EU SOCTA 2021

EUROPOL



EUROPEAN UNION

SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

A CORRUPTING INFLUENCE:

THE INFILTRATION AND UNDERMINING OF EUROPE'S ECONOMY AND SOCIETY BY ORGANISED CRIME

QL-09-21-093-EN-C / ISBN :978-92-95220-23-2 / DOI: 10.2813/02362
QL-09-21-093-EN-N / ISBN: 978-92-95220-22-5 / DOI:10.2813/346806



www.europol.europa.eu



PHOTO CREDITS
Europol: pages , 49, 51, 55, 56, 79 and 94.
GettyImages: pages 35, 38, 43, 53, 58, 67, 74, 78, 81, 84 and 86.
Freepik: page 45 and 54.

EUROPOL

EU SOCTA 2021 - SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

A CORRUPTING INFLUENCE:

THE INFILTRATION AND UNDERMINING OF EUROPE'S ECONOMY AND SOCIETY BY ORGANISED CRIME

TABLE OF **CONTENTS**

7 FOREWORD BY THE EXECUTIVE DIRECTOR

8 BACKGROUND

10 KEY FINDINGS
- 10 Criminal networks
- 12 Criminal activities

14 A MODERN HYDRA: SERIOUS AND ORGANISED CRIME IN THE EU

16 HOW SERIOUS AND ORGANISED CRIME OPERATES
- 18 Criminal networks and criminal entrepreneurs: A complex landscape
- 26 Organised crime undermines societies
- 34 Crime scenes: locations of crime in the EU

36 WHAT ARE THE MAIN SERIOUS AND ORGANISED CRIME ACTIVITIES IN THE EU?
- 38 Cybercrime
- 45 The trade in illegal drugs in the EU
- 54 Environmental crime
- 57 The trade in illegal firearms and explosives
- 59 Fraud
- 67 Match fixing and betting-related scams
- 68 People as a commodity
- 76 Document fraud
- 78 Product counterfeiting and intellectual property crime
- 83 Currency counterfeiting
- 84 Organised property crime

90 QUO VADIS? AN OUTLOOK ON SERIOUS AND ORGANISED CRIME
- 92 Key developments
- 94 The long-term impact of the COVID-19 pandemic
- 96 The potential impact of a global economic recession

98 CONCLUSION

100 ANNEX I – THE SOCTA METHODOLOGY

104 ANNEX II – LIST OF ABBREVIATIONS



FOREWORD BY
THE EXECUTIVE DIRECTOR

I am pleased to present the European Union Serious and Organised Crime Threat Assessment (EU SOCTA) 2021.

The SOCTA is Europol's flagship report delivering an insight into and assessment of serious and organised crime in the European Union. Looking back at the previous iterations of the SOCTA, I can see a clear progression to the deeper and more sophisticated understanding of the serious and organised crime threat facing the EU presented in this edition.

Once more, Europol has harnessed its position as the nerve centre of the EU's internal security architecture with its platforms, databases and services connecting law enforcement authorities across the EU and beyond.

Relying on a combination of operational insights, strategic intelligence and input from academia, the private and public sectors, the SOCTA 2021 is a multi-disciplinary and broad assessment of criminal threats.

I am particularly grateful to our colleagues in Member States, contributing partner states and organisations, who have contributed more information for this version of the SOCTA than ever before.

The intelligence picture and assessment presented in the SOCTA 2021 is a stark reminder of the dynamic and adaptable adversary we face in serious and organised crime in the EU.

The analysis indicates that criminal structures are more fluid and flexible than previously thought, use of violence by organised crime appears to be increasing, and use of corruption and abuse of legal business structures are key features of serious and organised crime activities.

The COVID-19 pandemic has had a significant impact on the serious and organised crime landscape in the EU. In the SOCTA 2021, we assess the long-term implications of these disruptive developments that have re-shaped some criminal activities and created new opportunities for some criminal networks. The SOCTA 2021 identifies key potential developments with an impact on serious and organised crime over the next four years. The outlook section also touches on the implications of a potential economic recession in the wake of the pandemic and how criminals will seek to capitalise on this. Serious and organised crime in the EU is a corrupting influence that seeks to infiltrate and undermine our economy and society.

An assessment of the criminal threats we tackle together also allows us to evaluate the best joint strategy to adopt. Europol is pioneering some innovative concepts such as a high-value target approach to fighting serious and organised crime. By analysing the roles played by those involved in organised crime, we can identify critical functions and individuals that constitute high-value targets. Targeting these critical operators and facilitators makes for a stronger and more disruptive law enforcement response.

Europol aims to be a leader in law enforcement innovation. In order to remain innovative, we need to understand the environment in which we operate and the challenges we need to tackle now and in the future.

The SOCTA 2021 provides such insights for Europol, for Member State law enforcement authorities, and our many partners around Europe and beyond. I hope this assessment is of use to you and that it can strengthen our concerted efforts to tackle serious and organised crime.

Catherine De Bolle
EXECUTIVE DIRECTOR EUROPOL

"I am concerned by the impact of serious and organised crime on the daily lives of Europeans, the growth of our economy, and the strength and resilience of our state institutions. I am also concerned by the potential of these phenomena to undermine the rule of law."

BACKGROUND

EUROPOL

Europol is the EU's law enforcement agency and it assists the Member States in their fight against serious international crime and terrorism. Established in 2000, Europol is at the heart of the European security architecture and offers a unique range of services. Europol is a support centre for law enforcement operations, a hub for information on criminal activities, and a focal point for law enforcement expertise. Analysis is central to Europol's activities. To give its partners deeper insights into the crimes they are tackling, Europol produces regular assessments offering comprehensive, forward-looking analyses of crime and terrorism in the EU.

THE EU SOCTA 2021

The EU SOCTA 2021 is the outcome of a detailed analysis of the threat of serious and organised crime facing the EU, providing information for practitioners, decision-makers and the wider public. As a threat assessment, the SOCTA is a forward-looking document that assesses shifts in the serious and organised crime landscape. The SOCTA 2021 sets out current and anticipated developments across the spectrum of serious and organised crime, identifies the key criminal groups and individuals involved in criminal activities across the EU and describes the factors in the wider environment that shape serious and organised crime in the EU.

The SOCTA 2021 is the most comprehensive and in-depth study of serious and organised crime in the EU ever undertaken.

The SOCTA 2021 provides an overview of the current state of knowledge on criminal networks and their operations based on data provided to Europol by Member States and partners and data collected specifically for the SOCTA 2021. In trying to overcome the established, and limiting, conceptualisation of organised crime groups, this assessment focuses on the roles of criminals within criminal processes and outlines how a better understanding of those roles allows for a more targeted operational approach in the fight against serious and organised crime.

Serious and organised crime represents a significant threat to the safety of EU citizens, undermines communities and causes substantial financial damages to the EU and its Member States. It weakens the rule of law.

In addition to victimising individual citizens, serious and organised crime severely affects economic development in Europe and beyond. Parallel underground economies deprive governments of income needed for investments in public services such as health, education and infrastructure. Crime has a direct negative impact on the quality of life of citizens in the EU and manifests in the shape of social exclusion, unemployment, inequality, sense of insecurity and the increased vulnerability of some groups to exploitation or recruitment.

The SOCTA is a product of close cooperation between Europol, the law enforcement authorities of the Member States and third parties such as EU agencies, international organisations and countries outside the EU with working arrangements with Europol. The involvement of these crucial stakeholders is also reflected in the SOCTA's role as the cornerstone of the European Multidisciplinary Platform Against Crime Threats (EMPACT) in the EU.

THE SOCTA METHODOLOGY

As part of an iterative process, the SOCTA methodology[1] has been further developed and refined by experts at Europol and from the law enforcement authorities of the Member States. The SOCTA methodology allows Europol to understand and assess serious and organised crime holistically. The SOCTA analyses and describes criminal markets and crime areas in the EU; the criminal networks or individual criminals carrying out these criminal activities; as well as the factors in the broader environment that shape the nature of serious and organised crime in the EU. Europol uses a mixed method approach involving qualitative and quantitative analysis techniques and a set of clearly defined indicators, to identify and specify the most threatening criminal phenomena in the EU. Europol arrives at the recommended priorities for the fight against serious and organised crime for EMPACT based on this methodology. The SOCTA methodology ensures transparency and reliability providing decision-makers with a solid basis for their deliberations.

More information on the SOCTA methodology is available in Annex I.

DATA AND SOURCES

The findings of the SOCTA 2021 are the outcome of detailed analysis of intelligence gathered as part of the largest data collection on serious and organised crime ever undertaken in the EU. Europol relied heavily on the operational intelligence held in its databases on serious and organised crime to provide a thorough and extensive analysis of the criminal threats facing the EU.

Member States, cooperation partners outside the EU and institutional partners contributed almost 4 000 questionnaires on criminal activities and criminal networks.

The amount of data provided for the SOCTA 2021 has increased by around 60 % compared to the SOCTA 2017.

STRUCTURE

The SOCTA opens with an analysis of the criminal networks and individual criminal actors active across the EU and provides information on cross-cutting issues that have an impact on or create the conditions for all criminal activities across the serious and organised crime landscape. These issues include corruption, money laundering and criminal content online. Key locations for crime in the EU are also presented.

The second chapter lists key developments, criminals and criminal networks, routes, locations and *modi operandi* for each of the criminal activities and criminal markets that make up serious and organised crime in the EU. Throughout the document, case examples highlight the real impact of serious and organised crime across the EU and demonstrate the success of international law enforcement cooperation.

The SOCTA 2021 closes by presenting a set of recommended priorities. Based on the outcome of a comprehensive analysis of the indicators and factors detailed in the SOCTA methodology, Europol recommends key priorities to tackle the most threatening forms of serious and organised crime.

EMPACT

EMPACT provides a robust framework that brings together the law enforcement authorities of the Member States, Europol and a wide range of multi-disciplinary partners in the fight against serious and organised crime. EMPACT translates strategic objectives at European level into concrete operational actions against serious and organised crime.

EMPACT is an instrument adopted by the European Union in 2010 to address the most significant criminal threats facing the EU. It optimises coordination and cooperation on the crime priorities agreed by all Member States. During the cycle, all concerned services and stakeholders, at national and EU level, are invited to allocate resources and mutually reinforce efforts. Considering the rapidly evolving nature of crime, Europol also prepares a mid-term review of new, changing or emerging threats, in cooperation with Member States and relevant EU agencies.

Relying on the analytical findings of the SOCTA 2021 and considering other strategic papers, assessments and policies, the Council will decide on the priorities in the fight against serious and organised crime for EMPACT from 2022 to 2025. These priorities will determine the operational work carried out in the framework of EMPACT for the next four years. The crime priorities agreed at European level in the context of EMPACT are reflected in operational activities at Member State level.

1 Council of the European Union 2019, SOCTA 2021 Methodology (13732/19).

KEY FINDINGS | CRIMINAL NETWORKS



Serious and organised crime remains a key threat to the internal security of the EU. All criminal activities assessed in the EU SOCTA 2021 have a serious impact on the EU. However, certain phenomena are particularly threatening and require urgent concerted action to address them.



The organised crime landscape is characterised by a networked environment where cooperation between criminals is fluid, systematic and driven by a profit-oriented focus. Several key actors cooperate in criminal networks with service providers and brokers in pivotal roles.



Similar to a business environment, the core of a criminal network is composed of managerial layers and field operators. This core is surrounded by a range of actors linked to the crime infrastructure providing support services, such as brokers, document fraudsters, technical experts, legal and financial advisors, money launderers and other service providers.



A key characteristic of criminal networks, once more confirmed by the pandemic, is their agility in adapting to and capitalising on changes in the environment in which they operate. Obstacles become criminal opportunities and may be as simple as adapting the narrative of a known modus operandi.

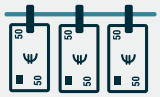


The use of violence by criminals involved in serious and organised crime in the EU appears to have been increasing in terms of the frequency of use and its severity. Criminals use violence indiscriminately and target victims without regard for their involvement or standing, often accepting harm to innocent bystanders. The threat from violent incidents has been augmented by the frequent use of firearms or explosives in public.



Corruption is a feature of most, if not all, criminal activities in the EU. Corruption takes place at all levels of society and can range from petty bribery to complex multi-million-euro corruption schemes. Corruption erodes the rule of law, weakens institutions of states and hinders economic development. Corruption is a key threat to be addressed in the fight against serious and organised crime. Almost 60 % of the criminal groups reported for the SOCTA 2021 engage in corruption[2].

2 Based on SOCTA 2021 data analysis.



The scale and complexity of money laundering activities in the EU have previously been underestimated. Serious and organised crime in the EU fundamentally relies on the ability to launder vast amounts of criminal profits. For this purpose, professional money launderers have established a parallel underground financial system to process transactions and payments isolated from any oversight mechanisms governing the legal financial system. This parallel system ensures that the criminal proceeds cannot be traced as part of a sophisticated criminal economy.



The use of technology is a key feature of serious and organised crime in 2021. Criminals exploit encrypted communications to network among each other, use social media and instant messaging services to reach a larger audience to advertise illegal goods or to spread disinformation. The online environment and online trade provide criminals access to expertise and sophisticated tools enabling criminal activities.



A potential deep economic recession following the COVID-19 pandemic will fundamentally shape serious and organised crime in the EU for the near future. Previous periods of economic stress can provide some degree of insight into how these developments might affect crime in the EU and what responses need to be formulated to counter existing and emerging threats to the EU's internal security during this time.



Legal business structures such as companies or other entities are used to facilitate virtually all types of criminal activity with an impact on the EU. Criminals directly control or infiltrate legal business structures in order to facilitate their criminal activities. All types of legal businesses are potentially vulnerable to exploitation by serious and organised crime. More than 80 % of the criminal networks active in the EU use legal business structures for their criminal activities. About half of all criminal networks set up their own legal business structures or infiltrate businesses at a high level.



The COVID-19 pandemic has had a significant impact on the serious and organised crime landscape in the EU. Criminals were quick to adapt illegal products, modi operandi and narratives in order to exploit the fear and anxieties of Europeans and to capitalise on the scarcity of some vital goods during the pandemic. While some criminal activities will or have returned to their pre-pandemic state, others will be fundamentally changed by the COVID-19 pandemic.



Serious and organised crime deeply affects all layers of society; in addition to the direct impact on the daily lives of EU citizens, it also undermines the economy, state institutions and the rule of law.

CRIMINAL ACTIVITIES

Over 80 % of the reported criminal networks are involved in the trade in drugs, organised property crime, excise fraud, THB, online and other frauds or migrant smuggling. Nearly half of these are involved in the drugs trade (38 %)[3].

The trade in illegal drugs continues to dominate serious and organised crime in the EU in terms of the number of criminals and criminal networks involved as well as the vast amounts of criminal profits generated as part of the production, trafficking and distribution of illegal drugs. Much of the violence associated with serious and organised crime is related to the trade in drugs.



Unprecedented quantities of **cocaine** are trafficked to the EU from Latin America, generating multi-billion-euro profits for the diverse range of criminals involved in the cocaine trade in both Europe and South America. The trade in cocaine fuels criminal enterprises that use their enormous resources to infiltrate and undermine the EU's economy, public institutions and society.



Similarly, the trade in **cannabis** is ubiquitous in the EU, affecting all Member States. Large amounts of cannabis are trafficked to the EU each year and EU-based criminals orchestrate the large-scale indoor and outdoor cultivation of cannabis in every Member State.



Criminal networks have been increasing their capacities for the production and distribution of **synthetic drugs.** European producers of these substances are among the most prolific criminal entrepreneurs worldwide, cooperating with criminal partners on a global scale in the sourcing of (pre-)precursor substances and the distribution of manufactured drugs.

The threat from **cyber-dependent crime** has been increasing over the last years, not only in terms of the number of attacks reported but also in terms of the sophistication of attacks. Cyber-dependent crime is likely significantly underreported. The rapidly progressing digitalisation of society and the economy constantly creates new opportunities for criminals involved in cyber-dependent crime. Fraud schemes take advantage of the digital era. Online fraud schemes target private individuals, businesses and public sector organisations.



There has been a continuous increase in activities related to **online child sexual abuse** over recent years. Online child sexual abuse likely remains highly underreported. Many victims remain unidentified and their abusers undetected.



The market for **migrant smuggling** services has been sustained despite the consolidation in migration flows reaching the EU since the height of the migratory crisis. Facilitation of entry in the EU fluctuates in line with the changing entry routes, whereas facilitation of secondary movements and legalisation of stay is less visible but equally profitable for criminal networks.The recklessness of criminal networks is clearly illustrated in this criminal activity. Irregular migrants are exposed to high fees for services that increasingly violate their physical and psychological integrity during the journey. In addition, they are often vulnerable to further exploitation upon arrival.



Several steps in the criminal process of **trafficking in human beings,** such as recruitment of victims and advertisement of services, have moved almost entirely to the online domain. The boundary between victim and accomplice has become blurred, with female victims also taking up organisational roles and with seemingly formal business agreements preventing victims from identifying as such.



The overall number of incidents of **organised property crime** remains high, especially for domestic burglaries, with more than one million cases a year, directly affecting millions of people. Mobile organised crime groups (MOCGs) continue to travel long distances from region to region and country to country committing organised property crime. The MOCGs easily shift from domestic burglaries to burglaries targeting business premises, physical ATM attacks, fraud schemes, cargo crime, pickpocketing, shoplifting or metal theft, depending on the season or market circumstances.



As part of excise fraud, **illicit tobacco products** are increasingly produced in the EU, in modern and more professional production facilities, established closer to destination markets.

A MODERN HYDRA: SERIOUS AND ORGANISED CRIME IN THE EU

EU citizens enjoy some of the highest levels of prosperity and security in the world. However, the EU still faces serious challenges to its internal security, which threaten to undo some of our common achievements and undermine shared European values and ambitions. As the EU is facing the COVID-19 pandemic, one of the most significant crises since the end of World War II, criminals seek to exploit this extraordinary situation targeting citizens, business and public institutions alike.

Along with terrorism, serious and organised crime continues to constitute the most pressing internal security challenge to the EU. Serious and organised crime encompasses a diverse range of criminal phenomena, from the trade in illegal drugs to crimes such as migrant smuggling and the trafficking in human beings (THB), economic and financial crime and many more.

The SOCTA 2021 provides an analysis of the nature and the scope of the challenge facing the EU. A better understanding of serious and organised crime will equip law enforcement authorities, policy- and decision-makers with better tools to counter these phenomena.

ORGANISED CRIME IS SIMPLE - AND COMPLICATED

Little has changed in what drives individuals to band together in organised criminal ventures: the desire to accumulate wealth by whatever means necessary. The profit-motive shapes crime schemes, drives cooperation and competition, and dictates risk-benefit considerations.

Organised crime is the domain of ruthless operators constantly seeking to identify and exploit vulnerabilities in our societies, economies, and laws. While its underlying motivations may not have changed, the structures, modi operandi and criminal operators encountered in fighting organised crime have undergone remarkable changes highlighting the versatility and flexibility of criminality.

A MODERN HYDRA

Law enforcement authorities have invested considerable resources to tackle this insidious form of crime. However, the flexible and changing nature of organised crime has allowed it to elude dismantlement and prolonged disruption. Serious and organised crime in the 21st century, in particular, is fluid and networked, connecting individual criminal entrepreneurs and smaller groups of criminals mediated by information and contract brokers and supported by criminal service providers lending advice and assistance with expertise in law, finance, logistics and many other specialist domains.

> Hydra, in Greek legend, a gigantic water-snake-like monster with nine heads, one of which was immortal. Anyone who attempted to behead the Hydra found that as soon as one head was cut off, two more heads would emerge from the fresh wound[4].
>
> Encyclopaedia Britannica

The experience of law enforcement authorities have shown that even successful and far-reaching disruption of criminal networks has little long-term consequence for the overall activities of organised crime. Like the Hydra of Greek mythology, removing one head does not kill the monster.

THE INSTRUMENTS OF SERIOUS AND ORGANISED CRIME

Criminals are adept at exploiting opportunities and turning others' crises into their fortune. Violence, corruption and deception are the key tools at their disposal.

The use of violence by criminals involved in serious and organised crime in the EU appears to have been increasing in terms of the frequency of use and its

4 Encyclopaedia Britannica 2021, Hydra – Greek mythology, accessible at https://www.britannica.com/topic/Hydra-Greek-mythology

severity. Criminals use violence indiscriminately and target victims without regard for their involvement or standing, often accepting harm to innocent bystanders. The threat from violent incidents has been augmented by the frequent use of firearms or explosives in public.

Corruption is a feature of most, if not all, criminal activities in the EU. Corruption takes place at all levels of society and can range from petty bribery to complex multi-million-euro corruption schemes. Corruption erodes the rule of law, weakens institutions of states and hinders economic development.

Organised crime undermines our economies, society and the institutions of state. The investment of billions of euros in illegal profits generated by organised crime in the EU in our licit economy distort competition and hinder economic development. Professional money launderers have established a parallel underground financial system to process transactions and payments isolated from any oversight mechanisms governing the legal financial system. This parallel system ensures that the criminal proceeds cannot be traced as part of a sophisticated criminal economy.

Criminals are highly adept at exploiting our economy for their purposes. Legal business structures such as companies or other entities are used to facilitate virtually all types of criminal activity with an impact on the EU. Criminals directly control or infiltrate legal business structures in order to facilitate their criminal activities. All types of legal businesses are potentially vulnerable to exploitation by serious and organised crime. More than 80 % of the criminal networks active in the EU use legal business structures for their criminal activities. About half of all criminal networks set up their own legal business structures or infiltrate businesses at a high level.

Criminals are digital natives. Virtually all criminal activities now feature some online component, and some phenomena have fully migrated online. Online marketpleaces, both on the surface and dark web, offer access to illicit goods and illicit services. Digital platforms provide access to encrypted communications and payment solutions.

IDENTIFYING THE MOST RELEVANT CRIME THREATS

All serious and organised crime phenomena are threats to the EU's internal security. The large majority (80 %) of criminal activities perpetrated by criminal networks involve drugs, organised property crime, various types of frauds, and crimes exploiting people as a commodity. These types of serious and organised crime were identified as particularly menacing based on an assessment of their threat, impact, and future evolution.

The trade in cocaine, cannabis, synthetic drugs and new psychoactive substances (NPS) is a key threat to the EU due to the levels of violence associated, the multi-billion euro profits generated and the substantial harm caused by it. Mobile Organised Crime Groups (MOCGs) active in burglaries throughout the EU victimise millions of EU citizens. Various fraud schemes generate multi-billion euro profits and significantly undermine the EU's economy. The COVID-19 pandemic has acted as a catalyst for the emergence of new online fraud schemes. The trafficking in human beings is a key threat to the EU. Several parts of the trafficking process have moved online, from recruitment of victims to advertisement of illicit services. Criminal networks profit from the despair of irregular migrants, charging high fees to smuggle them into or within the EU, or assist them in obtaining legal residence status.

Cybercrime is often perpetrated by individual criminals and remains significantly underreported. Cyberattacks have increased and have become more sophisticated. Online child sexual exploitation targets the most vulberable members of our society. Illicit waste trafficking increasingly takes places in the EU in addition to locations outside of Europe.

All crime areas discussed in the SOCTA 2021 represent considerable challenges to the EU. All forms of serious and organised crime deeply affect society and often have a direct and detrimental impact on the daily lives of EU citizens. These crime phenomena exert their corrupting influence to undermine the EU's economy, institutions of state and the rule of law.

The current crisis situation and the potential economic and social fallout threaten to create ideal conditions for the spread of organised crime in the EU. Criminals were already quick to adapt illegal products, modi operandi and narratives to the COVID-19 pandemic. In this way, they exploited the fear and anxieties of Europeans and profited from the scarcity of some vital goods during the pandemic. A potential deep economic recession following the COVID-19 pandemic may facilitate the growth of serious and organised crime in the EU. Entrepreneurial and ruthless criminal operators may further exploit existing vulnerabilities and turn them into opportunities for criminal involvement.

Serious and organised crime is a strong and resilient adversary representing a modern Hydra. This adversary can only be fought using a joint, concerted, and multi-disciplinary approach grounded in our common European values and the respect for fundamental rights.

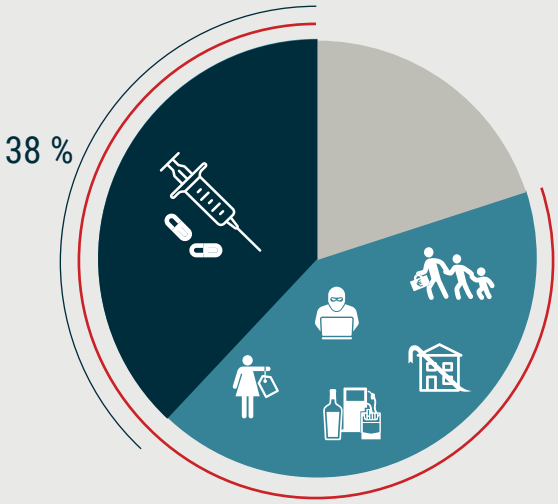


HOW SERIOUS AND ORGANISED **CRIME OPERATES**


46667
68639
29086
56288
35939
39866
36617
87912
63764
53635
22634
66961
46804
12222
63368
47026
87129
8605
19572
10263

CRIMINAL NETWORKS

CRIMINAL MARKET



80 %
are involved in drugs, organised property crime, excise fraud, trafficking in human beings, online and other frauds, and migrant smuggling

STRUCTURE AND COMPOSITION

40 %
hierarchical structure



60 %
fluid crime structure



1/4
have been active for more than 10 years



21 %
up to five members

79 %
six or more members

INTERNATIONAL DIMENSION AND MOBILITY



65 %
are composed of members of multiple nationalities

>180
nationalities involved

7 out of 10
are typically active in more than three countries



LEGAL BUSINESS STRUCTURES



80 %
use legal business structures for their criminal activities

MONEY LAUNDERING



68 %
use basic money laundering methods such as investing in property or high-value goods

CORRUPTION



60 %
engage in corruption

USE OF VIOLENCE



60 %
use violence to any extent

POLY-CRIMINALITY

▼ Decrease



40 %
engage in more than one main criminal activity

© EUROPOL 2021

CRIMINAL NETWORKS AND CRIMINAL ENTREPRENEURS: A COMPLEX LANDSCAPE

Organised crime is often described from the viewpoint of criminal activities. These activities can be measured and tackled relying on law enforcement expertise specific to different law enforcement domains such as the fight against drug trafficking, migrant smuggling or money laundering, among many others. However, the fight against organised crime ultimately needs to target the criminals and their networks who engage in criminal activities.

Understanding how criminals and criminal networks operate will allow law enforcement to more effectively identify and disrupt criminal operations. The most recent data used in the analysis for the SOCTA 2021 reveal that the serious and organised crime landscape is characterised by a networked environment where cooperation between criminals is fluid, systemic and profit-oriented. Criminals cooperate in the framework of criminal networks engaging with criminal service providers and brokers who occupy pivotal roles in the crime landscape.

Over 80 % of the reported criminal networks are involved in the trade in drugs, organised property crime, excise fraud, THB, online and other frauds or migrant smuggling. Nearly half of these are involved in the drugs trade (38 %).

Despite an increasing number of investigations into cyber-dependent crimes and other cybercrime activities, the number of criminal networks is low. One of the reasons could be that cybercrime involves many criminals operating individually and not in the framework of established networks.

Around 40 % of the criminal networks active in the EU engage in more than one main criminal activity.

A quarter of the criminal groups have been active for more than ten years. A third of the criminal networks has been active for less than three years.

The nature of organised crime is truly global. More than 180 nationalities are involved in organised crime activities in the EU. 65 % of the criminal groups active in the EU are composed of members of multiple nationalities.

More than 50 % of all reported suspected organised criminals active in the EU are non-EU nationals. Half of these non-EU nationals originate from countries in the EU's neighbourhood, such as the Western Balkan region, eastern European countries, and North Africa.

A majority of criminal networks (around 60 %) employ violence as part of their criminal businesses.

Around a quarter of criminal networks routinely use violence and intimidation in an offensive, planned, premeditated way. In some cases, these criminal networks make use of hitmen and kidnappers providing services of murder and intimidation or of enforcers and bodyguards. In some extortion cases, criminal networks hire members of other criminal networks to execute violent attacks when victims deny payment.

Almost 70 % of criminal networks are active in more than three countries.

TYPES OF ORGANISED CRIME

Different types of criminal networks are often clustered according to indicators such as:

- nationality or ethnicity (e.g. Chinese organised crime groups);
- criminal activity (e.g. MOCGs involved in property crime);
- structure (e.g. mafia-style OCGs, street gangs);
- or any other descriptive characteristic of criminal networks (such as value systems, e.g. outlaw motorcycle gangs and thieves-in-law).

Nationality, ethnicity, activity, structure or other descriptive indicators are often used to describe and classify criminal networks. However, such approaches are often reductive and do not necessarily highlight the most characterising element of the network.

In some cases, classifying criminal networks according to national or even ethnic homogeneity can be relevant for an investigation, because the nationality and/or ethnicity can be an important element in international collaboration. Strategically, the division of criminal groups according to ethnic homogeneity often lacks nuance. Almost two thirds of the criminal groups reported for the SOCTA 2021 are composed of members of different nationalities.

CAPTURING THE COMPLEXITY OF THE CRIMINAL LANDSCAPE

When analysing organised crime groups beyond the typical descriptive indicators such as nationality, criminal activity or common characteristics, in many cases the analysis reveals a fragmented landscape of different networks of collaborating individuals and groups. These actors interact with one another in the pursuit of common criminal objectives. This makes criminal operations more complex than if they were organised end-to-end by a single group. Moreover, at various points in the criminal process chain, criminals can operate in or provide services to several different networks.

Criminal networks are composed of contacts interacting with one another on a more permanent or ad hoc basis. Networks vary in size. Smaller networks often operate at a regional or local level, relying on autonomous partners. In many cases, these partners provide their services to multiple networks at the same time. Larger networks typically operate at an international level and are involved in more complex operations.

