SOCTA

2017

EUROPEAN UNION

SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

Crime in the age of technology

EUROPOL

SOCTA 2017

This publication and more information on Europol are available on the Internet:
Website: www.europol.europa.eu
Facebook: www.facebook.com/Europol
Twitter: @Europol
YouTube: www.youtube.com/EUROPOLtube

ACKNOWLEDGEMENTS

The EU Serious and Organised Crime Threat Assessment (SOCTA) is the product of systematic analysis of law enforcement information on criminal activities and groups 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 Analysis Work File on Serious and Organised Crime (AWF SOC) and external partners. Europol would like to express its gratitude to Member States, third countries and organisations, the European Border and Coast Guard Agency (Frontex), the European Union's Judicial Cooperation Unit (Eurojust), the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), INTERPOL, and the SOCTA Academic Advisory Group for their valuable contributions and input.

PHOTO CREDITS

Europol: pages 6 and 8
Shutterstock: pages 24, 28, 31, 32, 35, 40, 41, 42, 45, 47, 54, 55
Spanish National Police: page 18
Spanish Guardia Civil: page 48

SOCTA 2017

EUROPEAN UNION

SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

Crime in the age of technology

TABLE OF CONTENTS

FOREWORD
OF THE DIRECTOR

I am pleased to present the European Union (EU) Serious and Organised Crime Threat Assessment 2017 (SOCTA 2017). The SOCTA 2017 is Europol's flagship product providing information to Europe's law enforcement community and decision-makers. It serves as the cornerstone of the EU Policy Cycle for Serious and Organised Crime.

The Policy Cycle ensures effective cooperation between national law enforcement agencies, EU Institutions, EU Agencies and other relevant partners in the fight against serious and organised crime. This is the second edition of the SOCTA, following its inaugural edition released in 2013. The SOCTA 2017 delivers a set of recommendations based on an in-depth analysis of the major crime threats facing the EU. The Council of Justice and Home Affairs Ministers will use these recommendations to define priorities for the coming four years.

The SOCTA 2017 is the outcome of the work of many contributors from law enforcement authorities in the Member States, in countries with strategic and operational agreements with Europol, our institutional partners in the EU, and Europol.

Europol is a key partner to the Member States in meeting security challenges by providing a highly developed platform for the exchange of criminal intelligence as well as analytical and operational support for some of the most complex international investigations in the EU to date. In drafting the SOCTA 2017, Europol harnessed this unique information position.

The SOCTA 2017 represents the outcome of the largest data collection on serious and organised crime ever undertaken in the EU. Europol has been able to use its singular intelligence capability as the information hub for criminal intelligence in the EU to analyse and identify the key crime threats facing the EU today.

Informed by its analysis of the prevailing threat, the SOCTA 2017 identifies a number of key priorities, which, in Europol's view, require the greatest concerted action by Member States and other actors to ensure the most effective impact. These include cybercrime, the production, trafficking and distribution of illicit drugs, migrant smuggling, organised property crime, and trafficking in human beings (THB). In addition, Europol recommends focussing on three cross-cutting crime threats with a significant impact across the spectrum of serious and organised crime – document fraud, money laundering and the online trade in illicit goods and services. The SOCTA 2017 also explores potential links between serious and organised crime and terrorism.

In 2013, Europol reported the presence of at least 3,600 internationally operating Organised Crime Groups (OCGs) in the EU. In the SOCTA 2017, we identify approximately 5,000 international OCGs currently under investigation in the EU. This increase is primarily a reflection of a much improved intelligence picture. It is also an indication of shifts in criminal markets and the emergence of smaller groups and individual criminal entrepreneurs in specific criminal activities, especially those taking place online.

These developments highlight the complex dynamics that shape the serious and organised crime landscape in the EU. They also emphasise the need for the continued and enhanced exchange of information between law enforcement authorities as part of their day-to-day business. Connecting law enforcement authorities and facilitating the real-time 24/7 exchange of information remains Europol's core business.

The SOCTA 2017 is a forward-looking document that both describes and anticipates emerging threats from serious and organised crime. In this edition of the SOCTA, we highlight the role of technology in particular. Criminals have always been adept at exploiting technology. However, the rate of technological innovation and the ability of organised criminals to adapt these technologies have been increasing steadily over recent years. Developments such as the emergence of the online trade in illicit goods and services are set to result in significant shifts in criminal markets and confront law enforcement authorities with new challenges.

In identifying and specifying these challenges, Europol hopes to provide a tangible contribution to the efforts of Member States and the EU in fighting serious and organised crime. I look forward to Europol's continued support for and cooperation with law enforcement agencies and other partners in the EU and beyond.

Rob Wainwright

Director of Europol

INTRODUCTION

The European Union and Europol

The European Union (EU) is a unique economic and political partnership between 28 European countries.[i] It was created in 1958 as the European Economic Community with the aim to foster economic cooperation among its six founding partners. Since then, the number of EU Member States enlarged and the economic union developed into an organisation covering a wide range of policy areas. The official name changed to the European Union in 1993 to reflect the broader cooperation on which members' partnership is based. EU law is built on a series of treaties, voluntarily and democratically agreed by all Members. These agreements set out the EU's goals in its main areas of activity. There are three main institutions involved in EU legislation: the European Parliament, which represents the EU's citizens and its members are directly elected by them; the Council of the European Union, which represents the governments of the Member States who share the presidency on a rotating basis. The third institution is the European Commission, which represents the interests of the Union as a whole.

Europol is the EU's law enforcement agency and assists the Member States in their fight against serious international crime and terrorism. Established as an EU agency in 2009[1] , Europol, or the European Police Office, 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 as well as a centre for law enforcement expertise. Analysis is at the core of Europol's activities. To give its partners deeper insights into the crimes they are tackling, Europol produces regular assessments that offer comprehensive, forward-looking analyses of crime and terrorism in the EU.

The SOCTA 2017

The SOCTA 2017 is the most comprehensive study of serious and organised crime in the EU ever undertaken. It 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 2017 sets out current and anticipated developments across the spectrum of serious and organised crime, identifies the key criminal groups and individuals active 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 2017 also describes the dynamics that drive organised crime in the age of technology and reflects on how OCGs and individual criminal entrepreneurs seek to exploit the latest technological innovations.

The SOCTA is the 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 strategic or operational agreements with Europol. The involvement of these crucial stakeholders is also reflected in the SOCTA's role as the cornerstone of the EU Policy Cycle for Serious and Organised Crime in the EU.

[i] The Member States of the EU are: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

The EU Policy Cycle for Serious and Organised Crime in the EU

The Policy Cycle 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. The Policy Cycle translates strategic objectives at the European level into concrete operational actions against serious and organised crime.

The Policy Cycle is a methodology adopted by the European Union in 2010 to address the most significant criminal threats facing the EU. Each cycle lasts four years and 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. Emerging threats are also monitored so that they can be effectively addressed. Relying on the analytical findings of the SOCTA 2017, the Council of Justice and Home Affairs Ministers of the EU will decide on the priorities in the fight against serious and organised crime for the second full Policy Cycle from 2018 to 2021. These priorities will determine the operational work carried out in the framework of the Policy Cycle for the next four years. The crime priorities agreed at European level in the context of the Policy Cycle are reflected in operational activities at Member State level.

The SOCTA Methodology

As part of an iterative process, the SOCTA Methodology 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 OCGs 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. Using a mixed methods approach of qualitative and quantitative analysis techniques and a set of clearly defined indicators, Europol is able 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 the Policy Cycle based on this Methodology. The SOCTA Methodology ensures transparency and reliability providing decision-makers with a solid basis for their deliberations. The SOCTA Methodology is a public document and can be accessed online.[2]

Data and sources

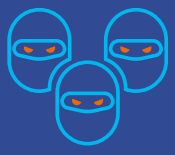
The findings of the SOCTA 2017 are the outcome of detailed analysis of intelligence gathered as part of the largest data collection on serious and organised crime ever undertaken in the EU. Member States, cooperation partners outside the EU and institutional partners contributed more than 2,300 questionnaires on crime areas and OCGs. The amount of data provided for the SOCTA 2017 has more than doubled compared to the SOCTA 2013.

In addition, Europol relied heavily on the operational intelligence held in its Analysis Work File on Serious and Organised Crime (AWF SOC) to provide a thorough and extensive analysis of the criminal threats facing the EU. Where appropriate, the data collected through questionnaires and available in Europol's databases were complemented by information from open sources.

The SOCTA 2017 is the most comprehensive study of serious and organised crime in the EU ever undertaken.

KEY JUDGMENTS

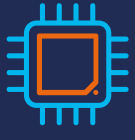
ORGANISED CRIME GROUPS



Serious and organised crime in the EU features a great variety of criminal activities, which are increasing in complexity and scale. The profits generated by some of the successful OCGs and individual criminals active in the EU are enormous and rival those of multi-national corporations.

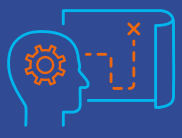
More than 5,000 OCGs operating on an international level are currently under investigation in the EU. The number of OCGs operating internationally highlights the substantial scope and potential impact of serious and organised crime on the EU.

TECHNOLOGY AND ENGINES OF ORGANISED CRIME



Criminals quickly adopt and integrate new technologies into their *modi operandi* or build brand-new business models around them. The use of new technologies by OCGs has an impact on criminal activities across the spectrum of serious and organised crime. This includes developments online, such as the expansion of online trade and widespread availability of encrypted communication channels, as well as other aspects of technological innovation such as more accessible and cheaper high-performance drone technology. Technology has a fundamental and lasting impact on the nature of crime.

Document fraud, money laundering and the online trade in illicit goods and services are the engines of organised crime in the EU. Although neither document fraud nor money laundering have a direct impact on most citizens in the EU, they facilitate most, if not all, other serious and organised crime. The online trade in illicit goods and services is expanding rapidly. Almost all types of illicit goods are now bought and sold via online platforms that offer the same ease of use and shopping experience as most legal online platforms. Depending on the type of commodity and service, this includes platforms both on the surface web and the Darknet. Data is also traded as a commodity. The online trade in illicit goods and services is foreseen to increasingly disrupt established criminal markets and their traditional distribution models over the next few years.



Many of the OCGs are highly flexible and display great adaptability in the speed with which they adjust their *modi operandi* or whole business models to changes in the environment. Many criminal activities are increasingly complex and require a variety of skills as well as technical expertise to carry them out.

The most threatening OCGs are those which are able to invest their significant profits in the legitimate economy as well as into their own criminal enterprises, ensuring business continuity and a further expansion of their criminal activities. The involvement in serious and organised crime may allow some terrorist groups to generate funds to finance terrorism-related activities.

An increasing number of individual criminal entrepreneurs offer Crime-as-a-Service (CaaS). The online trade in illicit goods and services enables individual criminals to operate their own criminal business without the need for the infrastructures maintained by 'traditional' OCGs.

CRIMINAL ACTIVITIES

Cybercrime is a key challenge to digital economies and societies. Cyber-dependent crime is underpinned by a mature CaaS model, providing easy access to the tools and services required to carry out cyber-attacks. Child Sexual Exploitation (CSE) perpetrated online is increasingly profit driven. The growth of card-not-present (CNP) fraud, coupled with successful industry measures to tackle card-present (CP) fraud, has resulted in CNP fraud accounting for 66% of total card fraud value.

Organised property crime encompasses a range of different criminal activities carried out predominantly by highly mobile OCGs operating across the EU. A steady increase in the number of reported burglaries over recent years is a particular concern in many Member States.

The illicit drugs market remains the largest criminal market in the EU. More OCGs are active in the production, trafficking and distribution of illicit drugs than any other phenomenon. The industrial-scale production of synthetic drugs within the EU continues to expand and cements the EU as a key source region for these substances distributed worldwide. OCGs maintain complex trafficking operations cooperating with OCGs on a global scale to orchestrate the wholesale importation of illicit drugs into the EU. Within the EU, the majority of OCGs involved in the distribution of illicit drugs deal in multiple illicit drugs, also called poly-drug trafficking.

Migrant smuggling has emerged as one of the most profitable and widespread criminal activities for organised crime in the EU. The migrant smuggling business is now a large, profitable and sophisticated criminal market, comparable to the European drug markets.

THB for labour exploitation is increasing and is expected to continue to expand. OCGs are expected to exploit the presence of a large number of potentially vulnerable persons in the EU following the migration crisis. Labour exploitation threatens to undermine the legitimate labour market lowering wages and impeding economic growth.

UNDERSTANDING
ORGANISED CRIME

DEFINING **SERIOUS AND ORGANISED CRIME**

OCGs are as varied as the markets they service and the activities they engage in. In many cases, OCGs reflect the societies, cultures and value systems they originate from. As societies across Europe become more interconnected and international in outlook, organised crime is now also more connected and internationally active than ever before.

Since the year 2000, the United Nations Convention against Transnational Organized Crime has provided an internationally shared definition of an organised criminal group as *"a group of three or more persons existing over a period of time acting in concert with the aim of committing crimes for financial or material benefit."* This definition was also adopted in the EU's Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime and continues to reflect law enforcement authorities' conceptualisation of organised crime across the world. However, this definition does not adequately describe the complex and flexible nature of modern organised crime networks.

OCGs operate in a criminal economy dictated by the laws of supply and demand and are favoured by social tolerance for certain types of crime such as the trade in counterfeit goods and specific frauds against public authorities or large companies. These factors will continue to shape the organised crime landscape. Individual criminals and criminal groups are flexible and quickly adapt to exploit new victims, to evade countermeasures or identify new criminal opportunities.

Who

ORGANISED CRIME GROUPS

CRIMINAL NETWORKS

CRIMINAL EXPERTS

How

CORRUPTION

COUNTERMEASURES AGAINST LAW ENFORCEMENT

CRIMINAL FINANCES (MONEY LAUNDERING)

DOCUMENT FRAUD

ONLINE TRADE

TECHNOLOGY

VIOLENCE AND EXTORTION

What

CURRENCY COUNTERFEITING

CYBERCRIME
Child sexual exploitation
Cyber-dependent crimes
Payment card fraud

DRUG PRODUCTION TRAFFICKING AND DISTRIBUTION

FRAUD
Excise fraud
Investment fraud
Mass marketing fraud
Payment order fraud
Value Added Tax fraud

ILLICIT WASTE TRAFFICKING

INTELLECTUAL PROPERTY CRIME

MIGRANT SMUGGLING

ORGANISED PROPERTY CRIME

SPORTS CORRUPTION

TRAFFICKING OF ENDANGERED SPECIES

TRAFFICKING OF FIREARMS

TRAFFICKING IN HUMAN BEINGS

ORGANISED CRIME GROUPS (OCGs) AND OTHER CRIMINAL ACTORS

5,000
international OCGs currently under investigation

>180
nationalities involved

The OCGs and individual criminals operating in the EU are highly diverse. They range from large 'traditional' OCGs to smaller groups and loose networks supported by individual criminals, who are hired and collaborate *ad hoc*. More than 5,000 OCGs operating on an international level are currently under investigation in the EU. This figure does not necessarily reflect an overall increase in organised crime activity in the EU compared to 2013, when Europol reported on the activities of 3,600 internationally operating OCGs in the EU. This increase is primarily a reflection of a much improved intelligence picture. The increase also points to the emergence of smaller criminal networks, especially in criminal markets that are highly dependent on the internet as part of their *modi operandi* or business model. Overall, the number of OCGs operating internationally highlights the substantial scope and potential impact of serious and organised crime on the EU.

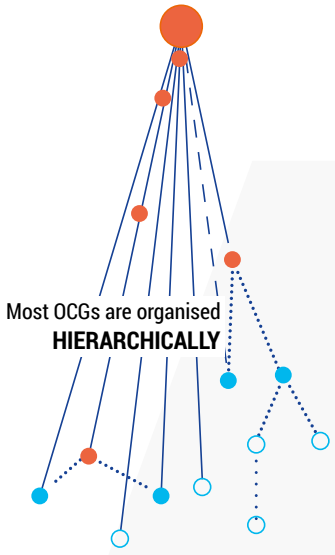
The criminal markets involving illicit drugs, trafficking of human beings and migrant smuggling attract the largest numbers of OCGs and continue to generate the greatest profits among the various criminal markets in the EU. However, emerging crime phenomena such as the online trade in illicit goods and services may eclipse these markets in size and profits in the future. The online trade in illicit goods and services is no longer merely a *modus operandi*, but an expanding, highly dynamic and substantial criminal market itself.

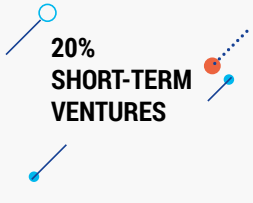
Over the past few years, criminals of more than 180 nationalities were involved in serious and organised crime in the EU. The majority of OCGs operating on an international level are composed of members of more than one nationality. Nonetheless, the majority of the suspects (60%) involved in serious and organised crime in the EU are nationals of a Member State.

Structure

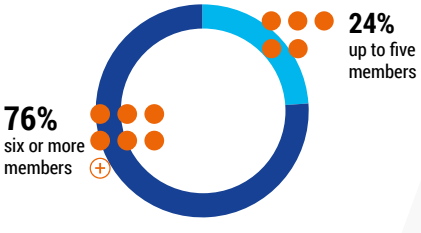
The diversity of the criminal actors operating in the EU is also reflected in the structures of the OCGs. 30% to 40% of the OCGs operating on an international level feature loose network structures. An approximate 20% of these networks only exist for a short period of time and are set up to support specific criminal ventures. Hierarchically structured OCGs continue to dominate traditional criminal markets.

The fragmentation of the serious and organised crime landscape and the emergence of more groups and looser networks detailed in the SOCTA 2013 did not affect all criminal markets. The fragmentation of criminal markets was particularly pronounced in relation to highly cyber-dependent criminal activities. Around these types of activities, an increasing number of individual criminal entrepreneurs come together on an *ad hoc* basis for specific criminal ventures or to deliver CaaS.





Composition

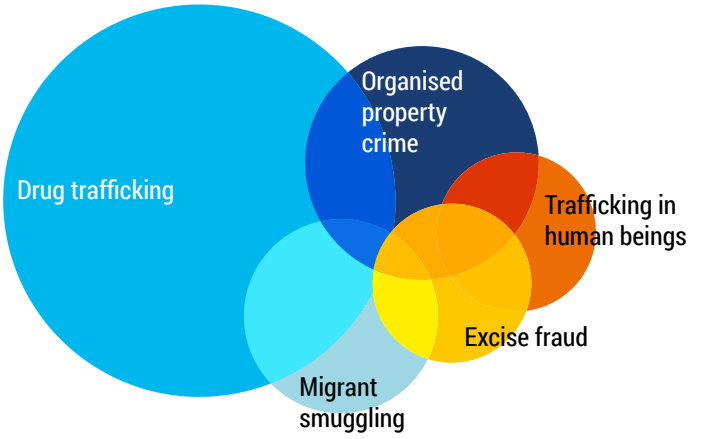


60% of the suspects involved in serious and organised crime in the EU are EU nationals.

Activities

More than one third of the OCGs active in the EU are involved in the production, trafficking or distribution of drugs. Other key criminal activities for OCGs in the EU include organised property crime, migrant smuggling, THB and excise fraud.

Involvement of OCGs active in the EU in different crime areas



INTERNATIONAL DIMENSION AND MOBILITY

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

TRENDS

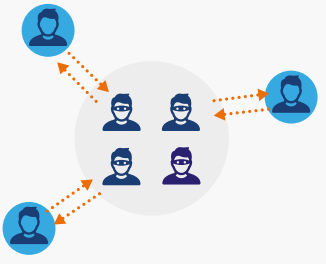
Poly-criminality

45%
of the OCGs reported for the SOCTA 2017 are involved in more than one criminal activity

Many OCGs have expanded their crime portfolio in response to the sustained high level of demand for smuggling services during the migration crisis.

