

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.

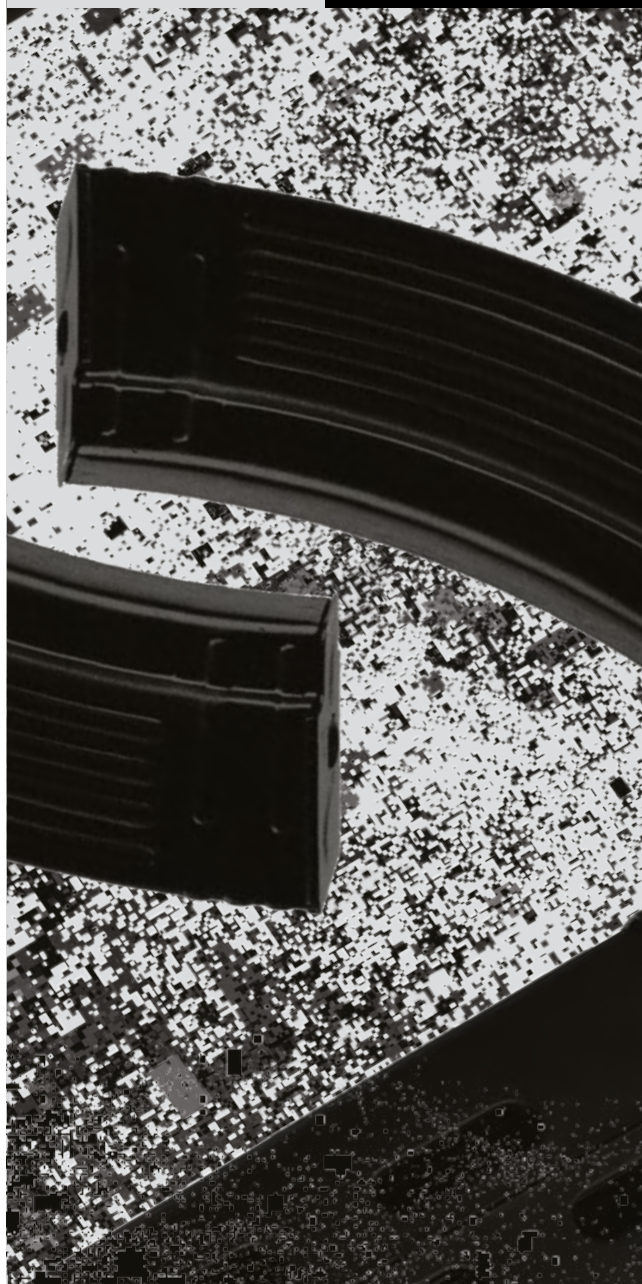
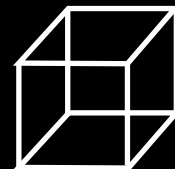
Both demand and supply of trafficked firearms and explosives remain high. Demand for firearms persists because they enable serious and organised crime-related violence and other forms of serious and organised crime, such as drug trafficking, extortion and racketeering, armed robberies, migrant smuggling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



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.

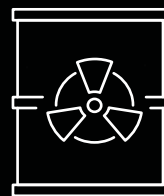
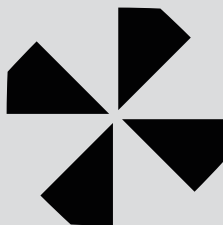
Trafficked heavy pyrotechnics enable multiple forms of serious and organised crime, and terrorism and violent extremism. Trafficked firearms enable violence among and within criminal networks. Spill-over of organised crime related violence into public spaces mentally and physically harms EU citizens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

CASE EXAMPLE – Assembled firearms sold to contract killers⁵⁴

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.

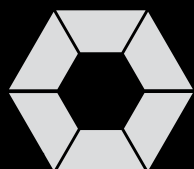
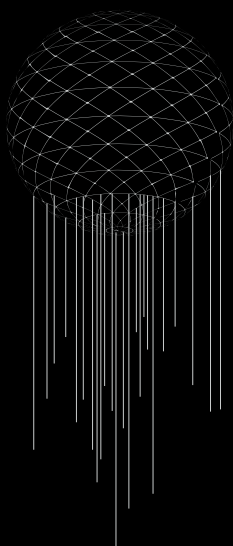


DETRIMENTAL IMPACT
ON OUR NATURAL
ENVIRONMENT AND
ECONOMIES



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.



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 waste⁵⁵

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 modus 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 modus 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.

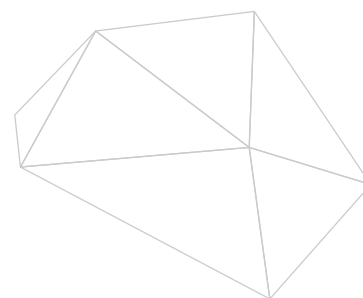
Criminal networks engaged in organised robberies travel across borders to carry out strategically planned offences.