The majority of the groups are loose networks or centre around a core group (60 %), while 40 % are hierarchically structured.

The increasing presence of loose and more organic networks is also a reflection of the increasing proliferation of the crime-as-a-service business model, which sees criminal networks and individual criminal entrepreneurs offer criminal activities as a service to others. Crime-as-a-service is a broad concept and may involve the delivery of any criminal services, ranging from the provision of technical cybercrime applications to money-laundering services.

In order to capture the full complexity and flexible nature of modern organised crime networks, other elements should be taken into account. This includes the roles occupied by individuals and groups in the networks, ad hoc collaboration, changing partnerships and cooperation between criminals of many nationalities. This can be used to guide an operational approach to identify weaknesses in criminal networks and high-value targets (HVTs)[5].

Focusing on the roles and crime infrastructure can also highlight the impact and importance of the actors involved in criminal activities. This approach allows for the identification of HVTs involved in criminal operations. HVTs may be embedded in a criminal network or operate independently, providing vital criminal services as money brokers, hitmen, lawyers, accountants, information and contact brokers, document forgers, providers of technical/encryption solutions, among others.

DEVELOPING A CONCEPT OF CRIMINAL PROCESSES

The process steps of a criminal activity are determined by the nature of the crime, such as the need to move physical goods or persons or to exploit infrastructures.

Most criminal activities entail three major consecutive process steps linked to the core activity:

- production/recruitment/acquisition;
- transport of persons/physical goods;
- exploitation of persons/distribution of the goods;

as well as two supporting process steps which can be performed subsequently or concurrently by actors in the criminal infrastructure:

- handling the money flow;
- the use of facilitating services including corruption.

The handling of the money flows and the use of facilitating services are transversal processes. Often they

5 HVTs are those suspects with a critical role within a criminal network whose identification and arrest would seriously damage the criminal network and the criminal activities it is involved in.

are offered as criminal expertise, which is not always available within the criminal group.

Criminal activities such as cybercrime and fraud often do not entail the transport of goods and consist of only three process steps: acquisition, the handling of money and the use of facilitating services.

Groups counting more than 100 members are mostly based on family or clan structures such as Italian mafia clans or criminal groups originating from traveller communities. Other larger groups are often constituted around a common value system such as outlaw motorcycle gangs or thieves-in-law.

A SERVICE-ORIENTED CRIMINAL ECONOMY

Money laundering is an essential component of the vast majority of criminal operations. Most groups and networks (68 %) use basic money laundering methods such as investing in property or high-value goods. Some rely on slightly more sophisticated methods such as the use of cash-intensive businesses.

Money laundering service providers and networks are mainly required to regularly launder large amounts of criminal proceeds using sophisticated and innovative schemes. 32 % of OCGs have access to and make use of these services.

In many cases, service providers enable access to a parallel banking system which allows criminals to transfer money to associates across the world.

Many illegal money brokers and bankers constitute HVTs as they are crucial in enabling money transfers and provide services to different clients. Tackling them will cause disruption in several process chains.

Brokers or intermediaries are crucial in connecting networks, individual criminals and groups. They enable and facilitate criminal business, linking producers with wholesale distributors, and distributors with transport providers.

They also facilitate access to informants, hitmen, document forgers and other criminal specialists.

Eliminating a broker can disrupt criminal operations and even whole criminal networks.

Low-level facilitators are not embedded within the core criminal groups in the criminal networks, but are external actors who facilitate part of the criminal process for financial gain. They can take on roles such as informants, strawpersons, money mules, sailors, pilots, bus drivers, students and fake spouses. In some cases, risk indicators can highlight straw owners who have dozens of vehicles or companies registered in their name. Acting on these straw owners can be a first step towards the detection, investigation and tackling of organised crime. In some cases, these facilitators are coerced through deception, extortion and violence.

Almost 60 % of the criminal groups reported for the SOCTA 2021 engage in corruption.

Many use corruption only occasionally, but a smaller proportion of criminal networks engages in frequent and proactive corruption targeting public servants or specific sectors as an intrinsic part of their business strategy. Individuals at all levels of society are targeted for corruption.

Complicit legal and financial advisors as well as lawyers and notaries provide information to criminals on police records and criminal proceedings and assist in setting up fraud schemes and networks of companies to acquire and launder money. They provide advice in setting up shell companies, foundations, trusts and also sometimes facilitate the takeover of legitimate companies to be used for criminal ends. When genuine, they can be important partners in the fight against organised crime.

More than 80 % of the criminal networks active in the EU use legal business structures for their criminal activities.

About half of all criminal networks set up their own legal business structures or infiltrate businesses at a high level.

Legal business structures can be used as tools to carry out core criminal activities, such as using waste management companies for waste and pollution crimes. In other cases, legal business structures are used as shell companies for money laundering purposes and other support functions.

CRITICAL ROLES IN CRIMINAL NETWORKS: HIGH-VALUE TARGETS

By analysing the roles played by those involved in organised crime, we can identify critical functions and individuals that constitute HVTs. Targeting these critical operators and facilitators makes for a stronger and more disruptive law enforcement response. HVTs are key enablers and facilitators of criminal processes. They are not limited to the obvious categories of leaders, organisers, brokers, coordinators, fencers or large-scale money launderers. They can also be persons offering specialist expertise or access to crucial contacts or infrastructures such as technical experts, legal and financial advisors or service providers. Tackling these criminal collaborators will maximise the impact of law enforcement actions.

The use of violence

While consolidated figures quantifying the number of violent incidents related to serious and organised crime are not available, the level of the use of violence associated with serious and organised criminality is perceived to have increased notably, both in terms of frequency and severity, over the last four years.

Violence in illicit markets is often a sign of growing competition (e.g. over the control of lucrative distribution networks or a particular geographic territory). Shifting power balances within or between competing organised crime groups, the impact of law enforcement efforts, or broader economic pressures can also generate violence.

Perpetrating violence on behalf of a criminal client is increasingly being marketed as a service, often via dark web platforms and encrypted communication applications. The violent acts on offer range from threats, intimidation, vandalism and assaults, to kidnapping, torture, mutilation and murder.

Violence is casually discussed and negotiated between criminals seeking violence as a service. The commission of violent acts is increasingly becoming a stand-alone business in the criminal environment. This increasingly diversified business model generates volatile trading relationships, and in turn heightens the sense of distrust among the service-oriented participants – leading to further competition and violence.

As part of this development, violence may become more common to traditionally non-violent criminal activities such as excise fraud or cybercrime.

Perpetrating violence on behalf of a criminal client is increasingly being marketed as a service, often via dark web platforms and encrypted communication applications.

The violent acts on offer range from threats, intimidation, vandalism and assaults, to kidnapping, torture, mutilation and murder.

Violence is employed by criminal networks for a variety of reasons against external parties such as competitors as well as non-criminals (e.g. witnesses and their solicitors, law enforcement and court officers). Internally, criminal networks employ violence against group members or their relatives.

Internal violence is mostly used to ensure discipline and to settle conflicts, to punish whistle-blowers and transgressions against the group's rules or for failed operations. In other cases, violence is used against incarcerated members of the group or their families, to intimidate them into not disclosing information. Internal violence can also be used for extortion within the group. Internal violence may target members at all levels – from lower ranking members and associates (e.g. drug couriers, strawmen, money mules, or other facilitators) to the most senior members as a result of the loss of a commodity or an internal struggle.

External violence is often employed against competing criminal groups, business partners or criminal service providers. Violence among rival groups or competitors is frequently reported in connection with drug trafficking (especially trafficking of heroin and cannabis), migrant smuggling and among criminal groups involved in THB. In some cases, the aim is not only to ensure control over a criminal market, but to dismantle rival criminal networks.

FLUID NETWORKS



BROKERS
Intermediaries that are crucial in connecting criminal networks and individual criminals



MONEY LAUNDERING SERVICE PROVIDERS
Money laundering service providers and networks launder large amounts of criminal proceeds using sophisticated and innovative schemes



LEADERS AND MIDDLE MANAGEMENT
Leaders and organisers overseeing and organising criminal activities



DOCUMENT FRAUDSTERS
Specialised criminals offering document fraud as a service



LEGAL AND FINANCIAL ADVISORS
Complicit legal and financial advisors such as lawyers and notaries provide expertise to criminals



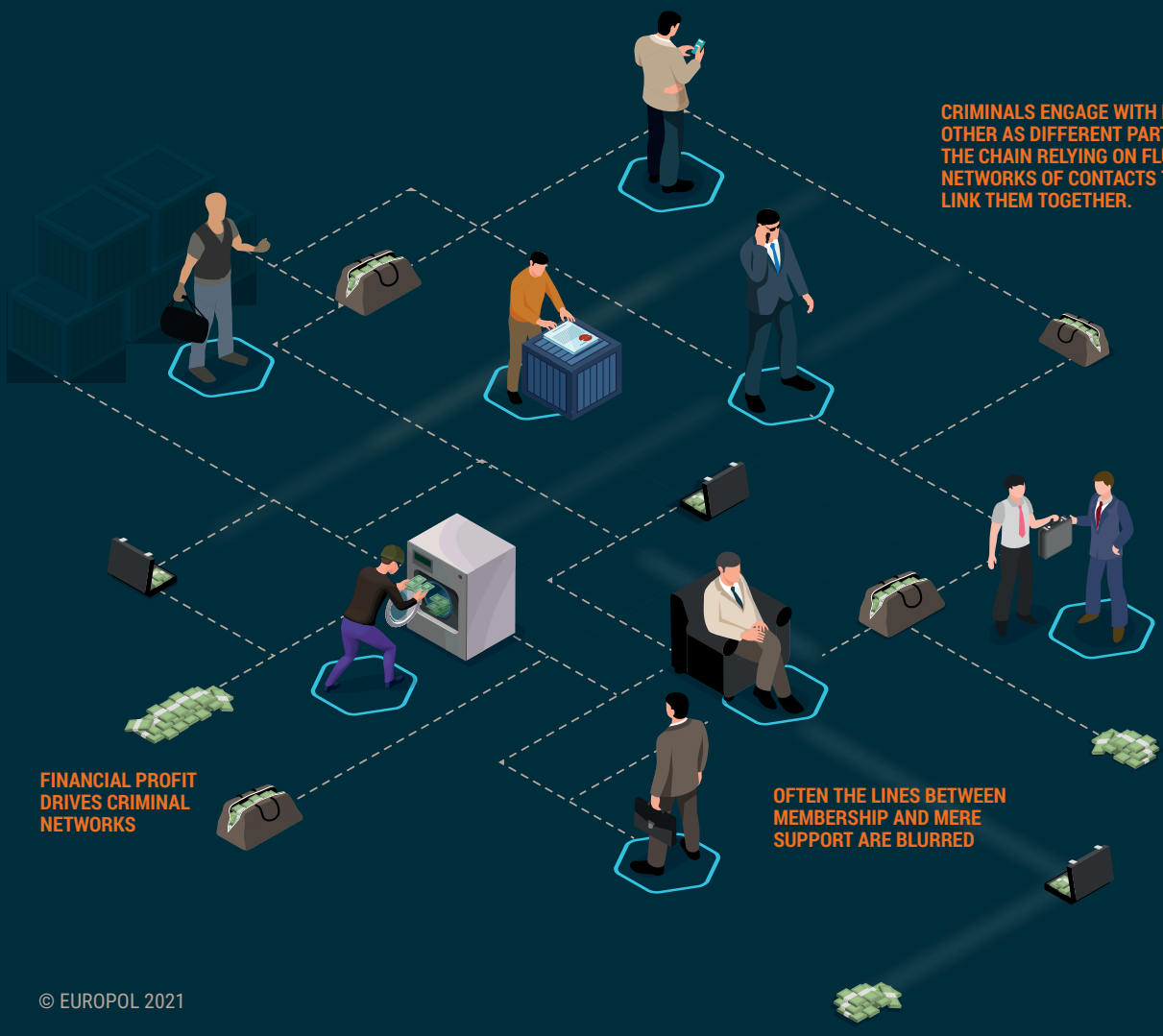
FENCES
Criminals specialised in the sale of stolen goods on behalf of other criminals



LOW-LEVEL FACILITATORS
Individual criminals typically engaging in occasional cooperation with other individuals and/or groups



TRANSPORTATION AND LOGISTICS PROVIDERS
Criminals specialised in transportation services or in facilitating the extraction of goods from airports and ports



© EUROPOL 2021

UNDERWORLD PRISON WITH TORTURE CHAMBER

In June 2020, the Dutch Police arrested six men suspected of planning kidnappings. The police discovered a warehouse containing seven maritime shipping containers that had been converted into cells and a torture chamber. The criminals had shared photos of one container equipped with a dental chair complete with straps on the armrests and footrest. Other torture instruments were visible in the photos. The containers had also been soundproofed. The upcoming kidnappings seemed to be prepared with great precision. The criminal network comprised several teams (including an observation team) and had stored weapons, police clothing, vans, stop signs and bulletproof vests.

Source: https://www.politie.nl/nieuws/2020/juli/7/11-onderwereldgevangenis-met-martelkamer-ontdekt.html

Date: 7 July 2020

Violence may also be used to show dissatisfaction with the quality of an illicit commodity or a criminal service, or simply as a favour or service to a criminal associate.

Legal business structures: key tools for organised crime

Criminals and criminal networks use legitimate business structures, such as companies or other legal entities, to enable or obscure criminal activities. Virtually all types of criminal activity in the area of serious and organised crime can potentially entail the abuse of legal business structures. Criminals infiltrate existing business structures to take advantage of the façade of legitimacy and evade law enforcement attention. Criminal groups also set up ad hoc businesses (i.e. 'front' or 'shell' companies) and use them to infiltrate the legal market.

The abuse of legal businesses can be systematic and long-term, or temporary and occasional. Sometimes the owner(s) of the legal business are also members of the criminal network and directly benefit from illicit activities. In other cases, legal businesses engage with criminals in a crime-as-a-service arrangement of cooperation. Criminal groups also infiltrate businesses by introducing criminal associates to the staff.

Legal business structures are also commonly used to launder the criminal proceeds and re-introduce them into the financial system. Money service businesses, offshore companies and cash-intensive businesses involved in hospitality and retail, among other sectors, are frequently used to move and launder illicit profits. Currency exchanges are used to integrate criminal proceeds into the legal economy.

The COVID-19 pandemic may be followed by an economic recession. It is likely that criminals will exploit vulnerabilities in the economy to infiltrate legal businesses in order to facilitate their criminal activities. This may entail loaning funds to struggling businesses and making them dependent on criminal financiers or directly buying up companies in financial difficulties.

Links between serious and organised crime and terrorism

Both terrorist and criminal groups operate outside the law and share the aim of eluding law enforcement authorities. However, their core motivations remain largely divergent: while organised crime seeks profit above all else, terrorists largely pursue political or ideological aims. In the EU, there is little evidence of systematic cooperation between criminals and terrorists. In addition, criminals are thought to be reluctant to cooperate with terrorists because of the attention such cooperation might attract from intelligence and law enforcement services. When it occurs, interaction between criminal and terrorist groups is mostly transaction-based.

The areas where the interests of criminals and terrorists overlap, and on which both groups are dependent, include the same sources for weapons, forged documents, finances and a shared pool of potential recruits.

ORGANISED CRIME UNDERMINES SOCIETIES

Corruption

Corruption is the abuse of entrusted power for private gain[6]. Corruption can take the form of bribery, influence peddling, nepotism, and abuse of authority, among others. As an enabler for crime and terrorism, corruption constitutes a threat to security. It is also detrimental to economic growth as it creates business uncertainty and imposes additional costs[7]. Corruption also undermines the effective running of state institutions and negatively impacts citizens' interactions with their governments and civil societies.

Corruption is an integral element of almost every organised crime activity. It is used to gain influence and to infiltrate private and public sector organisations.

Criminals use corruption to influence some sectors of critical importance to Member States, such as healthcare and pharmaceuticals, transportation, construction, tourism, education and research, waste management, aerospace and defence, agriculture, and labour and social protection.

Though widespread, corruption is insidious and often invisible. Presumed chronic under-reporting of corruption makes it difficult to evaluate the phenomenon as a criminal threat. The underlying mechanics of corruption have not changed over time. However, the means by which it is implemented reflects changes in technology and society. For instance, cryptocurrencies are increasingly used to make payments to corrupt officials and for money-laundering purposes. In addition, the digitalisation of public administration will lead to the increased targeting of individuals within companies and public services who can manipulate processes and decisions in digital systems or can otherwise facilitate access to valuable information.

Criminal finances and money laundering

Money laundering is the legalisation of criminally acquired funds derived from all profit-motivated crime. Money laundering was traditionally a parallel activity to a predicate offence – enabling criminals and terrorist groups to hide the sources of illicit income and assets. However, large-scale money laundering has evolved into complex schemes that are offered as services by specialised groups to other criminals for a fee.

Money laundering has a significant impact across a number of areas. Not only does the parallel economy of money laundering allow criminal structures to expand, it also causes considerable losses to public revenue, as well as other negative consequences such as infiltration into legitimate business, distortion of competition and the free market environment, compromise of business structures and exposing business sectors to risk, and jeopardising financial institutions with the potential of affecting entire financial systems.

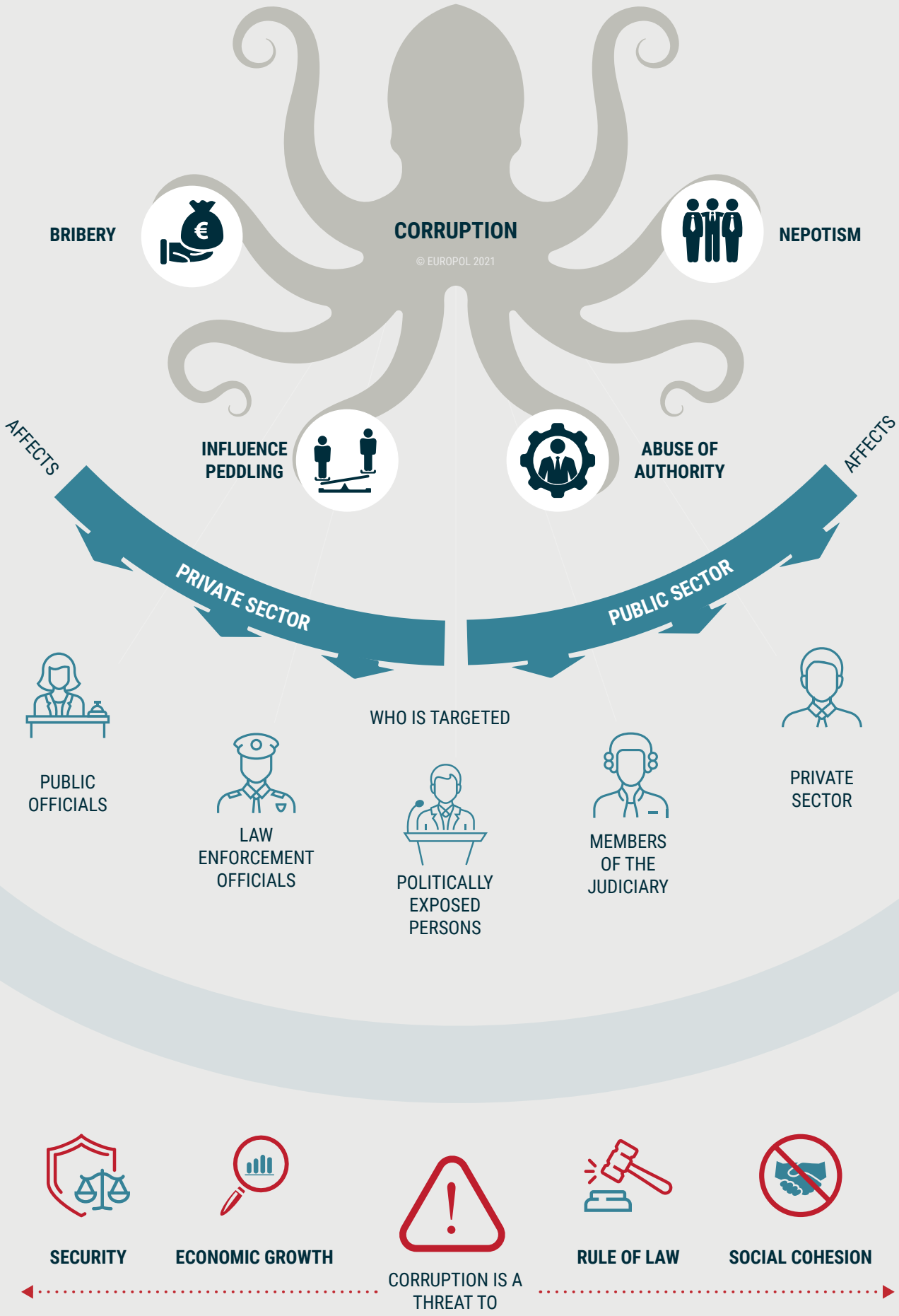
Since financial gain is the primary motivation behind almost all forms of serious and organised crime, the laundering of illicit proceeds forms an integral part of criminal infrastructures. Money laundering enables criminal networks to legitimise or conceal their assets from law enforcement, make profits and reinvest illicit funds into further criminality or terrorism. Both supply and demand in the area of money laundering are high, with demand being driven by the rate of profit and also by the level of difficulty faced in accessing the financial system.

The precise scale of illicit finance generated through money laundering is difficult to assess due to serious intelligence gaps on criminal turnover and profits.

Money laundering can range from self-laundering schemes to sophisticated, large-scale laundering services which require specialist organisation.

6 Corruptie.org 2021, What is corruption, accessible at http://www.corruptie.org/en/corruption/what-is-corruption/

7 European Commission 2017, Directorate-General for Migration and Home Affairs 2017, Special Eurobarometer 470, accessible at https://op.europa.eu/nl/publication-detail/-/publication/531fa14f-2b2b-11e8-b5fe-01aa75ed71a1/language-en; Contribution for the SOCTA 2021: European Commission (DG Home and DG TAXUD).


BRIBERY
CORRUPTION
© EUROPOL 2021
NEPOTISM
INFLUENCE PEDDLING
ABUSE OF AUTHORITY
AFFECTS
PRIVATE SECTOR
PUBLIC SECTOR
AFFECTS
WHO IS TARGETED
PUBLIC OFFICIALS
LAW ENFORCEMENT OFFICIALS
POLITICALLY EXPOSED PERSONS
MEMBERS OF THE JUDICIARY
PRIVATE SECTOR
SECURITY
ECONOMIC GROWTH
CORRUPTION IS A THREAT TO
RULE OF LAW
SOCIAL COHESION

ITALIAN OPERATION ARRESTS TEN MEMBERS OF AN ORGANISED CRIME GROUP

An international operation successfully dismantled an organised crime group which was suspected of money laundering and illegally trading gold. Ten members of the targeted organised crime group were arrested and four arrest warrants were issued for criminals in Romania and Turkey. The members of the organised crime group originated from China, Italy, Romania and Turkey. During the operation, the Guardia di Finanza seized EUR 260 000. In addition, the Judge for Preliminary Investigations in Bologna ordered the freezing of EUR 7.4 million in assets.

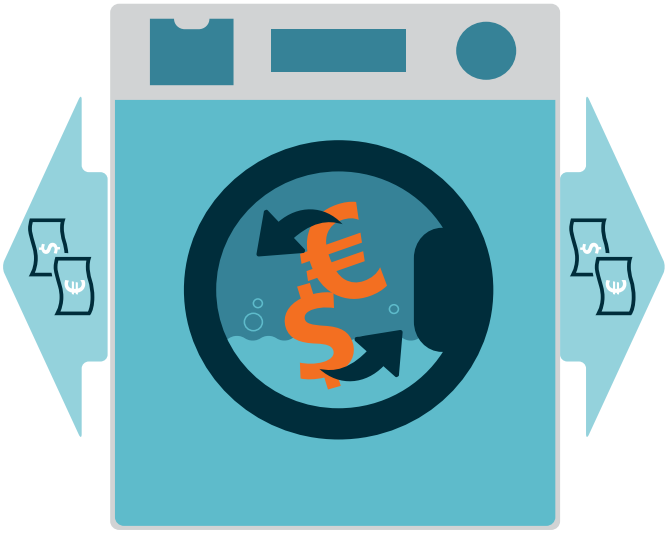
The aim of the operation was to dismantle the group, which was active in international money laundering. The Guardia di Finanza had been collecting evidence against the group for two years. The investigation led to the seizure of over 70 kg of gold (valued at EUR 2.5 million) and EUR 1.5 million in cash. The main target, a 50-year-old Turkish national, collected cash from Chinese business people wishing to commit tax evasion. He invested the collected cash and bought gold, which he traded on the legal gold market. He then transferred the profits to bank accounts in Romania and Turkey, and eventually to bank accounts in the UK owned by the Chinese criminals who led the crime group.

Source: https://www.europol.europa.eu/newsroom/news/italian-operation-arrests-ten-members-of-organised-crime-group

Date: 13 December 2018

While money laundering is the result of all profit-motivated criminal activities, the predicate crimes associated with money laundering investigations are most commonly fraud and drug trafficking offences. Of the criminal networks reported to be involved in money laundering as their main activity, nearly half (49 %) were also involved in drug offences, and nearly one third (33 %) in fraud.

Enhanced EU legislation in the field of anti-money laundering and the resulting increase of financial supervision in the banking sector has made it more difficult for criminal networks to introduce illicit proceeds into the legal economy through traditional banking channels. As a result, money laundering attempts are likely to be displaced towards sectors with nascent controls or limited oversight. This could include the use of underground remittance



agencies, alternative banking platforms, international trade, and anonymous virtual currencies. The use of cryptocurrencies is an area of growing concern, due to the absence of a common regulatory regime and the level of anonymity these products offer.

Professional money laundering networks continue to pose a major threat[8] .

Over half of all contributing countries reported the existence of specialised criminal networks and individual experts offering money laundering as a service on a subcontractor basis. Criminal networks appear to be increasingly outsourcing their money-laundering activities. Reasons for this could include the desire to distance themselves from the predicate offence or out of necessity for expert help on how to launder money without being detected[9]. Professional money laundering networks have the expertise and necessary infrastructure to exploit the legal financial industry and offer a wide range of laundering services to other criminal networks in exchange for a fee or a commission. These include currency conversion operations, international transfers bolstered by fictitious contracts and invoices, and alternative payment systems, as well as services designed to conceal beneficial ownership (e.g. locating investments or purchasing assets, establishing companies or legal arrangements, acting as nominees, or providing account management services).

CRYPTOCURRENCY-LAUNDERING-AS-A-SERVICE: MEMBERS OF A CRIMINAL ORGANISATION ARRESTED IN SPAIN

The criminals carried out several money laundering schemes involving the transfer from fiat currency to virtual assets in order to hide the illegal origin of proceeds. Some of the identified modi operandi used crypto automated teller machines (ATMs) and smurfing, a criminal method used to split illicit proceeds into smaller sums before placing these small amounts into the financial system to avoid suspicious transaction reporting.

The organisation managed a cryptocurrency exchange business, including two crypto ATMs to deposit criminal cash and transform it into cryptocurrency for the benefit of other criminal groups. Cash pick-ups carried out by cash-carriers followed by smurfing techniques to deposit the criminal cash in several bank accounts controlled by the organisation. The funds were moved through several accounts in the process of layering. The money was then exchanged into cryptocurrency.

Source: https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain

Date: 8 May 2019

8 Levi 2020, Trends in Organized Crime – Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation, accessible at https://doi.org/10.1007/s12117-020-09401-y

9 Financial Action Task Force (FATF) 2018, Professional Money Laundering , accessible at https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf

These networks typically maintain business structures, including shell companies in offshore jurisdictions and exploit legal entities registered in European countries on a large scale, especially in jurisdictions in which there is a heightened risk of money laundering. Professional money launderers also hold bank accounts in several countries, and are capable of employing a wide range of laundering techniques, ranging from cash couriers, money mule networks, underground banking to more complex techniques such as bitcoin trading and compensation schemes implemented by international brokers. Criminal networks who contract the services of professional money launderers are often involved in a range of crime areas; these are mainly drug trafficking, fraud and tax fraud, but can also include various other forms of trafficking and smuggling (e.g. human trafficking, firearms trafficking, and the smuggling of tobacco and alcohol), as well as THB and terrorism financing. Professional money laundering services are offered on a transactional basis; however, more stable relationships have also been observed as a result of longer-term cooperation. Some brokers are well-known and sought after, while other relationships are based on references. While more traditional forms of cooperation still exist, they tend to focus on shared infrastructure (companies, enablers, couriers, remitters) and occasional cooperation is related to recruitment and the maintenance of cash flows.

FOCUS ON ASSET RECOVERY – A KEY TOOL TO CONFRONT SERIOUS AND ORGANISED CRIME

Given that most offences are financially driven, asset recovery is a powerful deterrent in the fight against crime. It deprives criminals of their ill-gotten assets and denies them the capacity to reinvest them in further crime as well as to integrate them into the mainstream economy. However, the effectiveness of the EU in this domain is reportedly low, with more than 98 % of the proceeds of crime remaining in the hands of criminals [10].

Europol perceives a need to considerably strengthen the asset recovery regime in the EU and identifies several key points for improvement.

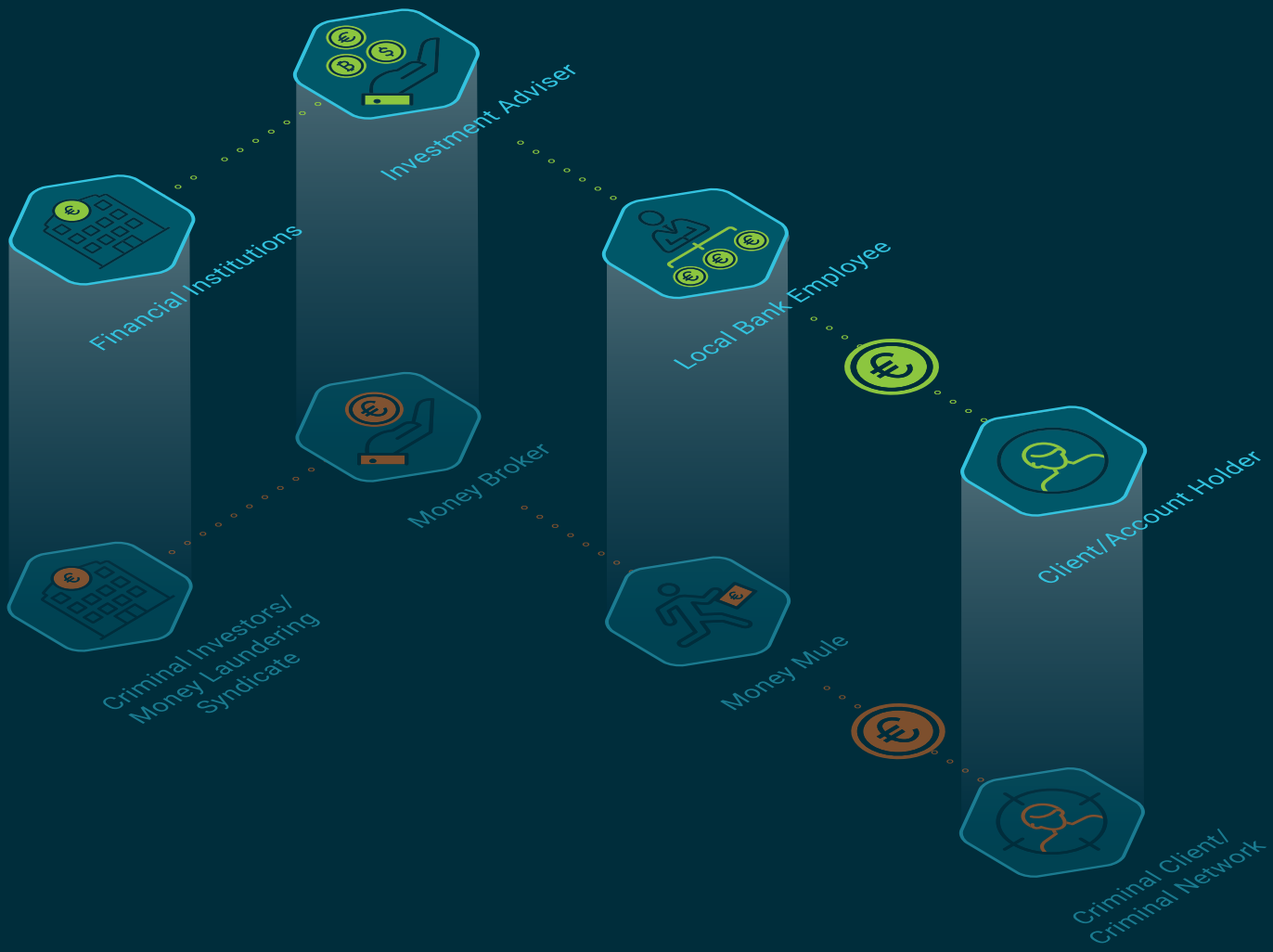
Asset recovery is a process with five stages: identification, freezing, management, confiscation and disposal. From the first to the last stage, the lifecycle of a criminal asset relies on the cooperation of different protagonists, which continues to represent a challenge in practice. Europol sees a need to better integrate and align the entire asset recovery process among law enforcement, judiciary and asset management offices.

In each Member State, asset recovery offices (ARO) are the specialised units for asset forfeiture. They may share their competency with other units at national level, but they are usually the main responsible units for international cooperation. From 2016 to 2020, according to information received by Europol, the volume of information exchanged among EU AROs in the framework of international cooperation doubled, while staffing levels increased by 18 % on average. This gap is one indicator of the difficulties for AROs to follow up on each case. Adequate prioritisation of asset recovery, also in the framework of SOCTA, needs to continue to promote this important law enforcement activity, with a view to strengthening the overall EU fight against crime.

10 Europol 2016, Does crime still pay? Criminal asset recovery in the EU [1 February 2016], accessible at https://www.europol.europa.eu/publications-documents/does-crime-still-pay

PARALLEL CRIMINAL FINANCIAL SYSTEM

There is a parallel underground financial industry providing services to criminals and their networks completely detached from the oversight mechanisms governing the licit financial services industry.



CRIMINAL SYSTEM

LEGAL SYSTEM

© EUROPOL 2021

Criminal content online

Commerce, communication and the access to information are dominated by the internet. The digital transformation of our economies, societies and private lives is progressing fast and will continue to impact all aspects of life. Unsurprisingly, these developments have also had a fundamental impact on serious and organised crime in the EU.

Virtually all criminal activities now feature some online components, such as digital solutions facilitating criminal communications.

The online domain has transformed retail and commerce. Digital marketplaces have made goods more accessible. Specialised websites and dedicated apps have quickly multiplied and have simplified access to all types of commodities and services.

The transformation of legal commerce has also been reflected in the criminal domain. Most illicit activities have at least partially moved online. The surface web and the dark web are exploited by criminals who offer all types of illicit commodities and most illegal services online. The availability and accessibility of secure online channels has resulted in a diversification of the platforms used for illegal online trade. The proliferation of encrypted communication channels and social media platforms allows criminals to easily advertise their illicit offers to a greater number of potential customers. Criminals use various countermeasures to ensure their operational security online, and rely in so doing on services such as virtual private networks (VPNs), proxies and anonymous or The Onion Router (TOR) browsers. Depending on the commodity or service offered, vendors use marketplaces, dedicated shops or internet fora on the surface and dark webs. Social media market places, closed groups and messaging services are widely used, as are encrypted messaging services.

Online retail offers direct access to a broader scope of consumers. This development has also entailed a steep increase in the use of small parcels, via postal or express courier services, to distribute illicit goods. Due to the high volume in post shipments, small consignments are less likely to be detected.

Social media mirror advertisements on websites and serve as dedicated channels for marketing or communication channels for criminal networks. All available illicit goods and services are also visible on social media.

Social media and instant messaging services are also used to spread disinformation. While spreading disinformation in itself often does not amount to criminal behaviour, it can encourage or facilitate criminal activities. Similar disinformation campaigns have also been instigated by fraudsters and counterfeiters in the context of the COVID-19 pandemic to generate sales for their products or to lure victims into fraud schemes.

Cybercrime services can be purchased by paying a user fee, a rental fee or a percentage of the criminal profits. Criminal tools such as malware, ransomware, phishing facilitators, sniffers, skimmers and distributed denial-of-service (DDoS) attacks are offered online, especially on the dark web. In addition, credit card information from the victims of fraud is sold as so-called credit card dumps. The crime-as-a-service business model makes criminal services easily available to anyone, lowering the level of expertise previously required to perform specific criminal activities.

Finally, online platforms provide accessible instructions on how to perform most crimes. Manuals and tutorials on offer range from the production of synthetic drugs, the manufacture of crude firearms and improvised explosive devices, to all types of cybercrime activities.

The dark web also shows high levels of volatility. Law enforcement successes in taking down popular market places, in combination with cyberattacks on platforms, exit fraud or voluntary closures, appear to have generated some distrust among users and may have slowed down the growth of this online environment [11].

Cryptocurrencies remain an important means of payment for criminal services and products. Their decentralisation and semi-anonymity continue to make them attractive for criminal transactions.

Cryptocurrencies are commonly used by fraudsters. Illicit proceeds may be already in the form of virtual currencies or digitally converted. New money laundering techniques relying on cryptocurrencies involve the use of mixing services and coin swappers.

11 Europol 2020, Internet Organised Crime Threat Assessment (IOCTA) 2020, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

ENCRYPTION

Encryption technology is widely used for both licit and illicit purposes. Encryption ensures privacy, confidentiality, data integrity, and protects personal data in communications. End-to-end encryption has become a standard security feature for many communication channels, including instant messaging applications and other online platforms[12]. Encryption benefits all users. Unfortunately, this includes criminals and their networks. Criminals have employed different types of encryption to protect their communications from law enforcement surveillance online and offline for many years.

DEDICATED ENCRYPTED COMMUNICATION PLATFORMS FOR CRIMINALS

Several providers offer secure communication services relying on modified mobile devices. Some of these services are believed to directly and intentionally cater for the communication needs of criminals. The devices offered by these communication services allegedly guarantee perfect anonymity and have functions, such as camera, microphone, GPS, USB ports, disabled. These services remove any association between the device or SIM card and the user. The encrypted interface is typically hidden and works as part of a dual operating system. These phones are sold via networks of underground re-sellers instead of being distributed via regular retail outlets.

In recent months, several investigations into these types of communication platforms have allowed law enforcement authorities in the EU to look into the operations of criminal networks. Millions of messages exchanged between criminals provide a unique, unprecedented insight into the criminal landscape.

12 Council of the European Union 2020, Council Resolution on Encryption – Security through encryption and security despite encryption [14 December 2020], accessible at https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/

CRIME SCENES:
LOCATIONS OF CRIME IN THE EU

International mobility is a defining characteristic of criminal networks. Some criminal operations have global reach beyond borders. Some locations feature characteristics that benefit serious and organised crime in the EU and beyond. These locations are used to facilitate a single or multiple criminal activities, sometimes simultaneously. Key locations attract criminals due to their geographic position, proximity to or connections with source countries and consumer markets. They may offer efficient transport infrastructures, business and investment opportunities or other advantages to criminals.

Key locations encompass specific locations such as particular cities, motorways or ferry connections as well as more general types of infrastructure, regions, or countries.

Criminal activities in border regions take advantage of the natural delineations of individual law enforcement jurisdictions which create options to evade law enforcement and provide proximity to multiple markets. Within the Schengen Area, border travel is unimpeded, allowing free movement of persons across borders. Geopolitical developments determine the relevance of specific regions for the flow of goods and people. Humanitarian emergencies, bilateral agreements and risk-reward considerations determine the attractiveness of a specific border region or section for criminals.

Urban areas are characterised by a concentration of people and often present a multitude of criminal opportunities. Burglaries are concentrated in urban areas. Pickpockets target victims in crowded places such as concerts, markets, on public transport or at railway stations. Organised robberies typically take place in urban areas and border regions. Victims of trafficking in human beings are typically exploited in urban areas where there is a larger potential client base. Capitals and major cities act as hubs along the main migrant smuggling routes. Here, migrants are temporarily accommodated in safehouses, receive fraudulent documents, plan and initiate secondary movements.

Remote areas provide more anonymity conducive to other criminal activities. Illicit tobacco production lines are usually set up in large warehouses in remote industrial areas, close to transportation hubs like motorways, border crossing points or ports. Remote areas in the countryside are ideal locations for the dumping of chemical waste from synthetic drug production, toxic waste from fuel laundering and other waste products. Thefts of construction and agricultural machinery are more likely to occur in rural areas. Archaeological sites and places of religious worship situated in remote areas are targeted for theft and looting. Trafficking of human beings for labour exploitation often takes place in rural areas home to agricultural production.

Airports are key transit points for goods and people, both licit and otherwise. Criminals make frequent use of the EU's main airports as well as smaller regional airports operating low-cost airlines. In addition, small airfields offer convenient access to the EU and specific regions. Trafficking activities by air have been disrupted during the COVID-19 pandemic. However, expansion plans for many major airports signal a further growth in passenger flows after the end of the pandemic.

A dense network of well-maintained motorways facilitates the free movement of goods and services within the EU. It is also a major crime enabler allowing criminals to travel and move goods quickly and anonymously. Travel by road is the most accessible way of travelling within the EU. Transport means on the road include lorries, vans, buses, cars, caravans, or taxis. Some vehicles are equipped with sophisticated concealment methods to hide drugs and other contraband or persons. Motorway infrastructure is used for smuggling raw material to production facilities and for distributing illicit goods produced in the EU or arriving at entry points.

Criminals use European rail infrastructure to transport illegal goods such as drugs, stolen vehicles (and their parts), illicit tobacco products, as well as irregular migrants. Both freight and passenger trains are used. Transport by train is of relevance for intra-EU trafficking (e.g. of cocaine), for export out of the EU (e.g. stolen vehicles) or for import into the EU (e.g. of precursors of synthetic drugs). Illicit cigarettes are concealed between legal cargo or in hidden compartments, which is then typically thrown out of the trains after entering the EU via an external border.

EU ports are key locations for incoming, outgoing and transiting shipments of illegal goods. Cocaine, heroin and precursors for synthetic drugs enter the EU through ports in large quantities.

Other illegal goods such as illicit waste, synthetic drugs produced in the EU, and stolen vehicles or parts are shipped throughout the world departing from EU ports.

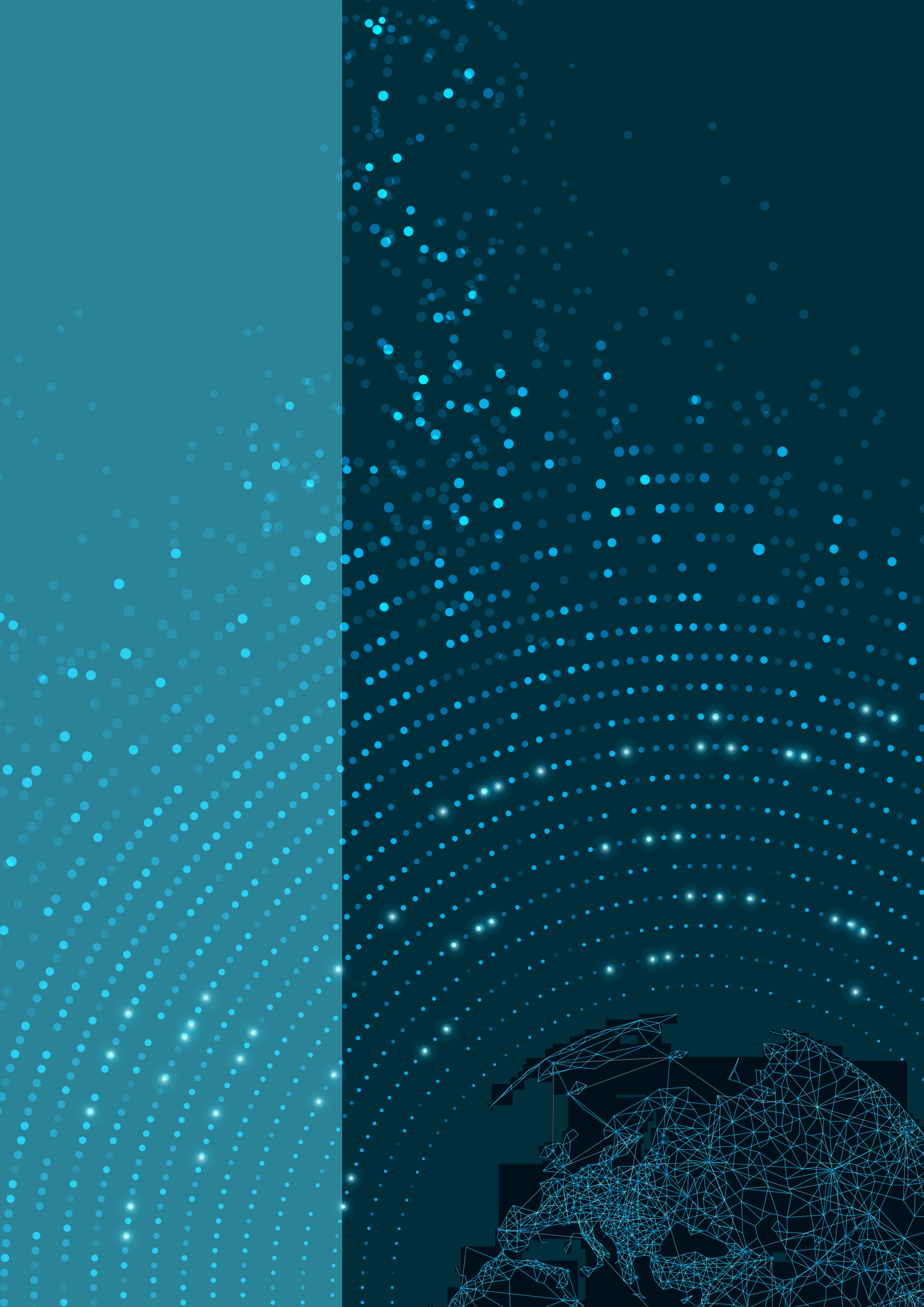
Accelerated by the COVID-19 pandemic, the shipping of orders placed online fulfilled by post and parcel services continues to expand in volume every year. Postal and parcel services are abused for the distribution of illicit goods such as drugs (cannabis, cocaine, synthetic drugs including new psychoactive substances), counterfeit currency, stolen and fraudulent documents and many other illegal commodities.

Clandestine locations such as private or rented apartments are used as pop-up brothels where victims are sexually exploited, including children. Apartments serve as safe houses used to conceal irregular migrants in between different legs of their journeys.

Reception centres for asylum applicants are targeted by human traffickers and migrant smugglers to recruit irregular migrants and potential trafficking victims. Upon their entry into the EU, facilitated irregular migrants and victims of THB are often accommodated in reception centres where they apply for international protection.



WHAT ARE THE MAIN SERIOUS AND ORGANISED **CRIME ACTIVITIES IN THE EU?**





CYBERCRIME

Cyberattacks targeting citizens, businesses and critical infrastructure

Cyber-dependent crime is any criminal activity that can only be committed using computers, computer networks or other forms of information communication technology (ICT). Such crimes are typically directed at computers, networks or other ICT resources. It includes the creation and spread of malware, hacking to steal sensitive personal or industry data, denial of service attacks to cause financial and/or reputational damage and other criminal activities.

The threat from cyber-dependent crime has been increasing over the last years, not only in terms of the number of attacks reported but also in terms of the sophistication of attacks. Cyber-dependent crime is likely significantly underreported.

Cyber-dependent crime causes significant financial loss to businesses, private citizens and the public sector each year through payments for ransomware, incident recovery costs and costs for enhanced cyber-security measures. Attacks to critical infrastructure have a significant impact and can potentially entail severe consequences, including loss of life.

The rapidly progressing digitalisation of society and the economy constantly creates new opportunities for criminals involved in cyber-dependent crime. The steady increase in the number of users and connections creates new vulnerabilities and opens more potential victims to cyberattacks. During 2020, the COVID-19 pandemic has seen a surge in connections from private to corporate systems as telework became the norm in many sectors and industries. This development has made many corporate networks more vulnerable to cyberattacks.

The availability of cybercrime services online as part of a crime-as-a-service business model makes cybercrime more accessible by lowering the technological expertise required to carry out these crimes.

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED

EMOTET has been one of the most professional and long lasting cybercrime services out there. First discovered as a banking Trojan in 2014, the malware evolved into the go-to solution for cybercriminals over the years. The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale. Once this unauthorised access was established, these were sold to other top-level criminal groups to deploy further illicit activities such data theft and extortion through ransomware.

The EMOTET group managed to take email as an attack vector to a next level. Through a fully automated process, EMOTET malware was delivered to the victims' computers via infected e-mail attachments. A variety of different lures were used to trick unsuspecting users into opening these malicious attachments. In the past, EMOTET email campaigns have also been presented as invoices, shipping notices and information about COVID-19.

EMOTET was much more than just a malware. What made EMOTET so dangerous is that the malware was offered for hire to other cybercriminals to install other types of malware, such as banking Trojans or ransomwares, onto a victim's computer.

This type of attack is called a 'loader' operation, and EMOTET is said to be one of the biggest players in the cybercrime world as other malware operators like TrickBot and Ryuk have benefited from it.

Its unique way of infecting networks by spreading the threat laterally after gaining access to just a few devices in the network made it one of the most resilient forms of malware in the wild.

The infrastructure that was used by EMOTET involved several hundreds of servers located across the world, all of these having different functionalities in order to manage the computers of the infected victims, to spread to new ones, to serve other criminal groups, and to ultimately make the network more resilient against takedown attempts.

Source: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

Date: 27 January 2021

Criminal services and tools such as malware, ransomware, DDoS and instructions to perform many types of attacks are offered online, often on the dark web. Cybercrime services and tools can be purchased by paying a user fee, a rental fee or even a percentage of the criminal profits. The affiliate model (also known as ransomware-as-a-service) allows ransomware developers and the cybercriminals that deploy the solutions to share the criminal profits. Developers offer technical expertise and support as service providers to affiliates who are often entry-level cybercriminals that identify and infect vulnerable targets.

Businesses are increasingly the targets of cyberattacks. Public institutions, including critical infrastructures such as health services, continue to be targeted by cybercriminals. A potential leak of data or service disruptions in these sectors could result in very high financial and social costs.

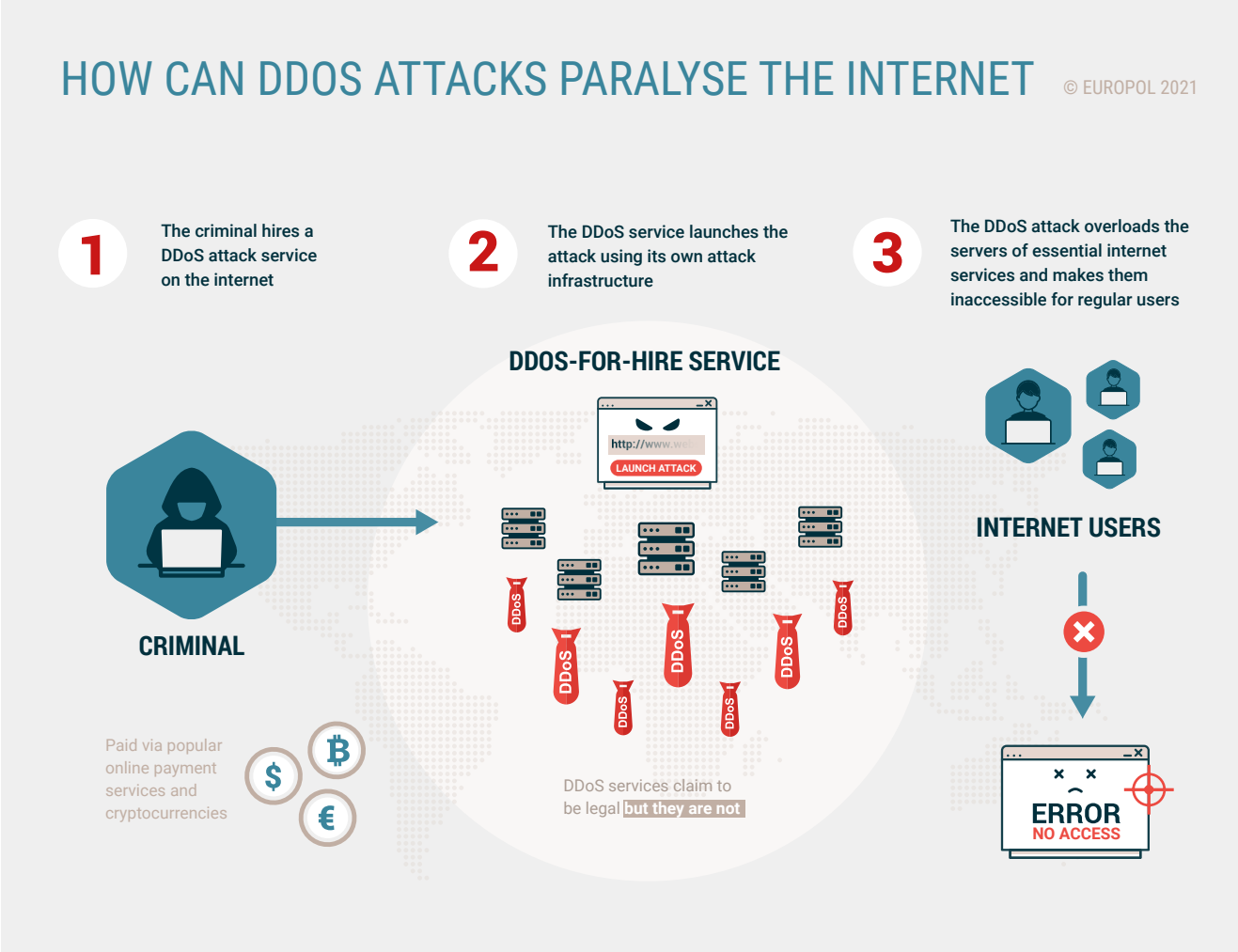
The threat from cyber-dependent crimes is set to further increase in volume and sophistication over the coming years. Cybercrime is highly dynamic, exploiting rapidly advancing technologies. Critical infrastructures will continue to be targeted by cybercriminals in the coming years, which poses significant risks. Developments such as the expansion of the Internet of Things (IoT), the increased use of artificial intelligence (AI), applications for biometrics data or the availability of autonomous vehicles will have a significant impact. These innovations will create criminal opportunities. The performance of AI systems and applications relies on data sets. Malicious access to these data entails the disclosure of personal information. If AI is used in decision-making systems, the manipulation of data may have serious consequences for individual users. The criminal use of AI, including the exploitation of deepfakes, is expected to increase in the future. The incorporation of AI into existing techniques may widen the scope and scale of cyberattacks[13].

The use of cryptocurrencies and the proliferation of anonymisation techniques, including encryption, will continue to grow.

Cyber-dependent crime comprises a number of different attack techniques and modi operandi, which are constantly evolving in order to exploit previously unknown vulnerabilities.

MALWARE

Malware is a common type of cyberattack that uses malicious code to infiltrate and take over a computer, network or mobile device. Malware attacks aim to steal data and carry out identity theft, cause service disruptions and support espionage.



13 TrendMicro, UNICRI and Europol 2020, Malicious uses and abuses of artificial intelligence, accessible at https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence

Cybercriminals deploying malware attacks are primarily driven by a profit motive and, to a lesser degree, attempts to build up their reputation in the hacking community.

Malware is a widely used cybercrime tool. Malware constantly evolves and is highly diverse, existing in hundreds of thousands of variants. The EU's cybersecurity agency ENISA reports the detection of 230 000 new strains of malware every day[14].

RANSOMWARE

Ransomware has been acknowledged as a key cybercrime threat for some years now. However, the number of attacks and the level of their sophistication continues to increase. The increase in the number of attacks on public institutions and large companies is particularly notable.

DISTRIBUTED DENIAL OF SERVICE

DDoS attacks are a well-known and persistent threat that are designed to disrupt or shut down a service/network by overwhelming it. Cybercriminals orchestrate persistent attacks which might be followed by ransom requests offering to cease the attack in exchange for a payment. Cybercriminals now increasingly target smaller organisations with lower security standards[15]. However, they continue to attack public institutions and critical infrastructures as well.

CRIMINAL OFFENDERS

Cybercrime is attractive to criminals due to the potential profits, limited risk of detection and prosecution, which if successful often only results in low sentences. Various types of criminals are involved in cyber-dependent crimes, ranging from structured criminal groups to lone offenders. Potential offenders without any specific expertise can also carry out cybercrime attacks by relying on tools and services available to them through crime-as-a-service.

Online child sexual exploitation

Online child sexual exploitation includes all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment.

Child sexual abuse is traumatic and often entails long-lasting and severe damage to the physical and psychological wellbeing of the victims, which can lead to self-harm, including suicide. This type of abuse typically also involves harassment, systematic abuse and verbal, psychological and physical violence against children.

There has been a continuous increase in activities related to online child sexual abuse over recent years. Child sexual exploitation targets the most vulnerable members of society.

Online child abuse material can easily be accessed on all types of devices, including mobile devices. The widespread abuse of encryption tools, including end-to-end encrypted apps, has lowered the risk of detection by offenders[16]. Offenders increasingly rely on anonymisation services such as virtual private networks (VPNs) or proxy servers. The number of reported incidents involving live distance child abuse has steadily increased in recent years. This development has further intensified during the COVID-19 pandemic. As a result of the lockdown measures imposed to halt the spread of the COVID-19 pandemic, children have been spending more time online unsupervised, making them more vulnerable to exploitation. While most of the cases of live distance child abuse take place in Southeast Asian countries, especially in the Philippines, cases of live distance child abuse in the EU have also recently been detected[17].

14 ENISA 2020, Main incidents in the EU and worldwide, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

15 Europol 2020, Internet Organised Crime Threat Assessment (IOCTA) 2020 [5 October 2020], accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

16 Eurojust and Europol 2019, Common challenges in combating cybercrime, accessible at https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime

17 Europol 2020, Internet Organised Crime Threat Assessment (IOCTA) 2020 [5 October 2020], accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Child sexual abuse material is typically produced in the victim's domestic environment and most often by those in the child's circle of trust[18].

Online offenders use fake identities and grooming techniques to gain the victim's trust and obtain illicit content by manipulating or blackmailing them. Victims are often recorded while performing sexual acts without being aware they are being filmed. Offenders use the word 'capping' (which comes from the phrase to capture material of victims) when talking about this kind of material. Child sexual abuse material is usually password-protected and stored locally or through online storage services. These hosting services are often unaware of the material hosted on their servers. Mobile devices are increasingly used to store and distribute child sexual abuse material.

Children now often have unsupervised access to the internet. This exposes children to the potential abuse by criminals as they often do not have the maturity to assess a relationship as friendly or abusive. The normalisation of sexual behaviours online also lowers the threshold for sharing self-generated content consensually or through coercion. The amount of self-generated material produced as a result of manipulation or ransom has increased.

Live distance child abuse refers to the phenomenon of a perpetrator paying to direct the live abuse of children through video-sharing platforms. The abuse is sometimes captured or recorded for further dissemination online, which results in the repeated re-victimisation of the child, as with other types of child abuse material. The vast majority of live-streamed abuse depicts girls below the age of 13 in a home setting[19].

Live streaming is a key threat and the number of incidents involving this type of abuse has been continuously increasing for several years now.

