Abstract
Europol used 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, 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 the trafficking in human beings (THB). In addition, Europol recommends focusing 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. SOCTA 2017 also explores potential links between serious and organised crime and terrorism. The European Justice and Home Affairs Council will decide on the EU crime priorities at its meeting of June 2017.

Key words:
Organised crime, Europol, policy cycle, crime priorities, Justice and Home Affairs
Introduction

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 (1). 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. In March this year the second edition of SOCTA was presented, following its inaugural edition released in 2013. 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 4 years. 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.

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 (2) endorsed by the Member States, Europol identifies the key threats from serious and organised crime facing the EU today and over the coming years.

The article below provides an overview of the main threats from serious and organised crime to the EU.

---

1 The EU Policy Cycle for Serious and Organised Crime in the EU 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 4 years and optimises coordination and cooperation on the crime priorities agreed by all Member States.

2 As part of an iterative process, the SOCTA Methodology is continuously reviewed 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. SOCTA analyses and describes criminal markets and crime areas in the EU; the criminal groups 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. The SOCTA Methodology was also reviewed by an academic advisory group.
Serious and organised crime in the EU

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 then also a key component of most, if not all, criminal activities carried out by criminal 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 vital role of technology for organised crime is clearly reflected in SOCTA 2017.

Criminal groups

Criminal groups are as varied as the markets they service and the activities they engage in. In many cases, criminal groups 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.

The criminal groups and individual criminals operating in the EU are highly diverse. They range from large ‘traditional’ criminal groups to smaller groups and loose networks supported by individual criminals, who are hired and collaborate ad hoc. More than 5 000 criminal groups 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 criminal groups 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 criminal groups operating internationally highlights the substantial scope and potential impact of serious and organised crime on the EU.

The diversity of the criminal actors operating in the EU is also reflected in the structures of the criminal groups. 30 % to 40 % of the criminal groups 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. 76% of the criminal groups reported to Europol for SOCTA 2017 are composed of six or more members. The fragmentation of the serious and organised crime landscape and the emergence of more groups and looser networks detailed in SOCTA 2013 did not affect all criminal markets. The fragmentation of criminal markets was particularly pronounced in relation to highly cyber-dependent criminal activities. This includes the large-scale online trade in counterfeit goods, firearms and some illicit drugs as well as different types of fraud such as card-not-present fraud. 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 Crime-as-a-Service (CaaS). However, the majority of international criminal groups in the EU are hierarchically structured.

**Poly-criminality**

45% of the criminal groups 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. During the migration crisis, the sustained high level of demand for smuggling services prompted many criminal groups previously involved in other criminal activities to expand their crime portfolio and become involved in the smuggling of migrants. Also the criminal groups 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. Poly-criminal groups most frequently combine the trafficking of cannabis and cocaine.

**Criminal activities**

More than one third of the criminal groups active in the EU are involved in the production, trafficking or distribution of drugs. The trafficking and distribution of cocaine and cannabis attract the largest number of criminal groups compared to other illicit drugs traded in the EU. The synthetic drugs market in the EU continues to expand, driven by large-scale production in the EU and the exportation of various substances to destinations worldwide. Other key criminal activities for criminal groups in the EU include organised property crime, migrant smuggling, THB and excise fraud.
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. Cybercrime encompasses a broad range of different criminal threats. However, the most threatening aspects of cybercrime involve various types of cyber-dependent crime such as the distribution of ransomware and malware, card-not-present fraud and the online trade in child sexual exploitation material.

The mature CaaS model underpinning cybercrime provides easy access to tools and services across the entire spectrum of cyber-criminality, from entry-level to top-tier players, or any other party, including those with other motivations such as hacktivists or even terrorists. 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, although ransomware has become the leading malware in terms of threat and impact. 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.

While neither offline nor online child sexual exploitation meet the criteria to be considered ‘organised crime’ this is still considered a high priority crime within the Member States due to the degree of physical and psychological damage to one of society’s most vulnerable groups — children. 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 are a growing number of forums on the Darknet dedicated specifically to the production, sharing and distribution of child sexual exploitation material.
Cybercrime is widespread and risks causing a loss of confidence in online business and/or electronic payments, which are vital for digital economies. The immediate impact of cyber-dependent crime involves the damage and destruction of data, direct financial loss, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. Payment card fraud results in substantial and direct financial losses.

Cybercrime continues to expand in scope and impact. Digital economies and societies are an attractive target for cybercriminals. Technological innovation holds exciting prospects for businesses and citizens alike, but also creates new attack vectors for those criminals seeking to capitalise on these developments. 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. Cybercrime will remain a key threat for the foreseeable future.