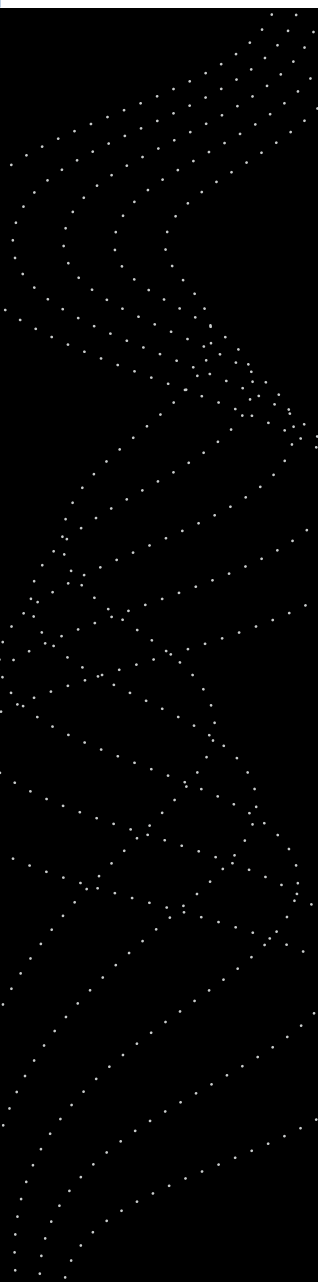
Some criminal networks are using cybercrime techniques such as manipulating security networks before carrying out physical robberies. Sometimes robberies also involve corrupt staff or security personnel.

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

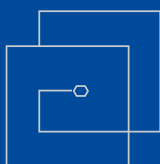
Criminal networks active in organised property crime inherently rely on fencing to make financial gains from the items they steal. Stolen goods, some of which are untraceable by nature, often find their way into the legitimate market and to unsuspecting customers, generally with no possibility of tracing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

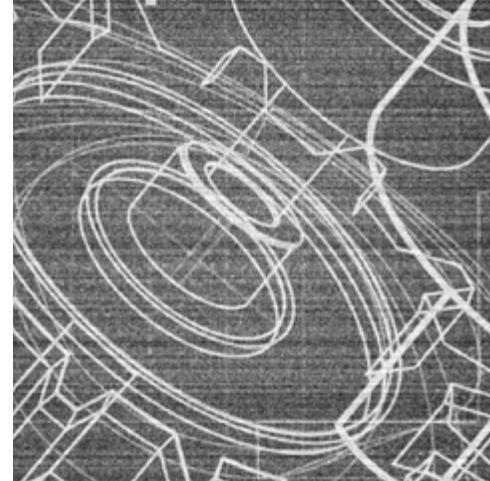
Stolen goods are sold on the black market or end up in the legitimate market, such as second-hand shops, pawnshops, goldsmiths, car dealers or retail shops.

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 entertainment⁵⁶. 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 platforms⁵⁷ 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 streaming⁵⁸. 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 too⁵⁹.

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 tasks⁶⁰.

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.

CASE EXAMPLE – Criminal network uses influencers to market illicit hormonal substances⁶¹

A criminal network, dismantled in 2023, produced and distributed illegal pharmaceuticals and anabolic steroids across the EU using popular social media influencers to promote the fake performance-enhancing substances. Network members had close ties with gymnasiums, which the networks supplied with the illegal goods. Amongst their clients were social media influencers with popular dietary and nutrition channels. One clandestine laboratory was dismantled, with over 1 million pills found at the production site.

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.

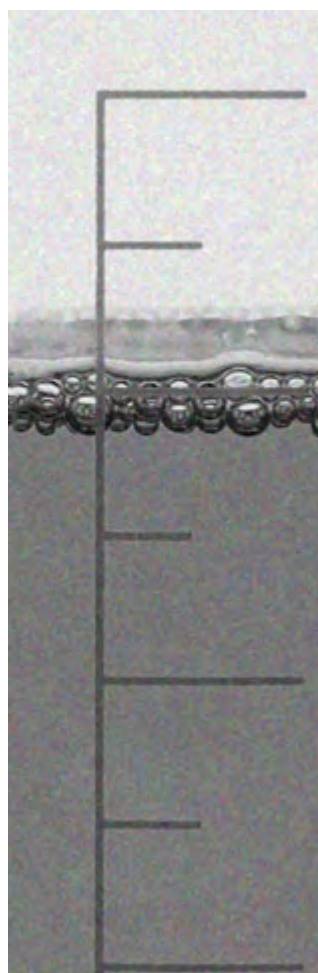
A steady yet increasing demand for fraudulent pharmaceuticals is anticipated, sustained by the expanding role of social commerce, online influencers and individuals' decreased purchasing power to afford genuine medicines. AI and technological advancements, including 3D printing, will continue to be leveraged 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 spices⁶². 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 production⁶³.