A large number of offenders access and exchange child abuse material online. A smaller number of offenders are involved in the production of materials and in the management of the technical platforms used to exchange abuse materials. Many of these key facilitators are believed to operate on the dark web to exchange expertise on how to maintain operational security and new technical capabilities. They use fora as meeting places where participation is structured similarly to criminal organisations, with affiliation rules, codes of conduct, division of tasks and strict hierarchies[20].

STOP CHILD ABUSE – TRACE AN OBJECT

Europol is currently in possession of more than 40 million images of child sexual abuse from around the world. In June 2017, it launched a crowdsourcing campaign called Stop Child Abuse—Trace An Object. Censored extracts from explicit images are regularly published on their website and members of the public are asked to help in tracing their location or country of origin.

These tips are then used to inform a competent law enforcement authority to further investigate the lead and to assist in the identification of the offender and the victim.

You can help as well! Follow the link to help stop child abuse: Trace an Object

STOPCHILDABUSE
TRACE an OBJECT

18 Australian Institute of Family Studies 2015, Conceptualising the prevention of child sexual abuse, accessible at https://acuresearchbank.acu.edu.au/download/5bb2f7760724b150faee97eef3bf9afcfd4cb50e87d7fbab4096c71055c5c82c/1704205/OA_Quadara_2015_Conceptualising_the_prevention_of_child_sexual.pdf

19 Internet Watch Foundation 2018, Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse, accessible at https://bit.ly/2rIT0LP

20 Europol 2020, Exploiting isolation – Offenders and victims of online child sexual abuse during the COVID 19 pandemic, accessible at https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic



Non-cash payment fraud and other cyber-scams

Non-cash payment fraud encompasses all kinds of fraudulent activities related to classical payment methods, including both card-present and card-not-present payments. Cyber-scams are a diverse range of fraud schemes that are exclusively or primarily perpetrated online. These may include, but are not limited to:

- Business email compromise (BEC) fraud, which targets businesses and organisations and continues to increase in the number of attempts and their sophistication;
- New modi operandi such as SIM Swapping and SMishing, which pose a significant risk to the victims' identities and finances[21] ;
- Online investment fraud, which targets thousands of EU citizens every year and increasingly relies on selling novel investments, such as cryptocurrencies;
- Phishing, which remains a significant threat and is further evolving in sophistication.

Non-cash payment fraud and cyber-scams are well established criminal activities that have been targeting the EU for decades now. The ongoing digitalisation of almost all aspects of life creates additional opportunities for cybercriminals.

The move toward cashless economies creates powerful incentives for payment fraudsters. Cybercriminals seek to compromise online payments, internet and mobile banking, online payment requests, contactless payments (both card-present and not) and mobile applications.

The increasing use of mobile devices for financial transactions and authentication processes has made them a target for cybercriminals.

21 Europol 2020, Internet Organised Crime Threat Assessment (IOCTA) 2020 , accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

TEN HACKERS ARRESTED FOR STRING OF SIM-SWAPPING ATTACKS AGAINST CELEBRITIES

The attacks orchestrated by this criminal gang targeted thousands of victims throughout 2020, including famous internet influencers, sport stars, musicians and their families. The criminals are believed to have stolen from them over USD 100 million in cryptocurrencies after illegally gaining access to their phones.

Initiated in the spring of 2020, the investigation uncovered how a network composed of a dozen criminals worked together to access the victims' phone numbers and take control of their apps or accounts by changing the passwords.

This enabled them to steal money, cryptocurrencies and personal information, including contacts synced with online accounts. They also hijacked social media accounts to post content and send messages masquerading as the victim.

This type of fraud is known as 'sim swapping' and it was identified as a key trend on the rise in the latest Europol Internet Organised Crime Threat Assessment. It involves cybercriminals taking over use of a victim's phone number by essentially deactivating their SIM and porting the allocated number over to a SIM belonging to a member of the criminal network.

This is typically achieved by the criminals exploiting phone service providers to do the swap on their behalf, either via a corrupt insider or using social engineering techniques.

Source: https://www.europol.europa.eu/newsroom/news/ten-hackers-arrested-for-string-of-sim-swapping-attacks-against-celebrities

Date: 10 February 2021



THE TRADE IN ILLEGAL DRUGS IN THE EU

EU drug markets are supplied by sophisticated criminal networks using a variety of modi operandi engaging in wholesale trafficking activities as well as mid-level and retail distribution. The trade in each of the four main commodity groups of illegal drugs dominating European drug markets has unique features. However, a number of elements are common to trafficking activities involving drugs.

The use of violence related to the trade in drugs has escalated notably in recent years. The trade in cocaine and cannabis in particular triggered a significant number of violent incidents, which included killings, shootings, bombings, arsons, kidnappings, torture and intimidation.

In some Member States, competition between drug suppliers has intensified, resulting in an increase in the number of violent clashes.

The nature of violent incidents appears to be changing as well. A growing number of criminals use violence more offensively. The availability of firearms and explosives is a key enabler for serious violence.

Corruption enables drug trafficking. Criminal networks involved in drug trafficking frequently use corruption. However, Member States continue to appear to be either reluctant to report corruption or to suffer from significant intelligence gaps.

Corruption is common in countries of origin and in transit countries for drugs destined for the EU.

Within the EU, recent large investigations supported by Europol have shown that the role of corruption has been largely underestimated.

Corruption is used to undermine transport infrastructure, pass border crossing points or gain access to ports and airports. Criminal networks have infiltrated transport infrastructure across the EU.

Technology is widely used to facilitate the production, trafficking and distribution of drugs. The production and trafficking of drugs is subject to continuous innovation. Encrypted applications, services and devices appear to have emerged as the primary means of communication

among criminals involved in the drugs trade. Encrypted software based on Pretty Good Privacy (PGP) and commercial encryption applications are commonly used. It is now quite uncommon for criminal networks to use unencrypted means of communication.

The online trade in drugs has continued to grow over recent years and has the potential to expand further. However, the supply of drugs via online platforms remains limited compared to traditional offline supply. The online trade in drugs typically takes place at retail level, involving frequent but small individual shipments[22]. Criminal networks engaged in wholesale trafficking of drugs continue to rely on offline logistics.

The use of dark web platforms to distribute drugs has increased, despite some significant law enforcement successes such as the takedown of some of the busiest platforms. These successes, in combination with cyberattacks on platforms, exit fraud or voluntary closures, appear to have generated some distrust among users and may have slowed the growth rate.

Illicit drugs cause serious and direct harm to consumers' health. Drug markets fuel a vast underground economy. Underground economies cause economic dependency, undermine local communities and perpetuate the presence of criminal structures. The presence of criminal networks in local communities undermines social values, weakens the rule of law and contributes to a culture of impunity.

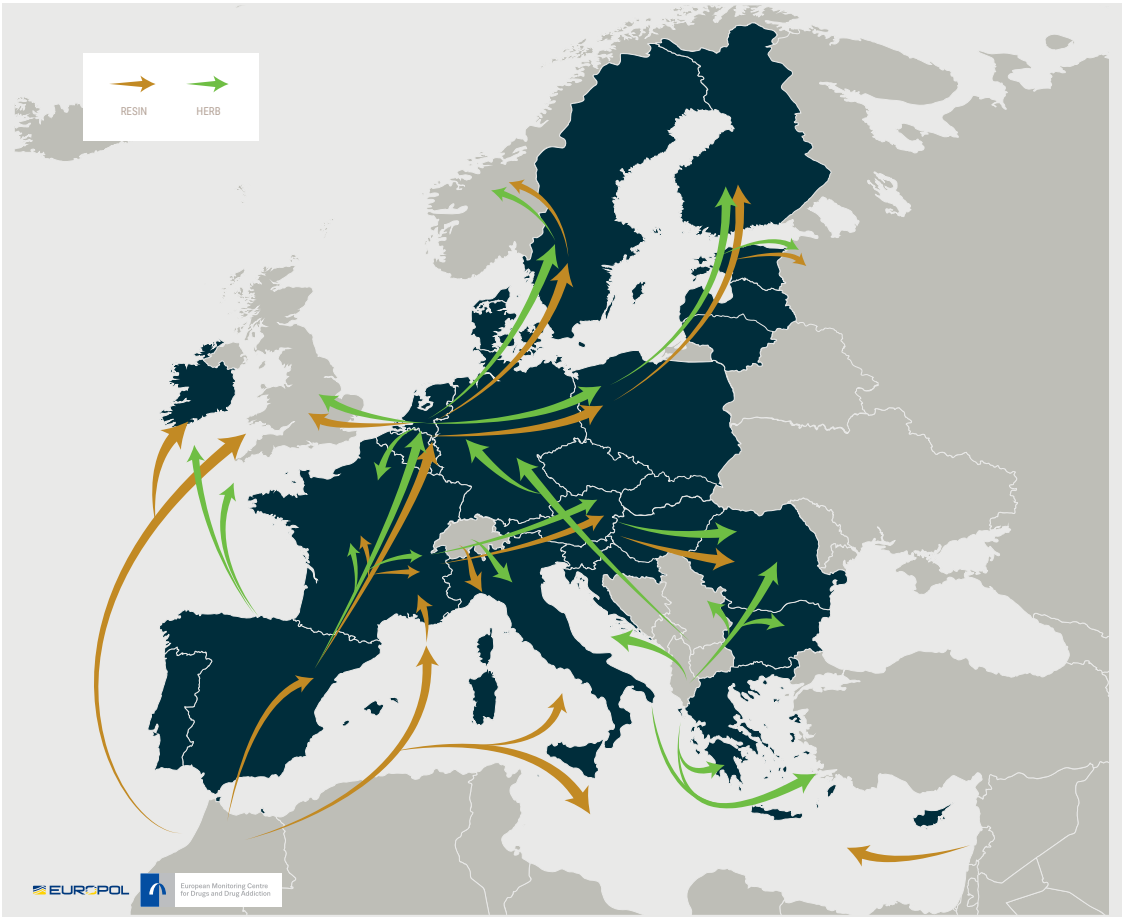
The production of drugs has a significant impact on the environment in the EU. Synthetic drug manufacturing produces significant amounts of hazardous waste. Dumping sites have increased as a result of adding additional steps for the conversion of (pre-)precursors into precursors and dump sites require a long and expensive cleaning process. Outdoor cannabis cultivation significantly damages fauna and flora.

Cannabis

The cannabis market remains by far the largest drug market in the EU, with a majority of Member States reporting that the trade in cannabis is either increasing or stable. Cannabis resin and herbal cannabis remain

CANNABIS

TRAFFICKING ROUTES TO AND WITHIN THE EU



EU DRUGS MARKET REPORT 2019 (EMCDDA AND EUROPOL); EU SOCTA 2021 DATA COLLECTION

22 EMCDDA and Europol 2019, EU Drug Markets Report 2019, accessible at https://www.emcdda.europa.eu/publications/joint-publications/eu-drug-markets-report-2019_en

the two main cannabis products traded in the EU. The average potency of both cannabis resin and herbal cannabis has increased over the last decade. A higher strength/potency of cannabis increases its potential harm.

The cannabis market is expected to remain the largest drug market in the EU. Cannabis trafficking will remain a significant source of income for a wide range of criminal networks. Herbal cannabis production is expected to continue to take place in and close to the profitable EU consumer markets.

EU-based cannabis cultivation will remain innovative in terms of growth, lighting and monitoring methods that increasingly apply laboratory technology to extract and test cannabis[23]. Criminal networks are expected to invest in these developments and a further diversification of cannabis products can be expected.

The distribution of cannabis using post and parcel services is set to further increase and is directly linked to the expanding online trade in drugs.

The establishment of legal cannabis markets in some countries outside the EU has led to the diversion of cannabis from legal supply chains and the emergence of new cannabis products that are difficult to detect on entry to the EU[24].

The indoor cultivation of cannabis in the EU remains the main source of herbal cannabis distributed within the EU. The EU-based production of herbal cannabis continued to expand over recent years.

Cannabis cultivation is believed to take place in all Member States, albeit with different levels of sophistication and scale.

ELECTRICITY BILL OF OVER EUR 1.5 MILLION LEADS POLICE TO 5 ILLEGAL HERBAL CANNABIS PLANTATIONS IN SPAIN

The organised crime network, comprised essentially of Albanian nationals, would locate and equip buildings in quiet areas in the suburbs of Barcelona, Spain, for the large-scale production of herbal cannabis (3-4 harvests per year).

The criminals were diverting the electric and water supply to illegally cultivate the plants indoors. Once harvested, the herbal cannabis was sent to the Netherlands hidden in pallets loaded onto lorries. These criminals widely used encrypted means of communication.

Source: https://www.europol.europa.eu/newsroom/news/electricity-bill-of-over-%E2%82%AC15-million-leads-police-to-5-illegal-marijuana-plantations-in-spain

Date: 26 November 2020

Albania remains a major source of herbal cannabis trafficked into the EU. Morocco remains the main source for cannabis resin trafficked to the EU. Some cannabis resin also originates from Afghanistan, Lebanon and Syria.

Criminal networks engaged in cannabis trafficking are highly organised. They are typically hierarchically structured with roles and levels well-defined around the leadership, or relatively tightly organised but unstructured, and surrounded by a network of individuals engaged in criminal activities. A large share of the cases reported to Europol featuring fatal and serious violence are related to drugs, in particular the trade in cannabis.

23 Cannabis Tech 2019, How Smartphone Apps are Helping the Cannabis Industry Evolve, accessible at https://www.cannabistech.com/articles/how-smartphone-apps-are-helping-the-cannabis-industry-evolve/

24 EMCDDA and Europol 2019, EU Drug Markets Report 2019, accessible at https://www.emcdda.europa.eu/publications/joint-publications/eu-drug-markets-report-2019_en

Cocaine

A number of indicators point to a significant increase in cocaine trafficking activities into the EU over recent years, including estimations that the global manufacture of cocaine is at an all-time high[25]. These indicators also show that EU cocaine seizures are at record heights[26] and that an increasing number of investigations and suspects are being reported to Europol. The purity of cocaine at retail is at the highest level ever recorded in the EU[27]. The majority of Member States report an increase in cocaine trafficking since 2016. The cocaine market has attracted a growing number of EU-based and non-EU criminal networks. More criminal networks have been reported as being involved in cocaine trafficking than for any other criminal activity. Along with the North American market, it is believed that the European market for cocaine is among the largest in the world.

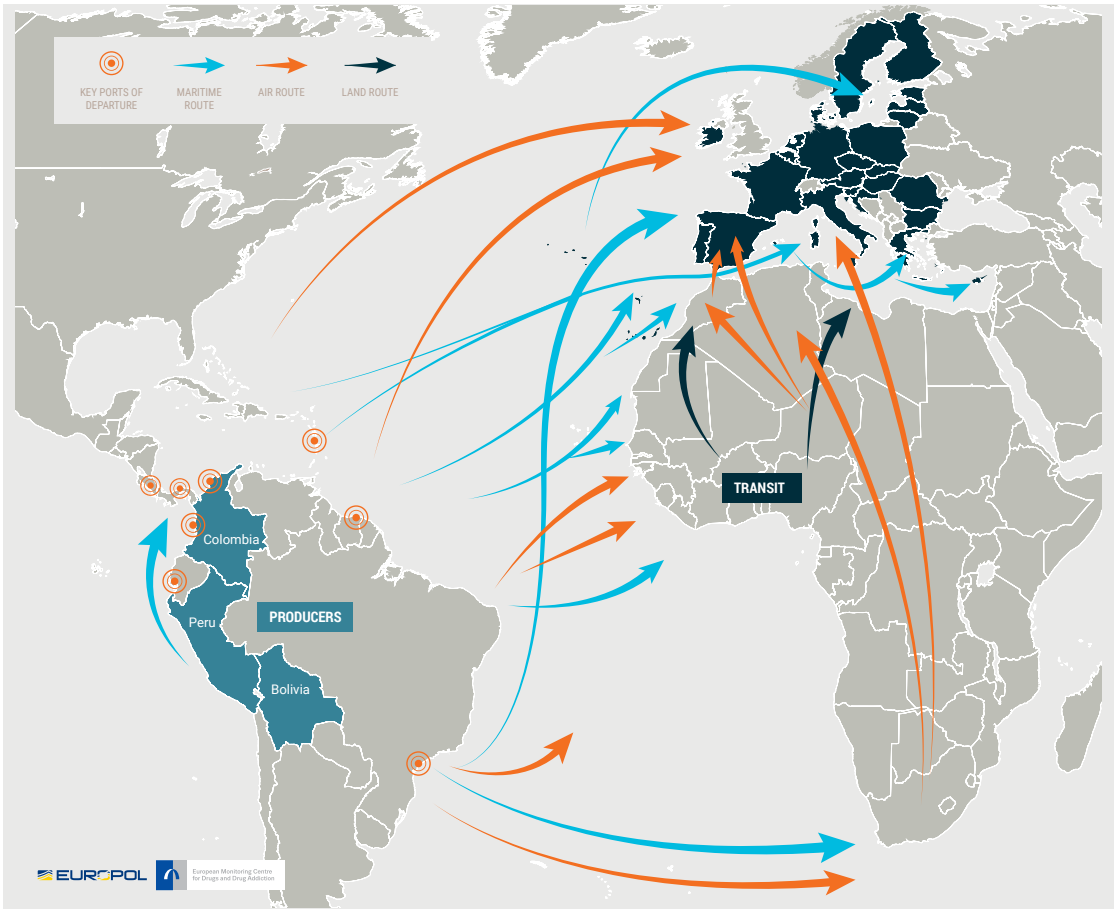
Europe has emerged a premier destination for cocaine traffickers.

This development has been attributed to the potential for further growth in the consumption of cocaine, higher prices for cocaine compared to the North American market as well as lower risks of interdiction and seizure[28].

Latin American criminal networks are expected to continue collaborating with international EU-based criminal networks, while EU criminal networks are expected to continue to be attracted by more favourable prices in countries that produce and transit cocaine and at the main EU distribution hubs. In the EU, high cocaine availability, low wholesale prices and a high level of purity are expected to remain features of the cocaine market in the short term.

COCAINE

TRAFFICKING ROUTES TO THE EU



EU DRUGS MARKET REPORT 2019 (EMCDDA AND EUROPOL); EU SOCTA 2021 DATA COLLECTION

25 UNODC 2020, World Drug Report 2020, accessible at https://wdr.unodc.org/wdr2020/

26 EMCDDA 2020, European Drug Report, Trends and Developments 2020, accessible at https://www.emcdda.europa.eu/publications/edr/trends-developments/2020_en

27 EMCDDA and Europol 2019, EU Drug Markets Report 2019, accessible at https://www.emcdda.europa.eu/publications/joint-publications/eu-drug-markets-report-2019_en

28 Global Initiative Against Transnational Organized Crime 2021, The cocaine pipeline to Europe, accessible at https://globalinitiative.net/analysis/cocaine-to-europe/

Cocaine smuggled to the EU mainly originates from Colombia[29], followed by Peru and Bolivia. The current record levels of cocaine production have resulted in an intensification and diversification of cocaine trafficking activities targeting the EU.

COCAINE CARTEL SHIPPING FROM SOUTH AMERICA BUSTED IN SPAIN AND THE NETHERLANDS

Law enforcement officers raided locations in the Dutch cities of Amsterdam, Papendrecht, Rotterdam, Utrecht and the Spanish cities of Valencia and Malaga. They arrested eight suspects (five in Spain and three in the Netherlands), one of them believed to be a leader of the network. During the operations, the officers from the Spanish police seized six tonnes of cocaine, jewellery, cash and encrypted devices. The suspects are believed to have used self-developed encrypted mobile applications to communicate with their counterparts. Individuals with military training and experience in war missions supported the logistical set-up of the criminal network.





Source: https://www.europol.europa.eu/newsroom/news/cocaine-cartel-shipping-south-america-busted-in-spain-and-netherlands

Date: 16 October 2020

Most of the cocaine seized in the EU is transported by ship, primarily in maritime shipping containers. Cocaine is trafficked to the EU directly from the producing countries as well as from neighbouring countries of departure in South America.

Cocaine trafficking affects all Member States. After arrival at the main EU distribution hubs, cocaine shipments are primarily trafficked by road transport in passenger vehicles and lorries to local markets.

29 EMCDDA and Europol 2019, EU Drug Markets Report 2019, accessible at https://www.emcdda.europa.eu/publications/joint-publications/eu-drug-markets-report-2019_en; UNODC 2019, World Drug Report 2019, accessible at https://wdr.unodc.org/wdr2019/

Intra-EU trafficking of cocaine may also involve commercial flights, light aircraft and helicopters, railway, sea transport, and post and parcel services. Cocaine loads are often hidden in sophisticated concealed compartments in cars, trucks and other vehicles. These are also used to transport cash back to the distribution hubs.

Cocaine trafficking is a key criminal activity for criminal networks. A large variety of individuals, groups and networks shape the complex supply of cocaine to the EU. Criminal networks engaged in cocaine trafficking are highly organised. They are typically hierarchically structured with roles and levels well defined around their leadership. Some large criminal networks are organised in several cells or branches operating in different territories or carrying out specific criminal activities.

The booming cocaine market has entailed an increase in the number of killings, shootings, bombings, arsons, kidnappings, torture and intimidation related to the trade in cocaine. The nature of the violence appears to have changed: a growing number of criminal networks use violence in a more offensive way.

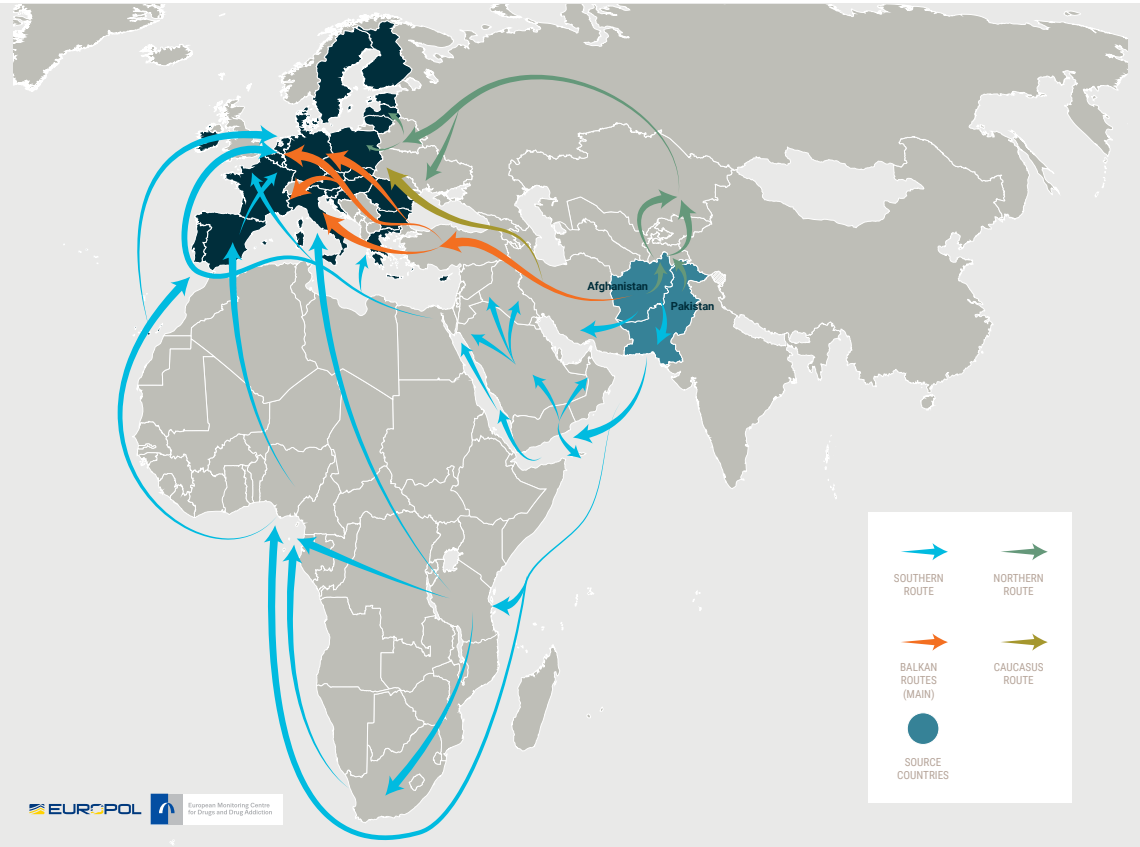
Heroin

The market for heroin has largely remained stable over the last four years. The price of heroin is also reported to have remained stable or decreased over the last four years. Over the last ten years, seizures in the EU have largely remained stable year-on-year. In 2018, the quantity of heroin seized in the EU increased to 9.7 tonnes, up from 5.2 tonnes in 2017, mainly due to large individual seizures made in the port of Antwerp[30].

The processing and production of heroin takes place in Afghanistan, Pakistan and Iran. In recent years, some laboratories processing morphine into heroin were discovered in the EU. This is an emerging phenomenon that should be monitored closely considering the increasing number of discovered multi-purpose laboratories in the EU that are used flexibly for the production of synthetic drugs, (pre-)precursor conversion and cocaine extraction. In some Member States, synthetic opioids, such as fentanyl and its analogues, may be partially replacing heroin as the preferred substance due to its greater potency and cheaper price.

HEROIN

TRAFFICKING ROUTES TO AND WITHIN THE EU



EU DRUGS MARKET REPORT 2019 (EMCDDA AND EUROPOL); EU SOCTA 2021 DATA COLLECTION

30 EMCDDA 2020, European Drug Report, Trends and Developments 2020, accessible at https://www.emcdda.europa.eu/publications/edr/trends-developments/2020_en

There has been little change in the way heroin is trafficked to the EU. The wholesale trafficking of heroin to the EU is believed to follow a number of established routes, including the Balkan routes from Turkey traversing the Balkan region as well as the South Caucasus route via Iran, Turkey, Georgia and Ukraine.

The Balkan routes remain the main entry routes for heroin trafficked to the EU. For the most part, heroin is trafficked along these routes in lorries hidden among legal freight and cover loads or in concealed compartments.

Acetic anhydride is the main precursor substance used in the production of heroin. It is widely used in the legal chemical industry in the EU. In line with the increased production output in the region of production, the illegal trade in acetic anhydride has also increased.

The trafficking and trade in heroin in the EU involves criminal networks composed of nationals of various Member States as well as non-EU citizens. Differentiating the involved criminal networks in the heroin trade by nationality is difficult. The region of origin for heroin trafficked to the EU features many ethnic communities based in different countries and across borders. For instance, suspects involved in the trafficking of heroin to the EU often have a Kurdish ethnic background, but may variably hold Turkish, Iraqi or Iranian nationality as well as EU citizenship.

LARGE-SCALE HEROIN SHIPMENTS FROM THE MIDDLE EAST: 2.4 TONNES OF HEROIN SEIZED AND TWO HIGH-VALUE CRIMINAL TARGETS ARRESTED

During the investigations and action day, more than 2.4 tonnes of heroin were seized. The majority of the heroin consignments were heading to the Netherlands and destined for the European illegal heroin market. The Turkish criminal network and their criminal logistic infrastructure and facilitators were dismantled. In total, 13 criminals were arrested in the Netherlands, Poland, Turkey and Belgium, including two high-value criminal targets. The heroin was hidden in food, in construction materials, compartments for goods in trucks and maritime containers.





Source: https://www.europol.europa.eu/newsroom/news/large-scale-heroin-shipments-middle-east-24-tonnes-of-heroin-seized-and-two-high-value-criminal-targets-arrested

Date: 16 March 2020

Synthetic drugs and new psychoactive substances

The production, trafficking and distribution of synthetic drugs has been previously reported as a highly dynamic crime area subject to rapid change and innovation in terms of the substances, production methods and suspects involved. This remains true and has been reflected in the increasing sophistication of business models, the innovation in the use of different (pre-) precursor substances, essential chemicals and synthesis routes in response to the scheduling of specific substances and other regulatory approaches to curbing synthetic drug production.

The trade in synthetic drugs in the EU is unique compared to other substances as the production of these drugs in most cases takes place in the EU and they are subsequently distributed on a global level and on European markets.

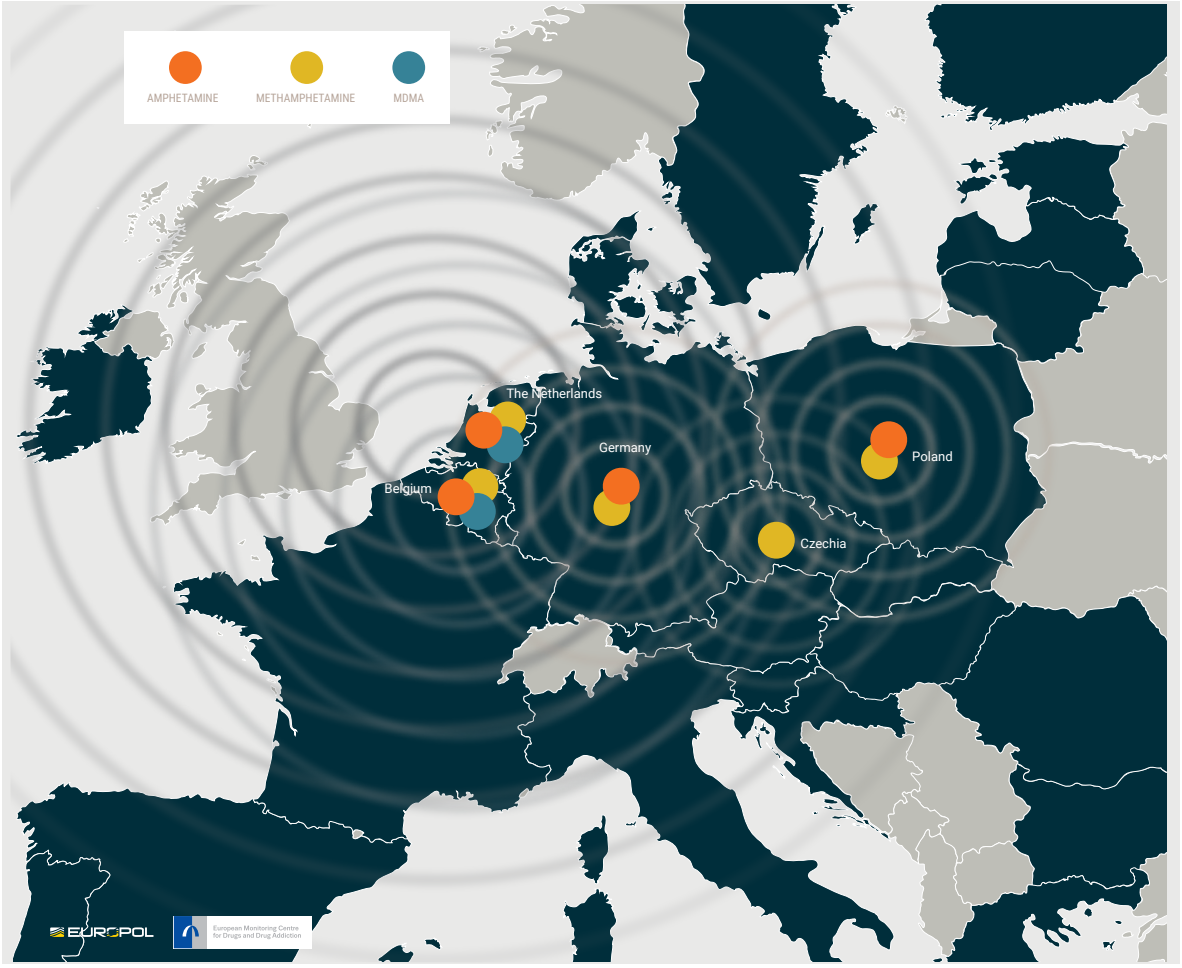
The large-scale production of synthetic drugs, especially those originating from the Netherlands and Belgium, is likely intended for distribution outside the EU and to meet demand on European markets.

The production of synthetic drugs in the EU is expanding and is expected to continue to do so in the near future. There is a risk that non-EU criminal networks with access to expertise and (pre-)precursor substances will increasingly get involved in synthetic drug production in the EU, potentially collaborating with established criminals, further contributing to an expansion of production capacities in the EU. The laboratories used for the production of synthetic drugs discovered in the EU are becoming more professional and versatile, delivering increasing production output and providing greater flexibility in terms of which substances are produced and how they are produced.

The EU is a major source for amphetamine-type stimulants distributed to consumers in the EU and all over the world. Major producers and suppliers of

SYNTHETIC DRUGS

MAIN CENTRES OF PRODUCTION IN THE EU



EU DRUGS MARKET REPORT 2019 (EMCDDA AND EUROPOL); EU SOCTA 2021 DATA COLLECTION

amphetamine and MDMA appear to be located in the Netherlands and, to a lesser extent, Belgium. In addition to these countries, (partial) amphetamine production also takes place in Poland, Bulgaria, Germany and Sweden.

Large-scale methamphetamine production in the Netherlands and Belgium has emerged over the last four years and may further increase in the future due to the strong profit incentives. An increasing number of laboratories have been discovered over recent years in both the Netherlands and Belgium.

While the availability of new psychoactive substances (NPS) in the EU remains a concern, the frequency with which they appear on European markets has slowed in recent years.

Dutch criminal networks are the leading producers of synthetic drugs such as amphetamine, methamphetamine and methylenedioxymethamphetamine (known as MDMA) in the EU. They cooperate with criminal distributors across the EU and worldwide. Dutch criminal networks are believed to exercise control over the production of these synthetic drugs in the Netherlands as well as in Belgium, where they control Belgian subsidiaries engaged in drug manufacturing.

Criminal networks and criminals active in the production of synthetic drugs display a particularly high degree of specialisation and task division. For instance, some criminal networks from Poland specialise in the acquisition and transportation of (pre-)precursor or essential chemicals to centres of production in the Netherlands and Belgium for all types of synthetic drugs, and to Czechia, primarily for the production of methamphetamine. Similarly, Bulgarian criminal networks engage less in production and appear to be more active in the procurement and provision of (pre-) precursors and other essential chemicals on behalf of producers. In many cases, the criminal networks responsible for the large-scale production of synthetic drugs hand the finished product over to a criminal network specialised in the logistics of transporting drug consignments to destination markets across the world.

Synthetic drug production in the EU generates significant amounts of chemical waste, which is frequently dumped by producers in public places and has a highly negative impact on the environment. Centres of production of synthetic drugs in the EU such as the Netherlands, Belgium and, to a lesser degree, Czechia and Slovakia are particularly affected by this toxic waste dumping. Producers of synthetic drugs make use of open borders and minimal checks by dumping waste in neighbouring countries close to drug production sites.





ENVIRONMENTAL CRIME

Waste and pollution crime

Illicit waste trafficking entails the 'illegal transportation, processing, disposal, recycling or recovery of various waste materials'. Trafficked waste materials include both non-hazardous and hazardous waste, including chemical waste, construction waste, urban solid waste, industrial waste, oils and oil blending, plastic waste, waste of electronic and electric equipment (WEEE), end-of-life vehicles and car parts (especially tyres and batteries), scrap metals, liquid manure, and black mass (powder derived from alkaline batteries). End-of-life maritime vessels are trafficked from the EU to Asia for demolition. Waste management is a lucrative and fast-developing industry, which increasingly attracts criminals.

The majority of the reported waste trafficking cases involved individuals working in or operating waste management companies as managers or staff, who violate national and international legislation and standards regulating the collection, treatment and disposal of waste to maximise profits.

The most successful waste traffickers are those who control the entire processing cycle, from source to destination countries. Criminals trafficking waste between different countries primarily use legal business structures to orchestrate waste crimes. Often multiple companies are owned by the same individuals or by strawpersons. The legal business structures frequently change leadership and are often terminated after a short period of activity, as a new trading entity takes over the business. Companies operating different stages in the waste cycle are often located in different jurisdictions.

Waste trafficking is strongly linked to other offences such as document fraud, economic fraud, tax evasion, corruption, money laundering, as well as theft and the dumping of waste from illegal drug production.

COVID-19 WASTE CRIME: EUROPE-WIDE OPERATION TO TACKLE UNLAWFUL SANITARY WASTE DISPOSAL

Since the outbreak of the COVID-19 pandemic, Europol has identified the potential growth of unlawful sanitary waste treatment and disposal, and has as a result launched operation Retrovirus. Officers carried out inspections and checks on sanitary waste plants and transportation, which were crucial in halting the illegal trafficking, storage, dumping and shipment of waste and document fraud.

Another trend identified during the operation was the possible pollution of urban residual waters. The Spanish Civil Guard launched operation Arcovid to investigate the filtering treatments of water for pollutants and the possible presence of COVID-19.





Source: https://www.europol.europa.eu/newsroom/news/covid-19-waste-crime-europe-wide-operation-to-tackle-unlawful-sanitary-waste-disposal

Date: 30 November 2020

Wildlife crime

Wildlife crime refers to poaching, collecting, trading (supplying, selling or trafficking), importing, exporting, processing, possessing, obtaining and consumption of wild fauna and flora, including timber and other forest products, in contravention of national or international law[31].

Wildlife crime increases the risks of extinction of endangered fauna and flora and of further degradation of biodiversity. Wildlife trafficking also presents risks to human health via the possible transmission of diseases.

31 CITES 2020, Wildlife crime, accessible at https://cites.org/eng/prog/iccwc/crime.php

Traffickers increasingly target endemic and non-CITES[32] -listed European species, in particular birds and big cats. There has also been an increase in demand for exotic reptiles. Traffickers may further concentrate their activities on endemic and non-CITES-listed specimens to circumvent current international legislative frameworks, which mostly cover endangered wildlife.

The majority of trafficked animals are sold and bought online. Sellers and buyers use online marketplaces, social media, mobile applications and specialised fora where networks of regular sellers and buyers discuss available merchandise, offers and prices or share knowledge and expertise on hunting and breeding techniques. Common encrypted communication tools such as mobile applications and online chats are widely used by traffickers, sellers and buyers.

Criminal groups composed of EU and non-EU nationals are involved in wildlife trafficking across several continents. The nationality of suspects largely depends on their role. Poachers and collectors almost always come from the country of origin of the trafficked specimens, while mules often have links to the countries of destination. Some wildlife traffickers reportedly also engage in excise fraud and drug trafficking.

28 BIRD TRAFFICKERS NETTING EUR 1 MILLION PER YEAR ARRESTED IN SPAIN

The investigation initiated in 2019 uncovered how this criminal group would sell these endangered species to North African buyers using forged documents. The criminals would then arrange for the birds to be smuggled out of Spain hidden in buses heading to the African continent. The traffickers were supported by a Moroccan citizen who worked in a travel agency and arranged the logistics. They also developed their illegal business online, where they would sell birds but never deliver them, despite the buyers having paid for them. In addition, over 400 marijuana plants were discovered during the house searches, indicating that this group of traffickers was involved in a variety of criminal activities.



It is believed that parrot smuggling worldwide is on the rise. Some species can reach several hundreds of thousands of euros on the black market. The demand driving this illicit trade comes from collectors and breeders, but also citizens who want them as pets. However, this desire to own such exotic birds is killing them off.

A number of parrot species are threatened with extinction due in part to pressures from collecting for the pet trade. There is however legal protection in place. All but two parrot species are protected under CITES, as a result of which their commercial trade is either prohibited or strictly regulated with export permits.

Source: https://www.europol.europa.eu/newsroom/news/28-bird-traffickers-netting-%E2%82%AC1-million-year-arrested-in-spain

Date: 19 July 2020

32 CITES is a multilateral treaty to protect endangered plants and animals.

THE TRADE IN ILLEGAL FIREARMS AND EXPLOSIVES

The trade in illegal firearms is a key enabler for other criminal activities such as drug trafficking and amplifies the threat they pose to the internal security of the EU. Violent acts carried out using illegal firearms and public shooting incidents generate a sense of insecurity and severely undermine public confidence in national authorities. Some indicators allow us to assess the overall availability of illegal firearms in the EU. These include the number of shooting incidents and the quantity of seized firearms, both of which suggest the wide availability and accessibility of illegal firearms in the EU.

The smuggling of large weapons caches to the EU is rare. Illegal firearms available in the EU are typically either diverted from legal supply chains, converted, reactivated or modified within the EU or originate from weapon stocks outside the EU.

In recent years, alarm and signal weapons have become extremely popular among criminals and feature in considerable figures in firearms trafficking and seizure cases. This is due to the fact that they can be easily converted into lethal weapons and are cheaper to procure.

Firearms are illicitly manufactured in the EU using clandestine workshops and gunsmiths. Firearms can be assembled from parts which are manufactured using 3D technology, acquired in countries where their sale is allowed and illegally transported to the EU, or illegally produced and used with genuine weapon frames.

The reactivation of deactivated and acoustic expansion weapons is a common source of firearms in the EU.





The diversion of firearms from legal supply is another significant source of illegal firearms in the EU. This includes the illegal sale of historical weapons and army surplus material. Firearms are also acquired by targeted thefts from hunters, collectors and sport shooters.

Illegal firearms and their parts have been traded online via the surface and dark web and distributed using post and parcel services for some time. The online sale of illegal firearms appears to have shifted away from dark web marketplaces to forums and other platforms after a number of marketplaces banned the sale of firearms. However, the scale of the online trade in illegal firearms has been assessed as limited compared to their offline supply. In addition, many offers for illegal firearms online are believed to be scams.

Various types of criminal networks are involved in the trade of illegal firearms in the EU. This includes EU-based and non-EU-based criminal networks. Criminal networks involved in the firearms trade typically feature the division of labour between members. Some members, such as gunsmiths, are highly specialised.

Firearms trafficking is often a subsidiary activity to drug trafficking. Drugs are sometimes used as currency to make partial payments for weapons.

FRAUD

Fraud schemes

Fraud offences are committed with the intention to defraud using false and deceitful pretexts resulting in the voluntary but unlawful transfer of values, goods or an undue advantage to the fraudsters.

Fraud schemes targeting private citizens, small and medium enterprises, global corporations and critical infrastructure are present in all Member States[33]. Fraud is believed to be under-reported as victimised individuals or companies seek to protect their brand name and putation rather than approach law enforcement. In addition, the under-reporting of fraud cases can also be attributed to the fact that insurance companies often do not compensate victims' financial losses incurred due to fraud.



33 Europol 2020, Enterprising criminals – Europe's fight against the global networks of financial and economic crime, accessible at https://www.europol.europa.eu/publications-documents/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime

The COVID-19 pandemic has presented unique opportunities for fraudsters seeking to profit from the insecurity, restrictions and booming demand for certain products as a result of this crisis[34].

The majority of investment, payment order and advance fee frauds are orchestrated using call centres operated by low-ranking members of criminal networks. Boiler room schemes involve criminals cold calling their victims. These schemes use call centres established in jurisdictions away from the locations of their victims, with the call centre fraudsters usually speaking their victims' native language fluently. Fraudsters use social engineering techniques to manipulate human behaviour and exploit weaknesses to gain information or compliance. Their deception often relies on creating scenarios and stories that target victims' vulnerabilities.

The list of fraud schemes presented here is nonexhaustive. Fraud schemes are constantly evolving and the tools and techniques used to perpetuate them can overlap between different types of frauds, often making it difficult to identify and distinguish between different types of fraud.

INVESTMENT FRAUD

Investment fraud schemes result in substantial financial damage to private individuals and companies. Investment fraudsters have been increasingly targeting the cryptocurrency investment market by operating fake websites offering bogus investment opportunities. Fraudsters commonly seek out victims on social media platforms.

FAKE INVESTORS BUSTED IN BELGIUM AND FRANCE

The criminal organisation managed to set-up a sophisticated system promising big gains on investments in bitcoin, gold and diamonds. The suspects were offering their financial services on online platforms. The criminal network also set up bogus companies as a part of their money-laundering scheme. The network was active in Belgium and France and controlled by an Israeli branch.

The suspects were promising between 5 % and 35 % return on investment. They then proceeded to pretend to manage the victims' portfolios and invited them to invest more money. To increase trust in their services, they paid interest on some of the victims' investments. Once the victims were won over, the fraudsters would offer bigger opportunities, which required higher amounts to be invested. A large French private company and a French local authority are among the victims of this network. The investments of the victims were placed on accounts in different EU Member States before being transferred to other international accounts.

The network is believed to be responsible for frauds amounting to at least EUR 6 million. The investigators have also discovered invoices for a few million euros, which the fraudsters had not yet finalised.

Source: https://www.europol.europa.eu/newsroom/news/fake-investors-busted-in-belgium-and-france

Date: 29 January 2020

34 Levi and Smith 2020, Australian Institute of Criminology Research Report – Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19.

Online advertisements invite victims to open online trading portfolios and lure them in with initial benefits. However, the fraudsters extract and disappear with the funds shortly after. Non-existing virtual currencies are also advertised as an investment opportunity. This type of fraud in particular appears to have become more common across the EU over the last four years.

CHIEF EXECUTIVE OFFICER FRAUD AND BUSINESS EMAIL COMPROMISE FRAUD

Chief Executive Officer (CEO) fraud is one of the most common types of payment order fraud. As part of this fraud, employees receive a payment order by email or a telephone call from a fraudster impersonating a company executive, often the CEO. The payment is instructed to be made out to bank accounts under the control of the fraudsters.

NON-DELIVERY FRAUD

Non-delivery fraud is a variant of payment order and advance fee fraud. Non-delivery fraudsters use fake web shops to advertise and sell non-existent goods.

During the first months of the COVID-19 pandemic, fraudsters exploited the high demand for and low supply of personal protective equipment and self-testing kits.

The number of websites and social media accounts fraudulently advertising these products increased significantly. The profits from these scams were significant and many of the victims were corporate and public entities, such as hospitals and clinics placing orders for supplies worth several millions of euros.

ROMANCE FRAUD

As part of romance fraud schemes, fraudsters contact potential victims with the objective of taking financial advantage of those genuinely looking for romantic partners. Fraudsters work to gradually establish trust with the victim and soon start eliciting personal details such as bank accounts, credit card numbers or ask for money.

FAKE INVOICE FRAUD

Fake invoice fraud, known as payment order fraud or ghost invoice fraud, is a form of acquisition fraud that involves requests for payments based on fictitious invoices issued to potential victims by fraudsters. This type of fraud relies on advertisements on sale webpages and the use of false, inflated or duplicate invoices. Criminals often impersonate legitimate suppliers and make a formal request to change the bank account to which genuine payments to that supplier are made. Fake invoices are sent via post and courier services or through emails.

SOCIAL BENEFIT FRAUD

Social benefit fraud causes significant financial loss to the budgets of Member States and potentially deprives those genuinely in the need of aid from state support. Social benefit fraud can entail fraud against medical insurance, employment benefits, unemployment allowances, or allowances for low-income workers and refugees. As part of social dumping fraud in the construction and transportation sectors, criminal networks create fake companies and claim benefits for non-existing employees. In another form of this fraud, employees continue to work while receiving unemployment benefits and receiving wages under the table from the employer.

BANK FRAUD

The most common form of bank fraud is loan and mortgage fraud. Fraudsters use companies to acquire mortgage loans using manipulated real estate transactions. Criminals recruit homeless and poor people as strawpersons to apply for loans from banks. In other instances, loans are requested based on forged passports. Another type of bank fraud sees accounts taken over to execute fraudulent transactions. Mortgage fraud is usually linked to document fraud.

SUBSIDY FRAUD

The number of cases involving subsidy fraud cases has steadily increased over the years. As part of subsidy fraud, criminals submit fraudulent applications for EU grants or tenders. Typically, these applications are based on false declarations, progress reports and invoices used to justify public expenditure or the fraudulent award of public tenders and/or subsidies.

Online fraud

Fraud schemes take advantage of the digital era. Phishing and hacking techniques are used to obtain personal information such as bank account information and banking login details from victims. Fraudsters use malware to intercept login details for online banking services.

Fraudsters adjust fraud schemes to consumer needs and changes in people's behaviour, often exploiting new technologies. Fraudsters increasingly use online platforms for social engineering. To perpetrate online fraud, criminals typically use tools and techniques linked to the authentication process to access sensitive information that helps them commit the frauds.

Criminal networks' capability to react to a changing environment has been particularly pronounced during the COVID-19 pandemic, which has prompted many individuals to primarily shop online using digital payment means. Cybercriminals have quickly developed COVID-19 themed scams and exploited the vulnerability of some victims to target them with investment and romance scams.

The move toward cashless economies creates powerful incentives for payment fraudsters. Cybercriminals seek to compromise online payments, internet and mobile banking, online payment requests, contactless payments (both card-present and not) and mobile applications. The increasing use of mobile devices for financial transactions and authentication processes has made them a target for cybercriminals.

The use of deepfakes will make it much more challenging to identify and counter fraud. Deepfakes mimic seemingly real photo, video and audio recordings of people. Fraudsters have already used voice impersonation as part of CEO fraud schemes and will likely expand the use of this technology as part of their criminal activities.

Customs import fraud

Customs import fraud resulted in financial losses of at least EUR 5.5 billion to the EU budget between 2016 and 2019. The evasion of duties on goods imported into the EU negatively affects the financial interests of the EU and threaten legitimate companies operating in the Member States. Dumping practices create unfair competition to legitimate businesses and their products and market distortion.

Customs import fraud involves the false declaration of the value and origin of goods, and of the classification that applies to them. This type of fraud can be perpetrated by:

- undervaluing imported goods on import declarations, often using fraudulent documents;
- incorrectly clarifying products imported to the EU by falsely declaring the category of goods according to the integrated Tariff of the European Union or TARIC code in order to pay a lower duty rate;
- falsely declaring the origin of goods to circumvent anti-dumping duties imposed by the EU on a particular product from a specific country;
- dumping products on the EU market at a lower price than the normal value of the product. The normal value is either the product price as sold on the home market of the non-EU company, or a price based on the cost of production and profit[35].

Criminals carrying out customs import fraud quickly adapt to customs controls at the entry points of the EU and often have good knowledge of the Union Customs Code and the relevant regulatory amendments.

Excise fraud

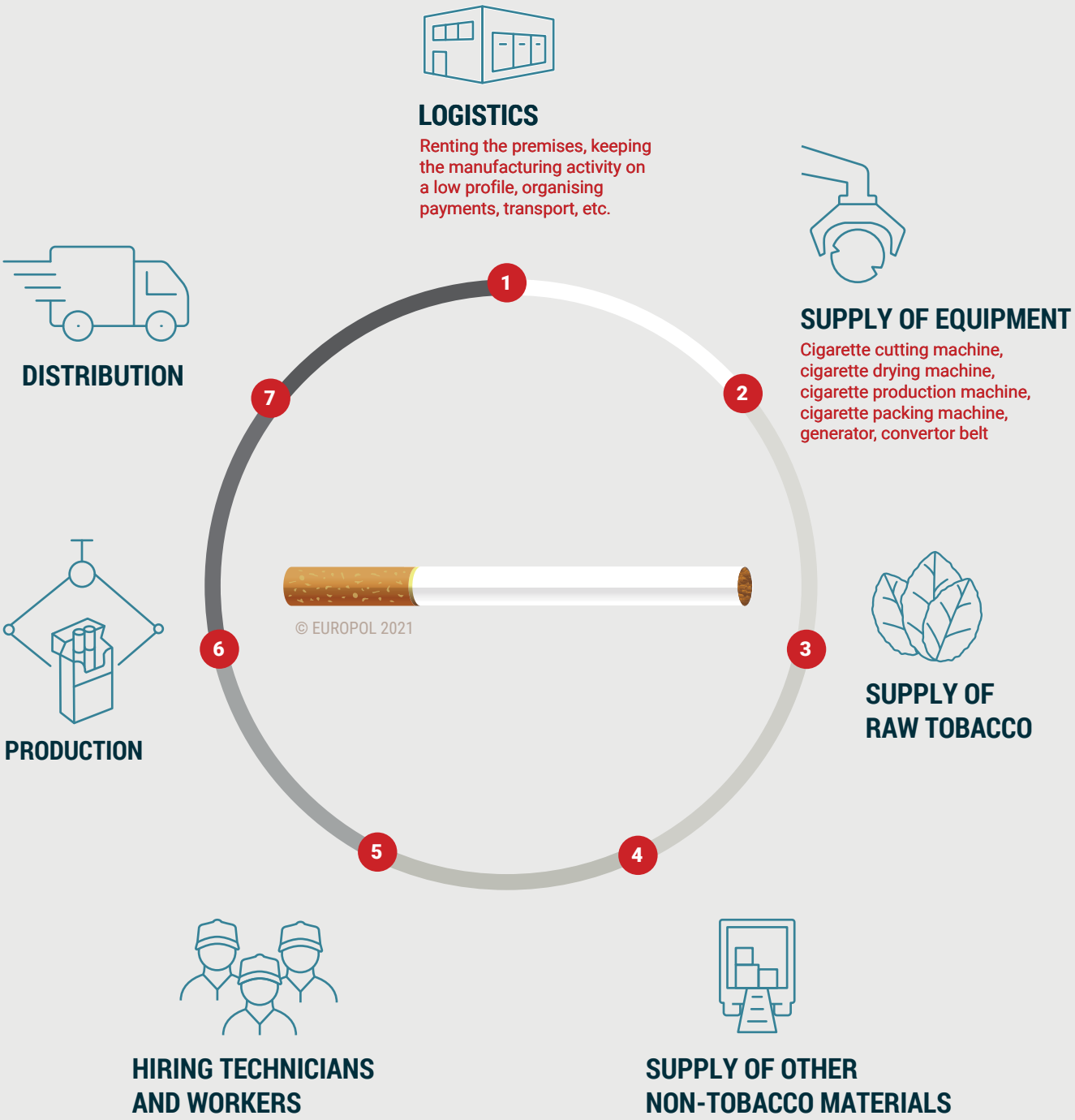
Goods such as alcohol, cigarettes and fuel are subject to excise duty upon production in or on import to the EU. Excise duties are indirect taxes on the sale and use of specific products. The EU has introduced the Excise Movement and Control System (EMCS), which provides Member States with an electronic system to monitor the movement of excise goods in real time, to ensure that duties are properly levied at the final destination.

EXCISE FRAUD –TOBACCO

Significant price differences between Member States, and between Member States and neighbouring non-EU countries are the main incentives for criminal networks involved in this profitable criminal activity.

35 European Commission 2020, Actions against imports into the EU – Anti-dumping, accessible at https://ec.europa.eu/trade/policy/accessing-markets/trade-defence/actions-against-imports-into-the-eu/anti-dumping/

THE BASIC STEPS OF THE ILLICIT CIGARETTE PRODUCTION PROCESS



FOUR METRES UNDERGROUND: ILLEGAL CIGARETTE FACTORY UNCOVERED IN A BUNKER IN SPAIN

In February 2020, the Spanish Civil Guard (Guardia Civil) dismantled an organised crime group involved in illegal cigarette manufacturing and drug trafficking. The Spanish law enforcement officers uncovered the manufacturing facility hidden in a bunker four metres underground. In the facility, believed to have been operating since 2019, workers made and packed the counterfeit cigarettes: a complete production line under one roof. Beds and living quarters for the workers were also found underground. This is the first underground factory to be discovered in the EU. Workers there were forced to work in extremely dangerous and toxic conditions. Locked up four metres underground, they were not allowed to leave the facility on their own, and no emergency security was in place.

Over 2 million counterfeit cigarettes were seized, produced in unsanitary conditions and with low quality components. The criminal network is estimated to make criminal profits of EUR 625 000 per week.

Source: https://www.europol.europa.eu/newsroom/news/four-metres-underground-illegal-cigarette-factory-uncovered-in-bunker-in-spain

Date: 20 February 2020

Criminals benefit from the price difference and the proximity of the markets to smuggle illicit tobacco products.

Smuggled cigarettes might be original (tax and value-added tax (VAT) fraud also arises when the goods are smuggled to the legal market), counterfeit, illegally produced within the EU, and 'illicit whites' produced legally in Belarus, Bulgaria, Moldova, North Macedonia, Russia, Ukraine, the United Arabic Emirates, and other countries. Illicit white cigarettes are illegally brought into the EU, without paying excise duties and VAT, and are placed outside legal channels, making huge profits forthe criminal networks. Illicit production of illicit whites in factories based in the EU has increased.

Illicit production facilities have been discovered in many Member States and illicit tobacco products are increasingly produced in the EU, closer to their destination markets.

EXCISE FRAUD – OIL

Excise duties on oil products are a major source of revenue for Member States. Different taxation is applied between Member States for the same oil products. The taxes levied on different types of oil products such as heating or agricultural oils is lower than the tax rate for diesel. Criminal networks abuse price differences as part of different oil fraud schemes. Fuel fraud causes revenue losses of billions of euros to Member States. The negative impact of fuel fraud on the environment is a significant concern in some Member States.

An increasing shift to non-fossil fuels will create additional opportunities for fuel fraudsters.

A 2018 EU Commission Directive introduces exemption from these limits for biofuels certified as low-risk[36].

36 EU Commission 2019, Delegated Act C(2019) 2055 final, supplementing Directive (EU) 2018/2001 as regards the determination of high indirect land-use change-risk feedstock for which a significant expansion of the production area into land with high carbon stock is observed and the certification of low indirect land use change-risk biofuels, bio liquids and biomass fuels, accessible at https://ec.europa.eu/energy/sites/ener/files/documents/2_en_act_part1_v3.pdf

Criminals will exploit emerging opportunities in this area by abusing biofuels in fraudulent biodiesel trades. Some schemes may involve the sale of biofuels that have not been sustainably produced as sustainable fuel.

The production and use of so-called designer fuels as diesel is still a significant threat, although progress has been made in countering this issue by law enforcement authorities. Designer fuel is a mixture of gas oil and other components added to modify the physical characteristics of the final compound to avoid taxation.

EXCISE FRAUD – ALCOHOL

The excise duties levied on alcohol vary across the EU, creating profit opportunities for excise fraud involving alcohol. Alcohol fraud schemes mainly target countries imposing comparatively higher taxes on alcohol products. Alcohol is smuggled across the EU using excise duty suspension schemes, typically described as (beer) carousels which abuse the EMCS system.

Value-added tax and missing trader intra community fraud

Value-added tax (VAT) fraud consists of avoiding the payment of VAT or fraudulently claiming repayments of VAT from national authorities following an illicit chain of transactions.

Missing trader intra community (MTIC) fraud is the abuse of the VAT system rules for cross-border transactions, involving the acquisition of goods (with 'exemptions with the right to deduct', also known as effective zero-rating) from another Member State which are then sold through a chain of companies to the consumer market with VAT added. The VAT is then not paid to the tax authorities. More complex cases of VAT fraud are known as carousel frauds.

VAT fraudsters continue to generate multi-billion-euro profits in the EU.

Up to EUR 50 billion are lost due to the activities of VAT fraudsters every year[37].

By creating economic imbalances and market distortion, these criminal activities weaken the integrity of the national and international markets and financial systems and support the growth of underground economies.

Technology and digital infrastructure is an essential component in the commission of VAT fraud for different purposes. Criminal networks use technology to conceal their criminal activities, for example remote servers and repositories for data storage (including cloud data storage and servers located outside the EU), digital and alternative payment platforms, VPN services, encrypted communication and use of different internet-based smartphone communication applications. A developing area of fraud within the EU is Voice over Internet Protocol (VoIP) fraud, in which the internet is central to the scam.

Criminal networks can now create and run companies from a single device, located in any country, and conduct trade and submit documentation online. Free software is also now available to manufacture fake invoices and bank statements. New methods of transferring money, such alternative banking platforms, together with electronic banking services, make it more difficult to identify perpetrators.

Criminal networks are extremely adaptable and flexible in response to new measures and changes in legislation, the market/economic situation and law enforcement action. The fraudulent schemes of criminal networks are constantly evolving and improving in order to take advantage of the weaknesses of the state and legislation. For example, criminal networks are able to repurpose their supply chains easily to take advantage of opportunities for fraud from trading in new commodities and are similarly quick to refocus and change modus operandi (such as switching commodities or countries in response to legislative changes like VAT reverse-charges). Criminals also take measures to avoid detection, such as substituting companies and frontmen, and exploiting new technological advances in order to incorporate companies and conceal ownership. The use of alternative banking platforms in carousel fraud and attempts to infiltrate the guarantees of origin markets are examples of the flexibility and adaptability of criminal networks active in this crime area.

Criminal networks continue to exploit legal business structures to create fictitious commercial deals and use missing trader companies to avoid tax liabilities.

37 European Commission 2018, VAT: EU Member States still losing almost €150 billion in revenues according to new figures, accessible at https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5787

Criminal networks are often also active in money-laundering activities to legalise their illicit proceeds; for some criminal networks, money laundering is a parallel activity to VAT fraud. Many criminal networks are involved in document fraud, most likely as part of the commission of VAT fraud. In cases where criminal networks were reported to be involved in other crime types, most often this related to other types of fraud.

VAT fraud is committed by professionals possessing good knowledge of the VAT system, legislation and tax administration procedures. Other professionals providing expertise to criminal networks include legal advisors, customs officers, computer/ICT specialists, financial and economic experts, money-laundering experts, auditors and persons with knowledge of logistics. Setting up an MTIC fraud scheme in the intangible goods sector requires in-depth knowledge of that business and its regulations. Criminal networks may also recruit members with expertise in trading specific commodities such as VoIP.

PAN-EUROPEAN VAT FRAUD CRIME GROUP DISMANTLED

Involving over nine EU Member States with the support of OLAF and Europol, operation OCTOPUS II ran between June and December 2017 and targeted criminal networks importing clothing and footwear from China into the EU by misusing Customs Procedure 42 00. This procedure entitles third-country importations to be released into free circulation with a deferred payment of the import VAT until the goods' arrival with the consignee. Unfortunately, criminals were quick to jump on the bandwagon: the value declared by the consignee to the customs was on multiple occasions underdeclared, or the goods went missing along the way. Five criminal networks were identified, and a number of shell companies were immediately closed down and over 500 000 counterfeit goods were seized in France alone.

The operation revealed that this type of large-scale fraud was the work of highly knowledgeable and well organised criminal networks who knew the ins and outs of the logistics circuits and control systems to subsequently abuse them.

Source: https://www.europol.europa.eu/newsroom/news/pan-european-vat-fraud-crime-group-dismantled

Date: 2 July 2018



MATCH FIXING AND BETTING-RELATED SCAMS

Match fixing damages the integrity of sports and has a significant impact on sports associations, which are at risk of losing sponsors. Sports corruption stigmatises athletes and has a negative impact on the sports industry.

While the percentage of fixed matches is estimated to be fewer than 1 % across all sports, high betting turnover results in millions of euros in profits for match fixers each year. The global annual criminal proceeds from betting-related match fixing are estimated at approximately EUR 120 million.

A number of sports clubs experienced significant financial strain as a result of the restrictions introduced to curb the spread of the COVID-19 pandemic. Many of these clubs operate in low-tier divisions and may be increasingly vulnerable to infiltration or buyout by criminal networks seeking to use the club for match fixing and other criminal purposes.

Match fixers are likely increasingly targeting the fast-developing e-sports market. There are indications of

e-sport manipulation, including extraordinary surges in betting activity and the deposit of unusually large sums on a bet just ahead of e-sport matches[38].

38 Interpol 2020, E-sports: keeping crime out of video game competitions, accessible at https://www.interpol.int/en/News-and-Events/News/2020/E-sports-keeping-crime-out-of-video-game-competitions

PEOPLE AS A COMMODITY

Migrant smuggling

Migrant smuggling is the process of facilitating the unlawful entry, transit or residence of an individual in a country with or without obtaining financial or other benefits. Migrant smuggling entails the facilitation of illegal entry to the EU and of secondary movements within the EU. It can also involve facilitating the fraudulent acquisition of a residence status in the EU. Migrant smuggling may entail land, sea or air transportation and often involves the use of fraudulent documents, including identity documents or fraudulent visas.

Organised migrant smuggling will remain a key activity for criminals, sustained by continued demand for facilitation services. The global population is expected to continue to increase, especially in some of the world's most unstable regions, where economic deprivation, conflicts[39] and climate change[40] will serve as key push factors. In addition, the medium and long-term health, economic and political consequences of the global COVID-19 crisis will fuel migration towards Europe and will likely sustain the demand for facilitation services for mixed migration flows. The perception of the EU as comparatively more economically, politically and environmentally stable will remain a key pull factor.

The proliferation of sophisticated digital technologies and the widespread use of social media and encrypted communications will create opportunities for migrant smugglers to propagate their services, to coordinate among each other and recruit victims, eluding law enforcement detection. The use of cryptocurrencies by smuggling networks has been recently reported and may increase in the foreseeable future. Migrant smugglers make frequent use of digital services and tools, such as social media and mobile applications for recruitment, communication in general and on money transfers, pick-ups and handover of migrants, mass-mobilisation of migratory movements, providing route guidance, sharing pictures and videos of documents and tickets, and monitoring law enforcement activities (via video surveillance and even with drones).

Criminal networks involved in migrant smuggling are characterised by agility and responsiveness to changes in their environment. The routes and modi operandi used by smugglers to facilitate migrants to and within the EU are flexible and shift depending on circumstances such as weather conditions, availability of transport logistics and the presence of risks such as increased law enforcement activity or travel restrictions.

The COVID-19 pandemic has highlighted that global crises do not diminish the demand for smuggling services to enter, transit or reside in the EU.

The demand for smuggling services towards Europe is expected to increase in the short and medium to long term.

Despite the fact that irregular migrants are customers of migrant smugglers and willingly pay them for their services, they are also often victimised. Migrant smugglers treat irregular migrants as commodities, often prioritising the aim of maximising profits over the risks to the migrants' physical and psychological health. Migrant smugglers frequently employ violence or the threat of violence: against migrants, against law enforcement officers when avoiding apprehension and occasionally against other smugglers active in the same area. Migrant smugglers put the lives of migrants at risk using unseaworthy vessels or concealing them in small confined spaces for prolonged periods.

Facilitation services for secondary movements are high in demand but often remain undetected due to the use of dangerous modi operandi. Facilitated secondary movements remain a major concern for the security of the EU.

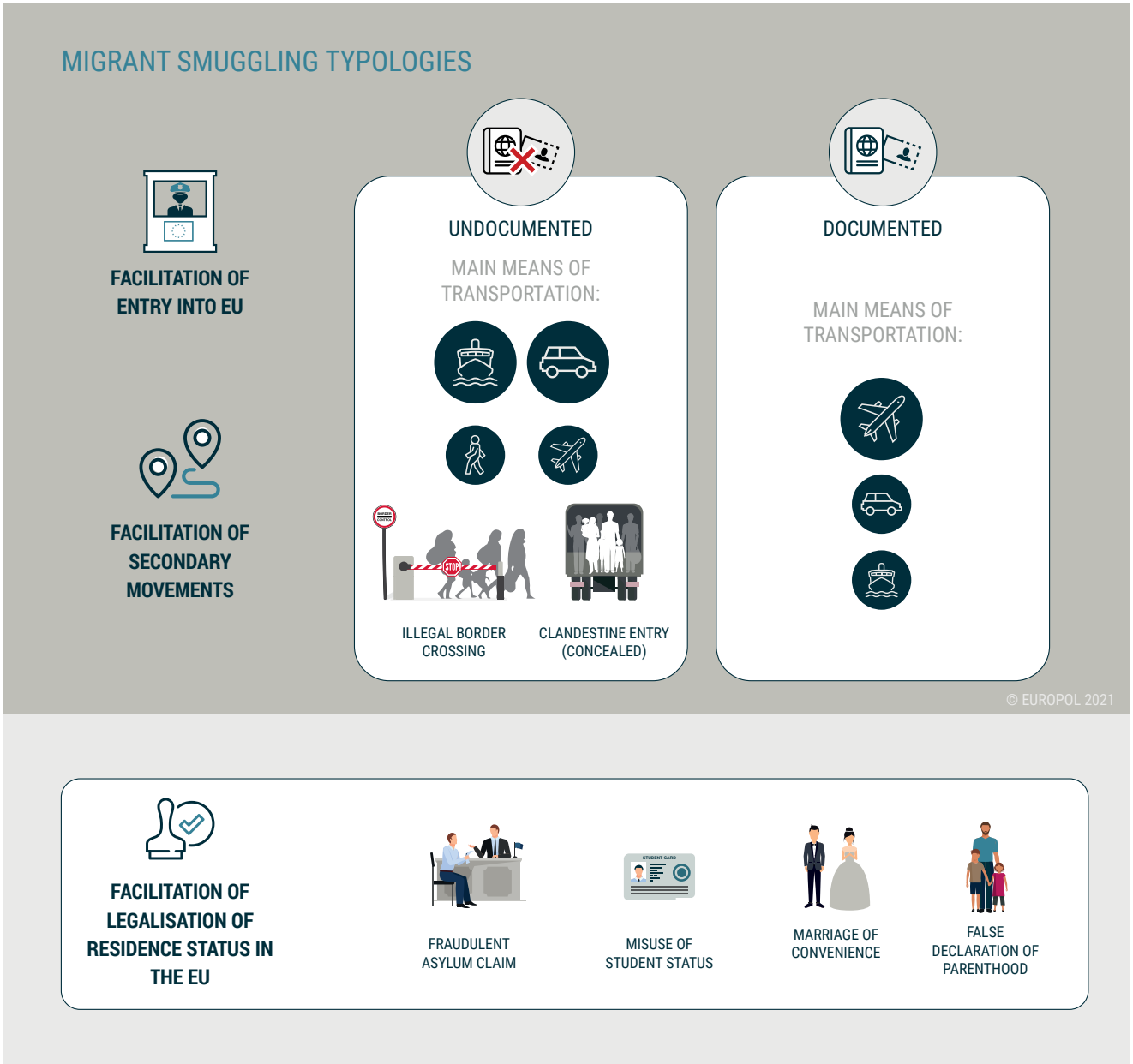
Approximately 50 % of the criminal groups involved in migrant smuggling were exclusively active in migrant smuggling. Migrant smugglers are on occasion also involved in the trafficking in human beings, drug trafficking, excise fraud, firearms trafficking and money laundering.

39 UNODC 2020, Working Group on the Smuggling of Migrants, accessible at https://www.unodc.org/unodc/en/treaties/CTOC/working-group-on-the-smuggling-of-migrants-2020.html

40 EMLO 2020, Bangladesh Report 2020: Costs of Climate inaction: Displacement and Distress migration, accessible at https://actionaid.org/sites/default/files/publications/ActionAid %20CANSA %20- %20South %20Asia %20Climate %20Migration %20report %20- %20Dec %20 2020_3.pdf

The three Mediterranean entry routes (Western, Central, and Eastern) are still predominantly used by smuggling networks to introduce irregular migrants into the EU. On the Western Mediterranean route, Algeria has recently emerged as a key departure point and the Canary Islands have been increasingly targeted along the West African[41] route .

Migrant smuggling networks provide several services beside transportation, such as provision of safe houses along the route and paperwork for the legalisation of their residence status through several means, including supply of fraudulent documents and/or Schengen visas, arrangement of marriages of convenience, false registered partnerships or false adoptions. Smugglers usually advise irregular migrants to apply for international protection in case of detection by law enforcement. This misuse of the asylum procedure enables the irregular migrant to temporarily legalise their residence status while onward facilitation is being arranged.



41 Europol 2020, Dangerous facilitation by rubber boats from Morocco to Canaries, accessible at https://www.europol.europa.eu/newsroom/news/28-arrested-for-smuggling-migrants-in-rubber-boats-morocco-to-spain

23 MEMBERS OF IRAQI MIGRANT SMUGGLING NETWORK ARRESTED IN FRANCE AND THE NETHERLANDS

In January 2020, France and Dutch law enforcement authorities, supported by Europol and Eurojust, dismantled an Iraqi migrant smuggling network that smuggled around 10 000 Afghan, Iranian, Iraqi and Syrian migrants from the French areas of Le Mans and Poitiers, to the UK.

The migrants were transported in life-threatening conditions, concealed in refrigerated – often-overcrowded – lorries (up to 20 migrants in a lorry). The migrants paid up to EUR 7 000 for the dangerous journey. The payments were collected via an undercover hawala banking system run from the Netherlands. This migrant smuggling network's illegal profits amounted to around EUR 70 million.

Source: https://www.europol.europa.eu/newsroom/news/23-arrests-in-france-and-netherlands-iraqi-kurdish-smuggling-network-busted

Date: 23 January 2020

Trafficking in human beings (THB)

The entire process of trafficking a victim currently features a number of online components, both on the surface and dark web. This development is set to become even more pronounced.

THB is a core activity of serious and organised crime in the EU and is set to remain a threat to the EU for the foreseeable future. Sustained demand for sexual services will continue to drive the sexual exploitation of victims. Similarly, the persistent demand for low-wage workers employed in manual jobs, both seasonal and throughout the year, will ensure opportunities for labour exploitation.

Trafficking in human beings is believed to remain significantly underreported. THB for labour exploitation in particular is increasing in the EU.

Some victims, and in some cases their family members, suffer from serious long-term consequences such as drug addiction and mental health challenges.

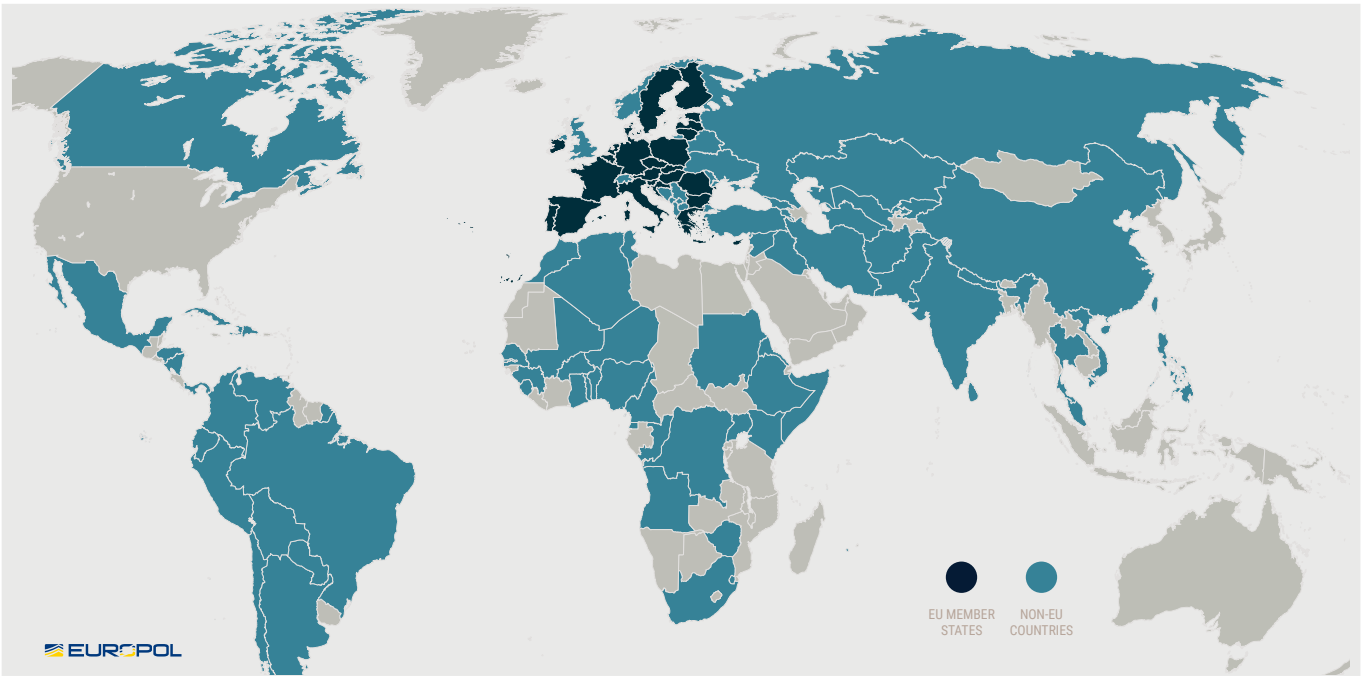
SEXUAL EXPLOITATION

Traffickers abuse victims of sexual exploitation, both adult and underage, male and female, in clandestine settings and public environments such as hotels, bars, restaurants, sauna clubs, strip clubs, night clubs, massage parlours and prostitution windows. These premises are usually owned by associates or by facilitators of traffickers who also profit from exploiting the victims.

Traffickers use online platforms and services to identify victims, orchestrate THB for sexual exploitation and advertise the services of victims. The use of websites to advertise the sexual services of victims to clients has become a fundamental feature of this type of exploitation.

SEXUAL EXPLOITATION

MAIN NON-EU COUNTRIES OF ORIGIN OF TRAFFICKING VICTIMS EXPLOITED IN THE EU REPORTED TO EUROPOL



EU SOCTA 2021 DATA COLLECTION; EUROPOL INFORMATION

It has been assessed that there has not been a significant increase in THB for sexual exploitation over the last four years. However, the sexual exploitation of victims of THB takes places in all Member States.

The origins of victims of THB used for sexual exploitation in the EU are highly diverse. Victims of 55 different nationalities from five different continents were reported.

These victims are mostly female, both adult and underage. They are typically recruited using false promises of well-paid jobs abroad, to escape precarious living conditions, financial instability and social and familial hardship.

Exploiters increasingly seek to exploit their victims in the context of supposedly voluntary business agreements. As part of these arrangements, the victims agree to engage in prostitution and hand over a share of their earnings in exchange for protection and support with administrative issues such as tax declarations, registration with chambers of commerce, or pension arrangements. This type of exploitation is particularly common in jurisdictions where sex work has been legalised.

Traffickers frequently use the lover boy method to lure underage victims into sexual exploitation. They increasingly meet and recruit minors online, where the latter can be particularly vulnerable and accessible.

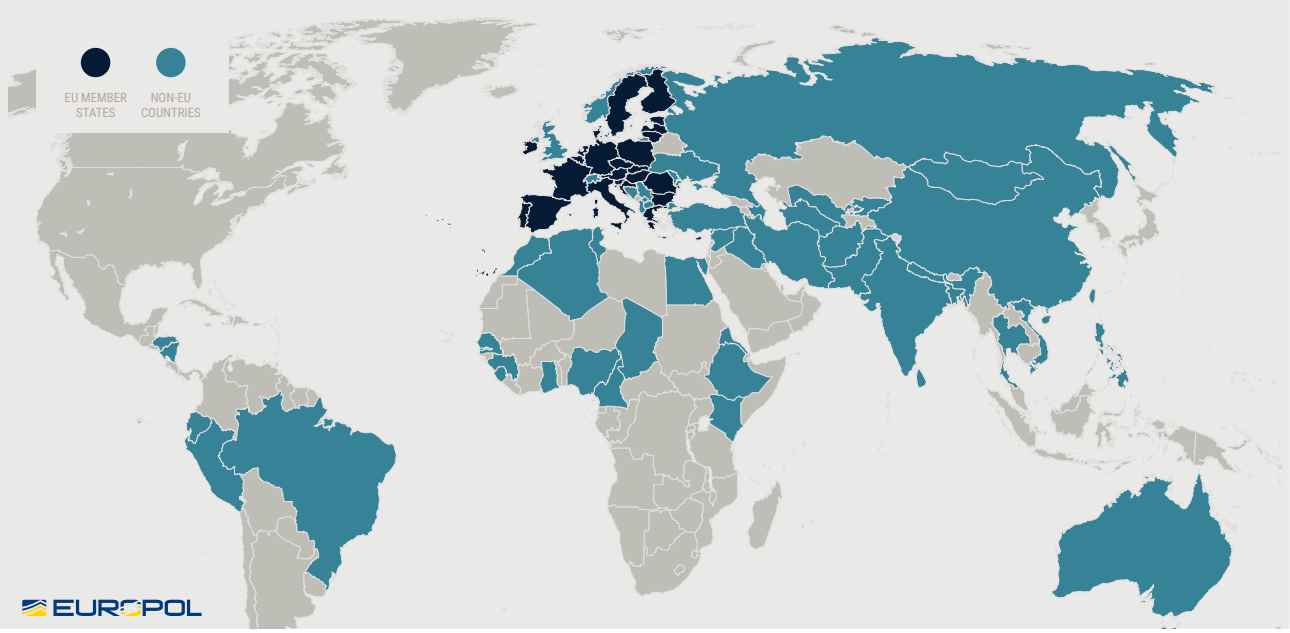
The sexual services of exploited underage victims are offered on dating and escort websites, where they are usually advertised as adults[42]. Traffickers also advertise child victims on dedicated websites where adults are specifically looking for sexual encounters with minors (known as sugar dates).

Minors are often abused in clandestine settings such as pop-up brothels. However, some exploitation also takes place in public venues such as hotels, restaurants, sex, night and strip clubs. Violence and illegal drugs are used to coerce victims.

42 Europol 2018, Criminal networks involved in the trafficking and exploitation of underage victims in the EU, accessible at https://www.europol.europa.eu/publications-documents/criminal-networks-involved-in-trafficking-and-exploitation-of-underage-victims-in-eu

LABOUR EXPLOITATION

MAIN NON-EU COUNTRIES OF ORIGIN OF TRAFFICKING VICTIMS EXPLOITED IN THE EU REPORTED TO EUROPOL



EU SOCTA 2021 DATA COLLECTION; EUROPOL INFORMATION

LABOUR EXPLOITATION

Trafficking in human beings for labour exploitation involves any work or service which is exacted from any person under the threat of a penalty and for which the person has not offered himself or herself voluntarily.

Labour exploitation occurs in various sectors of the economy. Some more loosely regulated sectors are particularly vulnerable.

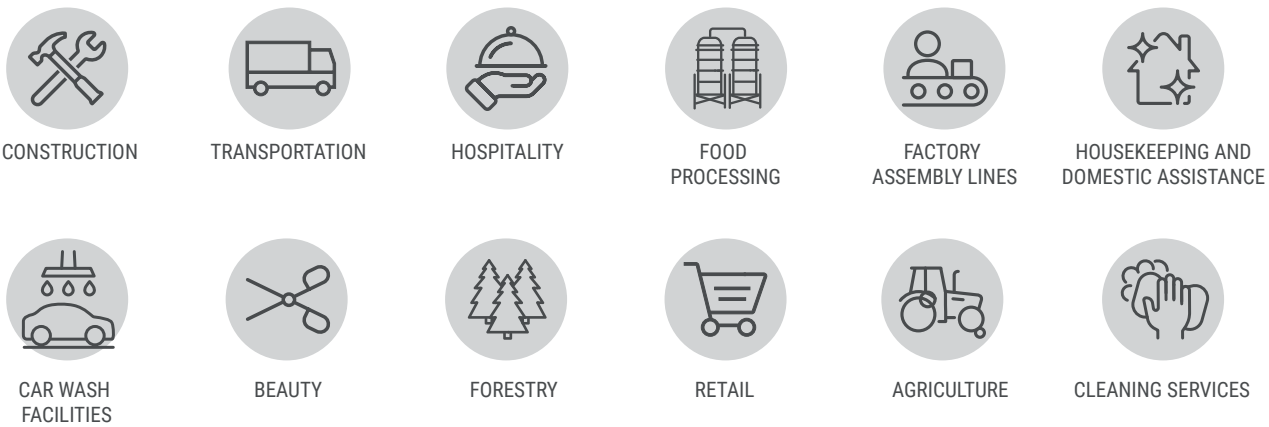
Victims are typically exploited as low-skilled, seasonal and cheap workers for transportation, construction, agriculture, forestry, food processing, factory assembly lines, hospitality, retail, carwashes, beauty and cleaning services, housekeeping and domestic assistance.

The exploitation of victims of THB for labour will remain a feature of the serious and organised crime landscape in the EU for the foreseeable future. The persistent need for low-wage workers employed in manual jobs, both seasonal and throughout the year, will sustain opportunities for labour exploitation.

MAIN INDUSTRIES

Targeted by criminal networks involved in labour exploitation

© EUROPOL 2021



PARALLEL INVESTIGATIONS BRING DOWN SEXUAL EXPLOITATION NETWORK AND FREEZE CRIMINAL PROFITS IN 12 COUNTRIES

Spanish authorities opened an investigation in 2016 targeting a Finnish national suspected of human trafficking for sexual exploitation and money laundering. The main suspect, based in Marbella, Spain, was allegedly managing websites advertising sexual services. The operation was triggered by an investigation into a criminal network trafficking victims of predominantly Nigerian origin. The website was advertising services of victims from different countries based in Sweden and Finland. Other criminal networks involved in similar activities were also advertising the services of their victims on these websites.

The suspected leader of the criminal group carried out criminal activities in at least 15 countries. He used intermediaries to channel criminal proceeds to international multi-currency bank accounts. In addition to using foreign companies and bank accounts, the money-laundering scheme also included relatively small investments in cryptocurrencies.

Source: https://www.europol.europa.eu/newsroom/news/parallel-investigations-bring-down-sexual-exploitation-network-and-freeze-criminal-profits-in-12-counties

Date: 10 July 2019

FORCED CRIMINALITY AND OTHER FORMS OF EXPLOITATION

Traffickers abuse their victims for forced begging, forced criminality, the removal of organs and tissues and at times to obtain financial and social benefits using their identities. Female victims are also trafficked to participate in illegal surrogacy programmes, sell their newborns, conclude sham marriages and as victims of domestic slavery. As with other types of THB, the recruitment of victims increasingly takes place online. Victims are lured with false job offers, advertisements to marry strangers and offers to purchase babies or organs. Most trafficked victims are homeless, suffer from mental and physical disabilities, are single parents with children or are elderly.

CHILD TRAFFICKING

Child trafficking is a heinous crime targeting a particularly vulnerable section of society. The trafficking and exploitation of underage victims occurs across the EU and targets both EU and non-EU victims. Criminals traffic children under various types of exploitation. Female victims face sexual exploitation and forced marriages to adult men. Traffickers exploit children as domestic servants, or force them to beg, pickpocket, shoplift or sell items. Children are also trafficked and sold through illegal adoption schemes.

Criminal networks comprised of both EU and non-EU nationals are involved in child trafficking in the EU. Trafficking networks involved in child trafficking can be divided into three main categories:

- criminal networks sexually exploiting both adults and minors;
- family clans abusing their children, or children of other families, and forcing them into begging, criminality and sexual abuse;
- criminal groups that are mainly involved in other criminal activities and make use of vulnerable children, often of non-EU origins, to perpetrate crimes.



The structure of the criminal networks varies according to the relationship between traffickers and victims. As for adult victims, trafficking networks are mainly composed of members sharing the same nationality as the victims[43].

Links between migrant smuggling and trafficking in human beings

Migrant smuggling and THB are sometimes seen as interrelated criminal offences. However, they are legally distinct offences. Migrant smuggling is a crime against the state, infringing national and international laws on entry, transit or residence of aliens[44]. The trafficking in human beings is a crime against a person and violates fundamental human rights[45]. The main criminal feature of migrant smuggling is the facilitation of illegal movement or stay of irregular migrants, whereas for trafficking in human beings the main crime component is the victims' exploitation. Exploitation includes the prostitution of others or other forms of sexual abuse, forced labour or services, including begging, slavery or practices similar to slavery, servitude, forcing to commit criminal activities, or removal of organs.

In most smuggling cases, irregular migrants voluntarily pay for the criminal service in order to reach their desired destination. However, especially in case of lengthy journeys and expensive travel arrangements (often including the provision of fraudulent documents), irregular migrants agree to indebt themselves and pay compensation upon arrival, through exploitative work conditions. Sometimes smugglers agree a certain price with the irregular migrants upfront and later demand or even extort additional sums from them and/or their families. In other cases, criminal networks target migrants already residing irregularly in the EU, and force them to work in highly exploitative conditions, leveraging their vulnerability and their willingness to accept any kind of job opportunity to remain and have an income.

43 Europol 2018, Situation Report on Criminal networks involved in the trafficking and exploitation of underage victims in the EU, accessible at https://www.europol.europa.eu/publications-documents/criminal-networks-involved-in-trafficking-and-exploitation-of-underage-victims-in-eu

44 Council Directive 2002/90/EC of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence.

45 Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

UNACCOMPANIED MINORS TARGETED IN RECEPTION CENTRES

The organised criminal group targeted unaccompanied minors in protection centres in Spain. They incited the minors to escape the centres and embark on dangerous journeys towards western Europe. The criminal group used recruiters from different countries to target migrants from their own national group (Algerian, Malian, Moroccan and Syrian).

The irregular migrants were transported from the Spanish port of Almería to France on buses owned by companies located in France, Morocco and Spain. The criminal group also used the buses to smuggle hashish, tobacco and hunting species. The goods and animals were hidden in holes in the vehicles, which had been specifically created to conceal their smuggling efforts. The investigation began with the arrest of a Spanish national in France who was driving a bus with 22 irregular migrants on board, six of whom were minors.

Source: https://www.europol.europa.eu/newsroom/news/29-arrests-in-france-and-spain-in-migrant-smuggling-case

Date: 17 September 2019

DOCUMENT FRAUD

Document fraud entails the production of false documents as well as the use of genuine documents obtained by means of deception, misrepresentation or theft. False documents can be complete counterfeits or partly forged. They can also be altered genuine stolen documents (including blank documents) or pseudo documents[46]. The falsification of documents can range from the straightforward extraction and/or insertion of pages and items (e.g. the removal of entry bans and the insertion of photos) to chemical and/or mechanical interference. Most often, computers with scanners and printing machines are used to imitate the original security features of travel and ID documents. Forgers also use face morphing technology to digitally merge the identity photographs of the actual holder of a document with that of a potential user, allowing one document to be used by two separate individuals.

Document fraud is an enabler for most criminal activities. This includes all types of cross-border crime, such as migrant smuggling, trafficking in human beings as well as the trafficking of drugs, weapons or stolen vehicles. Document fraud can also facilitate general financial fraud, corruption, property crime and terrorism.

Its prevalence is partly due to the fact that it does not necessarily require sophisticated tools or excessive monetary investment. Indeed, even though advanced technologies are occasionally used, most of the production can be done with standard equipment such as computers, scanners and printers.

FRANCE NABS THE LEADERS OF A DOCUMENT FRAUD NETWORK ACTIVE IN THE EU

A criminal network procured and distributed forged and falsified administrative documents to irregular migrants from North Africa based in France, Germany, Switzerland and most likely other EU countries. The criminal network produced the false documents in Athens and shipped them via courier companies. The beneficiaries, counterfeiters and suppliers communicated via social media networks.

The arrested gang leader, who was known to the German and Swiss law enforcement authorities, resided in Mulhouse, France. The suspect acted as a central interface between the counterfeiters in Greece and supervised a France-wide network of individuals hunting potential customers of illegal services. Another arrested suspect played a primary role in the recruitment of irregular migrants seeking false documents in the Paris region.

Source: https://www.europol.europa.eu/newsroom/news/france-nabs-leaders-of-document-fraud-network-active-in-eu

Date: 8 October 2020

46 False and Authentic Documents Online (FADO) Glossary: A pseudo document has the appearance of an existing document, but is not issued by an existing and legally recognised authority of a given State or organisation, recognised under international law. Pseudo documents include 'fantasy documents' which bear the name of imaginary states or organisations; 'camouflage documents' which come from countries and organisations that no longer exist or that have been renamed; and 'fictitious documents' which bear the name of an existing State or organisation but do not correspond to any real existing document in the country or organisation indicated.
European Commission 2020, False and Authentic Documents Online (FADO) Glossary, accessible at https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/false-and-authentic-documents-online_en

UNDERSTANDING THE DIFFERENT TYPES OF DOCUMENT FRAUD

GENUINE DOCUMENT

Criminal networks dealing with genuine documents exploit weaknesses in the issuance chain of documents and benefit from the ease with which citizens can claim new ones



FALSE DOCUMENT

© EUROPOL 2021

LOOKALIKE
Used by someone other than the legitimate owner, based on physical resemblance

EXPIRED
Used by its legitimate owner after its expiry date

FRAUDULENTLY OBTAINED
Through false supporting documents or corruption

FORGED
A genuine document with some alterations

COUNTERFEITED
An entirely fabricated document

STOLEN BLANK
From an administration and filled with the client's biographical data



PRODUCT COUNTERFEITING AND INTELLECTUAL PROPERTY CRIME

Counterfeiting of goods

Counterfeiting involves the manufacturing, selling or distributing of goods without the brand owner's authorisation. Counterfeits are often of inferior quality and infringe intellectual property rights.

The levels of counterfeit goods production and distribution have remained stable in the EU for the last four years. The sale of counterfeit goods via online platforms has become even more prevalent and mirrors the increasing role of the internet as the premier retail avenue for legal products and services. Online trade offers counterfeiters direct access to consumers, thereby reducing the number of intermediaries while having a greater reach. The majority of retail activity of counterfeit goods takes place online, on social media, commerce platforms as well as on dedicated websites. It is difficult to assess the demand for counterfeit goods as in many cases consumers are unaware they are purchasing a counterfeit item[47].

Counterfeit goods are typically manufactured outside the EU and then imported for distribution in stores, markets or online. Counterfeit items are imported ready for sale or semi-finished. The import of semi-finished products, in which labels and packaging are imported or produced separately, has been increasing as this method lowers the risk of detection at the border. Semi-finished goods are then assembled and sold in the EU.

Legal business structures are integral to the trade in counterfeit goods both as retail channels and to facilitate the movement of goods and to launder illegal profits. Document fraud is used widely and may involve falsified origin and travel documents.

Counterfeit and substandard plant protection products pose a significant and growing threat to the EU. These products are extremely dangerous for the environment and can heavily contaminate agricultural land and the foodstuff grown on it. Pesticides are among the most highly regulated products due to their potential impact. Pesticides are used to eliminate harmful organisms in plants, while still being safe for the environment and human health. If improperly produced, they can pollute the air, water and soil for a long period of time. The impact on health is not only limited to farmers and the farming community, but also extends to the consumers of cultivated food products. Illicit pesticides can be either counterfeit or substandard. While counterfeit pesticides are illegal copies of branded products, substandard pesticides include all the other uncertified or fraudulent products. Both categories are generally placed on the market without having been officially tested and authorised by the authorities.

47 Eurostat 2018, Handbook on the compilation of statistics on illegal economic activities in national accounts and balance of payments, accessible at https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/KS-05-17-202

NEARLY 28 MILLION COUNTERFEIT AND ILLEGAL GOODS INCLUDING 27 MILLION FACEMASKS WERE SEIZED

The operation led to 123 social media accounts and 36 websites selling counterfeit products to be taken down. During the operation, law enforcement authorities seized nearly 28 million illegal and counterfeit goods among which were 800 000 counterfeit items of clothing, sportswear, footwear, personal accessories, IPTV set-top boxes and toys. Ten people were arrested in Greece and 37 others were reported to the judicial authorities in Greece, Italy and Portugal. More than EUR 700 000 was also seized.



The COVID-19 outbreak led the involved authorities to adapt the initial scope of the operation to focus on issues triggered by the pandemic. As a result, counterfeit and not compliant medical equipment was also seized, including 27 million medical facemasks, by the Italian Finance Corps (Guarda di Finanza).

Source: https://www.europol.europa.eu/newsroom/news/no-safe-market-for-fakes-21-countries-target-illegal-goods-in-europe-wide-sting

Date: 25 September 2020

Food and drink fraud

Food fraud is a collective term used to describe the deliberate and intentional substitution, addition, tampering, or misrepresentation of food, food ingredients or food packaging; or false or misleading statements about a product for economic gain. Criminals counterfeit or manipulate food products or mislead consumers by altering labels, geographical indications or manufacturing processes. The production of illicit food products, especially drinks, is expected to become more sophisticated.

Illicit food products are increasingly marketed and sold online and this trend is set to continue to for the foreseeable future. Food products are increasingly mislabelled as organic.

Food fraud results in financial losses and reputational damage to legal producers as well as the loss of tax revenues. The trade in fraudulent food products distorts market competition, damaging fair production and distribution. The use of toxic or unsafe ingredients in the unregulated production of food products can have a negative impact on the health of consumers. Some fraudulent food products include dangerous ingredients such as methanol, mercury, fipronil, insecticides or pesticides. The consumption of meat from ill animals can provoke dangerous viral infections.

FAKE WINES SOLD UNDER EXPENSIVE ITALIAN LABELS OFF THE MARKET

The investigation discovered that low quality wines were refilled in bottles under original labels and then sold as real ones on a big online auction platform. The wines were sold in Belgium, France, Germany, Italy, Spain and the US, often ending in the glasses of unaware customers of wine bars and catering services. The empty authentic bottles were gathered from restaurants and delivered mainly by two individuals working in the food industry. These bottles were then refilled with cheap wines from different origins, purchased online or at hard discount stores. Afterwards, the bottles were sealed with corks and counterfeit capsules of a different or similar colour to the original. Packaging films and false masking guarantee seals were finally applied to conceal the lack of distinctive signs on the capsules used for the counterfeit units. Once a contact with a buyer was established via a large e-commerce platform, the counterfeiters expanded their promotional offers even further, setting prices far below the ones seen usually on the market. A magnum format (1.5 l) of some of the counterfeit wines typically exceeds EUR 1 000 per bottle.

Source: https://www.europol.europa.eu/newsroom/news/fake-wines-sold-under-expensive-italian-labels-market

Date: 30 June 2020

Pharma crime

PPharmaceutical crime involves the manufacture, trade in or distribution of fake, stolen or illicit medicines and other pharmaceutical products, as well as medical devices. The use of counterfeit medicines and medical supplies causes significant direct harm to the health of victims. Pharma crime also harms pharmaceutical companies and reduces the funds available for research and development and product innovation. Clandestine illicit pharmaceutical production sites harm the environment by producing and improperly disposing of chemical waste[48] .

The COVID-19 pandemic has prompted a surge in the trade of illicit medical supplies such as counterfeit face masks, gloves, hand sanitiser as well as fake vaccines. Legitimate suppliers were initially unable to meet the sudden increase in demand for personal protective equipment and sanitary products, which resulted in opportunities for criminals.

Criminals have exploited the pandemic by offering ineffective goods such as fake corona home test kits or fraudulent prescription medicines used to treat the disease. Soon after the news that the COVID-19 vaccine was ready for authorisation by health authorities, fraudulent offers of the vaccine appeared on the dark web.

The distribution of pharmaceutical goods is increasingly shifting from physical to online markets including dedicated platforms such as online pharmacies as well as widely used social media services. Most trading activity is believed to take place on the surface web. However, some pharmaceutical products are also distributed via dark web platforms.

48 OECD and EUIPO 2020, Trade in counterfeit pharmaceutical products, accessible at http://www.oecd.org/gov/trade-in-counterfeit-pharmaceutical-products-a7c7e054-en.htm



Digital content piracy

Online piracy is the practice of illegally copying and selling digital content, such as music, books, computer programs and games. Piracy evolves quickly in lock step with other technological advances. Piracy is now almost exclusively a digital crime as the distribution of physical copies of audio-visual content has almost entirely disappeared. Illegal streaming and internet protocol television (IPTV) are the most common ways to access this type of content. Online offers for these illicit services are widely available for monthly or annual subscriptions and in any language.

The use of illegal IPTV services has increased over recent years. The servers hosting these services are typically located in countries other than those where the subscriptions are sold[49]. Demand for digital content, both legal and illegal, has surged during the COVID-19 pandemic.

The distribution of content on physical media is expected to disappear entirely in the EU, as it is replaced by more easily accessible digital content. Virtual currencies will be widely used to pay for access to pirated content.

Legal ways of accessing online entertainment have multiplied and become cheaper for consumers. This is likely to make pirated content less attractive in the future[50].

49 Europol 2020, Viral marketing – Counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic, accessible at https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-substandard-goods-and-intellectual-property-crime-in-covid-19-pandemic

50 EUIPO 2019, Online copyright infringement in the European Union – music, films and TV (2017-2018), trends and drivers, accessible at https://op.europa.eu/en/publication-detail/-/publication/c3a53ca1-1bc3-11ea-8c1f-01aa75ed71a1

ILLEGAL STREAMING SERVICE WITH OVER 2 MILLION SUBSCRIBERS WORLDWIDE SWITCHED OFF

TThe investigation into the activities of the criminal network started in 2019 when the Spanish National Police detected several websites illegally distributing audio-visual content in different countries across Europe, Asia and the Middle East. The distribution of the illegal services, in breach of intellectual property rights, was set-up as IPTV and managed from Spain. The criminal network was offering illegally more than 40 000 TV channels, movies, documentaries and other digital content via websites hosted on an international network of servers. The illegal service was made available through an attractive web environment at prices much more competitive than the ones on the legal market. The criminal network had even put in place a sophisticated technical assistance and quality control through an own customer support online platform. More than 2 million subscribers were receiving these illegal services, with total profits for the criminal network at an estimated EUR 15 million. The investigation focused on shutting down the servers and disconnecting the IP addresses, and obtaining relevant information to effectively dismantle the criminal group.

Source: https://www.europol.europa.eu/newsroom/news/illegal-streaming-service-over-2-million-subscribers-worldwide-switched

Date: 10 June 2020

CURRENCY COUNTERFEITING

Currency counterfeiting includes the production and distribution of counterfeit currency, including the reproduction of individual security features.

The availability and distribution of counterfeit banknotes via dark web platforms has increased: various currencies and denominations are advertised and traded online, including material and equipment for illicit production, tutorials on how to produce counterfeit banknotes and information on protective elements.

Outside the EU, the highest quality and largest quantity of counterfeit euros are produced in Colombia and Peru[51]. China is the main resource country for materials (mainly fake holograms and other security features) for currency – particularly euro – counterfeiting.

SALE OF COUNTERFEIT EURO BANKNOTES VIA ILLEGAL PLATFORMS ON THE DARK WEB

Law enforcement authorities from 7 EU Member States carried out 36 house searches, detained 44 suspects for questioning, 11 of whom have been arrested, and seized counterfeit euro banknotes, drugs, weapons, doping substances, illegally procured medicines, forged documents and virtual currency. A clandestine documents print shop was also dismantled in Germany. Germany carried out 27 house searches and 9 other raids were done in Austria, France, Greece, Ireland, Luxembourg and Spain.

These joint activities were triggered when the Portuguese Judicial Police (Polícia Judiciária) dismantled a digital print shop in July 2019. This Europol-supported operation led to the arrests of five individuals suspected of producing and distributing counterfeit 10 and 50 euro banknotes mainly via the dark web. Over 26 000 fake banknotes were shipped to buyers all over Europe, making this criminal group the second-largest counterfeit currency producer operating on the dark web to be identified so far.

Source: https://www.europol.europa.eu/newsroom/news/no-crime-goes-unpunished-darknet-11-arrested-for-buying-counterfeit-euros

Date: 16 December 2019

51 European Commission 2020, Annex to Commission decision on the financing of the Pericles 2020 Programme and the adoption of the work programme for 2020, accessible at https://ec.europa.eu/info/funding-tenders/funding-opportunities/calls-for-funding/pericles-2020-programme-2020-ecfin-003-c5-call_en



ORGANISED PROPERTY CRIME

Fencing

Fencing is knowingly buying and selling stolen goods. Organised property crime fundamentally relies on fences. However, the processes and networks behind fencing are largely under-investigated. Key locations and routes for stolen goods are currently intelligence gaps.

Criminals active in organised property crime, including MOCGs, either set up their own fencing arrangements or work with independent fences. These independent fences work with criminals of different nationalities.

Stolen goods such as cosmetics and phones are often sold via local businesses such as second-hand shops, phone shops, jewellery shops, pawnshops, convenience stores and bars. These venues can be located in the home country of the criminals or in the country of the theft or other countries depending on the availability of local fencing networks. Another important sales channel are online platforms. Stolen goods are offered on the surface web on marketplaces or via classified advertisement sites dedicated to specific goods.

Organised burglaries and thefts

Organised burglaries and thefts involve the serial commission of burglaries and thefts by a group of criminals. Burglaries target all types of premises such as private homes, commercial and industrial or public buildings. Organised thefts typically involve physical ATM attacks, thefts from vehicles such as cargo theft, shoplifting, pickpocketing and metal theft.

Organised property crime is likely the most visible type of organised crime, with a direct impact on people and the private and public sector. More than one million cases related to burglary are reported in the EU each year[52].

In addition to the financial impact, burglaries and thefts perpetuate feelings of insecurity affecting hundreds of thousands of EU citizens.

The COVID-19 lockdown restrictions keeping citizens at home and limiting travel have had a significant impact

52 Eurostat 2020, Recorded offences by category – police data (crim_off_cat), accessible at https://ec.europa.eu/eurostat/web/crime/data/database

on organised property crime. The number of domestic burglaries and common thefts has generally declined following the imposition of the measures[53]. However, offenders have adapted by engaging in various types of schemes involving deception around the COVID-19 pandemic. Perpetrators use techniques such as the impersonation of representatives from public authorities or medical staff to gain access to private homes pretending to provide information material or hygiene products or conducting corona tests to steal valuables.

MOCGs continue to travel from region to region committing serial domestic burglaries of homes and apartments. The methods used for breaking and entering remain the same and include forcing windows and doors open using screwdrivers and crowbars, breaking locks by drilling into the door or window frame or climbing to higher floors and balconies looking for weak spots. In most cases, thefts are committed within a few minutes. Business premises such as shops, department stores, companies and banks are often targeted. Criminals continue to frequently enter premises through damaged walls and roofs. Ram-raids are still commonly used to burgle jewellery stores.

MASTERMINDS BEHIND GERMAN ROOFTOP BURGLARIES HALTED IN MOLDOVA

An investigation in Germany into a series of high-profile domestic burglary cases led to the arrest of members of a Moldovan MOCG. The offenders gained access to the victims' houses by removing panels from the roof and cutting a hole to gain access. This way the criminals avoided the doors and windows equipped with alarm systems. The total damage caused amounts to more than EUR 20 million from 22 separate burglaries.

Source: https://www.europol.europa.eu/newsroom/news/masterminds-behind-german-rooftop-burglaries-halted-in-moldova

Date: 6 December 2018

At present, physical ATM attacks are only regularly carried out in a limited number of Member States. However, attackers can easily change their countries of activity and this means that more Member States are likely to be confronted by this phenomenon in the near future. Physical ATM attacks are attractive for criminals as the immediate access to cash negates the need for an extensive network to sell stolen goods. It is often a convenient alternative for criminals already active in organised property crime. Although the success rate for attacks on ATMs is not very high, a single successful attack will result in a high return in most cases.

Cargo crime is the illicit acquisition of any type of cargo in transit from producer to distributor to customer, stolen during freight transport or from storage facilities that are part of the supply chain. Cargo crime entails theft or fraudulent acquisition when goods are diverted from their original destination. The losses caused by cargo crime in the eight most affected Member States exceeded EUR 75 million in 2019 and have a significant impact on supply chains.

Organised pickpocketing and distraction thefts continue to be carried out, targeting victims' mobiles phones and wallets in crowded places such as concerts, markets, public transport and railway stations. Criminals also engage in 'shoulder surfing' or 'shouldering', targeting elderly citizens to steal their debit card by distraction after looking over their shoulder to see the PIN.

Various scams and schemes are still used, such as fake officials, including false police officers and fake corona teams, and the nephew or grandchild trick, to

53 Europol 2019, How COVID-19-related crime infected Europe during 2020, accessible at https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020

target mainly elderly persons. During the COVID-19 pandemic, some perpetrators adapted their schemes to pretend to be sick relatives in need of money. Some also impersonate healthcare and law enforcement officials to gain access to homes.

Metal theft is driven by high prices for metal. Criminals monitor metal prices and carry out metal thefts when potential profits are most promising. In most cases, metal theft only requires simple construction tools, limited expertise and access to scrap dealers. Criminals target railway cables and churches for copper as well as the catalytic converters of vehicles for other precious metals.

Organised property crimes carried out in the EU continue to be perpetrated primarily by MOCGs. Mobility remains the key characteristic of these MOCGs and is used to avoid detection and minimise the risk of apprehension. MOCGs travel long distances and are typically active in several countries. They are highly flexible in the selection of their targets and will often change their country of activity to evade law enforcement or to respond to changes in the criminal landscape.

Organised robberies

A robbery is the felonious taking of property from another person or in his or her immediate presence, against his or her will, by violence or intimidation.

Organised robberies include robberies committed by criminal groups. In addition to the obvious psychological, physical and financial harm inflicted on victims of robbery, robberies also have a significantly negative effect of undermining the perception of public security, which indirectly reflects on the demographic and economic development of affected regions.

Violence is an integral part of the modus operandi of robbery and mainly involves the intimidation of shop owners, employees, customers and witnesses with firearms or other objects such as explosives, knives, axes or baseball bats. Attacks on cash transports sometimes involve the use of arms. The firearms used include pistols, rifles, assault rifles, automatic rifles, machine pistols, reactivated guns, air guns, gas pistols but also faithful copies such as plastic pistols.

There has been a shift from more secure targets, such as banks, towards less secure targets, including small local shops such as pharmacies or convenience stores. Elderly people are increasingly targeted in their homes.

Robberies have seen little or no changes in terms of modi operandi. Organised robberies are usually well prepared. The targets are scouted for days or even months, escape routes are planned and sometimes measures are taken to keep law enforcement at a distance. Robbers engage in hit and run tactics, use masks, dark clothes and gloves to disguise their identity and quickly leave the crime scene often via a different route than the route of arrival.

HUGGER MUGGERS ROB JEWELLERY AND LUXURY WATCHES

An international investigation led to the detection and arrest of 10 members of a criminal network specialised in the robbery of jewellery and luxury watches. The network used over 1600 stolen vehicles to commit these robberies. Some members had no fixed residence and were active throughout Europe. The criminals preyed on elderly and vulnerable individuals. The gang approached their victims in stolen vehicles, when one of the suspects, usually a woman, would get out the car and talk to the potential victim. The criminal would then hug the victim and snatch their jewellery.

Source: https://www.europol.europa.eu/newsroom/news/over-1-600-vehicles-worth-%E2%82%AC13-million-used-to-commit-robberies

Date: 24 May 2019

Organised robbers mostly target businesses with limited security arrangements in place, such as small banks, cash-intensive businesses or shops selling high-value goods. No special expertise is required to target these premises. Business targets include jewellery stores, pharmacies, electronic goods stores, clothing stores, banks, post offices, exchange offices, petrol stations and convenient stores.

Organised robberies are perpetrated by internationally active MOCGs as well as local criminals depending on the Member State and region. MOCGs are highly mobile, travel long distances to quickly execute robberies and leave the country of operation.

Hierarchically structured criminal networks such as thieves-in-law, Outlaw Motorcycle Gangs (OMCGs) and clan-based criminals are active in organised robberies.

Motor vehicle crime

Motor vehicle crime includes the theft or fraudulent acquisition (embezzlement, rental or lease fraud, insurance fraud) of vehicles or vehicle parts. Vehicles stolen in the EU are recovered mainly either in the country of the theft or in another Member State within a few days after the theft while still in transit. Only a very small percentage of stolen vehicles are recovered from outside the EU.

The declining trend in motor vehicle crime has been attributed to improved security measures implemented by vehicle manufacturers, law enforcement activities and the more extensive use of the European Car and Driving License Information System (EUCARIS) which enables countries to share vehicle and driving licence registration information.

Motor vehicles are illegally acquired by criminals either by theft or through fraud. Stolen vehicles are sold as such or for parts. The technical arms race between manufacturers and criminals is set to continue as motor vehicles are becoming more vulnerable to cyberattacks targeting the many digital components of modern vehicles. Vehicle security has further improved and requires most vehicle thieves to rely on electronic compromise of the vehicle systems.

Most vehicles are stolen using electronic devices to exploit new technologies, such as keyless entry for relay attacks, to reprogramme the vehicle and disable immobilisers, car alarms and tracking systems.

Member States continue to see an increase in the number of incidents related to the fraud and embezzlement of motor vehicles due to low down-payment requirements for the leasing or financing of vehicles and the accessibility of consumer credit. The most common fraud and embezzlement method is the leasing or purchase of a vehicle on loan using fraudulent documents and then disappearing with the vehicle and defaulting on payments.

To enable their transportation and sale, stolen vehicles receive a new identity and the identification features of vehicle parts are removed in most cases. Legislative loopholes in importation and registration procedures allow the re-registering of stolen cars. In order to do this, criminals change number plates, falsify vehicle identification documents and the vehicle identification numbers.

Criminals involved in motor vehicle crime rely on the complicity of corrupt officials in registration offices, vehicle inspection experts, customs officials and staff of insurances companies to legalise the status of stolen vehicles.

Vehicles are typically transported on their own wheels. In some cases, shipping companies are used to transport stolen vehicles over land on cargo trains or lorries or via sea in container ships. Stolen vehicle parts are transported in vans and lorries.

Vehicles are trafficked through a number of layers before reaching the final buyer. Criminals use legal business structures for a variety of purposes related to the purchase and sale of stolen vehicles and stolen vehicle parts. Sales channels include official car dealers, second-hand car dealers, vehicle repair shops as well as trade fairs or unofficial garages. Stolen vehicles and parts are increasingly sold online via a variety of platforms, including social media. The online business-to-business market for spare parts is expected to grow significantly in the coming years; criminals may seek to use these channels to sell their stolen goods.



The illegal trade in cultural goods

Cultural goods crime or the illegal trade of cultural goods includes three main criminal phenomena. Theft and robbery of original cultural goods; looting, the illicit removal of ancient relics from archaeological sites, buildings or monuments and illegal trade of these; and forgery, the illegal imitation of cultural goods from a specific artist or historical period for financial benefit by offering them with false features. The trafficking in cultural goods is assessed to remain a stable criminal activity, with demand sustaining trafficking activities at the same or potentially increasing levels for the foreseeable future.

Cultural goods traffickers have profited from a diversification of sales channels online, such as online auctions, flea markets and private sales sites, to expand their customer base. Stolen masterpieces are still traded through traditional black market channels while online marketplaces (social networks, classified ads websites) offer criminals new opportunities to sell lower value items that were previously not in demand.

Most commonly, cultural goods are stolen during burglaries or by theft by deception from places of worship, cultural heritage institutions, museums, private homes and private collections. Some of the thefts are carried out on the request of a sponsor. In some cases, stolen goods are replaced with forgeries. Theft by deception involves the use of false identity documents to gain access to secured premises such as archives, libraries or archaeological excavation sites to remove objects.

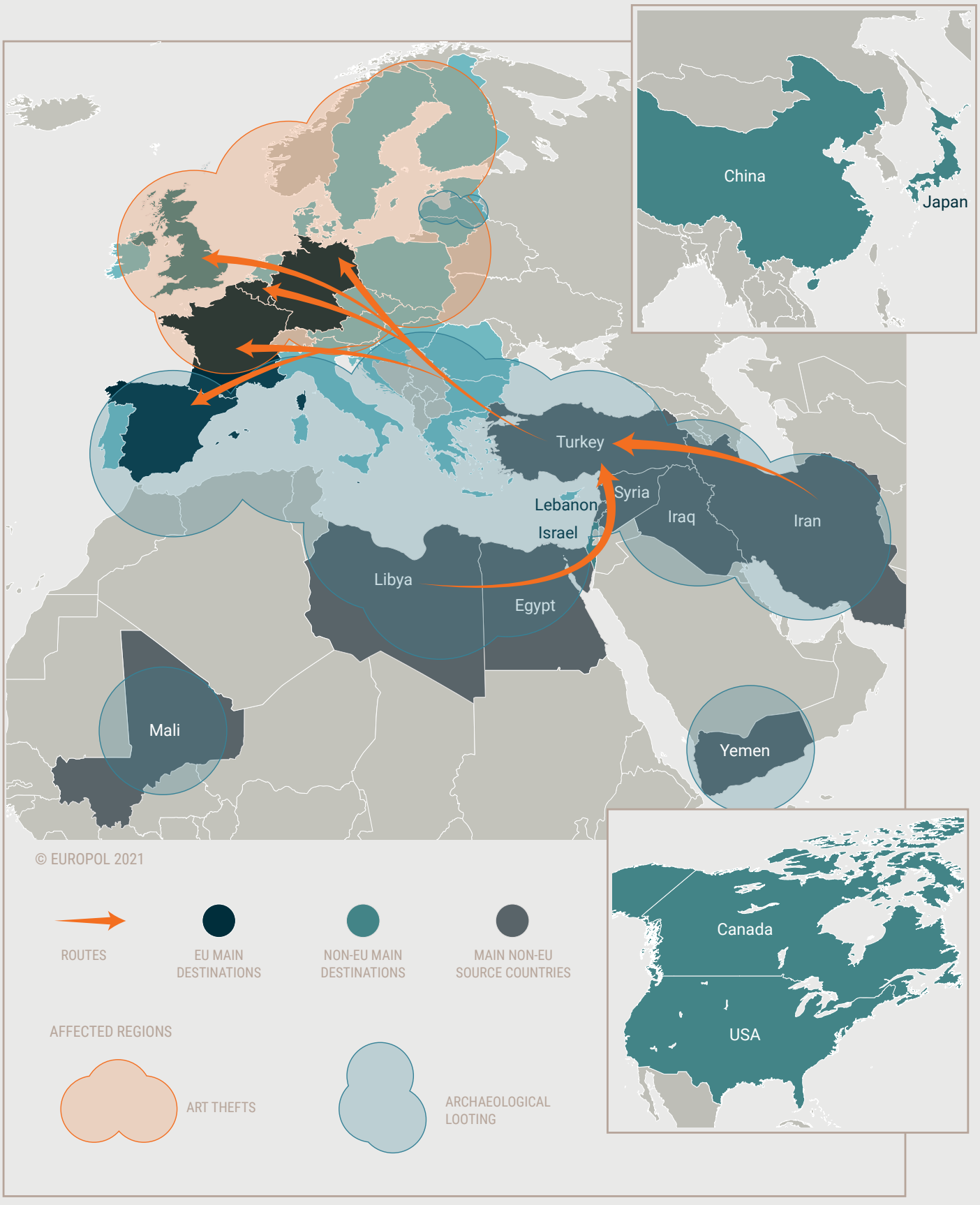
23 ARRESTS AND AROUND 10 000 CULTURAL ITEMS SEIZED IN AN OPERATION TARGETING ITALIAN ARCHAEOLOGICAL TRAFFICKING

When dismantling an international organised crime group of 23 members involved in large-scale trafficking of looted archaeological items, law enforcement authorities seized around 10 000 cultural items during 80 house searches. The network was active for many years and caused significant damage. The items were stolen from archaeological sites in Calabria, southern Italy, where the cultural heritage stems from the Greek and Roman period. The different rings of the network, led by two Calabrians living in the province of Crotone, included looters, fences, intermediaries and mules operating from different Italian regions. The key facilitators were also acting from Djion, Munich, London and Vršac, coordinating the supply chain.

Source: https://www.europol.europa.eu/newsroom/news/23-arrests-and-around-10-000-cultural-items-seized-in-operation-targeting-italian-archaeological-trafficking

Date: 18 November 2019

ILLEGAL TRADE IN CULTURAL GOODS
MAIN COUNTRIES INVOLVED



SOURCE: EU SOCTA 2021 DATA COLLECTION, EUROPOL INFORMATION

QUO VADIS? AN OUTLOOK ON **SERIOUS AND ORGANISED CRIME**



KEY DEVELOPMENTS

Serious and organised crime is both resilient and versatile and continues to evolve and adapt to reduce the risks to its own business, maximise profits, exploit new opportunities and evade law enforcement attention. In trying to anticipate the development of criminal phenomena in the EU, it is crucial to look at the broader changes in the environment in which crime takes place. In November 2020, a group of subject-matter experts from across various disciplines engaged in a systematic foresight exercise to identify key developments in the EU over the next five years. The exercise was followed by exchanges between law enforcement experts on the possible impact of these developments on the security of the EU. The developments outlined below are the outcome of this exercise.

DIGITALISATION

The EU is on a path towards total digitalisation – a development that will continue at a fast pace with significant impact on society, public administration, transport and trade. The COVID-19 pandemic has further accelerated this phenomenon. Substantial investments in infrastructure will be necessary to complete the transition to the digital era. Currently, Member States are progressing at different speeds in building up digital infrastructures; this may lead to potential vulnerabilities.

Government services are increasingly delivered digitally. Member States' government authorities are likely to increasingly offer services digitally to cut costs and enhance their accessibility.

Digitalisation is set to further increase the volume of digital personal data, which is mostly held by private companies. There is a risk that the exponential increase in data will overwhelm governments who are unable to manage, safeguard and effectively use this information. Cybercriminals will launch sophisticated and large-scale attacks against critical infrastructure to access and steal sensitive data.

States risk ceding control over many areas of finance and the economy to the private companies that dominate the digital space. Leading technology companies will entrench their monopoly positions, drawing on financial resources and superior engineering capacities.

The monopoly on data held by third parties will continue to pose increasing risks of manipulation and criminal use of personal information. Privacy and the ethical use of data are key topics to be addressed by law enforcement, legislators and policy makers.

Widespread adoption of cryptocurrencies by legitimate businesses and individuals could have a significant impact. Law enforcement authorities will need to find new ways to access information on financial transactions between criminals.

As digitalisation increases, so do the challenges from the increasing spread of misinformation, fake news and conspiracy theories. The use of deepfakes[54] will probably become a serious challenge for the digital environment[55]. Law enforcement authorities have limited powers to counter information manipulation, which can take the form of attempts to distort political discourse, manipulate elections, erode democratic principles, sow distrust in institutions, intensify social divisions, foster insecurity, and spread discrimination and xenophobia.

GEOPOLITICAL FACTORS

Recognising the internal-external security nexus is crucial in trying to understand upcoming challenges to the EU's internal security. The EU continues to engage with partners globally.

China's influence on trade, infrastructure and security at a global level, particularly in the Middle East, Central Asia and Africa, will shape the EU's foreign policy and security stance, including as regards the EU's internal security. This development will necessitate stronger European security autonomy and greater cooperation between national authorities in all security domains such

54 Deepfakes are media in which a person is replaced with someone else's likeness. Deepfakes leverage powerful techniques from machine learning and AI to manipulate or generate visual and audio content with a high potential to deceive.

55 Forbes 2020, Deepfakes Are Going To Wreak Havoc On Society. We Are Not Prepared [25/05/2020], accessible at https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared/?sh=5534e7b67494

as defence, intelligence and law enforcement. EU-based criminals will look to China for criminal opportunities while Chinese organised crime will use the country's footprint across the world to intensify their criminal operations outside China.

There is still significant conflict potential on the periphery of the EU, with active conflicts in Ukraine and between Armenia and Azerbaijan, as well as instability in Libya, the Sahel region and the eastern Mediterranean area.

Stability in certain post-conflict areas remains fragile and there is a risk of relapsing into active conflicts should conditions deteriorate.

Active conflicts may cause further mass migration movements towards the EU, fuelling the migrant-smuggling industry that has emerged over recent years.

THE GREEN TRANSITION

The green transition is the move towards a less resource-intensive and more environmentally sustainable way of life touching on all aspects of the economy, society and technology. The green transition is an opportunity for innovation and economic success. The financial system and green sectors will be increasingly interlinked.

Criminals will seek to profit from this development by orchestrating increasingly complex and far-reaching fraud schemes involving investments, energy and green certifications.

Waste management and recycling will become key sectors. A circular economy means a longer life span for goods and full waste-recycling systems will mean waste dismantling will be carried out within the same territory as production. Illicit waste management will be a significant growth sector as prices for legal waste management services will continue to increase. Illicit waste management can involve the unlawful reintroduction of waste in production cycles, the resale of hazardous waste mixed with other waste or the reuse of waste products as second-life goods.

Food security and food safety will become increasing concerns. Environmental crimes with significant impact on biodiversity (such as illegal fishing, illegal logging, and wildlife poaching) are very difficult to detect. Fraud related to food and the distribution of counterfeit products and beverages will increase, leading to a decline in consumer trust.



THE LONG-TERM IMPACT OF THE COVID-19 PANDEMIC

The COVID-19 pandemic has been a crisis of an unprecedented nature. The pandemic has proven to be more than a global public health crisis and has resulted in considerable changes in the serious and organised crime landscape in the EU and beyond. Criminals have quickly capitalised on these changes by shifting their market focus and adapting their illicit activities to the crisis context. The immediate impact of the COVID-19 crisis has been most visible in the counterfeiting and distribution of substandard goods, cybercrime, organised property crime, and various types of fraud schemes.

The mid- to long-term consequences of the pandemic will result in further vulnerabilities. A prolonged pandemic will put a heavy strain on European and global economies, with indications that some countries are already entering an economic downturn. Learning from previous crises, it can be anticipated that a volatile economic situation with growing poverty and social inequality will serve as a breeding ground for organised and serious crime.

Criminals will intensify their activities to fully exploit emerging vulnerabilities, in order to compensate for lost profit during the lockdown period. Criminals will continue to rely on the use of new technologies and further expand their technical capabilities.

Criminal groups have quickly adapted to profit from the new business opportunities the pandemic economy has presented, taking advantage of the increased and widespread demand for certain products. The supply of counterfeit and substandard medical equipment as well as sanitary and pharmaceutical products increased significantly both on the surface and dark web[56].

The pandemic has clearly highlighted the dynamic nature of cybercrime. Since the outbreak of the pandemic, an increased number of COVID-19-related domains have been created to support different cybercrime activities. The number of cyber-enabled and pandemic-related scams, COVID-19-themed malware, ransomware and phishing attacks notably increased during the pandemic,

56 Europol 2020, Viral marketing, accessible at https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-sub-standard-goods-and-intellectual-property-crime-in-covid-19-pandemic

targeting individuals, businesses and the health sector alike [57]. With the roll out of COVID-19 vaccination campaigns, it is expected that the number of vaccine-specific cybercrime activities will surge, including cyberattacks on pharmaceutical research.

The impact of the COVID-19 crisis on the drug markets has been relatively limited. Aside from initial and localised disruptions in the supply and distribution of drugs during the first lockdown, the trafficking of drugs has continued[58]. Despite fluctuations in the price and supply of drugs on the European market early in the pandemic, the drug market has largely returned to pre-pandemic levels.

The long-term consequences of the pandemic may manifest particularly severely in the area of financial crime[59]. Businesses operating in sectors suffering particularly negative economic pressures, such as the hospitality, catering and tourism sectors, are becoming more vulnerable to criminal infiltration[60].

Money laundering poses a high risk in times of financial crises. Criminals may increasingly attempt to launder money through dormant companies, buy out financially affected cash-intensive businesses, or invest in property in the construction sector[61]. As a result of heightened pressures exerted on banks during an economic crisis, due diligence procedures may be weakened elevating the risk of loan fraud. Money launderers may also increasingly misuse online financial services and virtual assets to conceal their illicit proceeds. Trade-based money-laundering activities are also expected to intensify.

The COVID-19 pandemic has led to a considerable increase in the output of sanitary and medical waste, posing a significant risk to the environment and public health alike[62]. A reduction in the number of inspections and controls of waste shipments by supervisory authorities enabled some criminals to traffic and illegally dispose of waste. Widespread economic hardship may open up additional opportunities for illicit waste traffickers. A general decline in corporate revenues may entice companies to take advantage of such illicit services in order to reduce waste disposal costs.

57 Europol 2020, How COVID-19 related crime infected Europe in 2020, accessible at https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020

58 Pandemic profiteering – How criminals exploit the COVID-19 crisis, accessible at https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

59 Levi and Smith 2020, Australian Institue of Criminology Research Report – Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19.

60 Based on the contribution by the Working Group on COVID-19 criminal threats and law enforcement responses 1st meeting; Europol 2020, Enterprising criminals: Europe's fight against the global networks of financial and economic crime, accessible at https://www.europol.europa.eu/publications-documents/enterprising-criminals- %E2 %80 %93-europe %E2 %80 %99s-fight-against-global-networks-of-financial-and-economic-crime

61 Europol 2020, Beyond the pandemic – how COVID-19 will shape the serious and organised crime landscape in the EU, accessible at https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu

62 Europol 2020, How COVID-19 related crime infected Europe in 2020, accessible at https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020; Based on the contribution by the Working Group on COVID-19 criminal threats and law enforcement responses 1st meeting.

THE POTENTIAL IMPACT OF A GLOBAL ECONOMIC RECESSION

The global COVID-19 pandemic and the restrictions imposed to stop the spread of the disease have been widely forecast to result in a deep and severe economic recession on a global scale. The EU will be significantly affected by this development. A severe economic recession or even depression may shape the serious and organised crime landscape in the EU for years to come.

Previous experiences from times of severe economic crisis, such as the financial crisis of the late 2000s and early 2010s, allow us to anticipate how another such economic crisis may influence the threat from serious and organised crime.

The economic downturn created by the global COVID-19 pandemic is expected to last well beyond 2021. 2020 saw the worst recession since the Great Depression[63]. The restrictions imposed to curb the spread of the coronavirus slowed down economic activity, resulting in a fall in consumer spending, retail sales and employment[64]. The level of output is expected to remain below its pre-pandemic levels for a prolonged period of time[65]. Some of the hardest hit industries, such as aviation, hospitality, culture and leisure, have yet to experience the full impact of the crisis, due to current government support schemes and stimulus packages[66]. The economic outlook remains bleak. The World Bank estimates that by 2025, output will still be 5% below its pre-pandemic trend, which could lead to a cumulative output loss equal to 35% of world output in 2019[67].

ING Groep NV has estimated that the economy will not return to its pre-pandemic levels until at least 2023[68].

The EU and Member States have established support and recovery funds on an unprecedented scale in order to mitigate the potentially catastrophic impact of a recession following the COVID-19 pandemic. The funds aim to support private companies of all sizes, the self-employed, non-profit organisations and private citizens. These funds have already been targeted by fraudsters seeking to illegally access these billion of euros of resources. While safeguards are in place to prevent abuse at national and European level, authorities have had to distribute these support payments so fast that this has weakened some of the due diligence procedures and already allowed some criminals to illegally benefit from these funds. Member States and the EU will seek to further support European economies with offers of financial and other support. It is expected that some criminals will specialise in abusing these vital schemes by orchestrating complex networks of companies in order to defraud public funds.

The potential loss of billions of euros of public revenues through VAT and other frauds directly affects taxpayer interests and the ability of governments to fund essential public services. Rising unemployment, reductions in legitimate investment and further constraints on the resources of public authorities may combine to present greater opportunities for criminal groups, as individuals and organisations in the private and public sectors are rendered more vulnerable to compromise.

The weak capitalisation of some EU-based companies due to the economic crisis may make them vulnerable to takeovers by criminals based inside and outside the EU

63 Financial Times 2021, Kristalina Georgieva: 'We are in a resilient place but cannot take stability for granted' accessible at https://www.ft.com/content/74cdb0f1-02ed-408f-ad19-6a6c7408d637

64 Deloitte 2021, Weekly global economic update accessible at https://www2.deloitte.com/us/en/insights/economy/global-economic-outlook/weekly-update.html

65 The World Bank 2021, Global Economic Prospects accessible at https://www.worldbank.org/en/publication/global-economic-prospects

66 Politico 2021, Two options for Europe's coronavirus economy: Bad or a lot worse accessible at https://www.politico.eu/article/europe-2021-coronavirus-economy-bad-or-worse/

67 The World Bank 2021, Global Economic Prospects accessible at https://www.worldbank.org/en/publication/global-economic-prospects

68 Bloomberg 2021, Double-Dip Recession Beckons in Europe as Lockdowns Drag On, accessible at https://www.bloomberg.com/news/articles/2021-01-12/euro-area-heads-for-double-dip-recession-as-lockdowns-drag-on

seeking a conduit to broaden their EU operations. Foreign investments in EU companies are largely positive and provide an influx of capital used to develop corporate structures and markets in the EU. However, they also entail the risk of EU economies being infiltrated with criminal funds generated outside the EU. This can allow criminals to establish a foothold in EU markets to the detriment of legally operating EU companies drawing on funds from legitimate sources. Extensive cooperation with compromised specialists in the legal and financial sectors underpins this activity, particularly in regard to investment firms and money service businesses. Here, too, employees are likely to experience the effects of a global economic crisis and may be more vulnerable to compromise by criminals.

A global economic crisis may bring ordinary EU citizens into closer proximity to organised crime. Communities may become more tolerant of certain types of crime such as the distribution of counterfeit goods or the cultivation of cannabis.

This may also make individuals more vulnerable to recruitment by criminal groups due to a lack of alternative legal prospects. Young people with advanced technical skills who are unable to gain employment in their chosen fields of expertise may turn to crime in order to finance themselves. This may result in a significant increase in the number of individuals engaging in cybercrime or offering cybercrime-related services.

CONCLUSION

The SOCTA 2021 is a comprehensive assessment of criminal threats facing the EU. As part of the development of the SOCTA, Europol carries out comprehensive data collection together with Member States and third partners. Europol also makes extensive use of the rich data sets already available at Europol in the form of its databases, case work and in-house expertise. Europol also seeks input from the private sector and academia in order to broaden the analysis.

All these elements result in sophisticated analysis and assessment of criminal threats in the EU. All the criminal phenomena discussed in the SOCTA 2021 are serious criminal threats. However, it is Europol's role to identify those that represent the most pressing and highest level of threat based on a transparent and consistent methodology. The methodology used to prepare the SOCTA and the prioritisation process has been developed based on customer requirements in close cooperation with Member States represented in the SOCTA Advisory Group and confirmed by the EU's Standing Committee on Operational Cooperation on Internal Security (COSI).

Europol has identified the following phenomena as key crime threats facing the EU:

- high-risk criminal networks (incl. corruption, money laundering, and the use of firearms)
- cyberattacks
- crimes against persons
- drugs
- fraud
- property crime
- environmental crime

The organised crime landscape is characterised by a networked environment where cooperation between criminals is fluid, systematic and driven by a profit-oriented focus. A key characteristic of criminal networks, once more confirmed by the pandemic, is their agility in adapting to and capitalising on changes in the environment in which they operate. Obstacles become criminal opportunities and may be as simple as adapting the narrative of a known modus operandi.

High-risk criminal networks can use corruption as an intrinsic part of their business model and to target public servants or sectors in strategic positions. Corruption erodes the rule of law, weakens institutions of states and hinders economic development. Corruption is a key threat to be addressed in the fight against criminal networks involved in any area of serious and organised crime. High-risk criminal networks in the EU fundamentally rely on the ability to launder vast amounts of criminal profits. For this purpose, professional money launderers have established a parallel underground financial system to process transactions and payments isolated from any oversight mechanisms governing the legal financial system. This parallel system ensures criminal proceeds cannot be traced as part of a sophisticated criminal economy, which allows high-risk criminal networks to flourish financially.

The threat from cyberattacks has been increasing over the last year not only in terms of the number of attacks reported but also in terms of the sophistication of attacks. Cyber-dependent crime is likely significantly underreported. The rapidly progressing digitalisation of society and the economy constantly creates new

opportunities for criminals involved in cyberattacks. The availability of cybercrime services online as part of a crime-as-a-service business model makes cybercrime more accessible by lowering the technological expertise required to carry out these crimes.

Migrant-smuggling networks increasingly put the physical and psychological integrity of irregular migrants in danger, aiming at maximising profits and reducing time and operational costs. Facilitation services for secondary movements are in high demand. Migrant-smuggling networks prove to be highly adaptable and able to quickly modify their business model and routes in response to evolving law enforcement activity, travel restrictions, logistical and environmental changes.

Highly organised smuggling networks also have connections or internal capabilities to exploit irregular migrants after they have arrived to their destination, through debt bondage. The online environment has become key to the recruitment and advertisement of trafficked victims for sexual exploitation and is serviced by brokers who maintain online platforms and capitalise on offering services both to criminal networks and to clients of sexual services.

The trafficking in human beings for labour exploitation remains underreported. Economic insecurity creates opportunities for traffickers to recruit/target victims in countries featuring high levels of unemployment, low average levels of education and poor awareness of labour rights.

Cocaine trafficking is a key activity for high-risk criminal networks active in the EU. EU-based criminal networks involved in cocaine trafficking have expanded their operations to have global reach. The number of violent incidents related to the trade in cocaine has been increasing. The nature of these attacks is also escalating in terms of impact and of victims, which now include journalists, lawyers, bystanders and others not involved in the cocaine trade. The cocaine market is a major source of income for criminals and enables the criminal infiltration of the licit economy.

Cannabis remains the most widely consumed illegal drug in the EU. The average potency of cannabis has increased over the last decade resulting in increasing potential harms to EU consumers. The cannabis market is a major source of profit for serious and organised crime in the EU. Criminal networks are heavily involved in the cultivation and trafficking of cannabis. The herbal cannabis cultivation close to the EU and within the EU has increased further. Relying on advanced agricultural cultivation equipment, criminal networks operating professional cultivation sites have been able to further increase their harvest yields. Cannabis resin continues to be trafficked in large quantities from Morocco to the EU.

The trade in synthetic drugs in the EU is unique compared to other substances as the production of these drugs in most cases takes place in the EU and they are subsequently distributed on a global level and European markets. The production of synthetic drugs in the EU is expanding and is expected to continue to do so in the near future. The criminal networks involved in the production of synthetic drugs have demonstrated their resilience and capacity to adapt to changes such as the banning of specific (pre-)precursor substances and essential chemicals by adjusting their production processes.

New fraud typologies are related involve online tools and digital techniques. Online fraud schemes feature diverse typologies. These may include, but are not limited to BEC fraud, which targets businesses and organisations and continues to increase in the number of attempts and their sophistication; SIM Swapping and smishing; online investment fraud, increasingly involving cryptocurrencies; phishing, which remains a significant threat and is further evolving in sophistication.

The overall number of incidents of organised property crime remains high, especially for domestic burglaries with more than one million cases a year, directly affecting hundreds of thousands of citizens. Criminals involved in organised property crime continue to travel long distances from region to region and country to country committing organised property crime. They easily shift between different types of burglaries and thefts.

Criminals primarily use companies to perpetrate environmental crimes. Criminals will increasingly seek to infiltrate and exploit the recycling and renewable energy industries. These two sectors are set to grow substantially and will attract both private sector investment as well as public funding.

Serious and organised crime remains a key security threat facing the EU and its Member States.

ANNEX I
THE SOCTA METHODOLOGY

The SOCTA methodology was developed by Europol in cooperation with the SOCTA Advisory Group composed of representatives of the Member States, EU agencies, third partner organisations, the European Commission and the Council General Secretariat. The SOCTA methodology is reviewed and amended by the SOCTA Advisory Group on a continuous basis. In 2019, new customer requirements were agreed for the preparation of the SOCTA 2021 and endorsed by the Standing Committee on Operational Cooperation on Internal Security (COSI)[69]. Based on these customer requirements, an updated, reviewed and improved methodology was agreed and implemented.

AIM AND SCOPE OF THE SOCTA

The aim of the SOCTA methodology is to help assess the key threats and understand the risks of serious and organised crime in the EU in a consistent way. The threat of serious and organised crime is determined by the activities of the organised crime groups and other criminal actors in different crime areas, its impact and geographical dimension and the use of crime infrastructure. The risk is determined by exploitable weaknesses or relevant developments in the environment (crime-relevant factors as drivers and facilitators of crime) and by their likelihood and consequences of change.

The conceptual model has four distinct steps of the SOCTA methodology: the focus, the tools (indicators), the analysis and prioritisation, and the result.

There are three integrated steps during the analysis. First, the identification of all current threats related to serious and organised crime, including the crime infrastructure used and geographical aspects. Secondly, the identification of exploitable weaknesses or relevant developments in the environment. Thirdly, the foresight based on the likelihood and consequences of change to identify key future threats. The key future threats are those threats in which the probability and impact are highest.

The SOCTA is focused on the following key areas which are also the starting point for the data collection:

- OCGs and other criminal actors;
- serious and organised crime areas;
- impact;
- crime infrastructure;
- the environment in which the criminal activities are embedded.

DATA SOURCES

Europol carries out internal and external data collection for SOCTA. Data for the purposes of SOCTA analysis is collected based on the three focus areas: OCGs and other criminal actors, serious and organised crime areas and the environment.

The reporting period covers the time from the last of the data collection for the SOCTA 2017 in January 2016

69 Council Document 9038/19, SOCTA Customer requirements (14/05/2019).

to December 2019. Contributors were asked asked to provide information on emerging trends and anticipated developments over the course of the next four years.

The qualitative and quantitative methods will be used to collect data already available at Europol for the purpose of analyses, information exchange or cross-checking. This will be carried out in compliance with the applicable data protection safeguards. For instance, data on suspects contributed to Europol, information from supported investigations and operations as well as changes in the flow of operational data to Europol were used to obtain an indication of threats. This information has been combined with desk research based on Europol's analysis reports (early warning notifications, intelligence notifications, threat assessments, situation reports) and other strategic reports developed by Europol, EU partner agencies, Member States or non-EU countries and partners. This provides a current but not complete threat picture across the EU and assists with the development of EU intelligence requirements.

Data collected internally was supplemented by external data collection. It is mandatory that all law enforcement and other relevant authorities of the EU Member States and relevant Justice and Home Affairs agencies contribute to the SOCTA. The qualitative and quantitative methods will be used to collect data from Member States and contributing partners using dedicated reporting templates. Information provided should originate from intelligence and ongoing or closed investigations and also reflect on emerging threats and national priorities.

There was one questionnaire per crime area (including break down crime areas). A reporting template has to be returned for every crime area, even if it is to report that the Member State has nothing to contribute to this crime area. Multidisciplinary input is crucial to achieve an integrated and integral approach and contributors are therefore encouraged to collect data from all available sources. However, Member States are requested to report nationally and therefore only one questionnaire per Member State is expected to be returned on each crime area.

Specific questionnaires were sent out to relevant non-EU countries, EU agencies and international organisations or cooperation platforms, who are requested to report on links to the EU or at the EU level.

Other relevant actors including those involved in the European multidisciplinary platform against criminal threats, EMPACT, within their respective mandated area and existing centres of expertise on serious and organised crime research (networks, academic institutions, global institutions and other centres of expertise) were invited to contribute.

Additional consultations, expert workshops or interviews were carried out with other EU agencies, academia or private sector representatives if needed to collect contextual or additional information.

Open source information was collected to complement the information from dedicated contributions and operational information analysed for the SOCTA. Official statistical data was used where available and applicable. Open source information was used to illustrate case examples or collect contextual information that may be missing from criminal intelligence. The use of open source materials has been verified and approved as part of the review process.

THREAT INDICATORS AND CRIME RELEVANT FACTORS

The SOCTA is a present and future-oriented threat assessment based on qualitative and quantitative analysis. In order to assess the threats of serious and organised crime, sets of indicators are used for serious and organised crime areas, OCGs, impact, crime infrastructure and environment. A balanced combination of these features and the likelihood of change is crucial to reach conclusions and produce recommendations regarding key serious and organised crime threats[70].

Indicators can be either descriptive indicators or threat indicators. Descriptive indicators (D) are merely used to analyse and describe the current threat. Threat indicators (T) are additionally used to assess the current threat and to compare them on the basis of the same threshold.

It is important to note that, regarding the SOC area and OCG indicators, a clear distinction has to be made between:

- the scale of the indicator (unknown, nil, low, medium, high);
- the value (weight) of each separate indicator, which is necessary in order to combine the scores on all indicators into one threat score.

For this purpose, a relative value (weight) is given to each of the OCG and SOC area threat indicators, determined by the SOCTA Advisory Group. The weights are also indicated as high (H), medium (M) or low (L).

70 A single indicator will never determine the overall threat.

INDICATORS FOR ORGANISED CRIME GROUPS

Nationality (D), Size of the group (D), Structure/type of the group and the cohesiveness (D), Sophistication of human resources (T), Geographical dimension and mobility (T), Continuity and resilience of the group (T), Financial resources (T), Other resources (D), Level of expertise (T), Crime areas (D), Modus operandi (D), Poly-crime activities (D), Links to other OCGs (T), Adaptability/flexibility (T), Turnover (T), Money laundering – level of sophistication (T), Use of legal business structures/infrastructure (T), Countermeasures (T), External violence (T), Internal violence (D), Corruption (T).

INDICATORS FOR SERIOUS AND ORGANISED CRIME AREAS

Modus operandi (D), Resource availability (T), Demand and supply (T), Evolution (T), Geographical distribution and displacement (T), Links to other crime areas (D), Number of OCGs/criminal groups active in the crime area (D), Nationality of the OCG members active in the crime area (D), Available expertise (T), Level of cooperation of the OCGs active in the crime area (T), Level of adaptability/flexibility of the OCGs active in the crime area (T), Money laundering – level of sophistication (T), Use of legal business structures (T), Level of countermeasures of the OCGs active in the crime area (T), External violence used by the OCGs active in the crime area (T), Level of corruption (T).

IMPACT INDICATORS

Financial/economic impact (T), Social impact (T), Health impact (T), Security impact (T), Political impact (T), Impact on the environment (T).

The impact indicators are assessed in terms of volume, frequency and seriousness of the known effects, resulting in a high, medium, low, or unknown effect.

CRIME INFRASTRUCTURE INDICATORS

Use of legal business structures (T), Money laundering (T), Identity/document fraud (T), Corruption (T), Countermeasures (T), Modus operandi (D), Transport and trade infrastructure (D), Technology and digital infrastructure (D).

This list can be completed with additional descriptive indicators, resulting from environmental scanning as validated by SOCTA Advisory Group.

ENVIRONMENT INDICATORS

Economic situation (D), Sociological situation (D), Geopolitical situation (D) (inside the EU; at the external borders of the EU; other countries outside the EU), Evolution of transport and trade infrastructure (D), Innovation and new technologies (D), Legislation (D), National strategies (D), Law enforcement activity (number of investigations, national priorities, participation in EMPACT OAP, budgetary changes, other challenges). (D)

Different aspects depending on crime area shall be taken into account additionally. This list can be completed with additional indicators, resulting from data collection and also from environmental scanning.

RESULTS

The analysis of the data on OCGs and serious and organised crime results in a list of recommended priorities on OCGs and serious and organised crime areas, in a format that enables informed decision-making on priorities.

The final SOCTA report will provide a detailed picture of current and future threats regarding crime areas, OCGs, and crime infrastructure, taking into account the impact and broader environment including the geographical aspects. Therefore, the SOCTA should be the key report for the development of recommendations[71] regarding serious and organised crime for the EU policy level. Additionally, the SOCTA should also inform regarding international serious and organised crime, including aspects such as poly-criminality.

71 As proposed during the SOCTA 2017 evaluation: more focus on OCGs, improved geographical dimension and foresight.

ANNEX II
LIST OF ABBREVIATIONS

ARO	Asset Recovery Office
ATM	Automated Teller Machine
BEC	Business Email Compromise
CaaS	Crime-as-a-Service
CEO	Chief Executive Officer
CITES	Convention on International Trade in Endangered Species
DDoS	Distributed Denial of Service
EC	European Commission
EEA	European Environmental Agency
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMCS	Excise Movement and Control System
ENISA	European Union Agency for Cybersecurity
EU	European Union
EU SOCTA	European Union Serious and Organised Crime Threat Assessment
EUCARIS	European Vehicle and Driving Licence Information System
EUIPO	European Union Intellectual Property Office
FADO	False and Authentic Documents Online
FATF	Financial Action Task Force
GPS	Global Positioning System
ICT	Information Communication Technology
IOCTA	Internet Organised Crime Threat Assessment
IOM	International Organisation for Migration
IoT	Internet of Things
IPTV	Internet Protocol Television
IT	Information Technology
JHA	Justice and Home Affairs
LE	Law Enforcement
LEA	Law Enforcement Authority
MDMA	Methylenedioxymethamphetamine
MOCG	Mobile Organised Crime Groups
MTIC	Missing Trader Intra-Community
NPS	New Psychoactive Substance
OCG	Organised Crime Group
OLAF	European Anti-Fraud Office

OMCG	Outlaw Motorcycle Gang
PGP	Pretty-Good -Privacy
SOC	Serious and Organised Crime
TARIC	Tarif Intégré Communautaire (Integrated Tariff of the European Communities)
THB	Trafficking in human beings
TOR	The Onion Router
UK	United Kingdom
UN	United Nations
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office on Drugs and Crime
US	United States
VAT	Value added tax
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WEEE	Waste of Electronic and Electric Equipment

ACKNOWLEDGMENTS

The EU Serious and Organised Crime Threat Assessment (SOCTA) is the product of systematic and comprehensive analysis of law enforcement information on criminal activities and networks affecting the EU. The SOCTA is designed to assist decision-makers in the prioritisation of serious and organised crime threats.

It has been produced by Europol, drawing on extensive contributions from the organisation's databases and external partners. Europol would like to express its gratitude to Member States, non-EU countries, EU agencies and institutions and international organisations for their valuable contributions and input.

SOCTA 2021

© European Union Agency for Law Enforcement Cooperation 2021

Reproduction is authorised provided the source is acknowledged. For any use or reproduction of individual photos, permission must be sought directly from the copyright holders.

Cite this publication: Europol (2021), European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg.

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

www.europol.europa.eu

Your feedback matters.

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

Your input will help us further improve our products.

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

EUROPOL

EU SOCTA 2021