**Drug production, trafficking and distribution**

The market for drugs remains the largest criminal market in the EU. 45% of the criminal groups active in the EU are involved in the production, trafficking or distribution of various types of drugs across Member States. The trade in drugs generates multi-billion euro profits for the groups involved in this criminal activity. The immense profits generated from the trade in drugs fund various other criminal activities. The production capabilities for synthetic drugs in the EU are expanding both in terms of the quantities produced and the number of production sites identified. Synthetic drugs are produced in the EU on an industrial scale and exported to destination markets across the world. Cocaine and cannabis continue to be trafficked wholesale in very large quantities to the EU and are distributed alongside heroin by poly-drug trafficking criminal groups in drug markets across Europe.

Drugs are responsible for a significant share of the trade in illicit goods via online platforms. Online trade is transforming the drugs trade, shifting the interactions between distributors from the street to online platforms. Technology also impacts on the production methods used to manufacture drugs in the EU. Technical innovation and the accessibility of sophisticated equipment have allowed criminal groups 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 equipment and production lines capable of producing synthetic drugs on an industrial scale. Drone technology is expected to advance, giving drones greater travel distance and the ability of carrying heavier loads, as well as making them more affordable. Criminal groups 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. The production, trafficking and distribution of illicit drugs remains a key threat to the EU and this threat is only enhanced by the availability of advanced production equipment and the shift to online platforms used to trade these illicit drugs.

The production, trafficking and distribution of illicit drugs are the foundation of organised crime in Europe involving more criminals than any other type of serious and organised crime in the EU. The criminals active in this area rely on established and highly successful business models, yet also display remarkable flexibility in adapting to law enforcement action, new legislation, technological innovation and new opportunities created by transport infrastructure developments. The production, trafficking and distribution of illicit drugs remain key threats to the EU.

Migrant smuggling

The migration crisis and the arrival of a large number of migrants in the EU have transformed migrant smuggling to a booming criminal business attracting criminal groups from across Europe and beyond. The scale of migrant smuggling activities in the EU is unprecedented and has increased significantly over recent years. Migrant smuggling is one of the most profitable and widespread criminal activities for organised crime in the EU.

The migration crisis has led to an expansion of the market for the services offered by migrant smugglers and is expected to emerge as a catalyst for a substantial increase in the number of incidents of exploitation in the EU. Migrants represent a large and continuously growing group of potential victims vulnerable to promises of work by criminals even if this entails exploitation. 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.

Migrant smugglers and their networks profit from the desire of irregular migrants to find safety and prosperity in the EU. They undermine the ability of law enforcement authorities to control migration flows and generate significant profits which are used to expand their criminal activities across different crime areas. The concentration of irregular migrants in some locations boosts local markets for illicit commodities such as stolen phones and drugs as groups involved in other criminal activities seek to profit from their presence. Some fraudsters may seek to exploit support systems for asylum seekers by trying to defraud healthcare and housing schemes.

Armed conflicts, population pressure and poverty in regions close to Europe will sustain migration flows to the EU. Migrant smuggling networks supply services to virtually all irregular
migrants arriving in the EU. Migrant smuggling will continue to be a key crime threat to the EU for the foreseeable future.

**Organised burglaries and thefts (organised property crime)**

Organised property crime encompasses a range of different criminal activities carried out predominantly by highly mobile criminal groups 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 criminal groups carrying different types of property crime are also highly diverse. 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.

Organised burglaries and thefts are particularly threatening types of organised property crime. Many Member States note a steady increase in the number of reported burglaries over recent years. Highly mobile criminal groups remain heavily involved in organised burglaries and thefts across the EU. The MOCGs involved in this crime area have become even more mobile in recent years operating across the EU and quickly moving between different Member States.

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. While most burglaries only require the use of rudimentary tools such as screwdrivers or crowbars, criminal groups also use increasingly sophisticated technologies and techniques to carry out burglaries, such as frequency inhibitors to disable alarm systems. Criminal groups 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.

Technology is also providing criminals with new methods of intrusion into ATMs and similar systems. 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 ATM’s operating system and force it to dispense cash. Criminal groups 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 accessed via online messaging boards and websites. As vehicles increasingly rely on keyless entry systems and other new technologies to aid navigation, driving and entertainment, this trend is set to intensify over the coming years.
Trafficking in human beings

THB for sexual and labour exploitation involves the recruitment, transportation, harbouring and exploitation of victims. The involvement of criminal groups in THB for labour exploitation is increasing in the EU. Economic disparity is a key driving force behind THB for labour exploitation. Criminal groups cater to the growing demand for cheap labour across many Member States and have access to a large number of potential victims.