Sharing Economy

An increasing number of individual criminal entrepreneurs come together on an ad hoc basis for specific criminal ventures or to deliver CaaS



Poly-criminality

45% of the OCGs reported for the SOCTA 2017 are involved in more than one criminal activity. The share of these poly-criminal groups has increased sharply compared to 2013.

OCGs also often engage in more than one criminal activity to mitigate risks, reduce operational costs and increase profit margins. The OCGs involved in the trafficking of illicit goods are the most poly-criminal groups in the EU. These groups typically traffic more than one illicit commodity such as counterfeit goods or different types of illicit drugs.

Many OCGs are highly flexible and able to shift from one criminal activity to another or to add new criminal activities to their crime portfolio. In many cases, OCGs operate on an on-demand basis and only become active once new profit opportunities emerge.

The integration of digital systems in many criminal activities and the expansion of the online trade in illicit goods and services is transforming serious and organised crime. Criminals are increasingly adapting the supply chain models of global online retailers.

The concept of CaaS has been an emerging feature of various criminal markets for some years. However, increasingly OCGs also openly advertise *ad hoc* opportunities for individual criminals to provide them with support or expertise for specific criminal ventures.

OCGs operating on an international level are typically active in more than three countries (70%). A limited number of groups is active in more than seven countries (10%).

Since 2012, Europol has been supporting the German-led ISEC project on "Strengthening cross-border operational cooperation in the fight against mobile organised crime groups (MOCGs) from the Baltic Sea Region, including Russian-speaking MOCGs". The project has resulted in the dismantling of more than 100 OCGs. A total number of 575 arrest warrants were issued. The damage caused by the MOCGs targeted by this project exceeded EUR 65 million. These MOCGs mainly carried out organised property crime, drug trafficking, document counterfeiting and money laundering.

Corruption

OCGs use corruption to infiltrate public and private sector organisations relying on bribery, conflicts of interest, trading in influence and collusion in order to facilitate their criminal activities. Corruption distorts legitimate competition and erodes public trust in authorities and legal systems.

Corruption is used to enable all types of criminal activity. However, the prevalence and scale of corruption associated with different crimes vary. Some criminal activities use corruption as an integral part of their *modus operandi*.

Corruption is increasingly facilitated by online services. Some criminals use cryptocurrencies and alternative banking platforms to transfer funds to their accomplices in the public and private sector. The use of these techniques makes it more difficult to detect financial flows and to uncover corruption.

OBJECTIVES OF CORRUPTION

Violence and extortion

OCGs tend to avoid the use of violence. Violence usually attracts law enforcement attention, which is often incompatible with the profit-driven motivations of those involved in organised crime.

OCGs mostly employ violence against members of their own or competing OCGs. Violent crimes targeting rival OCGs often take place in the context of "turf wars" over territory or influence. OCGs extort property or money from individuals by intimidating their victims, threatening to carry out serious harm and murder. Very few OCGs engage in extortion as their core activity. Some OCGs offer to carry out racketeering and extortion as a service for other criminal networks and lend "professional extorters" to affiliated OCGs.

Hostage takers kidnap, hold and release individuals in exchange for ransom payments. In the EU, this criminal activity is not widely carried out by OCGs. However, OCGs involved in migrant smuggling have been known to use the threat of kidnapping in order to extort debt payments.

Countermeasures against law enforcement

Countermeasures are the actions and behaviours of individual criminals and criminal groups to disrupt or prevent law enforcement activities against them. OCGs use various countermeasures to recognise and mitigate law enforcement actions.

The application of countermeasures requires an awareness of the methods and techniques used by law enforcement authorities in investigating criminal networks.

OCGs use a number of countermeasures to secure their communication against law enforcement surveillance. These include technical countermeasures such as the use of encryption, foreign and pre-paid SIM cards or satellite telephones as well as reliance on code. To evade physical surveillance during transport, OCGs frequently change vehicles, often hired or leased using fraudulent IDs.

ENGINES OF ORGANISED CRIME

Document fraud, money laundering and the online trade in illicit goods and services are the engines of organised crime. These cross-cutting criminal threats enable and facilitate most, if not all, other types of serious and organised crime. The business models of OCGs active across the spectrum of serious and organised crime rely on document fraud, money laundering and online trade to maintain their criminal enterprises.

CRIMINAL FINANCES AND MONEY LAUNDERING

Money laundering sustains and contributes to the growth of criminal markets across the EU.

Money laundering is linked to virtually all criminal activities generating criminal proceeds.

Money laundering allows OCGs to introduce the proceeds of crime into the legitimate economy. Almost all criminal groups need to launder profits generated from criminal activities. However, the way in which money laundering is carried out varies greatly depending on an OCG's level of expertise as well as the frequency and scale of money laundering activities. Criminal networks continuously seek to exploit the latest technological developments such as cryptocurrencies and anonymous payment methods. Rapid transaction processing and the proliferation of effective anonymisation tools are significant obstacles in the identification of the beneficial owners of criminal proceeds. A growing number of online platforms and applications offer new ways of transferring money and are not always regulated to the same degree as traditional financial service providers. Money launderers heavily rely on document fraud to facilitate their activities. Fraudulent documents such as false invoices and forged ID documents are used to conceal the origin of criminal cash, to open bank accounts or to establish shell companies. Money launderers provide services to both organised crime and terrorist organisations.

Money laundering syndicates

OCGs increasingly use money laundering syndicates acting as illegal service providers to launder money. In exchange for a commission of between 5% and 8%, these syndicates offer complex laundering techniques and carry out the laundering operations on behalf of other OCGs.

OPERATION SNAKE[3]

In 2015, Europol supported Spanish authorities in dismantling a Chinese network involved in the laundering of criminal proceeds from THB for labour exploitation, the production of counterfeit goods as well as excise tax fraud. Relying on middlemen and third parties, the OCGs had established complex corporate structures and various accounts to transfer money to China. In addition to their main criminal activities, the group also offered money laundering and international remittance services to other OCGs based in the EU in exchange for a negotiated percentage of the laundered funds. Between 2009 and 2015, the European branch of this OCG had laundered more than EUR 340 million.

Cash

Cash remains at the core of the money laundering business. Cash continues to be smuggled by couriers and, increasingly, by post and parcel services.

OPERATION KOURI[4]

In 2016, a Joint Investigation Team (JIT) composed of French, Belgian and Dutch investigators, Eurojust and Europol dismantled a complex network involved in the laundering of drug trafficking proceeds based in Morocco. Cash couriers travelling by car collected up to EUR 1 million per month in cash across Western Europe and transported it to Belgium and the Netherlands to be transferred to Morocco via the Middle East using the Hawala system. The operation resulted in the seizure of more than EUR 7.1 million in cash.

OPERATION SNAKE

Trade-based money laundering

Trade-based money laundering is a highly effective way of concealing criminal funds by manipulating or forging purchases or sales using double invoicing, false invoicing, over- and under-invoicing by companies that are owned by OCGs, their associates and relatives.

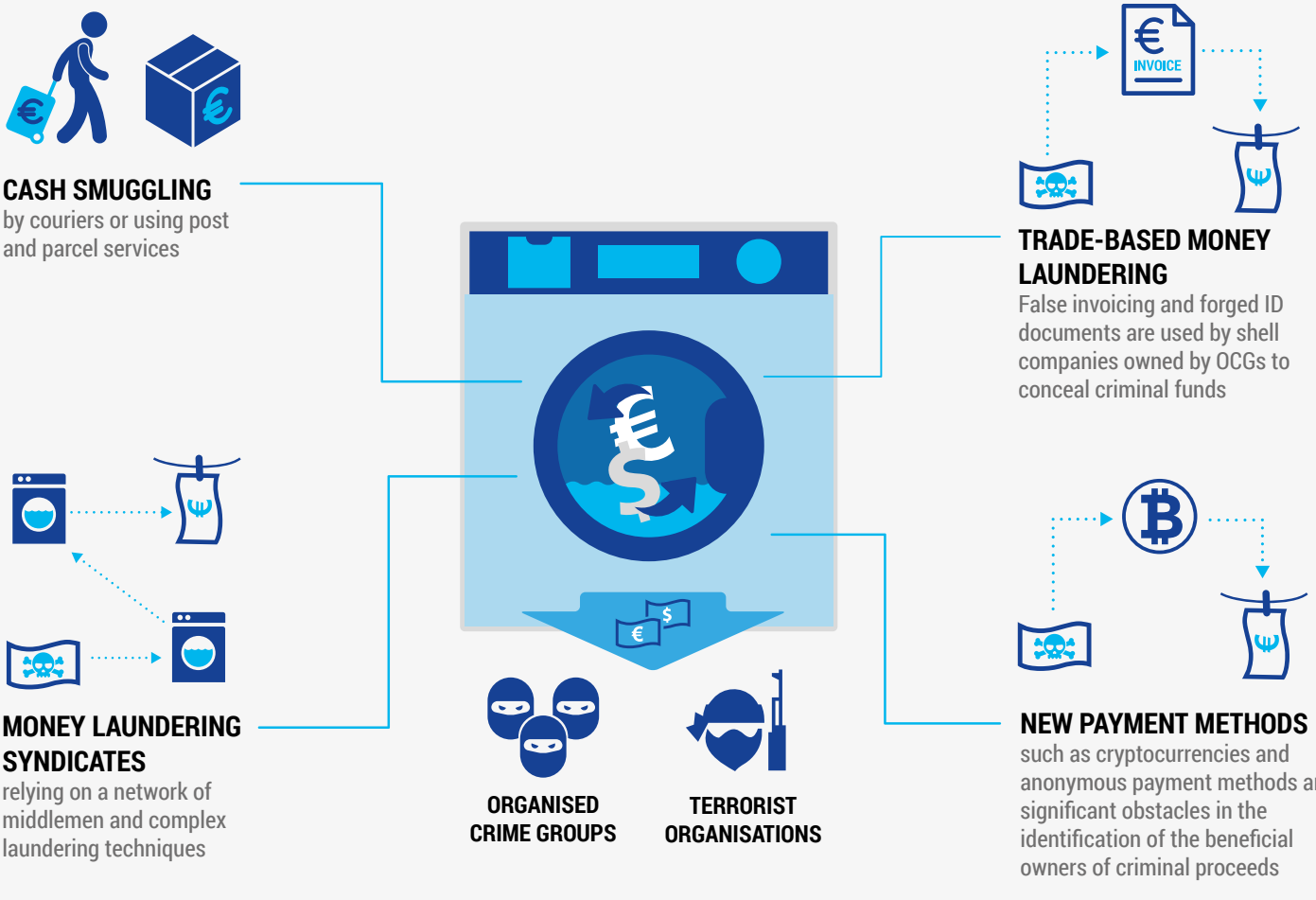
OPERATION KANDIL[5]

A 2016 investigation by French, Spanish, German and Dutch law enforcement authorities disrupted an OCG laundering the proceeds generated by the trade of heroin. This OCG collected proceeds throughout the EU and laundered the funds in Middle Eastern countries relying on cash couriers and trade-based money laundering techniques. The OCG purchased expensive second-hand cars, heavy machinery and construction equipment in Germany in cash and exported them to Iraq where they were again sold for cash. The group then used Money Service Businesses and Hawala to introduce the funds into the legitimate financial system, leaving virtually no paper trail.

New payment methods

New payment methods such as cryptocurrencies, prepaid cards, online payments and internet vouchers are continuously emerging and are generally less well-regulated than traditional payment methods. In combination with alternative banking platforms, these new payment methods allow the movement of large amounts of criminal funds. Underground banking systems are financial networks operating outside of normal banking channels to transfer money internationally, avoiding the fees and regulations of conventional banks.

MONEY LAUNDERING
Most common methods



DOCUMENT FRAUD

The use of fraudulent documents in the EU has significantly increased. It represents a significant threat to the EU.

Document fraud is a key enabler of all types of criminal activity as well as terrorism. Document fraud is also expected to emerge as one of the fastest growing criminal markets over the coming years.

High-quality counterfeit documents are primarily produced by highly specialised counterfeiters.

Fraudulent documents are increasingly traded online and trafficked using post and parcel services.

Document fraud is a key facilitator for organised crime. Document fraud entails the production and use of counterfeit documents as well as the use of genuine documents obtained by means of deception or misrepresentation. The production and use of fraudulent documents has also been linked to terrorist actors. Document fraudsters and forgers manipulate or produce all types of identity, travel and administrative documents.

Fraudulent documents are used and traded extensively among OCGs and represent a significant obstacle in the fight against serious and organised crime. Fraudulent IDs are in high demand and are the most commonly traded type of fraudulent document. Increasingly, fraudulent documents are traded online. Online marketplaces are used by criminals to display the range of genuine documents on offer and allow document forgers to receive orders directly from clients.

BERLIN CHRISTMAS MARKET ATTACK

On 19 December 2016, a Tunisian suspect drove a truck into a Christmas market in the centre of Berlin, Germany. The terrorist attack left 12 people dead and 56 others injured. The perpetrator was a rejected asylum seeker from Tunisia and had previously been suspected of involvement with the Islamic State. After his asylum claim was rejected, the suspect travelled throughout Europe using multiple identity documents under different aliases.

Understanding the different types of document fraud

GENUINE DOCUMENT

OCGs 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

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

The production of forged documents

Increasingly sophisticated security features protecting documents against forgery as well as improved technical control measures have compelled OCGs to improve the quality of fraudulent documents. Suppliers of raw materials now primarily rely on Darknet marketplaces to sell their products.

The sale and rental of genuine documents

The sale or rental of travel and identity documents such as passports is an increasing concern. There has been a significant increase in the number of lost and stolen documents in circulation. Instability and armed conflicts often allow criminal groups to obtain blank documents from the affected regions. This is also true for conflict zones on the periphery of the EU and has been highlighted by the widespread availability of thousands of non-EU blank identity documents.

A multi-purpose tool

Fraudulent documents are multi-purpose criminal tools and each document can be used repeatedly to support different criminal activities. Documents forgers are service providers often cooperating with multiple OCGs involved in various criminal activities.

THE MAIN CRIME AREAS LINKED TO OR SUPPORTED BY DOCUMENT FRAUD

DOCUMENT FORGERY AND MIGRANT SMUGGLING[6]

In May 2016, Greek and Czech law enforcement authorities arrested several suspects involved in the forgery of documents and migrant smuggling as part of an international investigation supported by Europol. The forged documents were subsequently provided to irregular migrants to enter the EU or to legalise their stays there. The investigation in Greece highlighted the structure and the hierarchy of the Athens-based network. The fees for the forged documents ranged from EUR 100 to EUR 3,000 per piece depending on the quality, type and country of issue. The documents forged by the criminal group included passports, national ID cards, visas, driving licences, asylum seekers' registration cards and residence permits.

Breeder documents

Breeder documents are documents that are used to obtain other forms of legitimate identification for the purpose of establishing a false identity. Fraudulent breeder documents are typically used to apply for genuine travel and identity documents and driving licences. Birth certificates, marriage records, work contracts or invitations to stay in the EU are forged in order to obtain visas, residency or work permits on false grounds.

FORGED
BIRTH CERTIFICATE
MARRIAGE RECORD
WORK CONTRACT
INVITATION TO STAY IN THE EU

VALID
VISA
RESIDENCY PERMIT
WORK PERMIT

ONLINE TRADE IN ILLICIT GOODS AND SERVICES

The online trade in illicit goods and services has been expanding steadily over recent years. It is expected that this trade will continue to grow rapidly for the foreseeable future and that online platforms will emerge as a key distribution platform for all types of illicit goods in the EU.

The Darknet is a key facilitator for various criminal activities including the trade in illicit drugs, illegal firearms and malware. Darknet marketplaces are becoming increasingly de-centralised.

Online platforms operating in the legal economy have had a profound impact on business models, shopping experiences and customer expectations. The multiplication of sales platforms makes online trade easier, more accessible and cheaper. This development has been mirrored in the online trade in illicit goods as criminals, like legitimate traders, look to opportunities online to grow their businesses.

Virtually all illicit commodities are now traded online either on dedicated criminal online marketplaces or by exploiting otherwise legal online platforms. The number of goods on offer and frequency with which new products become available indicates that the online trade in illicit goods is thriving and highly dynamic. Commodities such as cannabis, cocaine, counterfeit currency, counterfeit medicine, cultural goods, excise tobacco, firearms, heroin, hormonal substances, specimens of endangered species, stolen vehicle parts and accessories, synthetic drugs and new psychoactive substances (NPS), as well as compromised payment card data are sold and purchased online.

It is not only illicit commodities that are traded online, but also criminal services. The expanding CaaS business model provides customers with access to a wide range of criminal services. A prime example of this is cybercrime, where customers can access such services as malware coding, Distributed Denial of Service (DDoS) services, bulletproof hosting and anonymisation services, botnet hire and money laundering.

Vendors often attempt to hide illegal goods among legal products on online platforms on the surface web. In some cases, surface web vendors redirect their customers to mirror sites on the Darknet or advertise their products using false product designations or descriptions.

The online market caters to dealers who buy in bulk for re-sale as well as individual users. The diminishing reliance on access to street networks of consumers of illicit commodities challenges the established business models in many criminal markets.

As of January 2017, the TOR network had over 1.7 million directly connecting users, and hosted over 60,000 unique onion domains.[7] In one study, almost 57% of active sites could be classified as related to some form of illicit activity.[8]

Trade on the surface web

The distribution of illicit commodities via online platforms has soared in recent years and is expected to continue to increase steadily over the coming years. Online trade offers the opportunity to reach a huge number of potential customers. Illicit goods purchased online are predominantly trafficked using postal and parcel services.

THE SALE OF DRUGS VIA PHOTO-SHARING PLATFORMS

Photo-sharing applications and platforms are popular with a huge number of users. These services allow users to create communities around shared interests using hashtags. Drugs dealers and users make use of these platforms to form communities to discuss, exchange information and trade various types of illegal drugs. Potential customers scroll through pictures of advertised products and then contact the dealer privately using direct messaging functionalities. The eventual transaction takes place either face to face or via online payment and delivery by mail.