CASE EXAMPLE – Sophisticated euro banknote print shop detected in Italy⁶⁴

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 years⁶⁵. 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 evaluation⁶⁶.

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 network⁶⁷

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 misdeclaration⁶⁸. 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 products⁶⁹. 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 smokes⁷¹, 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 modus operandi⁷². 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 retail⁷³. 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 threats⁷⁴

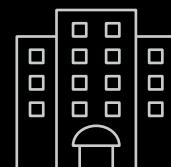
In early 2024, Dutch authorities arrested three individuals for allegedly exporting military-grade goods to Russia, in violation of European Union sanctions. The investigation, initiated in late 2022, coordinated among Dutch, German, Latvian and Lithuanian authorities with Europol's support, uncovered 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 transshipment. 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.

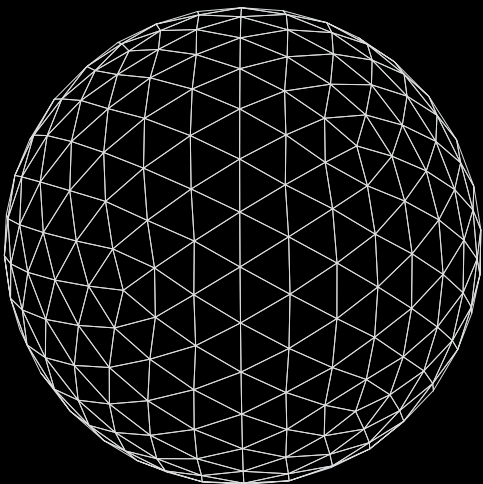
Outside the EU, certain routes – used to smuggle migrants, drugs, and firearms – are shared by criminal and terrorist actors. In some countries, particular terrorist organisations exert control over sites where illicit activities are carried out by local criminal networks; for instance, in locations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

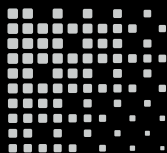
The resilience and agility of criminal networks are underpinned by strong cohesion between network members. Criminal networks come together around a common criminal enterprise and are often bound by a common regional area of activity, a common nationality, a shared origin or cultural background, a common 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 continents⁷⁵. 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.

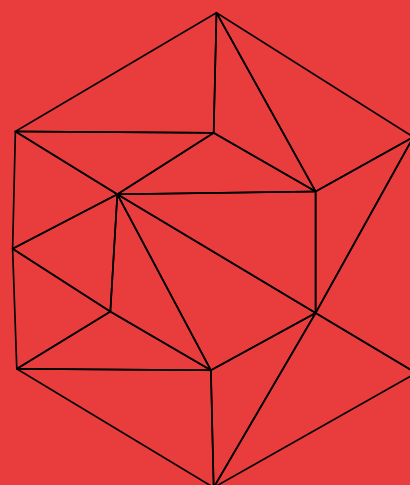
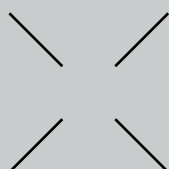
To the east, the Middle East and Asia are major sources of synthetic drugs (NPS and pre-precursors), heroin, counterfeit goods, and illicit tobacco products. They are also origin regions of victims of THB trafficked to the EU for sexual and labour exploitation, and of irregular migrants purchasing migrant 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.

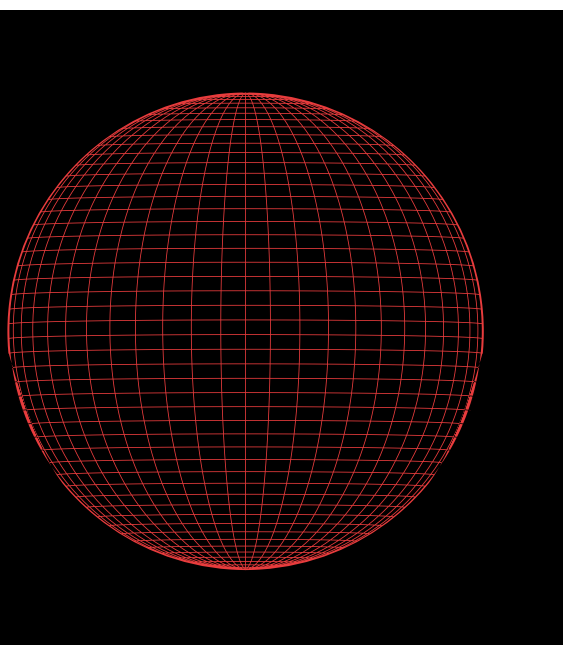


The geography of criminal networks

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(yber)c(r)ime-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 IPCCG 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