Migrants represent a large and continuously growing group of potential victims susceptible to promises of work by criminals even if this entails exploitation. Europol data shows that THB for labour exploitation involves victims of more than 58 nationalities exploited in the EU. There has been little change in the types of industries featuring labour exploitation. Vulnerable sectors include agriculture, catering, cleaning, construction, entertainment, fishing, hospitality, retail and transportation. The involvement of organised crime in orchestrating THB for labour exploitation continues to be under-investigated in many Member States. 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.

Traffickers continue to rely on the use of social media, VoIP and instant messaging applications. These technologies are employed at all stages of the trafficking cycle including the recruitment of victims, advertisement of services, and the monitoring of victims. In addition to recruitment via social media and online platforms, victims continue to be recruited by word-of-mouth and by exploiting family connections.

Cross-cutting criminal threats

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 criminal groups active across the spectrum of serious and organised crime rely on document fraud and money laundering to maintain their criminal enterprises. Europol then also strongly believes that disrupting document fraud, money laundering schemes and the online trade in illicit goods and services will significantly reduce the ability of criminal groups to grow their businesses and expand into new markets.
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

Most criminal groups and individual criminals active in serious and organised crime in the EU are driven by the imperative to generate and maximise profits. Criminal finance schemes allow criminals to transfer, launder and invest criminal proceeds in the legitimate economy and in their own criminal enterprises. These schemes utilise both traditional and innovative techniques. Traditional methods include the smuggling of cash, the use of Hawala and offshore tax havens as well as trade-based money laundering, the investment in real estate, art and high-value goods. Cash-intensive businesses and gambling services continue to be used to launder criminal proceeds.

Criminal finance has benefitted greatly from technological innovation such as the shift to online solutions for most financial services provided for the legitimate economy. The emergence of new forms of payment such as cryptocurrencies and the appearance of a plethora of highly diverse and often difficult to regulate online payment and banking platforms has afforded criminals with new ways of financing and expanding their criminal businesses. The rapid processing of transactions across multiple jurisdictions and the proliferation of encryption and anonymisation tools represent some of the most significant obstacles encountered in increasingly complex and technically demanding financial investigations.

Some criminal networks, also called money laundering syndicates, have specialised in operating complex criminal finance schemes providing money laundering services to criminal groups active across serious and organised crime. Their clientele include criminal groups involved in cybercrime, different types of fraud, drug trafficking, migrant smuggling, and THB. In some cases, the funds handled by these syndicates also benefit terrorist groups and may be used to finance terrorist acts.

Document fraud

Document fraud is a key facilitator for organised crime. Fraudulent documents are used and traded extensively among criminal groups and represent a significant obstacle in the fight against serious and organised crime. Fraudulent documents are multi-purpose criminal tools and each document can be used repeatedly to support different criminal activities. The production and use of fraudulent documents has also been linked to terrorist actors. 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. Organised criminals have been quick to exploit the shift to online solutions for many services in the legitimate economy such as registering companies or obtaining various documents from public authorities. The availability of technology and raw materials traded on the Darknet has resulted in enhanced and more accessible fraudulent documents. This new generation of high quality documents is difficult to detect during checks.
The online trade in illicit goods and services

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 indicate that the online trade in illicit goods is thriving and highly dynamic.

Firearms, in particular, are increasingly traded on online platforms including Darknet marketplaces. Both individual criminals and criminal groups obtain illegal firearms via these
Online trade allows individuals with no or limited connections to organised crime to procure firearms. The online trade in illegal firearms via various platforms is set to expand further over the coming years.

All types of commodities such as counterfeit medicine, cannabis, cocaine, heroin, synthetic drugs and new psychoactive substances, specimens of endangered species, excise tobacco, counterfeit currency, cultural goods, stolen vehicle parts and accessories, as well as compromised payment card data are sold and purchased online. In addition to illicit commodities, criminal services are also traded online. The expanding crime-as-a-service business model, prevalent in many crime areas, provides customers with access to a wide range of criminal services. Online trade will continue to prompt organised crime groups to develop new business models that increase profits and further reduce the risk of detection.

As the engines of organised crime, criminal finance, document fraud and the online trade in illicit goods and services will continue to drive organised crime forward. The online trade in illicit goods and services will increasingly shape business models and dictate the way successful organised crime groups operate. Europol recommends targeting these key cross-cutting threats to disrupt organised crime groups active across the landscape of serious and organised crime in the EU.

The full report can be accessed on the Europol website at: