentials, and are widely available on the dark web.

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

14 Europol, 2023, Internet Organised Crime Threat Assessment (IOCTA) 2023, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

15 Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system.

16 Ransomware is a type of attack where threat actors take control of a target's assets and demand payment in exchange for restoring access or withholding the release of stolen data.

17 Info-stealers, a type of malware that steals information from an infected device or system, can be used to steal login credentials by capturing keyboard input (keyloggers), credit card and banking details from websites (digital skimmers), cryptocurrency wallet configurations and data, messaging application data and files, private browser information, device contact lists, file transfer protocols, and VPN credentials, among others. Modern info-stealers are modular and able to extract different types of data from multiple systems and applications. Some info-stealers are designed specifically for mobile devices.

18 Europol, 2023, Internet Organised Crime Threat Assessment (IOCTA) 2023, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

19 Ibid.

20 Europol, 2024, Internet Organised Crime Threat Assessment (IOCTA) 2024, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

21 A Ponzi scheme is a fraudulent investment operation where fraudsters promise high returns in a short period with little or no risk. Early investors are paid returns using funds from newer investors, creating the illusion of a profitable enterprise. The money is not actually invested, and the scheme collapses when the fraudsters can no longer recruit new investors or when too many investors seek to withdraw their funds. Ultimately, the fraudsters often disappear with the remaining funds.

22 A pyramid scheme is a fraudulent business model where participants are promised quick and high earnings primarily for recruiting new members. Each new recruit must pay to join, with funds flowing upward to earlier participants, creating a structure that benefits those at the top.

23 Advance fee fraud is a type of fraud where significant financial gains are promised to victims in return for a small up-front payment and/or the provision of personal financial information. The fraudster promises a guaranteed return of benefit that in reality the victim will never receive.

24 Europol, 12 April 2024, 9 arrests in EUR 645 million JuicyFields investment scam case, accessible at https://www.europol.europa.eu/media-press/newsroom/news/9-arrests-in-eur-645-million-juicyfields-investment-scam-case

25 When the scheme involves communication between an employee and an executive of the organisation, often pressuring the employee into urgently transferring fund, the fraud scheme is known as chief executive officer (CEO) fraud.

26 Such instances are often referred to as invoice fraud.

27 Europol 2024, Internet Organised Crime Threat Assessment (IOCTA) 2024

28 Ibid.

29 Ibid.

30 TCSOs are hands-on abusers who, in order to perpetrate CSE, travel to so-called high-risk countries for victims of CSE.

31 Internet Watch Foundation, July 2024, What has changed in the AI CSAM landscape?, accessible at https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf

32 Europol, 28 February 2025, 25 arrested in global hit against AI generated child sexual abuse material, accessible at https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

33 Europol, 28 February 2025, 25 arrested in global hit against AI-generated child sexual abuse material, accessible at https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material?mtm_campaign=newsletter

34 European Labour Authority, 2024, Accommodation and food service activities: issues and challenges related to labour mobility, accessible at https://www.ela.europa.eu/sites/default/files/2024-10/horeca-report-ela.pdf

35 Europol, 08 February 2023, 28 arrested as Europe's biggest Chinese prostitution ring is dismantled, accessible at https://www.europol.europa.eu/media-press/newsroom/news/28-arrested-europes-biggest-chinese-prostitution-ring-dismantled; Europol, 27 January 2025, 30 arrested in crackdown on Chinese human trafficking ring in Spain and Croatia, accessible at https://www.europol.europa.eu/media-press/newsroom/news/30-arrested-in-crackdown-chinese-human-trafficking-ring-in-spain-and-croatia

36 Frontex, May 2024, Annual Risk Analysis 2024/2025, accessible at https://www.frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2024-2025.pdf; Frontex, September 2024, Strategic Risk Analysis 2024, accessible at https://www.frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Strategic_Risk_Analysis_2024_Report.pdf

37 Europol, 25 April 2024, 21 arrested in hit against migrant smuggling across the EU-Russian border, accessible at https://www.europol.europa.eu/media-press/newsroom/news/21-arrested-in-hit-against-migrant-smuggling-across-eu-russian-border

38 EUDA, 2024, European Drug Report 2024, accessible at https://www.euda.europa.eu/publications/european-drug-report/2024/drug-situation-in-europe-up-to-2024_en

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

40 EUDA and Europol, 2024, EU drug markets analysis: Key insights for policy and practice, accessible at https://www.europol.europa.eu/publications-events/publications/eu-drug-markets-analysis-2024-key-insights-for-policy-and-practice

41 Ibid.

42 EUDA and Europol, 2022, EU Drug Market: Cocaine, accessible at https://www.euda.europa.eu/publications/eu-drug-markets/cocaine_en

43 Europol, 26 August 2024, 28 arrested and cocaine lab dismantled in hit against drug traffickers, accessible at https://www.europol.europa.eu/media-press/newsroom/news/28-arrested-and-cocaine-lab-dismantled-in-hit-against-drug-traffickers

44 Europol, 2023, Criminal Networks in EU ports, Risk and challenges for law enforcement, p. 20, accessible at https://www.europol.europa.eu/publications-events/publications/criminal-networks-in-eu-ports-risks-and-challenges-for-law-enforcement

45 EUDA and Europol, 2023, EU Drug Market: Cannabis – In-depth analysis, accessible at https://www.euda.europa.eu/publications/eu-drug-markets/cannabis_en

46 EUDA and Europol, 2023, EU Drug Market: Cannabis – In-depth analysis.

47 Europol, 11 January 2022, 11 arrested in Spain and France for flying cannabis into Europe, https://www.europol.europa.eu/media-press/newsroom/news/11-arrested-in-spain-and-france-for-flying-cannabis-europe

48 EUDA & Europol, 2023, EU Drug Market: Cannabis – In-depth analysis.

49 EUDA and Europol, 2024, EU Drug Market: New psychoactive substances – In-depth analysis, accessible at https://www.euda.europa.eu/publications/eu-drug-markets/new-psychoactive-substances_en. It is, however, unclear if effective synthesis/production or only final processing and packaging took place in these laboratories.

50 Europol, 30 August 2024, Largest ever synthetic opioid laboratory in Poland dismantled, accessible at https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-synthetic-opioid-laboratory-in-poland-dismantled

51 EUDA, 2024, EU Early warning system intensive monitoring. N,N-Dimethyl etonitazene under intensive monitoring as of 5 July 2024.

52 EUDA and Europol, 2024, EU Drug Market: New psychoactive substances – In-depth analysis, accessible at https://www.euda.europa.eu/publications/eu-drug-markets/new-psychoactive-substances_en

53 EUDA and Europol, 2024, EU Drug Market: Heroin and other opioids, accessible at https://www.euda.europa.eu/publications/eu-drug-markets/heroin-and-other-opioids_en

54 Europol, 26 November 2024, Firearms trafficker supplying contract killers arrested in cross-border operation, accessible at https://www.europol.europa.eu/media-press/newsroom/news/firearms-trafficker-supplying-contract-killers-arrested-in-cross-border-operation

55 Europol, 14 February 2025, 13 persons arrested for illegally disposing 35 000 tonnes of hazardous waste, accessible at https://www.europol.europa.eu/media-press/newsroom/news/13-persons-arrested-for-illegally-disposing-35000-tonnes-of-hazardous-waste

56 Europol, 2023, European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime; EUIPO and Europol, 2024, Uncovering the ecosystem of intellectual property crime: a focus on enablers and impact, accessible at https://www.europol.europa.eu/publications-events/publications/uncovering-ecosystem-of-intellectual-property-crime; EUIPO, 2024, Apps and app stores – Discussion paper: Challenges and good practices to prevent the use of apps and app stores for IP infringement activities, accessible at https://www.euipo.europa.eu/fr/publications/apps-app-stores-challenges-and-good-practices

57 Europol, 2023, European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime

58 EUIPO and Europol, 2024, Uncovering the ecosystem of intellectual property crime: a focus on enablers and impact

59 Europol, 2023, European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime

60 EUIPO and Europol, 2024, Uncovering the ecosystem of intellectual property crime: a focus on enablers and impact

61 Europol, 30 March 2023, Gym doping bust: traffickers selling steroids to influencers, accessible at https://www.europol.europa.eu/media-press/newsroom/news/gym-doping-bust-traffickers-selling-steroids-to-influencers

62 Europol, 2023, European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime

63 Ibid.

64 Europol, 11 June 2024, Sophisticated banknote print shop dismantled in Italy, accessible at https://www.europol.europa.eu/media-press/newsroom/news/sophisticated-banknote-print-shop-dismantled-in-italy

65 The ECB's Counterfeit Monitoring System (CMS) is a database used by national competent authorities to record the identification of counterfeit currencies. The ECB agreed to give read-only access to their CMS database to Europol officials in the context of combating euro counterfeiting. For more information https://eur-lex.europa.eu/EN/legal-content/summary/counterfeiting-fraud-europol-european-central-bank-agreement.html

66 European Commission, 2021, The EU's 2021-2027 long-term Budget and NextGenerationEU, Facts and Figures, accessible at https://op.europa.eu/en/publication-detail/-/publication/d3e77637-a963-11eb-9585-01aa75ed71a1/language-en

67 Europol, 24 November 2024, 400 companies part of EUR 297 million VAT fraud network, accessible at https://www.europol.europa.eu/media-press/newsroom/news/400-companies-part-of-eur-297-million-vat-fraud-network; European Public Prosecutor's Office (EPPO), 28 November 2024, Investigation Admiral 2.0: Europe's biggest VAT fraud with links to organised crime, accessible at https://www.eppo.europa.eu/en/media/news/investigation-admiral-20-europes-biggest-vat-fraud-links-to-organised-crime

68 Europol, 2023, European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime

69 Europol, 2023, European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime

70 The Excise Movement and Control System (EMCS) monitors the movement of excise goods under duty suspension within the EU. It records, the movement between authorised consignors and consignees of alcohol, tobacco, and energy products for which excise duties have still to be paid. More than 100 000 economic operators currently use the system, and it is a crucial tool for information exchange and cooperation between Member States. The EU Commission has released the EMCS Mobile App (m-EMCS), intended for excise officers using the EMCS on the spot to monitor the movements of duty-suspended excise goods in the EU.

71 European Commission, 2024, Eurobarometer survey on Attitudes of Europeans towards tobacco and related products, accessible at https://europa.eu/eurobarometer/surveys/detail/29951

72 European Anti-Fraud Office, The OLAF report 2023, accessible at https://ec.europa.eu/olaf-report/2023/index_en.html

73 Europol, 2023, European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime

74 Europol, 24 January 2024, Three arrested for exporting military goods to Russia', accessible at https://www.europol.europa.eu/media-press/newsroom/news/three-arrested-for-exporting-military-goods-to-russia

75 Interpol, 2022, Global Crime Trend Summary Report, accessible at https://www.interpol.int/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

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