European Commission

Mapping the risk of serious and organised crime infiltrating legitimate businesses

Final report

Edited by Shann Hulme, Emma Disley and Emma Louise Blondes

Migration and Home Affairs

Mapping the risk of serious and organised crime infiltrating legitimate businesses

Final report

EUROPEAN COMMISSION

Directorate-General for Migration and Home Affairs
Directorate D – Law Enforcement and Security
Unit D.5 – Organised Crime and Drugs Policy

E-mail: HOME-NOTIFICATIONS-D5@ec.europa.eu

European Commission
B-1049 Brussels

Europe Direct is a service to help you find answers to your questions about the European Union.
Freephone number (*)**:**
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

PDF ISBN 978-92-76-30784-6 doi: 10.2837/64101 DR-02-21-244-EN-N

Table of contents

Tables

Figures

Boxes

Abbreviations

AML	Anti-money-laundering
AMLD	Anti-Money-Laundering Directive
AMO	Asset Management Office
ARO	Asset Recovery Office
ATM	Automated teller machine
BvD	Bureau van Dijk
CaaS	Crimes-as-a-Service
CCI	Control of Corruption Index
CNP	Card-not-present
CSD	Centre for the Study of Democracy
EBITDA	Earnings before interest, taxes, depreciation, and amortisation
ELV	End-of-life vehicles
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EUIPO	European Union Intellectual Property Office
EY	Ernst & Young
FATF	Financial Action Task Force
FinTech	Financial Technology
FIU	Financial Intelligence Unit
FRA	Fundamental Rights Agency
GDP	Gross Domestic Product
GTI	Government Transparency Institute
HICP	Harmonised Indices of Consumer Prices
IOCTA	Internet Organised Crime Threat Assessment
IPR	Intellectual Property Rights
MOCG	Mobile organised crime group
MTIC	Missing Trader Intra-Community
NGO	Non-government organisation
NPM	New payment method
NPS	New psychoactive substance
OCG	Organised crime group
PEST	Political, Economic, Social and Technological
SEG	Sustainable Eel Group
SOC	Serious and organised crime
SOCTA	Serious and Organised Crime Threat Assessment
TED	Tenders Electronic Daily
THB	Trafficking in human beings
T&T	Track and trace
UK	United Kingdom
UNODC	United Nations Office on Drugs and Crime
USD	United States Dollars
VAT	Value Added Tax
WHO	World Health Organisation

Glossary of key terms

Term	Definition used in this study
ATM physical attacks	Includes both burglaries (ram raids) and robberies. In the first case the ATM (or ATS) is attacked and either ripped out (ram raid) or the safe attacked in-situ (burglary). The attacks can be carried out by brute force, or by using explosives or gas. In the case of ATM-related robberies, attacks target the persons replenishing the ATM (or ATS) either when moving the cash to/from the terminal, or while conducting cash-replenishment activities. Also includes direct attacks on customers either at or near an ATM or bank premises (Gunn, 2020).
Cargo theft	The theft or hijacking of goods, ranging from electronics and clothes to vehicles and tobacco, while in storage or on the road (Savona & Riccardi, 2015). Road-related cargo theft is defined as any theft of shipments committed during road transportation or within a warehouse, but excluding internal petty theft (Europol, 2009).
Costs of criminal activities	These estimates monetise, where possible, the full range of harms to victims and society resulting from the estimated extent of each crime type. This includes the costs in anticipation of crime (such as security expenditure), costs as a consequence of crime (such as property stolen and emotional and physical impacts), and costs in response to crime (costs to the criminal justice system) (Levi et al., 2013).
Cryptocurrency (also virtual currency)	'A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically' (European Commission, 2016b). At the core of many of the new virtual currency systems lies the so-called Distributed Ledger Technology, which provides complete and secure transaction records without using a central registry.
Cryptocurrency exchangers	Providers engaged in exchange services between cryptocurrencies and fiat currencies (European Commission, 2016b). They facilitate buying and selling virtual currency units in exchange for fiat currencies or other virtual currencies, and have been described as 'bureau de change' of the virtual currency world and 'gatekeepers' between the virtual sphere and the real 'world' (European Commission, 2016a).
Cryptocurrency mixer or tumbler service	Services that mix identifiable (alternatively known as 'tainted') cryptocurrency funds, with untainted pools of funds to obfuscate the trail behind the cryptocurrencies. In other words, they obfuscate the origin, possession and movement of cryptocurrencies, although the extent to which they do so is a function of the process of tumbling, both in terms of encryption and mixing strategy (Chohan, 2017).
Cultural goods trafficking	The trafficking of art, elements of cultural heritage, and any other object of historical, artistic or archaeological interest (Armbrüster et al., 2011).
Custodian wallet provider	An entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies (European Commission, 2016b). Virtual equivalent to traditional financial institutions that provide bank or payment accounts to their customers. They allow users to store virtual currencies and initiate various payments and money remittances. Unlike ordinary software wallet providers, which basically offer applications for various electronic devices, custodial wallet providers also assume custody of the user's public and private key (fully or shared with one or more customers).
Digital wallets	Electronic applications that offer customers easy access to their funds, through cards or other payment instruments, and other data in order to make payments for goods or services, in stores or online over the internet; the wallet can be linked to payment accounts to fund payments and reduce the need to carry cash or plastic payment cards, and allow internet payments (EBA, 2018).
Domestic burglary	The forced or unforced illegal entry to a home or adjoining building (garages, sheds, etc.) with the intent to steal (Mawby, 2012). This differs from commercial or non-domestic burglary, which targets buildings such as grocery stores, malls, banks and warehouses (Mawby, 2012).

Term	Definition used in this study
E-money	Electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions – as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer (European Commission, 2009). The Financial Action Taskforce (FATF) defines e-money as a digital transfer mechanism for fiat currency – i.e. it electronically transfers value that has legal tender status (FATF, 2014).
Exploitation	Directive 2011/36/EU requires, at a minimum, the criminalisation of the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, including begging, slavery or practices similar to slavery, servitude, or the exploitation of criminal activities, or the removal of organs[1]. Directive 2011/36/EU expanded the definition of exploitation to include 'forced begging' and the 'exploitation of criminal activities' (in practice of covering 'pick-pocketing, shoplifting, drug trafficking and other similar activities'[2]), with terms that are not codified at the UN level. Both the Palermo Protocol and the European Directive stress that a victim's consent, intended or actual, is irrelevant as to the finding of a crime of trafficking in human beings. Additionally, both instruments establish a positive obligation for Member States to tackle trafficking in human beings, create reporting mechanisms and protect victims.
Financial technology (Fintech)	New tech that seeks to improve and automate the delivery and use of financial services. At its core, FinTech is utilised to help companies, business owners and consumers better manage their financial operations, processes and lives by utilizing specialised software and algorithms that are used on computers and, increasingly, smartphones (Investopedia, 2019).
Hawala and other similar service providers	Money transmitters, particularly with ties to specific geographic regions or ethnic communities, who arrange the transfer and receipt of funds or equivalent value – and settle through trade, cash and net settlement over a long period of time. Some of these service providers have ties to particular geographic regions and are described using a variety of specific terms, including hawala, hundi and underground banking (FATF, 2013).
Illicit flows or trafficking	The flow of money generated in illicit markets between different actors in the supply chain, including across national and international borders.
Illicit market	A place where the illicit trade in goods or commodities takes place.
Infiltration	Where an offender or criminal organisation invests either financial or human resources in the legal economy. Where investment typically involves acquisition or ownership, infiltration does not necessarily involve ownership of a given company, but it may also include human resources. Previous research has specified that infiltration requires that OCGs have some involvement in the decision-making process of the legal entity, however because OCGs may also operate as 'silent partners', we did not limit our exploration of infiltration to solely those who had some involvement in decision-making (Savona & Riccardi, 2015).
Investment	Acquisition of an asset in the legal economy (Savona & Riccardi, 2015).
Money remittance	A payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee (European Parliament, 2015).
Non-observed/underground economy (also shadow economy, informal economy, grey	Legal activities that are deliberately concealed from public authorities for the following reasons: to avoid payment of income, value-added or other taxes; to avoid payment of social security contributions; to avoid having to meet certain legal standards, such as minimum wages,

[1] Article 3 of the Palermo Protocol.
[2] These examples of criminal activities are only mentioned in the recitals of the Directive, and as such cannot be considered as legally binding in the same way as the operative provisions of the definition of trafficking in human beings.

Term	Definition used in this study
economy)	maximum hours, safety or health standards (OECD, 2002). It is often considered that the non-observed economy provides the link between and feeding ground for (recruitment opportunities, flows of non-observed payments, etc.) the black (illegal) economy and the white (legal) economy (Belev, 2002).
Organised crime group (OCG)	A structured association, established over a period of time, of more than two persons acting in concert with a view to committing offences – that are punishable by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty – to obtain, directly or indirectly, a financial or other material benefit (CofE, 2008).
Payment initiation service	A service to initiate a payment order at the request of the payment service user, with respect to a payment account held at another payment service provider (European Parliament, 2015).
Payment systems	Defined as 'a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions' (European Parliament, 2015).
Prepaid cards	Prepaid payment cards provide access to monetary funds that are paid in advance by the cardholder. While there are many different types of prepaid cards that are used in a variety of ways, they typically operate in the same way as a debit card, and ultimately rely on access to an account (FATF, 2006).
Privacy-focused cryptocurrencies	Cryptocurrencies that offer completely anonymous transactions. Some of them use complex technologies to complete cryptographically strong transactions, wherein both the sender and recipient of the transaction are hidden. Monero, Zcash and Dash are three of the most renowned privacy-focused currencies because of their privacy-enhancing algorithms and novel ring signatures (Dyson et al., 2019).
Profit	The proportion of revenues retained by traffickers after accounting for overhead costs.
Revenue	Typically derived by combining estimates of market size or volume of trade (within a specific geographic area) with data on the price of the illegal good or service. The specific approach to estimating economic value varies across each market, depending on the nature of the illicit activity and the availability of data. In general, the approach for estimating economic value is usually indirect and involves demand- or supply-based approaches. Demand-based approaches use indicator data on the specific use or consumption of goods or services, while supply-based approaches rely on data about the amount of goods or services traded or sold (Eurostat, 2018).
Robbery	A wide range of thefts that utilise violence or the threat of violence – from ATM attacks to bank and business robberies.
Smuggling of migrants	A crime involving the 'procurement for financial or other material benefit of illegal entry of a person into a state of which that person is not a national' or resident (UNODC, 2011b).
Trafficking in human beings (THB)	The recruitment, transportation, transfer, harbouring or reception of persons, including the exchange or transfer of control over those persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation includes, as a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, including begging, slavery or practices like slavery, servitude, or the exploitation of criminal activities, or the removal of organs.
THB for sexual exploitation	THB for sexual exploitation is recognised as violence against women and girls (European Commission, 2016c). Includes the exploitation of the prostitution of others or other forms of sexual exploitation wherein victims lack the autonomy and consent, including to make decisions about themselves, or regarding their schedule, working place, activities, clients and earnings. Sexual exploitation can take place at a variety of venues (both indoor and outdoor), and can take numerous different forms – street prostitution, window prostitution, brothels, strip clubs, pornography (recording and live streaming), escort services, massage

Term	Definition used in this study
	parlours, modelling agencies, and more (Eurostat, 2015). Prostitution is a high-risk sector for trafficking for sexual exploitation (European Commission, 2020g). Unlike volitional legal prostitution, victims of trafficking for sexual exploitation have lost their freedom to engage in a mutually agreed economic transaction with their clients (Eurostat, 2018). Often victims of trafficking for sexual exploitation do not self-identify as victims, although there are many indicators that can help identify a victim – such as the presence of coercion, threats and/or physical violence, abuse of the vulnerable situation of women and girls, deprivation of their personal documents or their financial means, or inability to speak the language of the location they are trafficked to. The harms of trafficking for sexual exploitation are gender-specific and are different from other forms of exploitation (European Commission, 2016c).
THB for labour exploitation	There is no common EU legal definition on the term 'labour exploitation'. Examples can include cases where victims are forced, intimidated, and/or misled, or their vulnerable position/precarious situation is abused to provide labour services in a legally regulated or unregulated and often dangerous environment. The EU's Fundamental Rights Agency (FRA) refers to severe labour exploitation as 'work situations that deviate significantly from standard working conditions as defined by legislation or other binding legal regulations, concerning in particular remuneration, working hours, leave entitlements, health and safety standards and decent treatment and which are criminal under the legislation of the EU Member State where the exploitation occurs. Hence, severe labour exploitation includes as a minimum coercive forms of exploitation, such as slavery, servitude, forced or compulsory labour, and trafficking prohibited by Article 5 of the EU Charter, as well as severe exploitation within the framework of an employment relationship, as covered by Article 9 (1) of the Employers Sanctions Directive.' (FRA, 2015; 2019). High-risk sectors include the agriculture, forestry, fisheries, construction and cleaning sectors, domestic work, care services, nursing homes and night shops.
THB for forced begging	No standard legal definition for THB for forced begging has been established on the EU level; however, key elements of this criminal activity have been identified by researchers. 'Classic begging', in the sense of simply begging strangers for change, is the basic practice (Healy, 2017). Begging can likely take a variety of forms: selling overpriced flowers or other tokens; cleaning car windows at a traffic light; providing small services at shopping centres such as packing bags and returning trolleys; playing musical instruments or performing acts. Forced begging can occur indoors and outdoors, with victims often moving from one busy place to another, meaning this type of trafficking is the most publicly visible out of all the four forms identified here. The exploitation period for forced begging can be long-term or short-term, and begging is often just one of the forms of exploitation that victims endure.
THB for organ removal	No standard legal definition for THB for organ removal exists. It relates to a 'range of illegal activities that aim to commercialise human organs and tissues for the purpose of transplantation' (Bos, 2015). The illegal activities that could be subsumed under this term include trafficking of persons with the intent to remove their organs. It should be differentiated from the criminal act of trafficking in organs, tissues and cells. According to the World Health Organization (WHO), illicit organ transplants represent between 5% and 10% of all organ transplants worldwide (Shimazono, 2007). Within the EU this is not a prevalent form of trafficking (European Commission, 2018b).

Acknowledgements

This study has been commissioned by the European Commission Directorate-General for Migration and Home Affairs (DG HOME). Representatives from DG HOME offered their expertise throughout the study, providing feedback on the methodology and research design, and commenting on draft versions of this report. We would like to thank all involved for their active engagement, constructive feedback and efforts to facilitate our activities.

We were privileged to benefit from the tremendous amount of knowledge and expertise of our expert panel, who offered their advice throughout the course of the study and provided feedback on the proposed methodology and work plan, and the interim and draft deliverables. The members of the expert panel were Giulia Berlusconi, Luca Giommoni, Michael Levi, Letizia Paoli and Lorenzo Segato.

We are also grateful to Stijn Hoorens (RAND Europe) and Claudia Gallo (Ernst & Young) for input, guidance and constructive criticism on earlier versions of this report, which they provided in their role as peer reviewers in the context of RAND Europe's Quality Assurance system. Thank you also to Kaitlin Ball for assistance in searching for cases of organised crime infiltration. Thank you to Richard Gilbert for copy editing this report and its annexes.

Stakeholder and expert consultations were essential for the successful completion of this study. Therefore, we are grateful for the time and hospitality we were offered by the large number of individuals who participated in an interview or who were consulted by other means. All organisations consulted as part of this study are listed in **Annex 1**.

The authors report no conflicts of interest. Any remaining errors contained in this report are the sole responsibility of the authors.

Executive summary

The economic and social harms from serious and organised crime (SOC) are multifaceted and wide-reaching, and span the individual, community and societal level. Appropriate targeting of resources to tackle SOC relies upon accurate information about the extent and nature of the phenomenon. However, the hidden nature of SOC means that measuring its size and scale is inherently challenging. The European Commission, DG Migration and Home Affairs, called for a study 'Mapping the risk of serious and organised crime infiltrating legitimate businesses' to improve the evidence-base in relation to SOC in the EU.

The research has been conducted by RAND Europe in collaboration with researchers from the Centre for the Study of Democracy (CSD), the Government Transparency Institute (GTI), Ernst & Young (EY) and Optimity Advisors.

The study has two principal objectives, each with sub-objectives:

- **Objective 1**: Analyse the dynamics of SOC and, to the extent feasible, provide 'facts and figures' in the EU and each Member State. This objective is comprised of three sub-objectives:
    - Provide a quantitative and qualitative analysis of nine illicit markets[3] in terms of revenues, actors and future trends and dynamics.
    - Provide a quantitative and qualitative analysis of investments made by organised crime groups (OCGs) in the EU legal economy in terms of business sector and asset type.
    - Analyse data on assets frozen and confiscated in the 28 EU Member States.
- **Objective 2**: Provide an in-depth analysis of the risk factors that facilitate the generation and the management of criminal finances by OCGs, including the risk factors facilitating infiltration in the legal economy:
    - Assess the risks of OCGs misusing legal entities.
    - Assess the risks from exploitation of new payment methods (NPMs), including non-banking funds-transfer methods, mobile payment methods and cryptocurrencies (or virtual currencies).
    - Assess the risk from exploitation of underground economic structures.
    - Analyse emerging enablers and risk trends in criminal finances in Europe.

The findings of the study have been used to produce a series of recommendations and policy ideas to assist policy-makers in tackling the infiltration of SOC in the legal economy. The scope of the study includes the UK, which at the time the study was commissioned remained within the EU. Where possible, the estimates of criminal revenues distinguish between those including and excluding the UK.

Methodology and approach

This study utilised a mixed-methods approach utilising a range of quantitative and qualitative data.

- In-depth **literature reviews** were carried out to map current knowledge from the last 10 years relating to each individual aspect of the study.
- **Interviews** were conducted with 102 experts and stakeholders from 66 organisations, including representatives from EU institutions, Member State organisations, law enforcement, asset seizure and recovery organisations, academic institutes and the private sector.
- **Surveys** of Asset Recovery Offices (AROs), Asset Management Offices (AMOs) and Financial Intelligence Units (FIUs) in the 28 EU Member States.
- The analysis of a range of **secondary data**, including two datasets containing company ownership and public procurement information.
- The collection of 81 **proven cases** of SOC investment or infiltration in the legal economy.

[3] The markets examined in this study are illicit drugs, trafficking in human beings, smuggling of migrants, fraud (MTIC fraud, IPR infringements, food fraud), environmental crime (illicit waste and illicit wildlife), illicit firearms, illicit tobacco, cybercrime activities and organised property crime.

- Three **case studies** to illustrate dynamics of SOC and the management of criminal finances by OCGs.

Key findings

Criminal markets

One of the primary objectives of this study was to estimate the **revenues** generated by actors operating across criminal markets in the EU. Revenue is the total amount of income generated from the sale of goods or services. Understanding the revenue generated by an illicit market does not capture harms such as violence, exploitation, deprivation, loss to legitimate business or environmental destruction. It is important that understandings of both revenue and costs inform policy-making. This study aims to make a significant contribution to the former.

This study estimates that the annual revenues of the nine main criminal markets in the EU ranged from €92 to €188 billion (mid-point of €139 billion) in 2019. It is not possible to directly compare this overall revenue figure for all nine markets with the figures estimated in previous similar studies (such as that of Savona & Riccardi (2015)), because the markets examined are not the same. However, for individual markets some comparisons can be made with the findings of previous studies. For instance, there seems to have been an upward trend in revenues generated through the trafficking of illicit drugs, Missing Trade Intra-Community (MTIC) fraud, and illicit waste trafficking.

It is useful to consider the relative scale of the markets examined in this study. The analysis shows that the largest markets in terms of revenue (from the lower boundary estimate) are MTIC fraud, illicit drugs, illicit tobacco (specifically cigarettes) and illicit waste.

Table E.1: Headline revenue estimates

Criminal markets and areas	Revenues, adjusted for inflation, 2019 (€ million)			Source of estimate
	Mid	Low	High	
Illicit drugs	30,688.41	26,708.13	35,514.56	EMCDDA & Europol (2019)
THB for sexual exploitation	7,185.93	401.94	13,969.91	New estimate
Smuggling of migrants	289.37	215.60	363.15	New estimate
MTIC fraud	77,425.00	50,858.00*	103,991.67	Frunza (2019), EY (2015)
Illicit waste*	9,506.62	3,723.49	15,289.74	New estimate
Illicit wildlife (European eels only)	18.05	4.71	31.39	New estimate
Illicit firearms	408.09	273.69	753.96	New estimate
Illicit cigarettes	8,309.15	8,012.62	10,087.48	New estimate
Card payment fraud	1,816.43	-	-	ECB (2018)
Cargo theft*	3,347.86	144.39	6,551.32	New estimate
ATM physical attacks*	22.00	-	-	EAST (2020)
Total	**139,016.91**	**92,181.00^**	**188,391.61^**	

Notes: Estimates have been adjusted for inflation using price-index data from Eurostat (2020). The low and high estimates have been generated using different methodologies, with each described in the annexes that support the market analyses. A common example is the use of a range of price data. In most cases, the mid estimate represents the mid-point (median) between the low and high value. These mid-point estimates should be interpreted with a high degree of caution because the distributions are not necessarily normally distributed, but have nevertheless been provided here for illustrative purposes. Unless otherwise stated, the estimates are for the 28 Member States, which includes the UK.
* Denotes estimates that do not include all 28 EU Member States: **MTIC fraud** lower bound estimate excludes HR and CY. **Illicit waste** estimates exclude BE, CY, LU, MT, SI. Lower bound **cargo theft** estimates exclude AT, BG, HR, CY, EE, FI, EL, LT, LU, ML, PL. Upper bound estimates exclude MT. **ATM theft** estimates exclude BE, BG, HR, EE, HU, LV, LT, MT, PL, SI. ^ Presumes card payment fraud and ATM attacks are equivalent to mid-point estimate.

Investments by OCGs in the legal economy

This study makes an important new contribution to the evidence on the sectors and assets of investment by OCGs in the EU. Investments are made by OCGs in the legal economy for a variety of reasons including to maximise profit, facilitate and conceal ongoing illicit activities, launder illicit proceeds, perpetrate fraud, exert control over territories or sectors, or strategically

influence local politics and public administration. Using data on cases of infiltration or investment, and information from Asset Recovery Offices and Asset Management Offices, our analysis shows that the predominant sectors of known investments by OCGs in the legal economy are property/real estate, transportation and construction.

This study provides insights into the investment strategies of OCGs. Based on analysis of the literature, proven cases and interviewee remarks, we provide evidence on how OCGs invest in the legal economy to minimise the risk that the illegal origin of the proceeds will be detected. The strategies we identified in our analysis include cash couriers, micro-transfers or micro-laundering, money muling or 'smurfing', mixing or tumbler services, cryptocurrency exchange services and straw ownership. There are clear links between the strategy employed and the illicit market through which the proceeds were generated. This is typically related to whether the criminal activity generates predominately cash or non-cash.

The freezing and confiscation of assets from SOC

The study provides an update on the availability and collection of statistical data on asset seizure and recovery from OCGs since the assessment by Savona & Riccardi (2015). The study found that considerable gaps remain in the collection of data on asset seizure and confiscation in the EU. Data collection is not centralised, resulting in gaps, fragmentation and inconsistencies. Data collection processes are still largely undertaken manually – use of IT systems or electronic databases is rare. There are differences between and within Member States as to what behaviours they classify as SOC.

Considering the limited data availability, it is not possible to reliably ascertain the overall number and value of assets frozen or confiscated at the EU-level. Attention should be paid to improving systems for data collection through automation, standardisation and harmonisation, to enable a more robust understanding of the extent of asset recovery in the EU.

Risk factors for SOC infiltration of companies and public procurement

The study uses analytical techniques to predict risk factors for SOC infiltration of companies and public procurement. This was informed by literature review, analysis of proven cases of SOC infiltration, and analysis of two secondary datasets: Bureau van Dijk (company ownership data) and Italian procurement data from ANAC, the Italian anti-corruption agency.

The analysis of individual financial and ownership risk indicators does not support the claim of the literature that SOC-infiltrated companies have a significantly different financial (e.g. share of current assets) or ownership profile (e.g. network centrality) than their non-infiltrated peers. When considering multiple dimensions at once (e.g. share of current assets, standard deviation of assets, standard deviation of revenue, and earnings before interest, taxes, depreciation, and amortisation (EBITDA) margin), the analysis revealed that companies infiltrated by SOC have a distinct profile. Extrapolations across the EU identified that corruption, high cash-intensity and weak legal frameworks are positively associated with SOC infiltration in the economy.

Regarding infiltration of public procurement, single bidding, number of contracts awarded by the procuring entity in the year, the share of a supplier in a buyer's annual spending, and relative price are all associated with higher probabilities of SOC infiltration. The extrapolations to the whole EU revealed a rich and diverse picture that only partially supports existing perceptions of where SOC infiltration is high. For example, some regions of France or Finland have higher than negligible risk of SOC infiltration.

The analysis demonstrates that it is both feasible and fruitful to build large-scale SOC risk-assessment tools based on micro-level databases describing companies and public procurement contracts, and that doing so would allow for frequent monitoring rather than one-off reports.

The exploitation of the underground economy for SOC

For the purpose of this study, the underground economy is defined as 'legal activities that are deliberately concealed from public authorities for the following kinds of reasons:

- to avoid payment of income-, value-added or other taxes;
- to avoid payment of social security contributions; or
- to avoid having to meet certain legal standards such as minimum wages, maximum hours, safety or health standards (OECD, 2002).'

The relative size of the underground economy is, according to estimates by Medina and Schneider (2019), larger in Eastern and Southern Europe than in Western and Northern Europe.

The exploitation of the underground economy by OCGs has received relatively little attention in the literature. To address this gap, we conducted interviews with experts and stakeholders to identify economic sectors that are prone to underground activities – namely, transport and logistics, entertainment, construction, finance and labour. The results of these interviews informed targeted literature searches to explore in greater depth the mechanisms of the underground economy, and the particular vulnerabilities of each sector to OCG exploitation. OCGs are in a particularly good position to exploit underground economy practices in sectors that are closely connected to many economic activities, and have a relatively centralised position in existing economic networks. The key findings of this analysis are summarised in Table E.2 below.