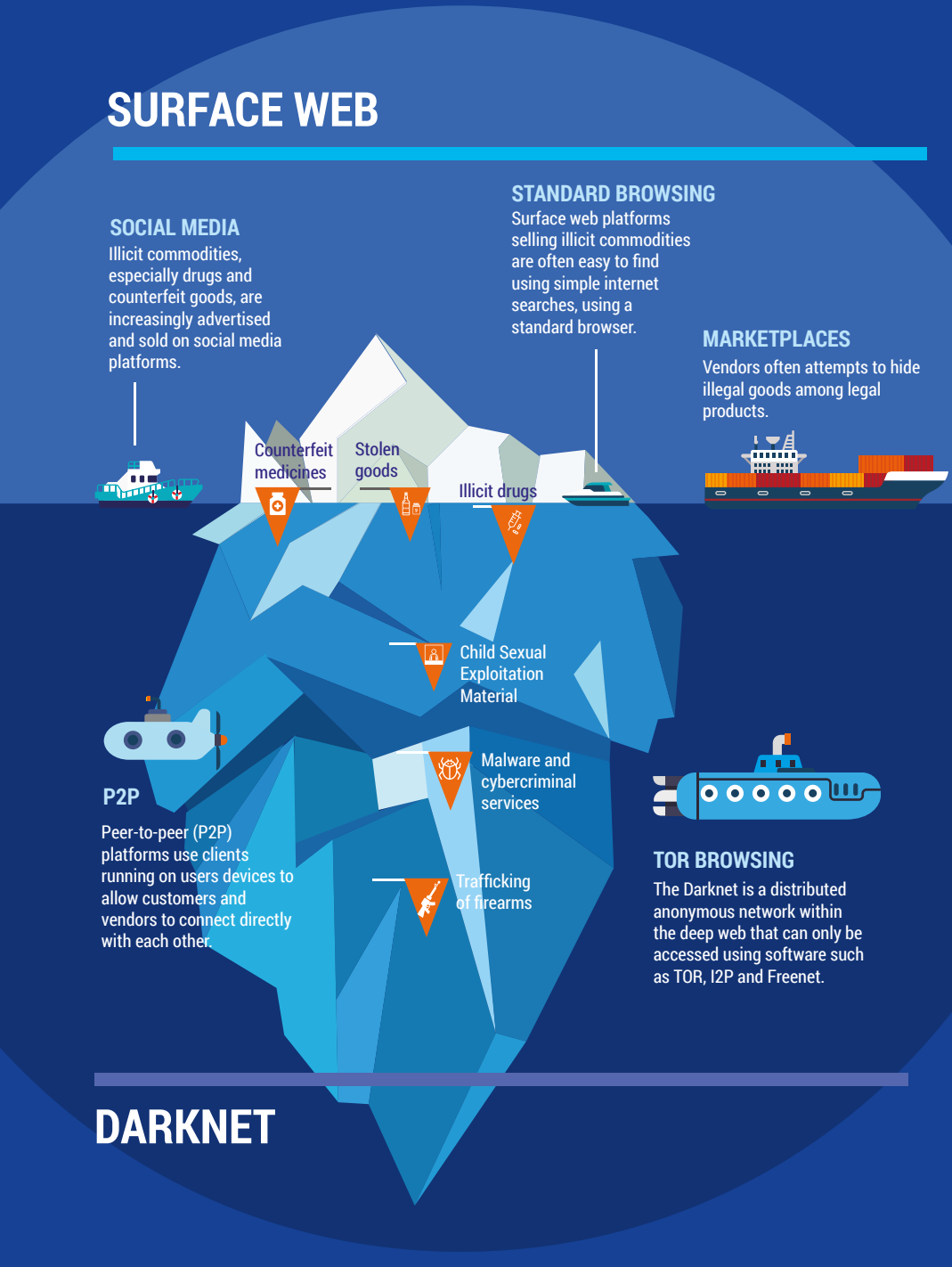
The Darknet

The Darknet is a distributed anonymous network within the deep web that can only be accessed using software such as The Onion Router (TOR), I2P and Freenet. While these tools were ostensibly developed for the purpose of legitimately protecting freedom and privacy, confidential business activities and relationships, they can equally be used by criminals for the same purpose - to conceal their identity and/or the hosting location of websites, forums and markets, collectively referred to as "hidden services".[9]

DARKNET ARMS VENDORS ARRESTED IN SLOVENIA[10]

Firearms traffickers use Darknet marketplaces to sell illegal firearms to private individuals, members of OCGs and terrorists based in the EU. In December 2016, Slovenian law enforcement authorities, with the support of Europol, arrested two suspects accused of selling various live firing weapons including automatic rifles, hand and smoke grenades as well as ammunition via a prominent Darknet marketplace. The firearms were paid for in Bitcoin.

It is estimated that **the top 1% most successful vendors are responsible for 51.5% of all transactions on Dark markets.**[11] Goods and services offered on the Darknet are available to anyone, be it an individual user, an OCG or terrorist group.[12]



Shift to Dark markets

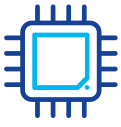
There is a shift from sales on the surface web to sales on the Darknet, typically when the status of a product or substance changes from being legal to illegal. For example, the sales of gun parts or de-activated firearms is legal in certain jurisdictions and therefore available on the surface web, but when the gun is assembled or re-activated it is illegal and will be sold on the Darknet. Likewise, a previously undiscovered New Psychoactive Substance (NPS) is initially unregulated and can be sold on the surface web, but as soon as it is regulated or restricted, sales will move to the Darknet. Dark markets are highly unstable. New decentralised markets are likely to overcome the weakness and vulnerability of being hosted in a specific location. These localised Dark markets cut out intermediaries, cater to sellers and buyers in their own language allowing them to interact directly. Transactions on local platforms enable sellers and buyers to avoid international mail systems by arranging the local collection of illegal goods.

Although the exact scale of the criminality on the Darknet cannot be fully determined as of yet, the Darknet is clearly an established criminal environment hosting an increasing number of platforms including Dark markets and other hidden services.

DRIVERS OF CRIME

Drivers of crime shape the nature and impact of serious and organised crime activities.[13] They include facilitating factors and vulnerabilities in society which create opportunities for criminals.

Technology



For almost all types of organised crime, criminals are deploying and adapting technology with ever greater skill and to ever greater effect. This is now, perhaps, the greatest challenge facing law enforcement authorities around the world, including in the EU.

Technological innovation continues to shape society and the economy, and by extension the serious and organised crime landscape in Europe. Criminal actors in the EU display a high degree of adaptability and creativity in exploiting and employing new technologies. While not all criminal activities are driven by technological developments, the internet and ever-increasing connectivity have an impact on virtually all types of serious and organised crime. Innovation in technology and logistics increasingly enable OCGs to commit crime anonymously, anywhere and anytime without being physically present.

The Internet of Things is constantly expanding. Connectivity of all types of devices, including phones and appliances, is increasingly a reality in households and businesses across the EU. However, these devices remain vulnerable to intrusion and criminals are already deploying techniques to compromise these devices in order to gain personal and financial information and confidential data on business transactions.

Geopolitical context

The serious and organised crime landscape in the EU is fundamentally affected by the geopolitical situation in and around Europe. The impact of conflicts on the periphery of the EU, such as in Libya and Syria, on serious and organised crime in the EU has already materialised and will continue to influence crime. Armed conflicts and poverty are the most significant push factors for migrants travelling to the EU. The emergence of new conflicts or destabilisation of countries on the periphery of the EU would sustain the migration flow to the EU. Armed conflicts close to the EU also entail the risk of returning foreign fighters as well as the large-scale trafficking of firearms originating from these regions.

Legal business structures

OCGs exploit various legal business structures and professional experts to maintain a facade of legitimacy, obscure criminal activities and profits, and to perpetrate lucrative and complex crimes. Legal business structures allow OCGs to operate in the legal economy and enable them to merge legal and illegal profits.

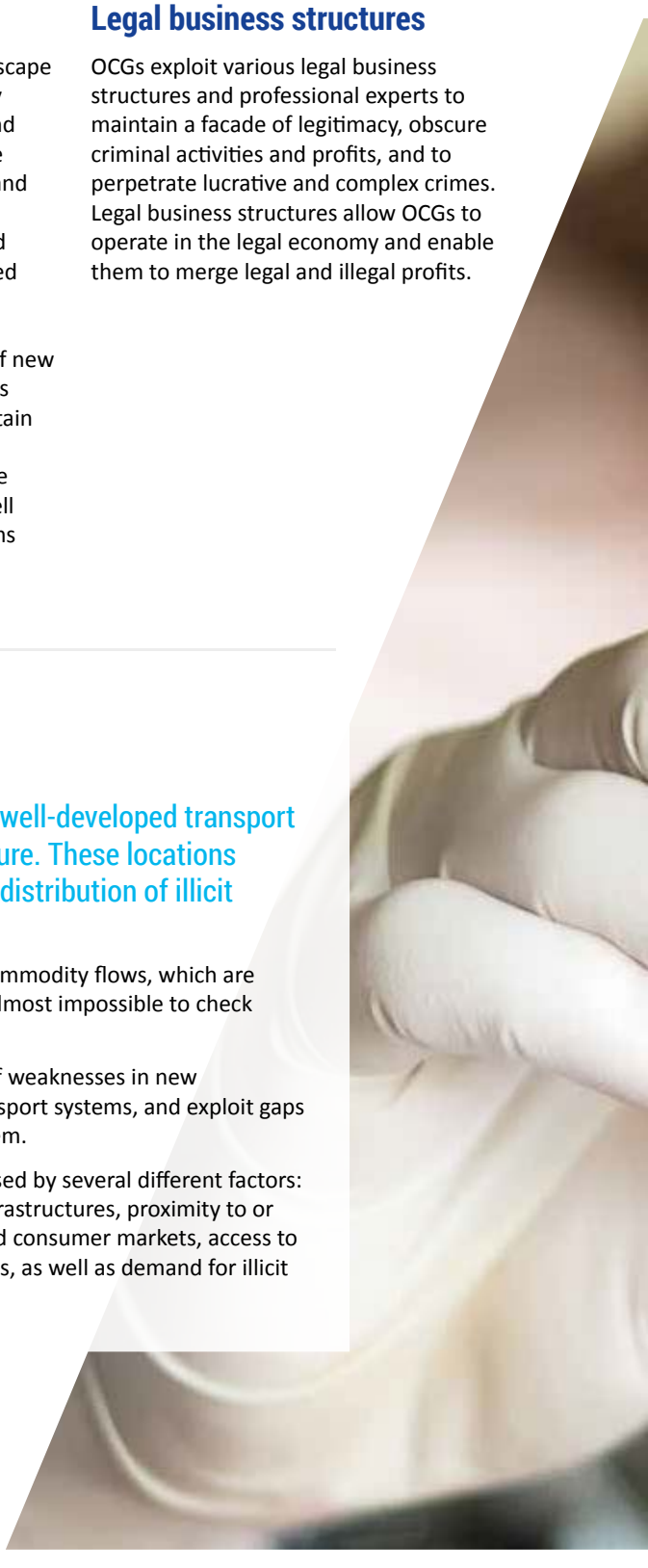
Key locations for crime

Key locations for crime feature well-developed transport and communication infrastructure. These locations are used to organise the global distribution of illicit commodities.

OCGs hide illicit goods among legal commodity flows, which are increasing in speed and volume and almost impossible to check thoroughly.

Criminal groups will take advantage of weaknesses in new technologies, such as automated transport systems, and exploit gaps in the legal frameworks regulating them.

Key locations for crime are characterised by several different factors: the presence of efficient transport infrastructures, proximity to or connections with source countries and consumer markets, access to business and investment opportunities, as well as demand for illicit commodities or services.



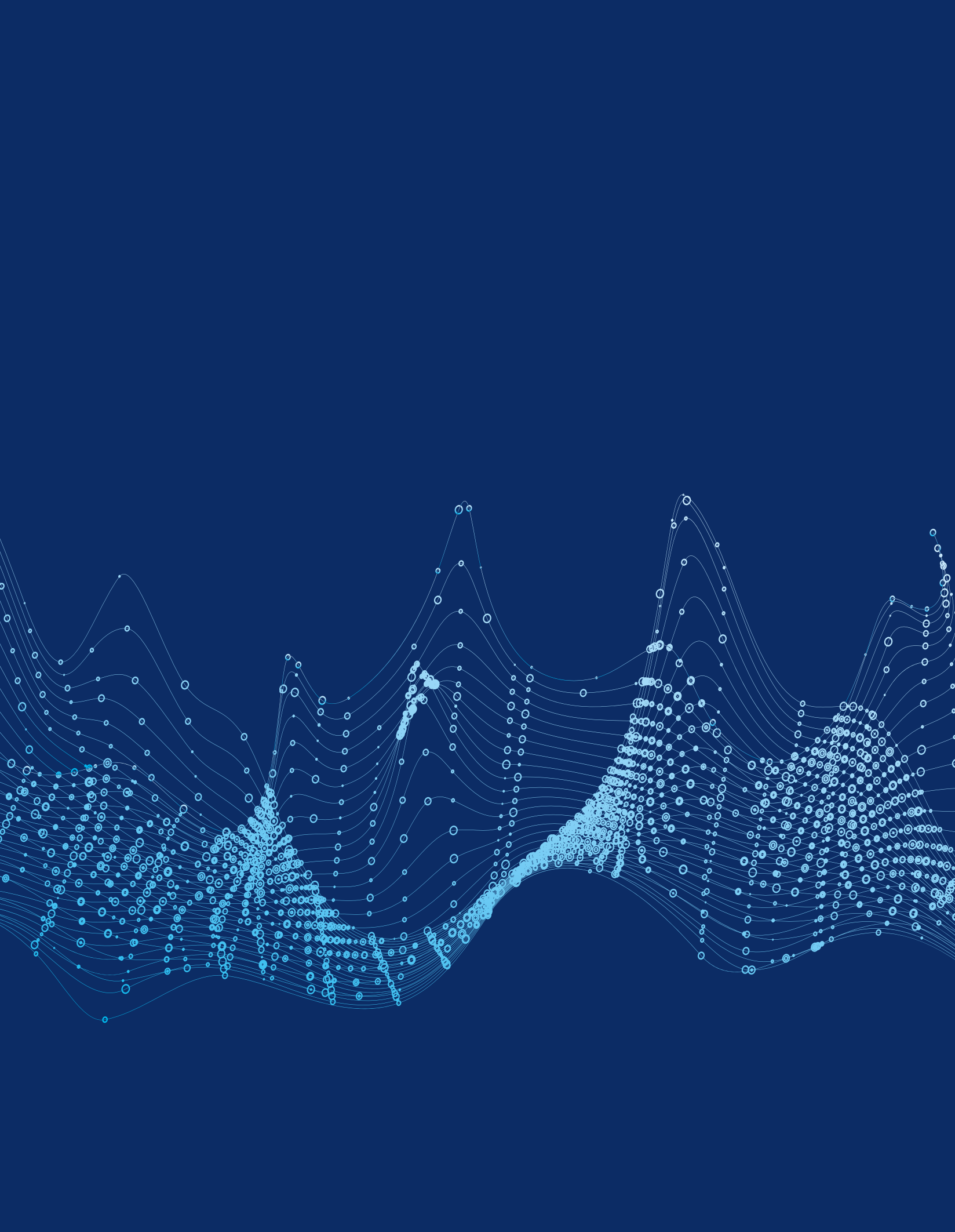
USING TECHNOLOGY TO FIGHT SERIOUS AND ORGANISED CRIME

Technology is also a significant aid to law enforcement authorities in the fight against serious and organised crime. This includes the use of advanced digital forensics tools, the deployment of predictive policing software driven by Big Data as well as drones for the monitoring of areas and large events.

ASSESSING **ORGANISED CRIME**

CRIMINAL MARKETS AND SERVICES

The criminal markets and criminal activities detailed in this chapter are presented in alphabetical order.



CURRENCY COUNTERFEITING

The production of counterfeit currency requires varying degrees of sophistication depending on the currency and level of quality of the resulting counterfeits. Counterfeit banknotes of various currencies are traded online on surface web and Darknet marketplaces. Consequently, counterfeit currency is increasingly trafficked using parcel services.

While the production of counterfeit currency is currently not a major threat to the stability of the euro, the common European currency remains popular with counterfeiters. The most commonly counterfeited euro banknote denominations are the EUR20 and EUR50 notes.[14] In 2016, the European Central Bank (ECB) decided to halt the production of EUR500 banknotes by the end of 2018 in an effort to fight money laundering as well as the production of counterfeit euro banknotes.

CYBERCRIME

CYBER-DEPENDENT CRIMES

A mature CaaS model underpins cybercrime, providing easy access to the tools and services required to carry out cyber-attacks.

Cryptoware (ransomware using encryption) is a significant threat to the EU, targeting not only citizens but increasingly public and private sector organisations alike.

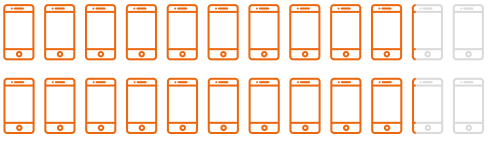
Network intrusions for the purpose of illegally acquiring data have significant impact globally, resulting in the loss of intellectual property and the compromise of mass amounts of data which can be used for further criminality including fraud and extortion.

Cyber-dependent crimes are offences that can only be committed using a computer, computer networks or other form of information communications technology. Cybercrime is a global phenomenon affecting all Member States and is as borderless as the internet itself. The attack surface continues to grow as society becomes increasingly digitised, with more citizens, businesses, public services and devices connecting to the internet.

OPERATION AVALANCHE[15]

On 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Lüneburg Police (Germany) in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Europol, Eurojust and global partners, dismantled an international criminal infrastructure platform known as 'Avalanche'. The Avalanche network was used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform. The global effort to take down this network involved the crucial support of prosecutors and investigators from 30 countries. The operation marks the largest-ever use of sinkholing to combat botnet infrastructures and is unprecedented in its scale, with over 800,000 domains seized, sinkholed or blocked.

Cybercrime continues to grow as society becomes increasingly digitised



85% of internet users feel at risk of becoming a victim of cybercrime

CRIME-AS-A-SERVICE

The digital underground

The CaaS model provides easy access to tools and services across the entire spectrum of cyber-criminality, from entry-level to top-tier players, including those with other motivations such as hacktivists or even terrorists. This allows even entry-level cybercriminals to carry out attacks of a scale disproportionate to their technical capability. Criminal forums and marketplaces within the deep web or Darknet remain a crucial environment for cybercriminals to communicate and are a key component for CaaS.

Malware and ID theft

Malware typically steals user data such as credit card numbers, login credentials and personal information from infected machines for subsequent use by criminals in fraud.

Cryptoware

Cryptoware (ransomware using encryption) has become the leading malware in terms of threat and impact. It encrypts victims' user generated files, denying them access unless the victim pays a fee to have their files decrypted.

Network attacks

Network intrusions that result in unlawful access to or disclosure of private data (data breaches) or intellectual property are growing in frequency and scale, with hundreds of millions of records compromised globally each year.

Payment order fraud

Criminals use fraudulent transfer orders to defraud private and public sector organisations. Fraudsters heavily rely on social engineering techniques and malware to carry out this type of fraud.

Payment card fraud

Compromised card data is readily available and easy to obtain on forums, marketplaces and automated card shops in the deep web and Darknet.

Online sexual exploitation

Child Sexual Exploitation Material is increasingly produced for financial gain and distributed through the Darknet. Coercion and sexual extortion are increasingly being used to victimise children.

Malware

The development and distribution of malware continues to be the cornerstone for the majority of cybercrime. Information-stealing malware, such as banking Trojans, still represent a significant threat. This type of malware typically steals user data such as credit card numbers and login credentials from infected machines for subsequent use by criminals in fraud.

Since late 2013, cryptoware (ransomware using encryption) has become the leading malware in terms of threat and impact. Cryptoware encrypts victims' user generated files, denying them access unless the victim pays a fee to have their files decrypted. Following the trend of information stealers, cryptoware campaigns are increasingly targeting public and private sector entities.

Network attacks

Network attacks vary in *modi operandi* and purpose. Website defacement is a common but low-impact attack, and often the trademark of hacktivist groups targeting government or public websites.

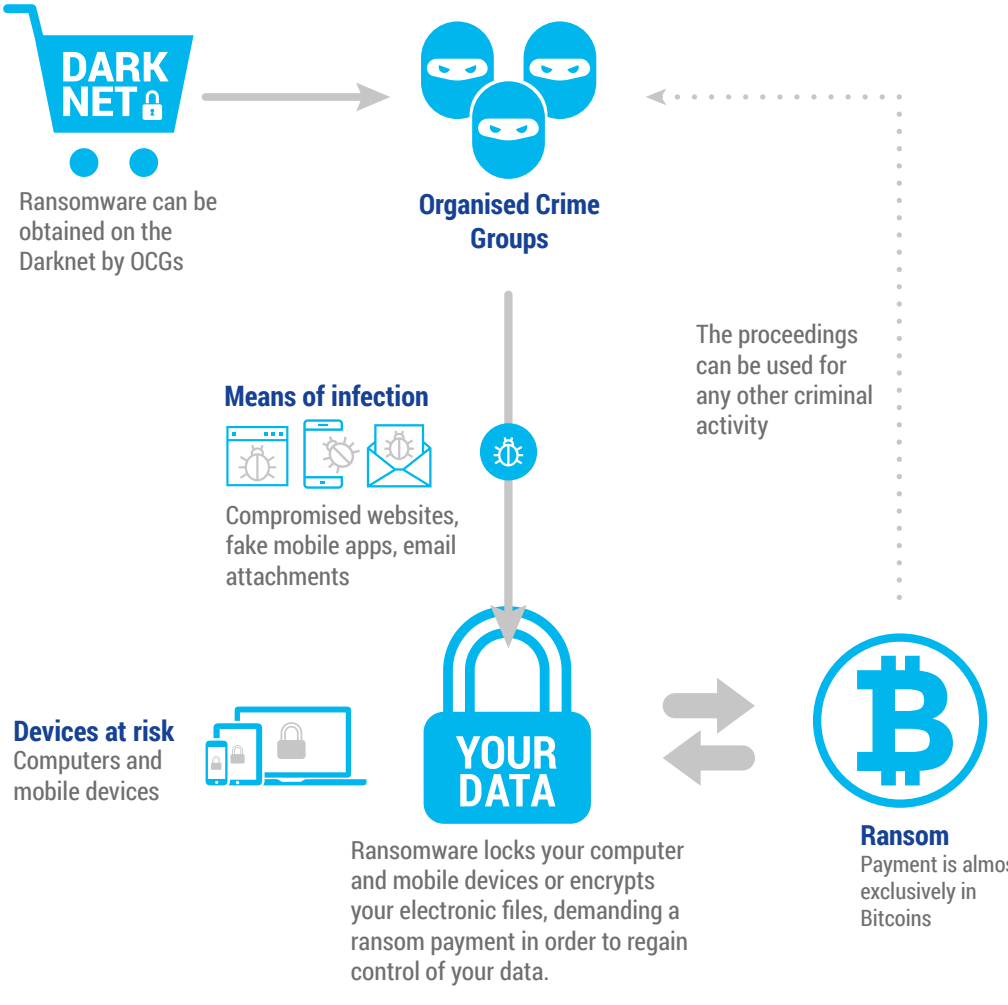
Network intrusions that result in unlawful access to or disclosure of private data (data breaches) or intellectual property are growing in frequency and scale, with hundreds of millions of records compromised globally each year.[16] Compromised data can be used for a variety of criminal purposes including fraud and extortion[17] and is highly valued by financially motivated criminals.[18]

Some Member States highlight the particular threat posed by insiders to a company's security. Any sector or network which holds data which can be monetised is a target for such attacks.

Data has become a key commodity for criminals.

Increasing internet connectivity by citizens, businesses and the public sector, along with the exponentially growing number of connected devices and sensors as part of the Internet of Things will create new opportunities for cybercriminals. Malware targeting smart devices will lead to new sources of data leakage and network compromise and create new botnets. Given the ease of entry into cybercrime, the use of cyber tools and services by traditional OCGs to enhance or expand their capabilities is likely to become more commonplace.

CRYPTOWARE
How it works



ONLINE CHILD SEXUAL EXPLOITATION (CSE)

Child Sexual Exploitation Material (CSEM) is increasingly produced for financial gain.

A growing number of Darknet forums facilitating the exchange of CSEM, coupled with the ease of access to these networks, is leading to an increase in the volume of material exchanged through the Darknet.

Coercion and sexual extortion are increasingly being used to victimise children. Offenders use these methods to obtain further child abuse material, for financial gain or to get physical access to the victim.

While neither offline nor online CSE meet the criteria to be considered 'organised crime' this is still a high priority crime due to the degree of physical and psychological damage to one of society's most vulnerable groups – children.

Online and offline child sexual exploitation are often considered two different crime areas. However, a number of offenders are involved in both. There are indications that this is the case for about 30% of offenders in possession of CSEM.

The increasing global availability of broadband internet and internet-enabled devices continues to fuel the growing number of both offenders and victims in this area. While the same can be said of any number of crime areas, this phenomenon is a major contributor to online CSE.

The internet provides offenders and potential offenders with an environment in which they can operate with an enhanced level of safety and anonymity. In particular, there is a growing number of forums on the Darknet dedicated specifically to the production, sharing and distribution of CSEM. Typically this refers to services on the TOR network. Peer-to-peer (P2P) file sharing applications are the preferred method of exchanging CSEM.

Commercial CSEM

Children are sexually exploited largely to satisfy the sexual appetites of those with a sexual interest in children. However, there is a growing trend in the production of CSEM for financial gain. A particular activity associated with commercial production of CSEM is that of Live Distant Child Abuse (LDCA). LDCA is a significant threat in this area of criminality. LDCA involves a perpetrator paying to direct the live abuse of children on a pre-arranged specific time-frame through video sharing platforms.

Self-Generated Indecent Material (SGIM)

There is a growing trend in the production of Self-Generated Indecent Material (SGIM) - typically teens or pre-teens taking indecent images of themselves to be shared privately with a partner or someone they believe they can trust, for example in grooming scenarios. Subsequently, these images can be distributed either accidentally or maliciously without the owner's consent.

Sexual extortion

Often associated with the production of SGIM is the growing practice of sexual extortion, whereby an offender uses an explicit image of a minor - obtained incidentally or through coercion or deception - to further coerce or extort the child into either producing more material or engaging in further online or even offline abuse. In some cases the perpetrator alternatively seeks financial gain.[19]

PAYMENT CARD FRAUD

Payment card fraud is a low-risk, high-profit activity. Compromised card data is readily available and easy to obtain on forums, marketplaces and automated card shops in the deep web and Darknet. Payment card fraud can be split into two distinct crime areas: *Card-present fraud* and *card-not-present fraud.*

Some OCGs run 'laboratories' to study ATMs in order to conduct targeted attacks.

Card-present fraud (CP)

CP fraud requires an offender to present a physical card at an automated teller machine (ATM), Point of Sale (POS) or other terminal. This crime has two stages: obtaining a card, and the use of the card. The cards used are either lost or stolen genuine cards, or counterfeit cards. Unlike fraud using lost or stolen cards, fraud using counterfeit cards is typically committed outside the Single Euro Payments Area (SEPA).

Some OCGs have partly industrialised their processes, using workshops to produce counterfeit cards.

Card-not-present fraud (CNP)

CNP fraud involves the use of card data to make fraudulent purchases online or by telephone. Unlike CP fraud, the data required is only that needed to make an online credit card purchase – the name of the card holder, billing address, card number, expiry date and security code. The fraud, commonly referred to as 'carding', is committed across all sectors but the purchase of physical goods, airline tickets, car rentals and accommodation with compromised cards have generally seen an increase throughout the EU. Where CNP is used to fraudulently purchase goods, like CP fraud, offenders will typically purchase high-value goods with the intention of reselling them. Offenders will often use packet mules or reshipping services to safely receive their fraudulently obtained goods.

CNP is fuelled by the availability of compromised card data resulting from data breaches, information stealing malware and phishing. As many data breaches often involve the compromise of millions of card details at once, there is a considerable excess of card data compared to the demand. Among the places where compromised card data can be found are an increasing number of illegal carding sites on both the deep web and Darknet where not only card data can be purchased but offenders can learn about how and where to 'card'. New payments methods provide offenders with new opportunities to use compromised card data. By uploading the card data to smartphone services, offenders can make "in app" or "on site" payments to apps which they control.

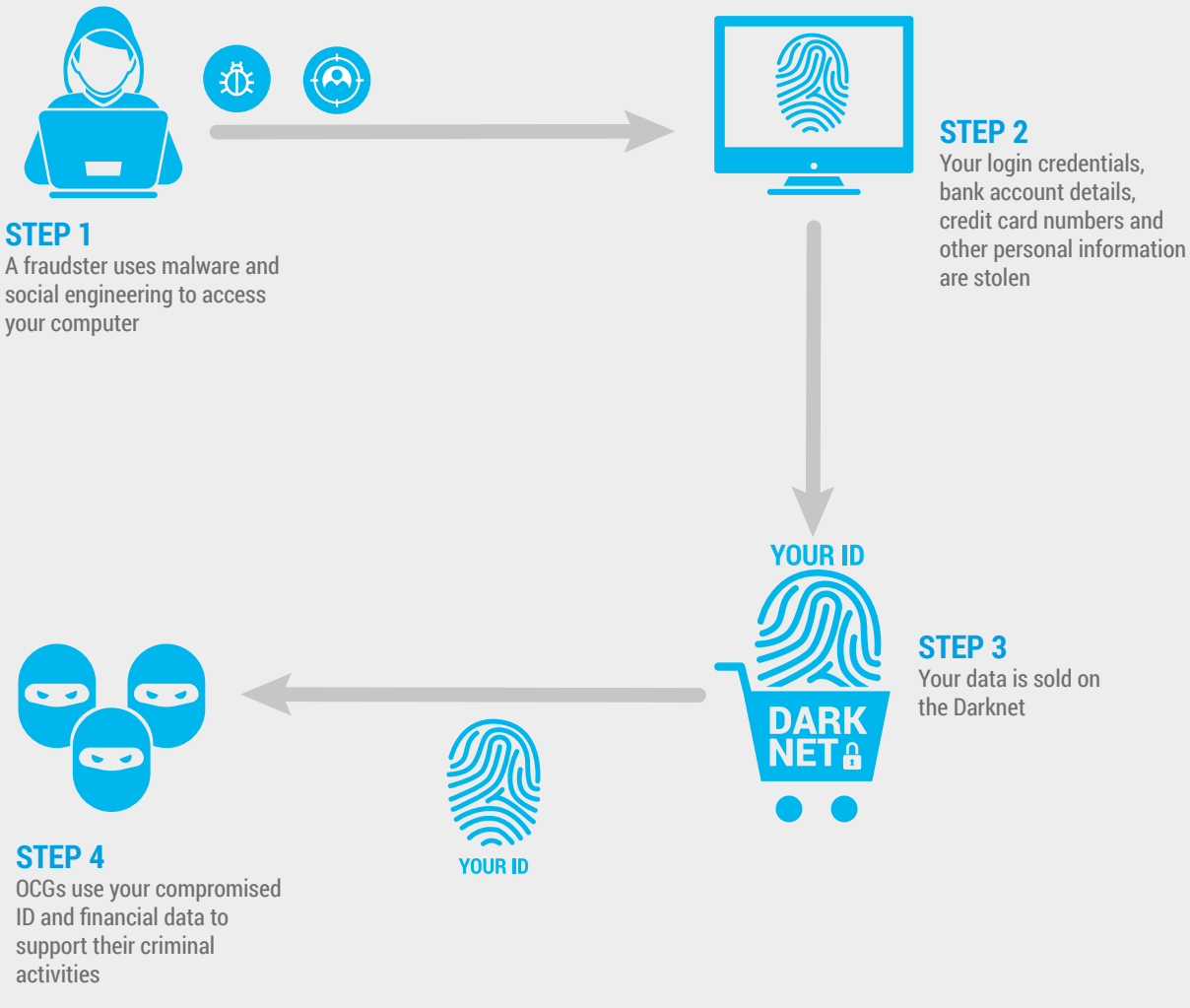
The growing e-commerce industry will result in a parallel growth of CNP fraud, especially as industry measures at preventing CP fraud become more effective. Criminal *modus operandi* will be shaped by industry measures to counter payment card fraud.

Emerging and alternate payment options such as contactless payment using Near Field Communication (NFC) will drive innovation within OCGs to enable them to abuse new technologies. New electronic/card-less payment methods may however ultimately result in a downwards trend in card fraud.

INTERNATIONAL CRIMINAL NETWORK BEHIND LARGE-SCALE PAYMENT FRAUD DISMANTLED[20]

In September 2016, Italian and Romanian law enforcement authorities supported by Europol disrupted an international criminal group responsible for large-scale misuse of compromised payment card data, prostitution and money laundering. The criminal network used sophisticated ATM skimming devices which allowed them to compromise ATMs and deceptive phishing techniques to perform a high volume of fraudulent transactions. Estimated losses incurred by the criminals' activities amount to several hundred thousands of euros. Micro-camera bars, card readers, magnetic strip readers and writers, computers, phones and flash drives, several vehicles, as well as thousands of plastic cards ready to be encoded were seized in several locations.

ID THEFT AND PAYMENT CARD FRAUD



GLOBAL ACTION AGAINST AIRLINE FRAUDSTERS[21]

Global Airport Action Days combine the efforts of law enforcement and private sector partners to combat the fraudulent online purchases of flight tickets, which is estimated to cost the industry over EUR 1 billion per year. Fraudulent online transactions are highly lucrative for organised crime and are often purchased to facilitate more serious criminal activities including migrant smuggling, THB, drug trafficking and terrorism. In October 2016, the fifth Global Airport Action Day was organised through coordination centres at Europol, INTERPOL Global Complex for Innovation in Singapore and Ameripol in Bogota. The activity was supported by Canadian and US law enforcement agencies. Representatives from airlines, online travel agencies, payment card companies, Perseuss and the International Air Transport Association (IATA) worked together with law enforcement officers deployed in the airports. Eurojust assisted throughout the action week, together with the European Border and Coast Guard Agency (Frontex) which deployed officers to 20 airports, assisting in the detection of identity fraud, fake documents and migrant smuggling. 193 individuals suspected of traveling with airline tickets bought using stolen, compromised or fake credit card details were detained. 43 countries, 75 airlines and 8 online travel agencies were involved in this global operation which took place at 189 airports across the world.

DRUG PRODUCTION, TRAFFICKING AND DISTRIBUTION

Drug markets remain the largest criminal markets in the EU. More than one third of the criminal groups active in the EU are involved in the production, trafficking or distribution of various types of drugs. The trade in drugs generates multi-billion euro profits for the groups involved in this criminal activity. The EU retail drug market is estimated to be worth at least EUR 24 billion a year.[22] The immense profits generated from the trade in drugs fund various other criminal activities allowing OCGs to thrive and develop their criminal enterprises at the expense of the health, prosperity and security of EU citizens.

OCGs involved in drug trafficking heavily rely on corruption to facilitate their trafficking activities. They also make use of fraudulent documents such as fake import or company registration certificates to import illicit drugs among legal goods, to procure pre-precursors and purchase equipment used as part of production processes.

Drug market generates

~24 EUR billion/year in profits

>35%

of the criminal groups active in the EU are involved in the drug market

419 previously undetected NPS reported in the EU for the first time over the past five years

Online trade

Criminals continuously seek out methods and technologies to make their business models more effective and increase profit margins. Online marketplaces on the Darknet are now a key platform used to advertise and sell all types of drugs. The anonymous nature of online transactions on these marketplaces and the use of cryptocurrencies reduce the risks of detection by law enforcement authorities for both vendors and buyers.

Technology

Technical innovation and the accessibility of sophisticated equipment have allowed OCGs to maximise the production output of individual sites. Large-scale cannabis cultivation sites are often maintained using professional growing equipment such as climate control systems, CO2 and ozone generators. Similarly, laboratories manufacturing synthetic drugs feature advanced chemical equipment and production lines capable of producing synthetic drugs on an industrial scale.

Drone technology is expected to advance allowing drones to travel greater distances and carry heavier loads as well as making them more affordable. OCGs involved in drug trafficking will likely invest in drone technology for trafficking purposes in order to avoid checks at border crossing points, ports and airports.

>75%

of the OCGs involved in the trafficking of one drug also traffic and distribute other types of drugs.

~65%

of OCGs involved in the drug trade are simultaneously involved in other criminal activities such as the trade in counterfeit goods, THB and migrant smuggling. Drugs are also used as a means of payment among criminal groups.

TRENDS

SYNTHETIC DRUGS

The market for synthetic drugs continues to be the most dynamic of the drug markets in the EU.

ONLINE TRADE

Online marketplaces on the Darknet are now a key platform used to advertise and sell all types of drugs.

CUTTING - EDGE TECHNOLOGY

Technical innovation and sophisticated equipment allow OCGs to maximise the production output.

TOXIC WASTE

The production of synthetic drugs generates large quantities of highly toxic and dangerous waste. Dump sites often remain contaminated for a significant period of time and their recovery is costly.

LIBYA

Libya is emerging as a new distribution hub for cannabis resin trafficked to the EU across the Mediterranean Sea.

CANNABIS

Cannabis remains, by far, the most widely consumed illegal drug in the EU.[23] Cannabis is distributed on EU markets as cannabis resin and herbal cannabis. In recent years, herbal cannabis has been increasingly popular with consumers, which has led to an increase in the production and availability of herbal cannabis within the EU and in countries close to EU markets.

Growing equipment, seeds and other raw materials used for cannabis cultivation in the EU are readily available online and often originate from the Netherlands. The indoor cultivation of herbal cannabis in the EU is expected to further expand over the coming years with new growing techniques and increasingly sophisticated growing technologies being used by OCGs in order to increase harvest yields and profits. Outdoor cultivation of herbal cannabis remains limited compared to the indoor cultivation of cannabis.

Albania remains the main source of herbal cannabis trafficked to the EU. The main source of cannabis resin consumed in the EU is Morocco from where it is trafficked to the EU primarily by sea and road transport. Cannabis resin originating from Morocco is increasingly smuggled to the EU across the Mediterranean Sea departing from Libya. Cannabis resin shipments are transported across the Mediterranean Sea to the Spanish coast using high-powered vessels where they are dropped into the sea and retrieved by OCGs on local fishing vessels or pleasure boats using GPS signalling devices.

The market for cannabis remains by far the largest drug market in the EU.

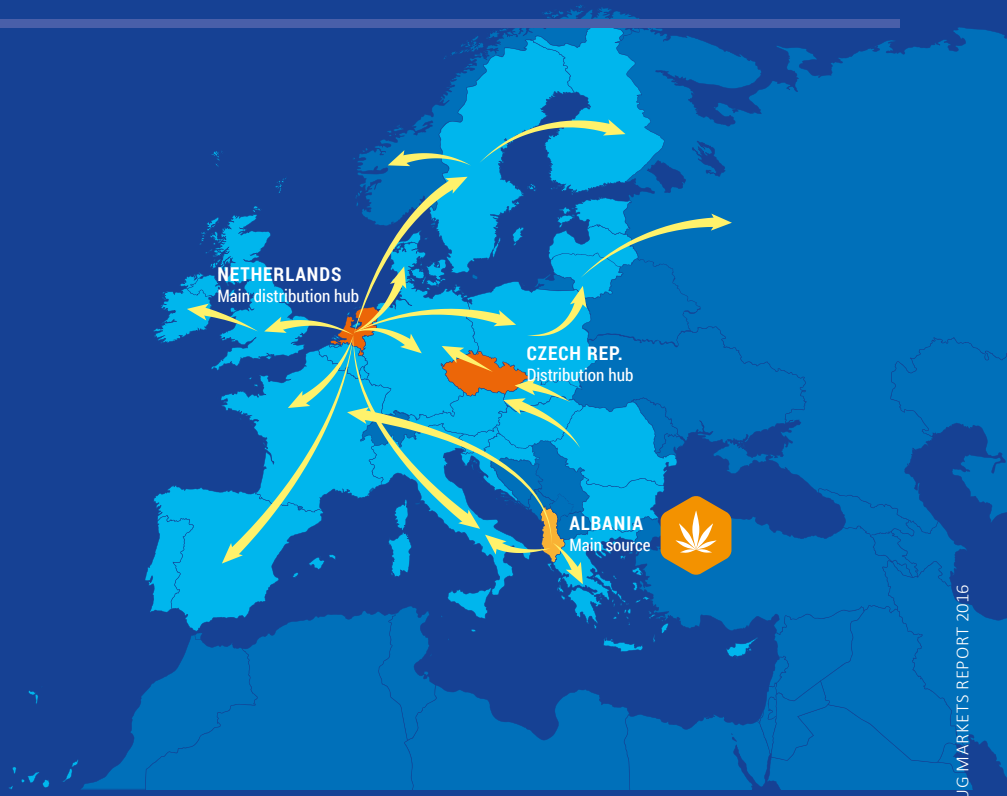
'ROSE OF THE WINDS' – INTERNATIONAL OPERATION AGAINST DRUG TRAFFICKING[24]

In December 2016, a multinational police team including Europol announced the arrest of a major Moroccan drug kingpin. The work that led to this arrest began in April 2016. The Moroccan national had orchestrated a multi-tonne drug delivery. This is the latest successful result achieved by JOT 'Rose of the Winds'. Approximately one week prior to his apprehension, the Spanish Guardia Civil, supported by Europol, the French Direction Nationale du Renseignement et des Enquêtes Douanières and the Italian Guardia di Finanza, localised and intercepted a merchant vessel flying the flag of Panama. The ship was subsequently escorted to the port of Almeria, where a thorough search revealed the illegal cargo of 19.6 tonnes of cannabis resin. The crew were arrested and the shipment was seized. The investigations also revealed a poly-crime involvement of the transnational organised crime networks active in large-scale drug trafficking in the Mediterranean Sea. Namely, concrete and recurrent links with migrant smuggling and cocaine trafficking have been ascertained.

CANNABIS HERB

Production, trafficking and distribution

The **indoor cultivation** of herbal cannabis in the EU is expected to further expand over the coming years with new growing techniques and increasingly sophisticated growing technologies being used by OCGs.



CANNABIS RESIN

Cannabis resin continues to be trafficked in large quantities from **Morocco** to the EU.

Libya is emerging as a new distribution hub for cannabis resin trafficked to the EU across the Mediterranean Sea.

SOURCE: EMCDDA & EUROPOL EU DRUG MARKETS REPORT 2016

CANNABIS

Means of transportation

COCAINE

Cocaine is primarily produced in Colombia, Peru and Bolivia and trafficked to the EU via other South American countries such as Brazil, Venezuela, Argentina, the Caribbean Sea region and West Africa. Over the last two years, the production of cocaine in Colombia has intensified significantly. An increase in the production output in Colombia will likely impact on the EU in the form of intensified trafficking activity as well as greater availability of cocaine on drug markets in the Member States.

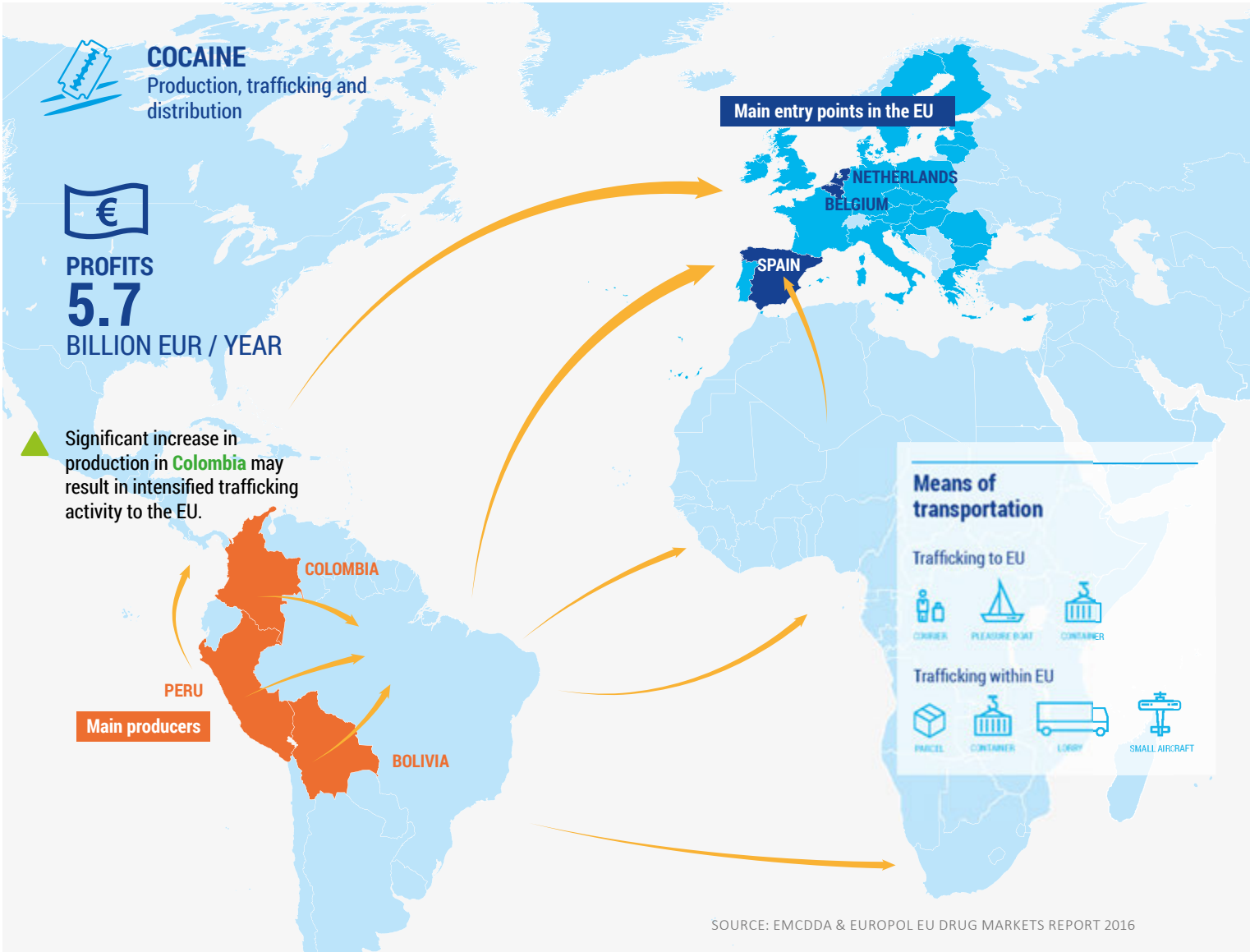
The trafficking *modi operandi* associated with the trade in cocaine have largely remained the same. Cocaine is typically trafficked as part of large shipments in containers or in smaller quantities by couriers.

Large shipments of cocaine are trafficked in containers hidden among legal goods or as part of the rip-on/rip-off *modus operandi*. Brazil is a key point of departure for cocaine couriers travelling directly to the EU. The United Arab Emirates (UAE) and destinations in East Africa have emerged as hubs for cocaine couriers travelling to the EU. Cruise ships departing from the Caribbean Sea region are increasingly being used to traffic cocaine to the EU.

More OCGs are involved in cocaine trafficking than any other criminal activity in the EU.

OPERATION FULECO

Brazil is among the main countries of departure for couriers trafficking cocaine to the EU. This has been confirmed by the results of Operation Fuleco, an effort by Member States supported by Europol targeting cocaine couriers arriving to the EU's major airports. During Operation Fuleco, nearly 200 cocaine couriers were arrested and almost 500 kilograms of cocaine seized in the Netherlands, Spain, Portugal, the United Kingdom, France, Belgium, Germany and Ireland. Operation Fuleco took place in June and July 2014 and involved 12 Member States including Austria, Belgium, Bulgaria, the Czech Republic, France, Germany, Ireland, the Netherlands, Romania, Spain, Sweden and the United Kingdom.



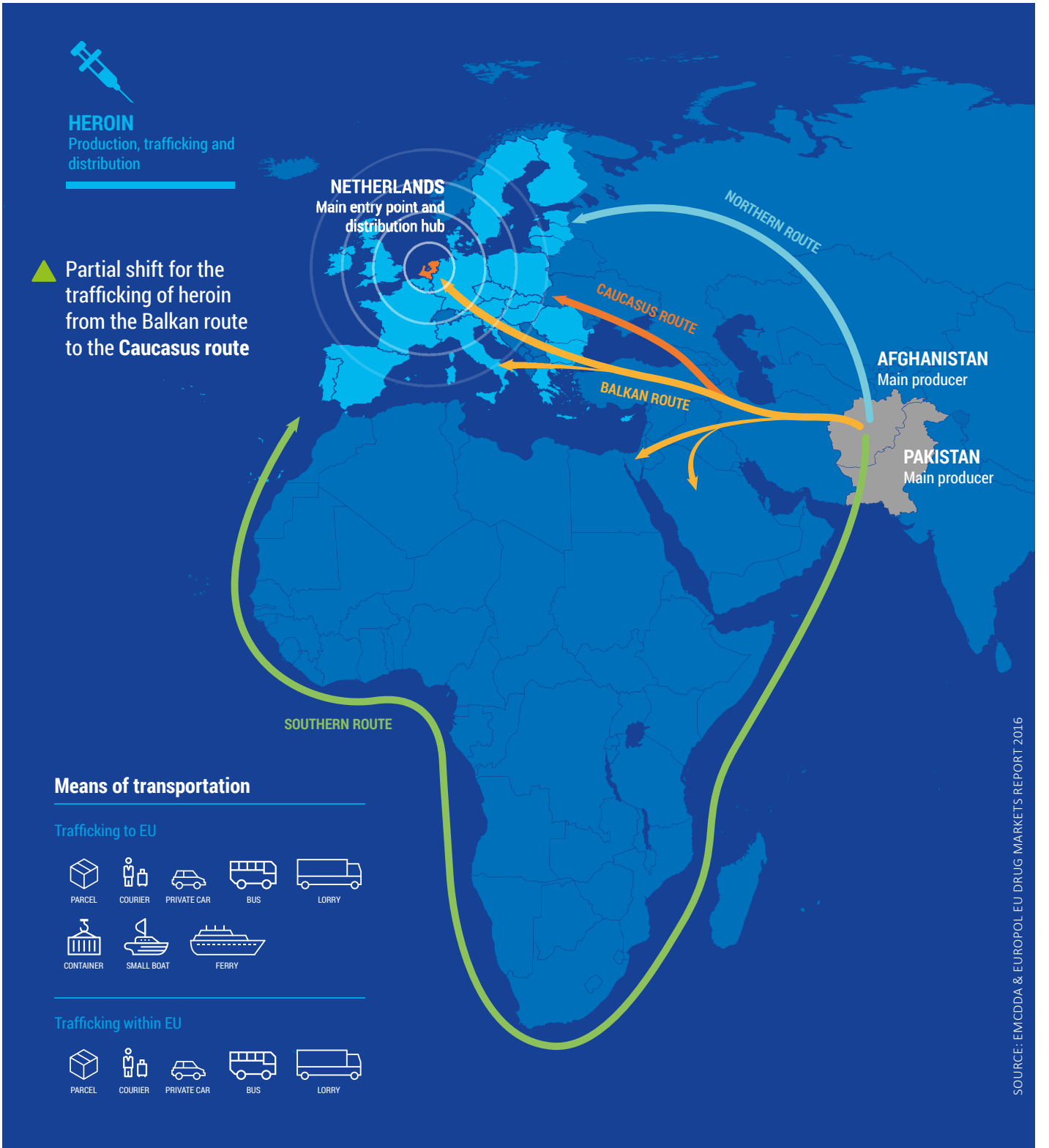
SOURCE: EMCDDA & EUROPOL EU DRUG MARKETS REPORT 2016

HEROIN

Afghanistan remains the leading producer of heroin trafficked to the EU. The production output of opium and heroin in Afghanistan is very high and is projected to remain so for the foreseeable future.

Production of heroin remains rare in the EU. However, depending on the development of the demand for heroin and potential disruptions to trafficking activities from Afghanistan further laboratories may emerge in the EU in the future. Heroin is also available on online marketplaces and is occasionally distributed across the EU in small quantities via post and parcel services.

The Balkan route remains the main entry route for the trafficking of heroin into the EU.

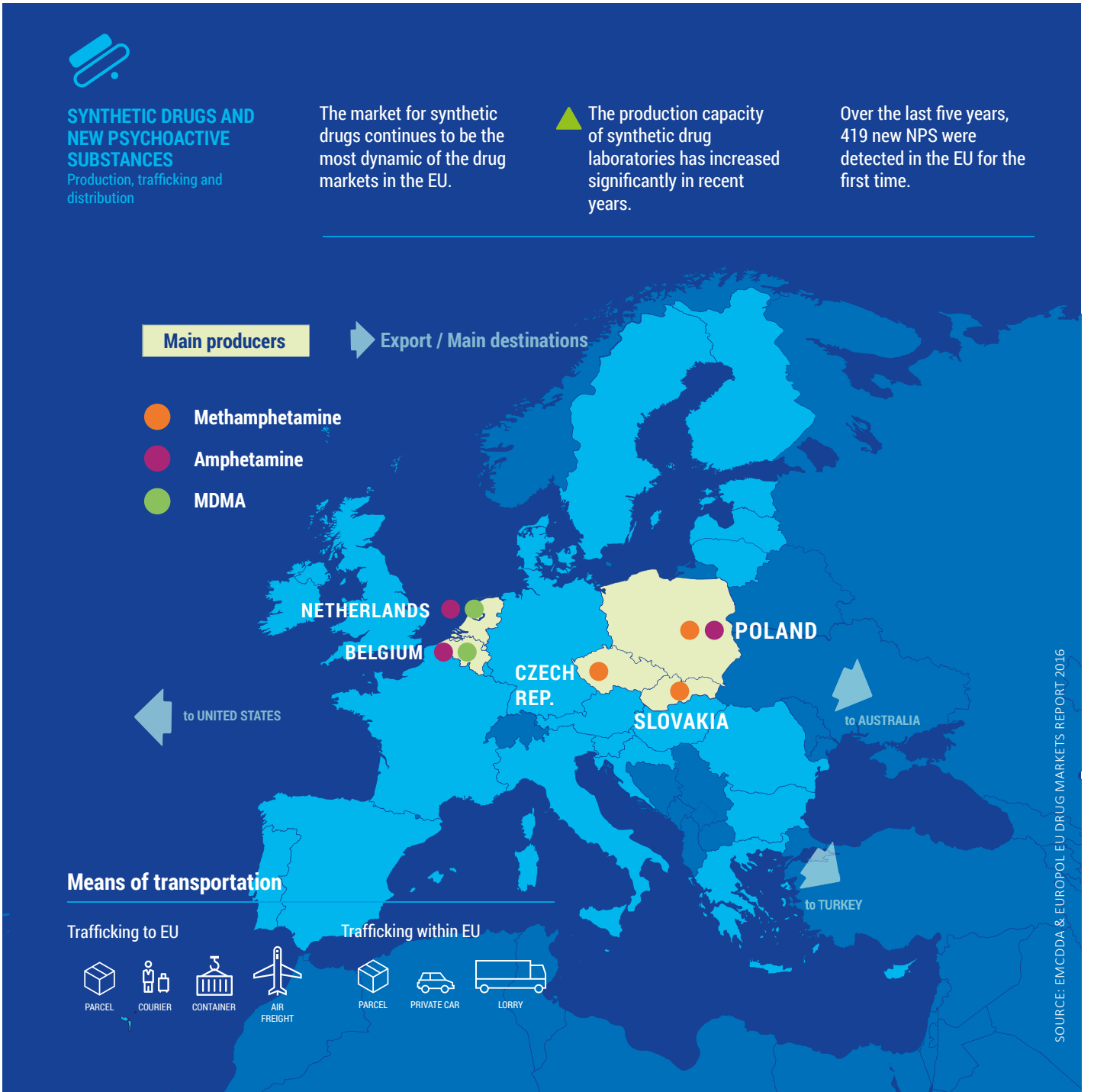


SYNTHETIC DRUGS AND NEW PSYCHOACTIVE SUBSTANCES (NPS)

The production of different types of synthetic drugs takes place in various Member States. The intended destination markets for synthetic drugs produced in the EU vary according to the substance and production location. A share of the large-scale production of 3,4-methylenedioxy-methamphetamine (MDMA), amphetamine and, to a lesser extent, methamphetamine in the Netherlands and Belgium is intended for trafficking to markets outside the EU, while the production of synthetic drugs in other parts of the EU predominantly supplies domestic and neighbouring EU markets.

The Netherlands and Belgium remain a globally significant production and distribution hub for MDMA and amphetamine. The OCGs involved in the production of synthetic drugs are highly flexible and have significant financial resources to constantly explore new market opportunities such as engaging in the production of other synthetic drugs including mephedrone.

Production sites for methamphetamine are expected to also appear in other Member States in greater numbers in the future, especially those with existing production capabilities for amphetamine.



Precursors and pre-precursors

OCGs producing synthetic drugs in the EU continue to be highly flexible and will remain so in the future. They are quick to adopt alternative precursor and pre-precursor substances in reaction to any shortages in established precursor substances. China remains a major supplier of pre-precursor substances and essential chemicals as well as hardware and glassware for synthetic drug laboratories in the EU.

Some OCGs have specialised in the procurement and production of pre-precursor and precursor substances supplying OCGs producing and distributing synthetic drugs in the EU.

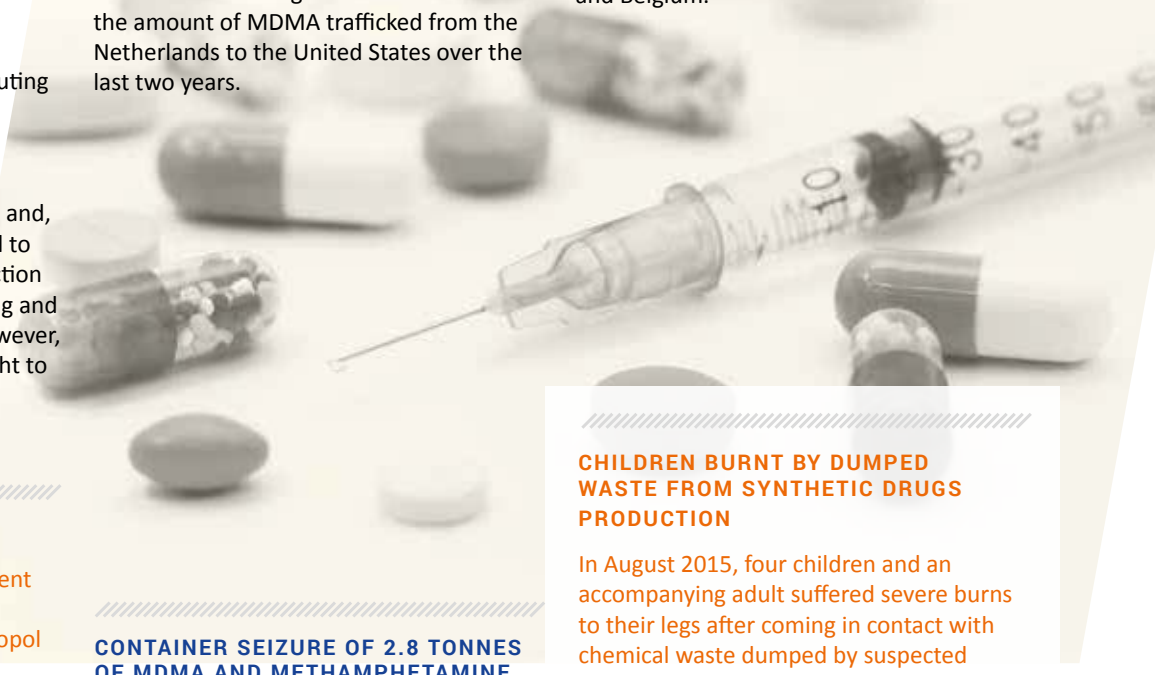
NPS

NPS continue to be produced in China and, to a lesser degree, India and trafficked to the EU in large quantities. NPS production in the EU is largely limited to packaging and re-selling of imported substances. However, some limited NPS production is thought to take place in the EU.

OPERATION ALIMAYA

In March 2016, Spanish law enforcement authorities in cooperation with other Member States and supported by Europol were able to dismantle a network importing and distributing large quantities of dangerous NPS in the EU. This network used various companies to import and sell these substances, especially synthetic cannabinoids from China, generating significant profits. Coordinated action in March 2016 involving house searches at four locations resulted in the seizure of 550 litres of acetone, 75,000 envelopes used for packaging different NPS brands, NPS worth more than EUR 1.5 million. This investigation highlights the profits involved in the distribution of NPS.

The great quantities of MDMA and amphetamine produced by Dutch OCGs are not solely intended for distribution in the EU. The MDMA and amphetamine output from production in the Netherlands and Belgium is trafficked to destination markets around the world. Australia remains among the most significant destination markets outside the EU for synthetic drugs produced in the Netherlands and Belgium. In some cases, large shipments of synthetic drugs are trafficked to destinations outside the EU in maritime shipping containers. There has been a significant increase in the amount of MDMA trafficked from the Netherlands to the United States over the last two years.



CONTAINER SEIZURE OF 2.8 TONNES OF MDMA AND METHAMPHETAMINE VALUED MORE THAN USD 1.5 BILLION[25]

In November 2014, Australian law enforcement authorities seized a maritime shipping container holding approximately 2.8 tonnes of MDMA and methamphetamine. The load was estimated to have a street value of more than EUR 1.4 billion (USD 1.5 billion). At the time, the value and size of the seizure was unprecedented. The container arrived in Australia from Europe and was seized following an intelligence operation. The seizure led to the arrest of several individuals in Australia and Australian law enforcement authorities suspect the involvement of several OCGs in the production, trafficking and intended distribution of this shipment. This seizure highlights the scope of the trafficking of synthetic drugs from the EU to destination markets around the world.

The production of synthetic drugs generates large quantities of highly toxic waste. OCGs dump this waste away from production laboratories to conceal their location. Dump sites often remain contaminated for a significant period of time and their recovery is costly. The dumping of toxic waste in public places also entails significant risks for the health and safety of citizens. In recent years, the number of dump sites discovered in the EU has been increasing. Dump sites are most frequently discovered in the Netherlands and Belgium.

CHILDREN BURNT BY DUMPED WASTE FROM SYNTHETIC DRUGS PRODUCTION

In August 2015, four children and an accompanying adult suffered severe burns to their legs after coming in contact with chemical waste dumped by suspected synthetic drug producers in Belgium. Some of the waste produced as part of the manufacture of synthetic drugs is highly dangerous. Drug producers frequently dump this type of waste away from their laboratories in order to disguise their locations.

HORMONAL SUBSTANCES

There is a growing market for illegal hormonal substances in the EU. These substances are both trafficked to and illegally produced in the EU.

Hormonal substances trafficked to the EU typically originate from China, India and Thailand. However, over the last few years production facilities for illicit hormonal substances have also been discovered in the EU.

ENVIRONMENTAL CRIME

Environmental crime covers a diverse range of different offences including the improper collection, transport, recovery or disposal of waste, the illegal operation of a plant in which a dangerous activity is carried out or in which dangerous substances or preparations are stored, the killing, destruction, possession or trade of specimens of protected wild fauna or flora species, and the production, importation, exportation, placing on the market or use of ozone-depleting substances.

Environmental crime is characterised by its impact on the natural environment. The environmental impact manifests itself in increasing levels of pollution, a degradation of wildlife, a reduction in biodiversity and the disturbance of ecological balance. Environmental crime puts public health at risk.

ILLICIT WASTE TRAFFICKING

The use of legal business structures for illicit waste trafficking activities by criminal actors are an inherent feature of this crime area. In many cases, criminal actors and legal businesses are indistinguishable from one another. As part of this development, criminals involved in illicit waste trafficking have moved towards the more complex business model of illicit waste management rather than just illegally dumping waste. Illicit waste traffickers now operate along the entire waste processing chain, heavily relying on the use of legal business structures for their activities.

The trafficking of illicit waste typically involves the use of fraudulent documents.

TRAFFICKING OF ENDANGERED SPECIES

The trafficking of and trade in endangered species involves the collection or processing of animals and plants protected by national and international regulations. The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) provides the international framework for the protection of endangered species and aims to ensure that international trade in specimens of wild animals and plants does not threaten their survival.

The EU is primarily a transit region for endangered species trafficked to destination markets in Asia and North America. The most commonly trafficked species and wildlife products trafficked from, to and via the EU include glass eels, reptiles, exotic birds, pangolin, fish, narwhal meat, shells, corals, date mussels, timber and ivory.

The number of OCGs involved in the trafficking of and trade in endangered species is low, but believed to be increasing. The OCGs involved are highly specialised and typically only focus on this specific activity.

IVORY TRAFFICKING

In November 2016, Austrian law enforcement authorities seized 560 kilograms of trafficked ivory, the equivalent of 590 elephant tusks. Ivory is worth more than EUR 1,000 (USD 1,000) per kilogram on the Austrian black market. German law enforcement authorities seized 1,200 kilograms of ivory at a Berlin airport, Germany, in May 2016. Raw and manufactured ivory were falsely declared and destined for Vietnam.

FRAUD

EXCISE FRAUD

Alcohol, cigarettes and mineral oils are subject to excise duty upon production in, or on import to, the EU. OCGs use various *modi operandi* to avoid excise duties and generate significant profits selling both genuine and counterfeit excise goods at lower prices than their licit equivalents. Excise tax fraud is driven by legislative differences and varying excise tax rates applied by different jurisdictions.

FUEL FRAUD

Fuel fraud is a growing phenomenon and typically involves base-oil fraud, also called 'designer fuel' fraud and fuel laundering. This type of fraud requires significant expertise, which is usually only available from trained chemists or similar professions.

Excise goods are increasingly offered and bought online.

UNDERSTANDING EXCISE FRAUD
ABUSE OF DUTY SUSPENSION SCHEMES

The abuse of duty suspension schemes are the main *modi operandi* used to avoid the payment of excise duties on alcohol products and are also increasingly used to avoid excise duties on tobacco products. These *modi operandi* involve the exploitation of the EU Excise Movement Control System (EMCS), a computerised system registering the movement of excise goods within the EU, and the T1 procedure, which is applied for excise goods under suspension schemes imported from outside the EU, by falsely declaring the real destination and quantities of excise goods imported into the EU.

How does it work?

In relation to alcohol products, as part of the import process for the EMCS and the T1 procedure, criminals declare a Member State which applies low excise rates as the intended destination of the trafficked goods. Accomplices in the declared country of destination, such as corrupt warehouse employees, confirm receipt of the goods. However, in reality the goods are exported to countries applying high excise rates. The goods appear legitimate as documents certify that any excise obligations due were paid. If the product originates from a country applying high excise rates, the goods often do not leave the country at all and the movement of the goods is purely virtual.

In other cases, traffickers file an application for the transfer of one load and use a duplicate of the transport authorisation to import multiple loads without paying excise duties.

INVESTMENT FRAUD

Investment fraud schemes generate huge profits. One investigation revealed estimated profits of up to EUR 3 billion generated by one OCG.

Successful investment fraud schemes typically use various social engineering techniques to operate. Fraud schemes relying on social engineering are particularly hard to counter.

What is social engineering?

Social engineering techniques are a key element to many different types of fraud. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

OPERATION BATEO

In 2015, law enforcement authorities in the EU launched an investigation into an OCG with ties to Germany, Portugal and Spain. This OCG operated a sophisticated pyramid fraud scheme offering investments into a music sharing platform and other online services. The OCG used various front companies. The investigation was able to identify more than 50,000 victims in 34 countries. Overall, the OCG was able to generate an estimated profit of more than EUR 3 billion.

UNDERSTANDING INVESTMENT FRAUD

Criminals orchestrate various investment fraud schemes. The most common schemes encountered in the EU include:

Fraudsters operating **Boiler room schemes** use cold-calling to contact their victims and pressure them into investing in non-existent or very low-value stocks. Fraudsters often use false documents and certificates to present their company and the offered stock as legitimate.

As part of **Ponzi schemes**, fraudsters attract a group of initial investors with promises of very high returns in a very short time. The fraudster starts to repay the initial investors to attract more victims using funds accrued from additional investors. In reality, the money is not invested and the fraudsters ultimately disappear with the funds. The money is laundered through multiple bank accounts held by various front companies in different jurisdictions.

Pyramid schemes operate on the same model as Ponzi schemes. However, the initial investors are actively involved and are required to recruit new investors in order to get profits.

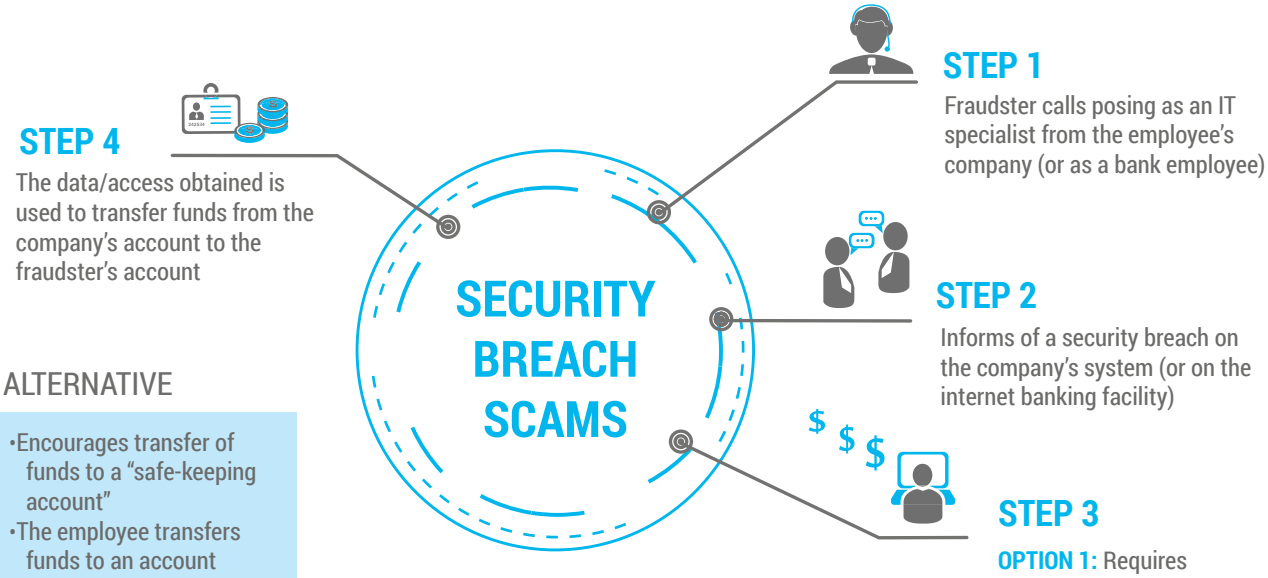
MASS MARKETING FRAUD

Mass marketing fraud schemes rely on mass-communication media, including telephones, the internet, mass mailing, television and radio, to contact victims and solicit money or other items of value in one or more jurisdictions.

Fraudsters already rely on social media and instant messaging applications to obtain sensitive information or elicit payments from their victims.

Between May 2014 and May 2015, a UK-based OCG defrauded over EUR 690,000 (GBP 600,000) from pensioners across the country. Posing as police officers, OCG members contacted victims by phone to warn them of the risk of fraud involving their bank. The victims were encouraged to transfer their savings to safekeeping accounts controlled by the fraudsters.[26]

Scams relying on phishing or cold-calling can target thousands of victims at once. In one cold-calling case, one telecommunications provider was confronted with 3.6 million attempts against 90,000 victims.

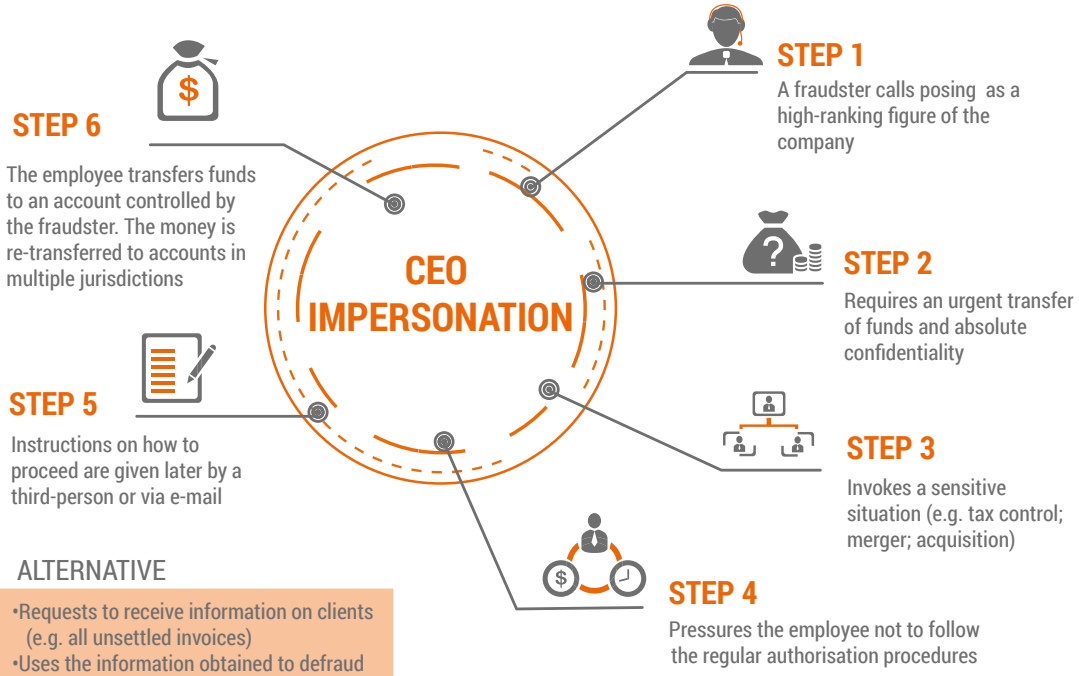


PAYMENT ORDER FRAUD

Criminals use fraudulent transfer orders to defraud private and public sector organisations. Typically, the affected organisations are active internationally. This increasingly common type of fraud is also referred to as CEO fraud, wire transfer fraud or business e-mail compromise. Fraudsters heavily rely on social engineering techniques and malware to carry out this type of fraud. OCGs organising CEO fraud schemes targeting organisations based in the EU typically operate remotely from outside the EU.

Typically, stolen funds are transferred through series of accounts in various Member States before reaching destination accounts outside the EU.

UNDERSTANDING FRAUDULENT TRANSFER ORDERS



ALTERNATIVE

- Requests to receive information on clients (e.g. all unsettled invoices)
- Uses the information obtained to defraud clients

VALUE ADDED TAX (VAT) FRAUD

VAT frauds are highly complex forms of tax fraud relying on the abuse of the VAT rules for cross-border transactions. VAT fraudsters generate multi-billion euro profits by avoiding the payment of VAT or by fraudulently claiming repayments of VAT by national authorities following a chain of transactions. The most common form of VAT fraud is Missing Trader Intra-Community (MTIC) fraud.

Changes in commodity prices have an impact on the profitability of MTIC fraud schemes involving specific commodities or services. This is particularly true for fraud schemes involving the energy sector and related commodities, which are subject to frequent price fluctuations.

UNDERSTANDING VAT FRAUD

MTIC FRAUD

Cross-border transactions within the EU are zero-rated, which means that the payment of the VAT is not due until the goods are sold at their destination. This enables traders to import goods without accounting right away for the VAT. In simple MTIC cases, fraudsters sell the goods, charge the VAT to buyers without remitting the value to the tax authorities.

More complex cases of VAT fraud are typically known as carousel frauds. As part of these fraud schemes goods are imported and sold through a series of companies before being exported again. The exporters of these goods claim and receive the reimbursement of VAT payments that never occurred.

OTHER TYPES OF FRAUD

Insurance fraud

Fraudsters defraud hundreds of millions of euros from private and public insurance providers each year. OCGs are increasingly involved in fraud schemes targeting health care systems.

In 2015, German law enforcement authorities dismantled a Russian-speaking OCG providing nursing services in order to defraud health care insurance providers.

Benefit fraud

Benefit fraud schemes cause significant financial losses for all Member States. OCGs and individual fraudsters target social and labour benefit schemes to defraud the state of regular benefit payments. Benefit fraud is strongly linked to THB and migrant smuggling.

Procurement rigging

Procurement procedures are frequently the target of corruption. Criminal groups use bribes to elicit information or directly influence the evaluation of bids in order to win public service tenders in competition with legal businesses. This type of manipulation is particularly notable in the energy, construction, information technology and waste management sectors.

EU subsidy fraud

OCGs have repeatedly attempted to defraud EU funds by submitting applications for EU grants or tenders. Typically, these applications are based on false declarations such as fraudulent progress reports as well as fraudulent documents such as fake invoices.

Loan and mortgage fraud

Fraudsters organising loan or credit fraud schemes typically rely on fraudulent documents to obtain bank loans, which are never paid back.

INTELLECTUAL PROPERTY CRIME

The infringement of intellectual property rights is a widespread phenomenon in the EU. Cheap counterfeit copies of popular goods remain highly popular with consumers. Criminals are able to produce counterfeit goods in large quantities at minimal costs and use online platforms to easily and effectively market their products internationally. Counterfeiting and piracy are terms used to describe a range of illicit activities related to Intellectual Property Rights (IPR) infringement. Most counterfeit goods infringe a trademark, which means that a good is produced without the authorisation of its rights holder. OCGs are increasingly involved in the violation of IPR.

OCGs produce a wide range of counterfeit goods and manufacture sub-standard goods distributed on EU markets including food and beverages, pesticides and pharmaceutical products. Counterfeit and sub-standard goods pose significant risks to the health and safety of consumers.

China remains the source country of most of the counterfeit goods trafficked to the EU. The trade in goods between the EU and China has expanded significantly in recent years. China is the biggest source of imports to the EU by far.

POLY-CRIMINAL OCG INVOLVED IN THE TRADE IN COUNTERFEIT GOODS AND DRUG TRAFFICKING

In 2015 and 2016, Europol supported an operation targeting an Italian OCG selling counterfeit champagne in various Member States. Investigations in Italy and Germany revealed that some of the suspects were also involved in the trafficking of cocaine. During house searches in Germany, investigators seized more than 12,000 bottles of fake champagne. The investigation also uncovered links to VAT and excise fraud.

In 2015, more than 80,000 seizures were registered by customs authorities in the EU. These shipments contained more than 40 million articles worth an estimated EUR 642 million. Cigarettes remain the most frequently seized counterfeit product accounting for 27% of all seizures, followed by other goods such as batteries or air fresheners at 10% as well as toys at 9%. Regular household items such as body care articles, medicines, electrical household goods represent 25.8% of the total number of seized counterfeit products.

Online distribution

Online marketplaces are the key distribution channel for counterfeit goods. The sales volume of counterfeit goods online has increased significantly over recent years. Counterfeiters use social media platforms to advertise their products and steer potential consumers to online sales platforms. The sale of counterfeit goods online is closely related to the increasing use of parcel and postal services to distribute counterfeit products, which is difficult to detect among an increasing flow of licit goods sold online and sent via postal freight.

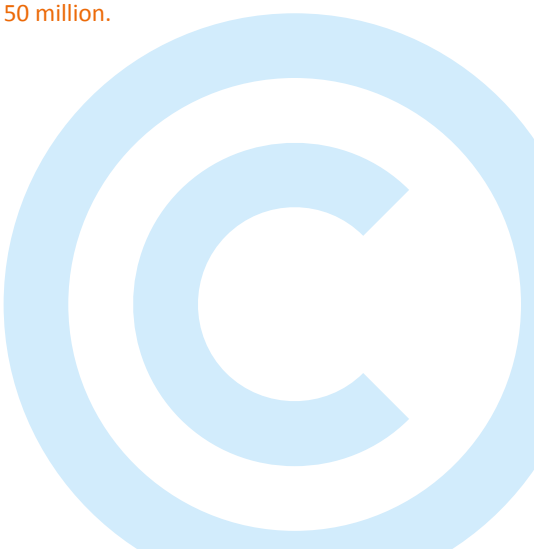
Counterfeit pharmaceuticals

While the counterfeiting of pharmaceuticals previously primarily affected lifestyle medicines, counterfeiters increasingly target almost all types of medicinal products including cancer medication and various types of medical devices.

Counterfeit goods not only cause losses in unpaid duties and taxes, but also reduce the sales volume, profits and investments of legitimate businesses. This removes incentives for investment in research, development and innovation.

Thousands of online shops are used to sell counterfeit goods. In 2016, Operation In Our Sites (IOS) resulted in the seizure of 4,780 domain names and associated online shops selling counterfeit merchandise.

The distribution of counterfeit pharmaceutical products online is particularly dangerous. In 2016, Operation Pangea IX specifically targeted online vendors of counterfeit medicines. The operation resulted in the seizure of potentially dangerous medicines worth more than EUR 50 million.



ORGANISED PROPERTY CRIME

Organised property crime encompasses a range of different criminal activities carried out predominantly by mobile OCGs operating across the EU. Organised burglaries, thefts and robberies as well as motor vehicle crime and the trafficking of cultural goods all fall into this broad category of criminal activity. However, the OCGs carrying out different types of property crime are also highly diverse. Some OCGs are highly specialised in specific types of crime or *modi operandi*, while others are active in several types of property crime and other forms of serious and organised crime. MOCGs typically operate in and predominantly target the most prosperous Member States in Western and Northern Europe. Despite the highly organised nature of MOCG operations, the organised crime involvement in property crimes remains under-investigated. In many cases, incidents of property crime are still classified as petty criminality without recognising the organised crime aspect.

Online marketplaces have made it easier to advertise and sell stolen goods. These marketplaces are now used extensively to sell stolen goods, particularly low-bulk high-value goods such as phones, tablets and other electronic equipment. Legal business structures are used extensively to fence stolen goods, often in the country of origin of the MOCGs involved in organised burglaries and thefts.

Organised burglaries and thefts

Some Member States note a steady increase in the number of reported burglaries over recent years. This increase particularly affects business premises, which are targeted much more frequently than before. Burglaries of business premises often involve intrusion into the property via the roof.

Many incidents of pickpocketing are not attributed to organised crime. However, the scale and level of organisation of pickpocketing raids across many Member States suggests that MOCGs are heavily involved.

OCGs make use of various online services to facilitate their burglaries. This includes checking on social media platforms whether individuals are away from targeted residences, scouting targeted neighbourhoods using free online navigation tools and fencing goods via online marketplaces.

In September 2015, Europol supported French, Belgian and Moldovan law enforcement authorities in disrupting the activities of a Moldovan OCG carrying out serial burglaries targeting bicycle shops. The offenders typically stole luxury bikes worth more than EUR 10,000 each. The bikes were transported from Paris to Moldova on long-distance passenger busses. The bikes were eventually sold in Ukraine as well as via online marketplaces. This OCG was highly mobile and operated with a strict division of tasks between group members.

Organised robberies

MOCGs are increasingly targeting commercial premises for armed robberies, which typically have less sophisticated security measures in place. Attacks on banks and other cash-intensive businesses have declined notably in recent years due to the security measures put into place at their locations.

Jewellery stores and other businesses selling highly valuable and compact goods remain popular targets for armed robbers using various methods of attack including smash and grab.

LOGICAL ATTACKS ON ATMS

As part of a new modus operandi, attackers drill or burn small holes into the ATM case in order to reach the ATM's computer hardware components. The attackers use this access to intrude into the ATM's operating system and force it to dispense cash.

Motor vehicle crime

The theft and fraudulent acquisition of motor vehicles remains a lucrative business for the various OCGs involved in this criminal activity. Some OCGs steal specific vehicles to order for clients based in destination countries. While the overall number of stolen vehicles appears to have remained stable in many Member States over recent years, the number of recovered vehicles has dropped considerably across several Member States. This trend likely indicates a further shift from individual offenders to the involvement of more professional OCGs.

ELECTRONIC COMPROMISE

OCGs involved in the theft of motor vehicles increasingly rely on high-tech tools to gain access to vehicles and to overcome security measures. Information on how to overcome car security systems can be easily found on online messaging boards and websites. In many cases, the tools used for electronic compromise are readily available to order online and often originate from China.

Some OCGs steal cars as part of burglaries and home jacking attempts. MOCGs target residential homes with high-value cars parked outside, breaking and entering these premises to retrieve the original car keys and steal the vehicle. Vehicle theft is intimately linked to document fraud. OCGs use fraudulent documents to give stolen cars new identities for registration or exportation purposes.

OCGs increasingly rely on technical tools and expertise to overcome new vehicle security measures.

The trade in spare parts is increasingly taking place on online marketplaces. OCGs have adapted to this and now rely on these platforms to sell the cannibalised spare parts from stolen vehicles.

Cultural goods trafficking

The conflicts in Libya, Syria and Iraq are thought to have resulted in the intensified trafficking of cultural goods from this region to the EU. This trend is expected to continue due to persistent instability in the region and the lack of law enforcement resources to prevent or intercept trafficking activities in origin and transit countries. A small portion of the funds generated by cultural goods trafficking in the Middle East and North Africa region could potentially be used to support terrorist organisations. However, the profits achieved from cultural goods trafficking for these organisations are thought to be low compared to other revenue streams.

WAR CRIMES

In some cases, the destruction, removal and trafficking of cultural goods in the context of an armed conflict can amount to a war crime. Significant cultural goods are protected by international law. International humanitarian law and international criminal law have established various forms of attack against cultural property as war crimes. Activities related to the destruction or trafficking of cultural goods amounting to war crimes potentially have an impact on the EU. The deliberate destruction of archaeological and cultural heritage in Palmyra as well as other places in Syria and Iraq could potentially be considered a war crime according to the Rome Statute of the International Criminal Court.[27] Subsequently, law enforcement authorities seized cultural goods originating from Palmyra and trafficked to Europe.

3,561 ARTEFACTS SEIZED IN OPERATION PANDORA[28]

In January 2017, Europol joined forces with law enforcement authorities from 18 countries, Interpol, the United Nations Educational, Scientific and Cultural Organization (UNESCO), and the World Customs Organization (WCO) to tackle the theft and illicit trafficking of cultural goods.

Operation Pandora was successfully led by Cypriot and Spanish police:

- 3,561 works of art and cultural goods were seized, almost half of which were archaeological objects; 500 archaeological objects were found in Murcia, Spain, of which 19 were stolen in 2014 from the Archaeological Museum in Murcia;
- over 400 coins from different periods were seized following investigations into suspicious online advertisements.

Several of the retrieved artefacts are of great cultural importance in the archaeological world, such as a marble Ottoman tombstone and a post-Byzantine icon depicting Saint George, along with two Byzantine artefacts. All of them were seized in Greece during actions carried out by the Hellenic Police.

The illegal online trade in cultural goods is expanding.

PEOPLE AS A COMMODITY

MIGRANT SMUGGLING

Migrant smuggling has emerged as a highly profitable and widespread criminal activity for organised crime in the EU. The migrant smuggling business is now a large, profitable and sophisticated criminal market, comparable to the European drug markets.

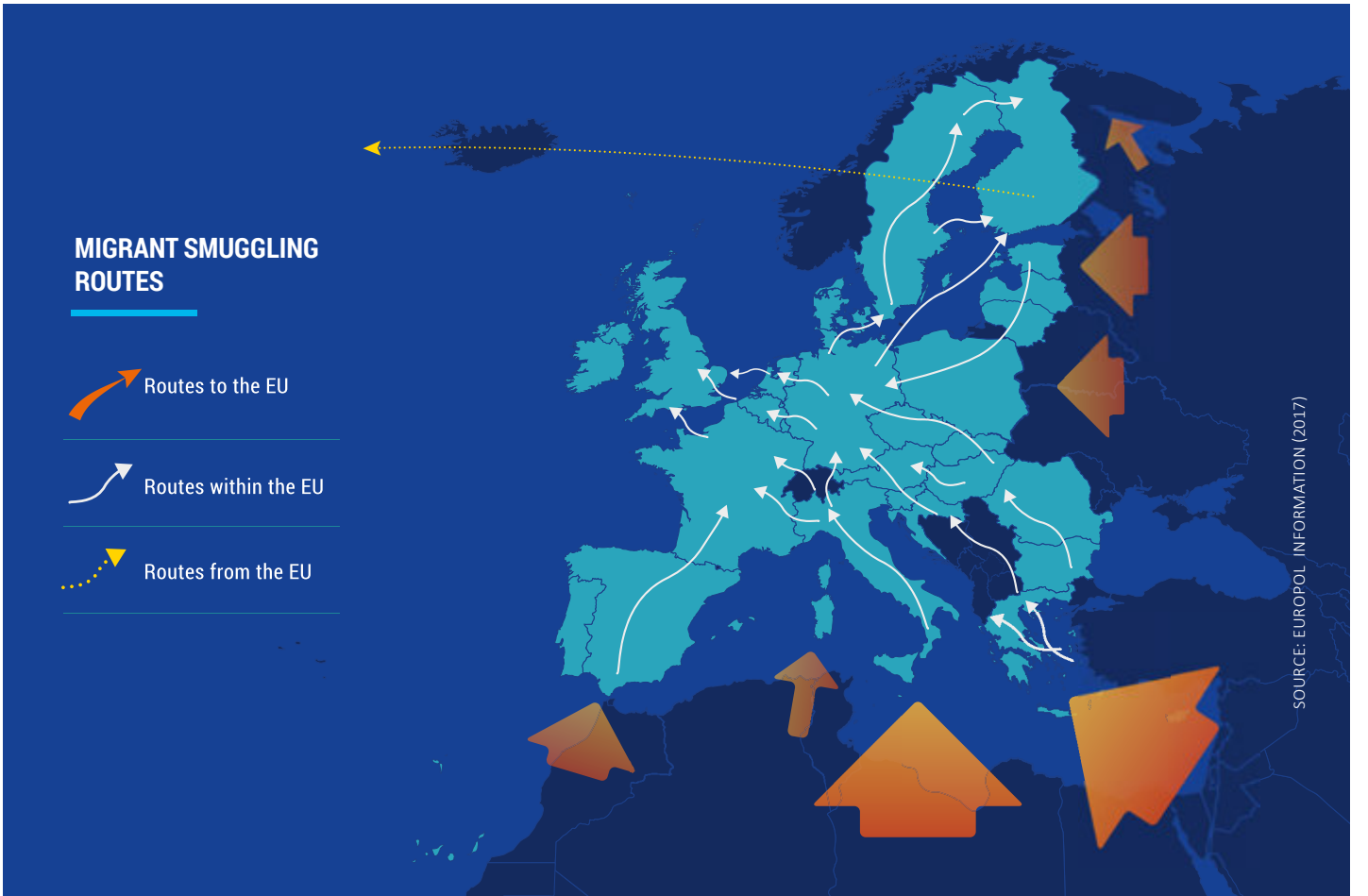
The demand for and supply of smuggling services has grown significantly since 2014. More than 510,000 illegal border crossings between border-crossing points at the external border of the EU were registered in 2016.[29] This is a substantial decrease compared to 2015, when over one million irregular migrants entered the EU on the Eastern Mediterranean and Central Mediterranean routes.[30] Nearly all of the irregular migrants arriving in the EU along these routes use the services offered by criminal networks at some point during their journeys.

During 2016, 1,234,558 applications for asylum were recorded in the EU. In 2015, the European Asylum Support Office (EASO) reported just over 295,000 positive decisions on asylum applications by Member States.[31] This means that a large number of irregular migrants who did not apply for asylum or whose applications were rejected may attempt to stay illegally in the EU.

In addition to the transportation of migrants, document fraud has emerged as a key criminal activity linked to the migration crisis. The provision of fraudulent documents will continue to represent a substantial threat to the security of the EU. Fraudulent documents are used and can be re-used for many different criminal offences.

Armed conflicts, economic and population pressures in Africa and the Middle East will continue to act as the main push factors for irregular migrants travelling to the EU. Migrant smuggling to and within the EU will remain a key criminal threat.

The number of unaccompanied minors present in the EU has increased significantly in recent years as a result of the migration crisis. This group is very vulnerable to all types of exploitation.



Migrant smuggling – a daily business

In 2015, migrant smuggling networks offering facilitation services to reach or move within the EU generated an estimated EUR 4.7 billion to EUR 5.7 billion in profit. These profits have seen a sharp decline in 2016, dropping by nearly EUR 2 billion between 2015 and 2016. This development is in line with the overall decrease in the number of irregular migrants arriving in the EU and as a result of a fall in the prices for migrant smuggling services following the peak of the migration crisis in 2015.

OCGs involved in migrant smuggling display an unprecedented level of organisation and coordination. While established smuggling *modi operandi* remain unchanged, migrant smugglers have shown great versatility in the means of transport, concealment methods and technologies they use.

Migrant smuggling is a multi-national business. Migrant smugglers originating from over 122 countries are involved in facilitating the journeys of irregular migrants to the EU. Most migrant smuggling networks are composed of various nationalities involving both EU and non-EU nationals.

Migrant smuggling networks heavily rely on social media to advertise smuggling services. Migrant smugglers make use of ride-sharing applications and P2P accommodation platforms to provide a cover for their smuggling activities. This leaves regular users at the risk of inadvertently becoming facilitators by unknowingly transporting or hosting irregular migrants.

Migrant smuggling is a highly profitable criminal activity featuring sustained high levels of demand and relatively low levels of risk. Some OCGs previously involved in other criminal activities such as the illegal trade in excise goods, drug trafficking or organised property crime have added migrant smuggling to their portfolio of criminal activities. Migrant smuggling does not require access to significant resources and OCGs can rely on their existing knowledge of routes and infrastructure used to smuggle goods across borders. The distinction between legal and illegal activities is increasingly blurred. Individual criminal entrepreneurs can step in and out of criminal activities by providing ad hoc services, especially taxi and truck drivers.

OPERATION DAIDALOS

In March 2015, Operation Daidalos targeted a criminal group smuggling irregular migrants from Greece to other Member States which was involved in the production and distribution of forged travel documents. In addition to providing these documents to irregular migrants, the group also sold these to other OCGs. The criminal network operated primarily in Greece.

Illegal but not undocumented – document and identity fraud

Service packages offered by migrant smugglers now frequently include the provision of fraudulent travel and identity documents. Fraudulent documents allow irregular migrants to enter and move within the EU as well as to change from irregular to legalised residence status under false pretences or by using fake identities. Migrant smuggling networks are increasingly offering tailor-made facilitation services including high-quality fraudulent documents.

The abuse of genuine passports by look-alikes continues to be the main modus operandi used by document fraudsters. ID cards are the most commonly detected document used as part of document fraud. In 2015, they accounted for 50% of all detections in the EU. In 2016, more than 7,000 people were detected with fraudulent documents on entry at the external borders of the EU.[32]

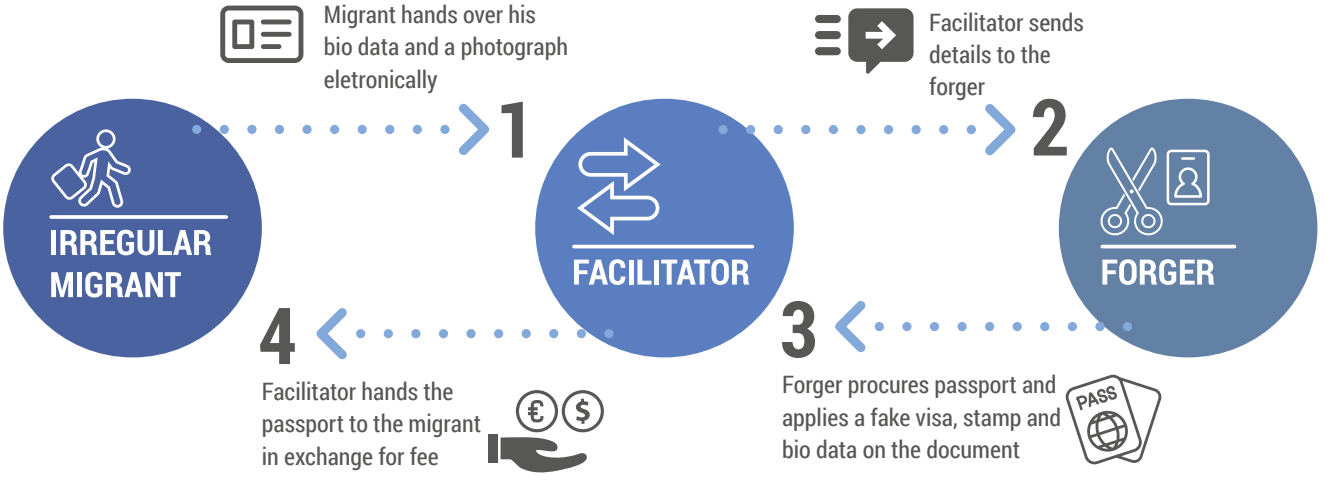
An emerging market

Both the quantity and the quality of fraudulent documents circulating in the EU have increased. The sustained increase in demand for fraudulent documents has prompted established counterfeiters to increase their production output and establish new print shops.

Abuse of legal channels

Migrant smugglers frequently abuse legal channels to facilitate the entry of irregular migrants to the EU or to legalise their stay. The abuse of legal channels involves a variety of *modi operandi* including sham marriages, bogus paternity, false employment contracts, fake invitation letters, false medical visas, and false claims of being victims of trafficking or refugees.

BUSINESS MODEL
Supply of fraudulent documents



▲ **The demand for smuggling services has grown significantly since 2014.**

▲ **Migrant smuggling to and within the EU will remain a key criminal threat.**

FACILITATION SERVICES

Migrant smuggling networks offer their services including transportation, accommodation, the provision of fraudulent documents and information on contact points in other countries.

TRANSPORTATION & ACCOMMODATION

Migrant smugglers pass irregular migrants from one network to another along the route of the migrants' journey.

EU suspects typically work as drivers transporting irregular migrants within the EU to destination countries.

COMMUNICATION VIA SOCIAL MEDIA

Migrant smugglers widely rely on social media and use online platforms such as ride-sharing websites, or P2P accommodation platforms, to arrange facilitation services.

DOCUMENT FRAUD

Document fraud has emerged as a key criminal activity linked to the migration crisis.

TRAFFICKING IN HUMAN BEINGS (THB)

THB for sexual and labour exploitation includes the recruitment, transportation, harbouring and exploitation of victims. OCGs involved in THB typically operate in independent cells that deal with the various stages of recruitment, transport and exploitation.

Traffickers rely heavily on document fraud to enable their trafficking activities. This includes the use of fraudulent identity, travel and breeder documents as well as the abuse of legal channels such as the EU visa regime for tourism, study and work visas. OCGs involved in THB also continue to exploit asylum provisions in order to traffic non-EU nationals into the EU. On many occasions, victims are provided with fraudulent documents to conceal their real identity and age.

THB for sexual exploitation

The sexual exploitation of EU nationals no longer relies predominantly on the use of violence and coercion towards victims. Some OCGs are increasingly relying on threats of violence towards victims and their families rather than attacking the victim. Victims originating from outside the EU are still routinely subjected to violence, debt bondage, passport confiscation and other forms of coercion as an integral part of trafficking *modi operandi.*

THB for labour exploitation

The involvement of OCGs in THB for labour exploitation is increasing in the EU. OCGs cater to the growing demand for cheap labour across many Member States and have access to a large number of potential victims. THB for labour exploitation threatens to infiltrate the legal economy, where it lowers wages and hampers economic growth.

THE BUSINESS MODEL

There has been little change in the types of industries featuring labour exploitation. Traffickers continue to target less regulated industries as well as those featuring seasonal demand for workers. Vulnerable sectors include agriculture, catering, cleaning, construction, entertainment, fishing, hospitality, retail and transportation.

Traffickers take advantage of discrepancies in labour legislation to organise the exploitation of victims in the grey zone between legal employment and labour exploitation. Some victims receive wages equivalent to the minimum standard in their countries of origin.

However, these are far below acceptable salaries in countries of exploitation where they do not have sufficient resources to cover their living expenses. These wage dumping practices seriously undermine the legal labour market in countries of destination and make it difficult for victims of labour exploitation to be recognised as such.

The trafficking of victims within the EU remains a key threat.

The migration crisis has resulted in an increase in the number of potential victims of THB. A growing number of vulnerable adults and unaccompanied minors in the EU are likely to be targeted by traffickers.

CRIMINAL GANG ACCUSED OF TRAFFICKING OVER 150 WOMEN INTO PROSTITUTION DISMANTLED BY AUSTRIA[33]

In November 2016, Austrian law enforcement authorities with the support of Europol dismantled a Chinese OCG involved in the trafficking of up to 300 women. Victims were lured to Austria on promises of work as nannies or masseuses. They were provided with forged documents and brought to Austria illegally. Upon their arrival in Vienna, OCG members took away the victims' IDs. The women were placed in so-called "sex studios" owned by the OCG and forced to work as prostitutes. After a few weeks they were transferred to other brothels in Austria.

Trafficking of underage victims

Traffickers often specifically target underage victims, both male and female, to sexually exploit them. The exploitation of underage victims is not always motivated by financial profit. In some cases, underage victims are trafficked for the purpose of producing CSEM, which is traded on online platforms.

TRAFFICKING VICTIMS FORCED INTO CRIMINALITY[34]

In November 2016, a Spanish investigation supported by Europol resulted in the arrest of 16 suspected traffickers and the rescue of nine minors. The OCG trafficked young women and forced them into pickpocketing in various Member States. The victims were initially lured to Spain and travelled there using counterfeit documents. In Spain, the traffickers trained the victims in pickpocketing techniques and forced them to commit thefts in crowded areas and on public transport. The OCG shared family ties and was hierarchically structured operating in smaller groups in different European cities. The larger criminal network was mainly composed of nationals from Bosnia and Herzegovina and traded the victims from one group to another for an estimated EUR 5,000 each.

LABOUR EXPLOITATION

▲ THB for labour exploitation is increasing in the EU.

Traffickers continue to target less regulated industries as well as those featuring seasonal demand for workers.

SEXUAL EXPLOITATION

The traditional trafficking flow from Eastern Europe to Western Europe has been replaced by multiple and diverse flows of victims all over the EU.

▲ OCGs have further increased the use of legal businesses that can conceal exploitations such as hotels, nightclubs and massage parlours.

CHILD TRAFFICKING

Traffickers often specifically target underage victims, both male and female, to sexually exploit them.

Traffickers continue to rely on the use of social media, Voice-over-IP (VoIP) and instant messaging applications at all stages of the trafficking cycle.

Links between migrant smuggling and trafficking in human beings

OCGs involved in THB often exploit existing migratory routes to traffic victims within the EU. While the migration crisis has not yet had a widespread impact on THB for labour exploitation in the EU, some investigations show that traffickers are increasingly targeting irregular migrants and asylum seekers in the EU for exploitation. Irregular migrants in the EU represent a large pool of potential victims susceptible to promises of work even if this entails exploitation.

SHAM MARRIAGES

There has been an increasing number of reports of incidents of sham marriages in several Member States. This increase is likely related to the migration crisis and an increase in the number of irregular migrants seeking to transition to legal residence status after failed asylum applications.

MIGRANT SMUGGLING AND HUMAN TRAFFICKING RING OPERATING VIA THE MEDITERRANEAN[35]

In November 2015, a joint operation between Spanish and Polish law enforcement authorities, coordinated by Europol, revealed the operation of a migrant smuggling network exploiting irregular migrants from Pakistan in restaurants in Spain. Irregular migrants were forced to work long hours in appalling conditions without salary, holiday or social security to repay their debts to smugglers for the travel and provision of fraudulent documents. The migrant smugglers used the criminal proceeds to invest in new restaurants, which were also used for the exploitation of irregular migrants.

SPORTS CORRUPTION

Criminal networks use match-fixing to manipulate the outcomes of sports matches, which skews betting odds and allows them to generate significant profits. Match-fixing in the EU primarily affects football games. However, match-fixers are also targeting tennis, snooker and dart competitions.

In some cases OCGs have infiltrated sporting clubs in order to orchestrate money laundering schemes.

FOOTBALL AND MONEY LAUNDERING

In May 2016, as part of Operation Matrioskas, law enforcement authorities dismantled a Russian-speaking OCG which had infiltrated football clubs and laundered several million euros across the EU. The OCG used middlemen to purchase football clubs experiencing financial pressure. The group was able to conceal their money laundering activities among the large financial transactions and cross-border money flows, which are not unusual for professional football clubs. Weak governance allowed the OCG to use the clubs to launder money by over- or under-valuating players on the transfer market as well as by accepting bids for television rights deals.

TRAFFICKING OF FIREARMS

The proliferation and availability of illegal firearms in the Member States increases the risk of their use by terrorist groups to carry out attacks in the EU.

Illegal firearms are increasingly accessible due to their availability online.

Recent terrorist attacks in the EU carried out by jihadist terrorists using trafficked firearms have demonstrated the lethal consequences of the trade in illicit firearms. Several incidents of violent clashes between criminal gangs have highlighted that the use of illegal firearms remains a significant threat to EU citizens.

ONLINE TRADE

Firearms are frequently traded on online platforms including Darknet marketplaces. Both individual criminals and OCGs obtain illegal firearms via online marketplaces. This development has resulted in a significant increase in the use of parcel and postal services to traffic firearms and firearm components.

Online trade allows individuals with no or limited connections to organised crime to procure firearms. These individual criminal actors increasingly engage in the trafficking of firearms and firearm components as part of a CaaS business model and have emerged as key distributors of illegal firearms in the EU. The online trade in illegal firearms via various platforms is set to expand further over the coming years.

DIVERSION FROM LEGAL SUPPLY

Firearms traffickers are highly adept at exploiting legal loopholes and differences in regulatory regimes between Member States to divert firearms from legal suppliers. The reactivation of deactivated weapons and conversion of blank-firing firearms are among the main sources of illegal firearms trafficked in the EU. Firearms traffickers often convert blank-firing firearms or reactivate deactivated firearms purchased from legal dealers based in countries applying less stringent acquisition rules such as more permissive licensing and registration requirements.

Various conflict zones in the periphery of the EU have the potential to emerge as major sources of firearms trafficked to the EU.

In June 2016, Italian law enforcement authorities arrested two members of the mafia clan 'Ceusi' on charges of firearms trafficking. The suspects had purchased over 160 decommissioned firearms from Slovakia. Some of the firearms were reactivated and sent to Malta in parcels. The Italian OCG maintained links with Egyptian OCGs involved in migrant smuggling activities.[36]

Using post and parcel services is now the most common way of trafficking firearms in the EU.

LINKS BETWEEN SERIOUS AND ORGANISED CRIME AND TERRORISM

Terrorism and the groups carrying out terrorist offences have evolved significantly over the last decade. The EU has been the target of repeated terror attacks and plots in recent years. The investigations into the terrorist attacks in Brussels and Paris, carried out in March 2016 and November 2015 respectively, uncovered the involvement of some of the perpetrators in different types of serious and organised crime including the trafficking of illicit drugs, as well as personal contacts with criminal groups involved in the trafficking of firearms and production of fraudulent documents.

Recent investigations have revealed that terrorist groups have made use of migrant smuggling networks to allow their operatives to enter the EU. However, these cases do not suggest that terrorist groups maintain sustained engagement with OCGs involved in migrant smuggling.

The profit-driven nature of organised crime activities is in many cases incompatible with terrorist acts, which attract a great degree of media and law enforcement attention to the perpetrators.

The pursuit of criminal activities in support of terrorist activities is not a new phenomenon. However, the involvement of suspects with extensive criminal backgrounds and access to the resources and tools of organised crime networks in terrorism is particularly threatening in light of the fast pace of radicalisation and willingness to very quickly engage in terrorist attacks following the beginning of the radicalisation process.

The threat emanating from links between serious and organised crime and terrorism is two-fold. Firstly, the potential exploitation of OCG infrastructures to procure tools, such as firearms or fraudulent documents, and move goods and people may deliver lethal weapons used in attacks in the EU to terrorist groups. Secondly, involvement in serious and organised crime may allow terrorist actors to generate funds to finance terrorism-related activities.

The suspects are involved in various crime areas including money laundering, migrant smuggling, heroin and firearms trafficking, organised property crime and THB. These suspects are typically involved at a low level in organised crime and do not fill major roles within organised crime networks.

CONCLUSIONS

Tackling organised crime in the age of technology

Serious and organised crime is a key threat to the security of the EU. Criminal groups and individual criminals continue to generate multi-billion euro profits from their activities in the EU each year. Some parts of the serious and organised crime landscape in the EU have changed drastically in recent years - in large part due to advancements in technology that have had a profound impact on the wider society and economy.

Technology is a key component of most, if not all, criminal activities carried out by organised crime groups in the EU and has afforded organised crime with an unprecedented degree of flexibility. This flexibility is particularly apparent in the ease with which criminals adapt to changes in society.

The internet, the multitude of online platforms and communication channels it hosts have had a huge impact on society, strengthening and transforming the economy, driving innovation and shaping social interaction. However, it is also a key enabler of criminal activity and plays a role in all types of criminality.

The impact of technology on crime, however, extends beyond the internet and involves all kinds of technical innovation such as advances in drone technology, automated logistics, and advanced printing technologies.

The role of the SOCTA

The vital role of technology for organised crime is reflected in the data collected and analysed for the SOCTA 2017. For the SOCTA 2017, Europol has undertaken the largest-ever data collection on serious and organised crime in the EU.

Europol relied on more than 2,300 questionnaires contributed by Member States, Europol's operational and strategic partners outside the EU and our institutional partners as well as operational intelligence held in Europol's databases to produce the most detailed assessment of the nature and scale of criminal threats facing the EU and its Member States yet.

Based on an in-depth analysis of this data and a methodology endorsed by the Member States, Europol identifies the key threats from serious and organised crime facing the EU today and over the coming years.

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. In addition to five specific criminal activities carried out by organised crime in the EU, Europol is also recommending to focus on three cross-cutting threats that enable or enhance all types of serious and organised crime.

SPECIFIC PRIORITY CRIME THREATS:

- Cybercrime
- Drug production, trafficking and distribution
- Migrant smuggling
- Organised property crime
- Trafficking in human beings

CROSS-CUTTING PRIORITY CRIME THREATS:

- Criminal finances and money laundering
- Document fraud
- Online trade in illicit goods and services

<table>
<tr><th>CRIME AREAS</th><th>Currency counterfeiting</th><th>CYBERCRIME</th><th>DRUG TRAFFICKING</th><th>Environmental crime</th><th>Fraud</th><th>Intellectual property crime</th><th>ORGANISED PROPERTY CRIME</th><th>MIGRANT SMUGGLING</th><th>Trafficking of firearms</th><th>TRAFFICKING IN HUMAN BEINGS</th></tr>
<tr><td rowspan="8">THREATS</td><td rowspan="4">Production</td><td>Online child sexual exploitation</td><td>Synthetic drugs production in the EU</td><td rowspan="3">Illicit waste trafficking</td><td>Excise fraud</td><td rowspan="2">Online trade in counterfeit goods</td><td rowspan="2">Burglaries and theft</td><td rowspan="2">External borders of the EU</td><td rowspan="3">Online trade (including de/reactiva-tion)</td><td>Labour exploitation</td></tr>
<tr><td rowspan="3">Cyber-dependent crime (malware, cryptoware, etc.)</td><td>Trafficking of precursors and pre-precursors</td><td rowspan="2">MTIC fraud</td><td rowspan="2">Sexual exploitation</td></tr>
<tr><td rowspan="4">Import of cocaine to the EU via major ports and couriers</td><td rowspan="3">Production of counterfeit goods in the EU</td><td rowspan="3">Motorvehicle crime</td><td rowspan="3">Secondary movements</td></tr>
<tr><td rowspan="4">Distribution including online</td><td rowspan="4">Trafficking of endangered species</td><td rowspan="2">Investment fraud</td><td rowspan="3">Traditional trafficking</td></tr>
<tr><td rowspan="2">Payment card fraud (card-not-present fraud)</td><td>Poly-drug trafficking in the EU</td><td>Trafficking of counterfeit goods (not online) in the EU</td><td>Organised robberies</td><td>Risk for labour exploitation</td><td>Child trafficking</td></tr>
<tr><td>Large-scale cannabis production and trafficking in the EU</td><td>Sports corruption</td></tr>
<tr><td rowspan="6">CROSS-CUTTING CRIME THREATS</td><td colspan="10">Corruption</td></tr>
<tr><td colspan="10">Countermeasures against law enforcement</td></tr>
<tr><td colspan="10">Criminal finances and money laundering</td></tr>
<tr><td colspan="10">Document fraud, including identity fraud</td></tr>
<tr><td colspan="10">Extortion</td></tr>
<tr><td colspan="10">Online trade in illicit goods (firearms, counterfeit goods, drugs)</td></tr>
</table>

HIGH THREAT THREAT

ANNEX

LIST OF ABBREVIATIONS

ATM	Automated teller machine
AWF SOC	Analysis Work File on Serious and Organised Crime
CaaS	Crime-as-a-Service
CNP	Card-not-present
COSI	Standing Committee on Operational Cooperation on Internal Security
CP	Card-present
CSE	Child Sexual Exploitation
CSEM	Child Sexual Exploitation Material
DDoS	Distributed denial of service
EASO	European Asylum Support Office
ECB	European Central Bank
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMCS	Excise Movement and Control System
EU	European Union
IPR	Intellectual Property Rights
LDCA	Long-distance child abuse
MDMA	3,4-methylenedioxy-methamphetamine
MOCG	Mobile organised crime group
MTIC	Missing Trader Intra Community
NFC	Near Field Communication
NPS	New Psychoactive Substances
OCG	Organised crime group
P2P	Peer-to-peer
POS	Point of Sale
SEPA	Single Euro Payments Area
SOCTA	Serious and Organised Crime Threat Assessment
THB	Trafficking in Human Beings
TOR	The Onion Router
VAT	Value Added Tax

REFERENCES

[1]Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), accessible at https://www.europol.europa.eu/publications-documents/council-decision-of-6-april-2009-establishing-european-police-office-europol

[2]Council Document 12159/12, Serious and Organised Crime Threat Assessment (SOCTA). Methodology (04/07/2012), accessible at http://data.consilium.europa.eu/doc/document/ST-12159-2012-INIT/en/pdf

[3]Europol 2015, Large Chinese money laundering network dismantled (12/05/2015), accessible at https://www.europol.europa.eu/newsroom/news/large-chinese-money-laundering-network-dismantled

[4]Europol and Eurojust 2016, Hawala money laundering ring dismantled by Joint Investigation Team (29/11/ 2016), accessible at https://www.europol.europa.eu/newsroom/news/hawala-money-laundering-ring-dismantled-joint-investigation-team

[5]Europol 2016, Iraqi money laundering syndicate based in Germany dismantled with support of Europol and Eurojust (31/03/2016), accessible at https://www.europol.europa.eu/newsroom/news/iraqi-money-laundering-syndicate-based-in-germany-dismantled-support-europol-and-eurojust

[6]Europol 2016, Dozens arrested for massive document forgery and migrants smuggling (31/05/2016), accessible at https://www.europol.europa.eu/newsroom/news/dozens-arrested-for-massive-document-forgery-and-migrant-smuggling

[7]https://metrics.torproject.org

[8]D. Moore and T. Rid 2015, Cryptopolitik and the Darknet, p. 21

[9]Europol 2016, Internet Organised Crime Threat Assessment (IOCTA) 2016, p.47

[10]Europol 2016, Darknet arms vendors arrested in Slovenia with support of Europol (20/12/2016), available at https://www.europol.europa.eu/newsroom/news/darknet-arms-vendor-arrested-in-slovenia-support-of-europol

[11]Carnegie Mellon University 2015, Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, available at https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf

[12]Europol 2016, Internet Organised Crime Threat Assessment (IOCTA) 2016, p.49

[13]In 2014, Europol published a report on the future of serious and organised crime "Exploring tomorrow's organised crime", which highlighted key drivers for change which have an impact on serious and organised crime in the EU. The report is available on Europol's website at https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime

[14]European Central Bank 2016, Annual Report 2015, p. 76

[15]Europol 2016, 'Avalanche' network dismantled in international cyber operation (01/12/2016), accessible at https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

[16]Symantec 2016, Internet Security Threat Report, p.54

[17]Europol 2016, Internet Organised Crime Threat Assessment (IOCTA) 2016, p.36-37

[18]Verizon 2016, 2016 Data Breach Investigation Report, p.4

[19]Europol 2016, Internet Organised Crime Threat Assessment (IOCTA) 2016, p.24

[20]Europol 2016, International criminal network behind large-scale payment fraud dismantled (07/09/2016), accessible at https://www.europol.europa.eu/newsroom/news/international-criminal-network-behind-large-scale-payment-fraud-dismantled

[21]Europol 2016, Global action against airline fraudsters (19/10/2016), accessible at https://www.europol.europa.eu/newsroom/news/global-action-against-airline-fraudsters-193-detained

[22]EMCDDA & Europol 2016, EU Drug Markets Report 2016, p. 23

[23]EMCDDA & Europol 2016, EU Drug Markets Report 2016, p. 60

[24]Europol 2016, 'Rose of the Winds' – International operation against drug trafficking (01/12/20160, accessible at https://www.europol.europa.eu/newsroom/news/%E2%80%98rose-of-winds%E2%80%99-%E2%80%93-international-operation-against-drug-trafficking

[25]ABC News 2014, Six charged after drug bust which seized 2.8 tonnes of MDMA and methamphetamine worth $1.5 billion (29/11/2014), accessible at http://www.abc.net.au/news/2014-11-29/six-charged-over-enormous-$1.5b-drug-bust/5927904

[26]BBC 2015, Gang guilty over £600,000 phone scam against pensioners (10/12/2015), accessible at http://www.bbc.com/news/uk-35064360

[27]European Parliament 2015, Parliamentary questions: Answer given by Vice-President Mogherini on behalf of the Commission (22/09/2015), accessible at http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2015-008402&language=EN

[28]Europol 2016, 3561 artefacts seized in Operation Pandora (23/01/2017), accessible at https://www.europol.europa.eu/newsroom/news/3561-artefacts-seized-in-operation-pandora

[29]Frontex 2017, Risk Analysis for 2017

[30]UNHCR 2015, Over one million sea arrivals reach Europe in 2015, accessible at http://www.unhcr.org/news/latest/2015/12/5683d0b56/million-sea-arrivals-reach-europe-2015.html

[31]EASO 2015, Latest Asylum Trends – 2015 Overview, accessible at https://www.easo.europa.eu/sites/default/files/public/LatestAsylumTrends20151.pdf

[32]Frontex 2017, Risk Analysis for 2017

[33]Europol 2016, Crime gang accused of trafficking over 150 women into prostitution dismantled by Austria (17/11/2016), available at: https://www.europol.europa.eu/newsroom/news/crime-gang-accused-of-trafficking-over-150-women-prostitution-dismantled-austria

[34]Europol 2016, Europol teams up with Spanish authorities to bring down human trafficking network (29/11/2016), available at https://www.europol.europa.eu/newsroom/news/europol-teams-spanish-authorities-to-bring-down-human-trafficking-network

[35]Europol 2015, Hit on migrant smuggling and human trafficking ring operating via the Mediterranean (03/11/2015), available at: https://www.europol.europa.eu/newsroom/news/hit-migrant-smuggling-and-human-trafficking-ring-operating-mediterranean;

[36]Europol 2016, Weapons smugglers arrested in Italy with the support of Europol (09/06/2016), accessible at https://www.europol.europa.eu/newsroom/news/weapon-smugglers-arrested-in-italy-support-of-europol

ISBN 978-92-95200-77-7
DOI 10.2813/114730
QL-04-17-236-EN-N

EUROPEAN UNION

SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

SOCTA 2017

EUROPOL

Eisenhowerlaan 73, 2517 KK
The Hague, the Netherlands

www.europol.europa.eu
Follow us