Table E.2: Underground economy exploitation by organised crime groups

Economic sector	Underground economy mechanisms	Vulnerabilities of the sector	Nature of OCG exploitation
Transport and logistics	Undeclared cargo and freight Work performed by people without sufficient vetting	Inadequate screening of cargo and freight Insider threats New technologies and digital infrastructures increase anonymity of customers and are vulnerable to intrusion	Trafficking of illicit goods like drugs, tobacco, firearms, counterfeit goods THB and migrant smuggling MTIC fraud Theft of cargo Attacks from firearms and explosives
Entertainment	Undeclared work Undeclared provision of services Provision of services by agents lacking authorisation	Grey zones within existing regulatory regimes Existence of interconnected 'ancillary' industries Absence of an aggrieved party inclined to report 'vice' offences	Provision of 'ancillary' services to entertainment operations Organisation of entertainment services Money-laundering
Construction	Unreported work Work performed by individuals lacking authorisation Work performed in violation of existing health and safety standards	Complex economic activity requiring many types of specialised input High personnel turnover and temporary nature of work Connection to other economic activities (e.g. real estate trade)	Supply of personnel, incl. certification and qualification Provision of ancillary services, e.g. site security Money-laundering THB
Finance (particularly informal value-transfer systems, like hawala)	Hidden transactions Provision of services by agents lacking authorisation	Weak regulation of financial services Anonymity of virtual currencies Untraceable transactions through informal value-transfer systems	Money-laundering and concealment of criminal finances Doing business on crypto markets

A case study approach was used to explore THB for labour exploitation. The analyses revealed that OCGs employ several underground economy practices and structures in each stage of the trafficking:

- First, in the recruitment stage, victims are often offered contracts by intermediaries that are legitimate business entities, which act as recruitment agencies despite not being licensed as such.
- Second, when contracting victims, perpetrators use a variety of underground economy practices for tax evasion, such as abuse of EU posted workers' regulations and bogus self-employment.
- Third, in the transportation stage, perpetrators often use services provided by unlicensed operators who sometimes charge exorbitant fees.

- Fourth, in the exploitation stage, letter-box companies are used as sub-contractors (often deliberately creating a cascade of sub-contractors) in order to conceal the exploitation of victims and the evasion of due taxes, social insurance and health contributions.

The use of new and non-banking payment methods for SOC

NPMs are payment innovations that give customers the ability to carry out payments through technical devices such as personal computers and mobile phones. The number of transactions with NPMs among the general population in the EU has increased three-fold in the last 10 years, which provides important context for investigating their use by OCGs. NPMs are vulnerable to exploitation for money-laundering, although not all types of NPMs present the same level of risk. Our analysis of the literature and expert and stakeholder insights finds:

- **Cryptocurrencies** are regularly used in most types of cybercrime, particularly illicit trading through dark-net markets. The drivers of use include perceived anonymity, global reach, speed of transactions and regulatory and institutional gaps.
- **Prepaid cards** are rarely used compared to cash and other NPMs. The drivers of use include anonymity and their wide acceptance as means of payment.
- **Digital and mobile wallets** are used less frequently than cryptocurrencies, though may be used moderately in certain cybercrimes, like phishing and child sexual exploitation material.
- **Other innovative and mobile payment services** are rarely used compared to cash and bank transfers.
- **Hawala and similar services** operate outside the regulated financial system and are regularly used in the smuggling of migrants. There are differences in use between countries.

Cash remains the preferred currency for OCGs – even those operating in cybercrime markets – mainly because of its anonymity. Factors inhibiting the use of NPMs by OCGs range from the need for technical savviness, the risk of fraud, the elevated cost of transactions (compared with cash) and the growing risk of detection as certain products are increasingly monitored.

Possible emerging threats

The study identified six emerging threats or enablers that may shape the management of criminal finances by OCGs in the next five years. A PEST (Political, Economic, Social and Technological) framework was used for analysing trends that emerged from the literature review and interviews.

Table E.3: Future threats or enablers

PEST	Trend
Political	**Brexit** could expose the UK to illicit investments where it diverges from the EU regulatory framework. For instance, the UK's decision not to be bound by the 6th Anti-Money-Laundering Directive (AMLD) could be potentially detrimental to the UK's fight against money-laundering, and the proposal to create 10 new freeports has raised concerns about increased opportunities for illicit cross-border trade. **Golden visa schemes** continue to vary in their requirements and due-diligence checks across the EU, presenting potential opportunities for illicit investments.
Economic	**Cash and high value goods** will continue to pose a threat to anti-money laundering (AML) efforts as they are difficult to trace. The **green economy** could present risks for the placement and transfer of criminal finances by OCGs due to the absence of harmonised regulations across the EU. For instance, there is evidence of OCGs exploiting the European carbon-credits market for money-laundering.
Social	**SARS-CoV-2 (COVID-19) pandemic** and the resultant economic volatility may change the modus operandi of money-laundering by OCGs, such as through increases in the use of onshore financial systems and increasing use of NPM and non-banking payments.
Technological	**The use of cryptocurrencies** by OCGs is expected to continue to grow; this will in turn increase demand for automated, decentralised cryptocurrency exchanges and potentially lead to a shift towards more privacy-oriented currencies (like Monero). However, cryptocurrencies will probably not replace cash as the preferred means of money-laundering for OCGs.

1. Introduction

Shann Hulme and Emma Disley, RAND Europe

The European Commission (hereafter, 'the Commission') has funded this study 'Mapping the risk of serious and organised crime infiltrating legitimate businesses' to improve the evidence-base in relation to serious and organised crime (SOC) in the EU. This study examines the scale, actors, modus operandi and trends with regard to the priority criminal markets within the EU. In addition, the study explores the intersection between legal and illegal markets, including the grey or underground economy, to illustrate how organised crime groups (OCGs) may exploit the various layers of the economy for the placement and transfer of criminal proceeds.

The research has been conducted by RAND Europe in collaboration with researchers from the Centre for the Study of Democracy (CSD), the Government Transparency Institute (GTI), Ernst & Young (EY) and Optimity Advisors.

1.1. The need to understand the scale of revenues from serious and organised crime

As awareness has grown internationally of the harms caused by SOC, there has been a concomitant increase in research efforts seeking to define and measure the problem. Several studies have shown that the revenues generated through SOC are substantial. In 2011 the United Nations Office on Drugs and Crime (UNODC) estimated that the amount of money available for laundering through the financial system was $1.6 trillion (USD) – equivalent to 2.7% of global Gross Domestic Product (GDP). Related proceeds from drug trafficking and transactional organised crime activities were estimated at $870 billion (USD) as at 2009 (UNODC, 2011a). In the European context, Transcrime estimated that some of the main illicit markets[4] generated around €110 billion per year, which represented approximately 1% of EU GDP in 2010 (Savona & Riccardi, 2015). Many other studies have estimated the revenues generated by actors within specific criminal markets or particular countries or regions.

In recognition of the negative impacts that SOC has upon the security of individual citizens, communities, businesses and Member States, tackling SOC continues to be a priority for the EU and its Member States. Some of the key EU policy actions are outlined in the box below. Note that these actions are not exhaustive.

Box 1.1: Policy action in the EU to tackle serious and organised crime

Established at the Paris G7 summit in 1989, the inter-governmental **Financial Action Task Force (FATF)** aims to set international standards to prevent money-laundering and terrorist financing, whilst also generating the political will to bring about national legislative reform (Economic Declaration, 1989).

The **European Crime Prevention Network (EUCPN)** was set up in 2001 as an EU-wide platform for best practice, research and information exchange on local, national and European-level crime prevention and includes projects on organised crime. As part of this, the **European Network on the Administrative Approach (ENAA)** was formed to tackle SOC, and over time evolved into a network of National Contact Points (NCPs) who act as a gateway to law-enforcement agencies, government departments, administrative bodies and academia, and facilitate multidisciplinary information exchange (ENAA, 2020).

The **EU Policy Cycle / EMPACT (European Multidisciplinary Platform Against Criminal Threats)** is the cornerstone of EU action against SOC. It was launched in 2010 as an intelligence-led, multi-disciplinary approach to coordinating the fight against SOC (Europol, 2017b). The priorities adopted by the Council of Justice and Home Affairs are based on recommendations identified in the EU Serious and Organised Crime Threat Assessment (SOCTA) prepared by Europol, as well as other assessment and policies.

Concerns regarding SOC infiltration are recognised in the **European Agenda on Security** (European Commission, 2015). In outlining one of the three key priorities – 'disrupting organised crime', it is unambiguously stated that 'international criminal networks use legal business structures to conceal the source of their profits, so action is needed to address the infiltration of the licit economy by organised crime' (European Commission, 2015). A number of efforts have been made or are underway to improve the responses to this phenomenon (European Commission, 2019d), including the revised EU legal framework on **anti-money-laundering** (AML)[5], the Regulation on the mutual recognition of **freezing**

[4] Trafficking in illicit drugs, illicit trafficking in firearms, illicit trade in tobacco products, counterfeiting, missing trader intra-community (MTIC) fraud and cargo theft.

[5] The 5th AMLD (amending the 4th AMLD) was published in the Official Journal of the EU on 19 June 2018, and was due to be transposed by Member States by 10 January 2020.

orders and confiscation orders[6], and the new regulatory framework on controls on cash entering or leaving the European Union[7].

Tackling the external dimension to organised crime has also been identified as a necessary priority within the **EU's Foreign and Security Policy** (European Union, 2019c). For example, EU assistance as part of Advisory Missions in Iraq saw assistance in security reforms supporting the country's police and criminal justice system to fight terrorism and organised crime, and to protect culture heritage (European Union, 2019c). Commentators have however questioned whether priorities fostering external human security can be compatible with the internal security priorities of Member States (Stambøl, 2019).

The **Internal Security Fund (ISF)** was established for the period 2014 to 2020 to promote the implementation of the Internal Security Strategy, law enforcement cooperation and the management of the EU's external borders. The ISF Police is one of the instruments of the ISF that focuses on combatting cross-border SOC, and reinforcing coordination and cooperation between law enforcement authorities and other national authorities. For the period 2014 to 2020 there was over €1 billion for funding actions under the ISF Police instrument (European Commission, n.d.).

Most recently, in July 2020 the European Commission set out the **EU Security Union Strategy** for the period 2020 to 2025. The new strategy includes measures and detailed action for tackling organised crime, including trafficking in human beings (THB), illicit drugs, illicit firearms and the smuggling of migrants; as well as a commitment to review the framework on seizing criminal assets (European Commission, 2020d).

The scale, products, modus operandi and actors operating within criminal markets are ever-changing. According to Europol, OCGs are increasingly poly-criminal and cross-border in their operations (Europol, 2017b). There are also growing threats in relation to cyber security and the exploitation of technology for the perpetration of criminal activities (European Commission, 2020d; Europol, 2019a). The revenues generated by SOC are reinvested in further illicit activities or enter the legitimate economy, serving to undermine the business environment, leading to corruption and lack of trust in institutions, while negatively impacting upon the growth potential of the economy (Pinotti, 2015).

The appropriate targeting of resources to tackle SOC and its associated social and economic harms relies upon accurate and up-to-date information about the extent and nature of the phenomenon. This study uses current data and novel methodologies to produce an updated and robust understanding of SOC within the EU, which is intended to inform policy-makers in their ongoing fight against SOC and the infiltration of OCGs in the legal economy.

1.2. The objectives of the study and its utility for policy-makers

The study has two principle objectives, each with sub-objectives:

- **Objective 1**: Analyse the dynamics of SOC and, to the extent feasible, provide 'facts and figures' in the EU and each Member State. This objective is comprised of three sub-objectives:
  - Provide a quantitative and qualitative analysis of nine illicit markets[8] in terms of revenues, actors and future trends and dynamics.
  - Provide a quantitative and qualitative analysis of investments made by OCGs in the EU legal economy in terms of business sector and asset type.
  - Analyse data on assets frozen and confiscated in the 28 EU Member States.
- **Objective 2**: Provide an in-depth analysis of the risk factors that facilitate the generation and the management of criminal finances by OCGs, including the risk factors facilitating the infiltration in the legal economy:
  - Assess the risks of OCGs misusing legal entities.
  - Assess the risks from exploitation of new payment methods (NPMs), including non-banking funds-transfer methods, mobile payment methods and cryptocurrencies (or virtual currencies).
  - Assess the risk from exploitation of underground economic structures.

[6] This regulation was adopted in November 2018 and will come into effect 24 months after publication in the EU Official Journal. It replaces the 2003 and 2006 framework decisions on mutual recognition of freezing orders and mutual recognition of confiscation orders.
[7] Regulation 2018/1672. This regulation repeals Regulation EC No 1889/2005 and shall apply from 3 June 2021.
[8] The markets examined in this study are illicit drugs, trafficking in human beings, smuggling of migrants, fraud (MTIC fraud, IPR infringements, food fraud), environmental crime (illicit waste and illicit wildlife), illicit firearms, illicit tobacco, cybercrime activities and organised property crime.

- Analyse emerging enablers and risk trends in criminal finances in Europe.

The findings of the study have been used to produce a series of recommendations and policy ideas to assist policy-makers in their fight against SOC in the EU. The overarching utility of this study for policy-makers, researchers and other stakeholders is summarised in the box below.

Box 1.2: Utility of this study for policy-makers and stakeholders

The findings of this study can be used by policy-makers, researchers and other stakeholders for:

- Targeting resources towards criminal markets and geographical regions where revenues generated are high.
- Improving future data-collection and estimation of each criminal market.
- Ongoing monitoring of the revenues generated through SOC and their investment and infiltration in the legal economy.
- Informing understanding of where the risk of organised crime investment in the legal economy is high.
- Identifying companies and government contracts that are at an increased risk of organised crime infiltration.
- Exploring the vulnerabilities within legal economic sectors that may be exploited by criminal actors.
- Drawing attention to future and emerging threats in relation to the use of new and non-cash payment methods by OCGs, as well as strategies for the management of criminal finances by OCGs.

1.3. Key concepts and terminology

1.3.1. What is serious and organised crime?

SOC is typified as being broad, ambiguous and difficult to capture in a definition (Carrera et al., 2016). EU harmonisation measures based upon the United Nations Convention against Transnational Organised Crime have aimed to facilitate judicial cooperation and mutual recognition across Member States (Carnevale et al., 2017). OCGs are defined by the EU Council Framework Decision 2008/841/JHA as 'a structured association, established over a period of time, of more than two persons acting in concert with a view to committing offences which are punishable by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty, to obtain, directly or indirectly, a financial or other material benefit' (CofE, 2008).

While the broad nature of this definition means that, as highlighted by Paoli (2014), 'any group from the Sicilian Cosa Nostra to a burglars' clique, from Al Qaeda to a youth gang engaging in assaults, can be considered a form of organised crime', this is the definition adopted for the purposes of this study, to maintain consistency with the EU policy environment and previous research.

1.3.2. What is investment and infiltration?

Prior research has defined the infiltration of OCGs as having the following requisite elements (Savona & Riccardi, 2018):

- a natural person belonging to a criminal organisation or serving as figurehead of the organisation for infiltration;
- an investment of financial and/or of human resources from the OCG; and
- the ability of the OCG to ultimately participate in the decision-making process of the infiltrated legitimate entity.

This is the definition adopted for the purposes of this study to ensure consistency with previous research and to build upon current knowledge.

Organised crime infiltration in legitimate businesses encompasses several types of actions, including investment, money-laundering or placement of figureheads at managerial positions. These concepts are explained below.

- **Investment** refers to the acquisition of an asset in the legal economy (Savona & Riccardi, 2015), such as through bonds, options, real estate properties or companies possessed or acquired by an individual or entity belonging or acting on behalf of an OCG. It does not include consumption spending (Ferwerda and Kleemans, 2019; Kruisbergen et al., 2015).
- **Money-laundering** is the action of cleansing illegally earned money by giving it an artificial legitimate origin. Traditional conceptions of money-laundering suggest that laundering follows a three-stage process of placement, layering and integration (Gilmour and Ridley, 2015). However, more recent research has shown that not all three phases are necessary for money-laundering to have occurred, not all criminal proceeds are laundered, and the process of laundering is often perceived to be more complex than it is (Levi and Soudijn, 2020).
- **Placing figureheads** involves OCGs placing members or relatives at strategic positions to influence the decision-making in their favour (Savona and Berlusconi, 2015).

1.4. Methodology and cross-cutting data-collection activities

This study utilised a mixed-methods approach to analyse a range of quantitative and qualitative data. The data-collection activities are explained in detail in **Annex 1** and are briefly summarised below. At the beginning of each section of the report these icons are used to signify the methodologies that informed the findings and direct the reader to seek further detail in the Annex.

In-depth literature reviews were carried out to map current knowledge (i.e. from the last 10 years) relating to each individual aspect of the study

Interviews were conducted with 102 experts and stakeholders from 66 organisations, including representatives from EU institutions, Member State organisations, law-enforcement, asset-seizure and recovery organisations, academic institutes and the private sector.

Surveys were conducted among Asset Recovery Offices (AROs), Asset Management Offices (AMOs) and Financial Intelligence Units (FIUs) in the 28 EU Member States.

A range of **secondary data** was analysed, including two datasets containing company ownership and public procurement information.

81 **proven cases** of SOC investment or infiltration in the legal economy were collected.

Three **case studies** were examined to illustrate dynamics of SOC and the management of criminal finances by OCGs.

The scope of the study and the data analysed was for the 28 EU Member States, which at the time the study was commissioned included the United Kingdom (UK).

Box 1.3: What is the value added from this report?

The study:

- Presents an updated lower, upper and mid-point estimate of the revenues generated through SOC across the nine priority criminal markets in the EU.
- Is one of the first to estimate criminal revenues from THB for sexual exploitation and illicit wildlife trafficking in the EU.
- Employs new and improved methodologies to produce updated revenue estimates for smuggling of migrants, illicit waste, illicit firearms, illicit tobacco and cargo theft.
- Produces a systematic appraisal of methodologies used for producing revenue estimates, and includes a series of recommendations for improving data collection and estimation in this regard.
- Comprehensively reviews the academic and grey literature on the main criminal markets operating within the EU, in terms of prior market estimates, market actors and future trends and dynamics.
- Provides an updated assessment of the availability of statistics on frozen and confiscated assets

in the EU.

- Produces new insights on SOC infiltration of companies and public procurement, using data analytics and big data.
- Presents an appraisal and summary of estimates of the size and extent of the underground economy in the EU.
- Analyses the vulnerabilities within legal sectors that are exposed to SOC.
- Includes case studies to explore infiltration of the legal economy by OCGs in particular sectors and contexts.
- Identifies possible emerging threats with regard to the management of criminal finances by OCGs over the next five years.

1.5. Structure of this report

The remainder of this report is separated into two chapters, as detailed below with links to the relevant sections and attachments.

Chapter 2 presents the analysis of the nine selected priority criminal markets. It begins with a discussion of key concepts and terminology, the overarching analytical approach, and a summary and aggregation of headline revenue estimates for each market. This overview is followed by an analysis of each market in terms of revenue, actors and future trends. **Section 2.1** focuses on illicit drugs, **Section 2.2** on THB, **Section 2.3** on smuggling of migrants, **Section 2.4** on fraud (including Missing Trader Intra-Community (MTIC), intellectual property right (IPR) infringements and food fraud), **Section 2.5** on environmental crime (including illicit waste and illicit wildlife trafficking), **Section 2.6** on firearms, **Section 2.7** on illicit tobacco, **Section 2.8** on cybercrime, and finally, **Section 2.9** on organised property crime. The purpose of this chapter is to provide an up-to-date picture of the SOC economy in the EU.

Chapter 3 builds upon the findings of Chapter 2 to consider what happens to criminal proceeds once they are earned. **Section 3.1** covers types and sectors of investments by OCGs in the legal economy and strategies for investment. **Section 3.2** explores tools used by authorities to recover investments through asset freezing and confiscation. **Section 3.3** analyses the risk factors for OCG infiltration of legitimate companies and government contracts. **Section 3.4** describes the characteristics and extent of the underground or 'shadow' economy in the EU and provides an overview of the vulnerabilities within economic sectors that are susceptible to OCG exploitation. **Section 3.5** explores the emergent use of NPMs by OCGs in their operations and for investment and laundering. **Section 3.6** looks to the future, presenting an analysis of the emerging threats regarding the management of criminal finances by OCGs in the EU in the next five years.

This report offers a series of **recommendations** for use by policy-makers. These recommendations are presented within each respective section of the report.

To be read in conjunction with this report is a range of **technical annexes** that provide comprehensive and additional details in relation to the aspects summarised in this report. These annexes are intended to be read by those with a more in-depth interest in the aspects summarised in this policy report.

The terminology used throughout this report is defined in the **Glossary** at the start of this document.

2. Criminal markets

Shann Hulme and Emma Disley, RAND Europe

Key findings:

- This study estimates that the annual revenues of the nine main criminal markets in the EU ranged from €92 to €188 billion (mid-point of €139 billion) in 2019.
- It is not possible to directly compare this overall revenue figure for all nine markets with figures estimated in previous similar studies, because the markets examined are not the same.
- The available evidence suggests an upwards trend in revenues generated through the trafficking of illicit drugs, MTIC fraud and illicit waste trafficking.
- New estimates are produced in this study for the revenues from THB and illicit wildlife trafficking. Since *revenues* from these markets have not previously been estimated (albeit, other estimates exist of harms and costs other than revenues), comparisons over time are not possible.
- It is useful to consider the relative scale of the markets examined in this study. The analysis shows the largest markets in terms of revenue (from the lower boundary estimate) are MTIC fraud, illicit drugs, illicit tobacco (specifically cigarettes) and illicit waste.
- Importantly, estimates of the revenues generated through crime – which are the focus of this study – are only one element of the costs of SOC. Understanding the revenue generated by an illicit market does not capture harms such as violence, exploitation, deprivation, loss to legitimate business or environmental destruction. It is important that understandings of both revenue and costs should inform policy-making. This study aims to make a significant contribution to the former.

Literature review	Interviews	Secondary data
		

The selection of criminal markets examined in this study

This study presents an analysis of nine criminal markets. These markets were selected for analysis because they were identified as priority crime areas in the EU Policy Cycle for organised and serious international crime – or EMPACT (European Multidisciplinary Platform Against Criminal Threats) – for the period 2018 to 2021. This study builds upon an existing and growing evidence base on criminal markets in the EU. Of particular relevance is a previous Commission-funded study by Transcrime – Project Organised Crime Portfolio (OCP) – that was published in 2015 and which also sought to produce estimates of the revenues generated from criminal markets in the EU (Savona & Riccardi, 2015). While the approach and methodologies employed herein are not directly comparable to those adopted by Transcrime or others, to maximise the utility of this report for policy-makers we have attempted to draw some tentative conclusions about change in the scale of markets over time.

Table 2.1: Criminal markets and activities examined in this study

	EU Policy Cycle priority crime area for 2018–2021	Examined in previous Commission-funded study	Section of this report
Illicit drugs	√	√	2.1
Trafficking in human beings (THB)	√	√	2.2
Smuggling of migrants	√		2.3
Fraud	√	√	2.4
Environmental crime	√		2.5
Illicit firearms	√	√	2.6

	EU Policy Cycle priority crime area for 2018–2021	Examined in previous Commission-funded study	Section of this report
Illicit tobacco		√	2.7
Cybercrime	√		2.8
Organised property crime	√	√	2.9

The difference between estimates of revenue, profit and cost

One of the primary objectives of this study was to estimate the revenues generated by actors operating across criminal markets in the EU. **Revenue is the total amount of income generated from the sale of goods or services**. Understanding the revenues generated through crime is important because revenue is a motivator for organised crime, and the investments of revenues in the legal economy may serve to undermine the business environment, lead to corruption and lack of trust in institutions, and negatively impact upon the growth potential of the economy (Pinotti, 2015).

Importantly however, **estimates of the revenues generated through SOC do not capture broader harms** such as violence, exploitation, deprivation, loss to legitimate business or environmental destruction. There have been a number of other studies that have quantified such costs (see for example, Anderson et al., 2013; Anderson et al., 2019; Levi (2016); Mills et al., 2013). Some criminal markets – particularly intellectual property rights (IPR) infringements and counterfeiting, organised property crime, and cybercrime – have been predominantly examined from the perspective of cost or impact, rather than revenue. This reflects the wider interest in quantifying the impact of such crimes on victims (e.g. loss of property) and legitimate industry (e.g. loss of sales). While such estimates are useful and important, these types of costs are not the focus of this study.

This study focuses on revenue as a prelude to exploring criminal investment and infiltration in the legal economy. Importantly however, an understanding of both revenue *and* other harms, as well as the expected sustainability of particular threats, are necessary for informing effective policy action.

This study also does not estimate the net profit of actors involved in SOC, as this would require data on the overhead costs of criminal actors, which is infrequently available nor reliable. Moreover, illicit financial flows or trafficking are not examined in this study, as this would require a breakdown of different levels of the supply chain and the flow of money between these different actors and geographic areas. Each of these concepts, which are different from revenue, are defined in the box below.

Box 2.1: Cost, net profit and illicit financial flows

Estimates of **cost** monetise, where possible, the full range of harms to victims and society resulting from the estimated extent of each crime type. This includes the costs in anticipation of crime (such as security expenditure), costs as a consequence of crime (such as property stolen and emotional and physical impacts), and costs in response to crime (costs to the criminal justice system) (Levi et al., 2013).

Net profit is the proportion of revenues retained by criminal actors after accounting for overhead costs.

Illicit flows or trafficking estimates capture the flow of money generated in criminal markets between different actors in the supply chain, including across national and international borders.

Caveats and criticisms of producing revenue estimates

The hidden nature of SOC inherently challenges the measurement of the phenomenon. There is a well-established literature base that discusses the problems and pitfalls associated with efforts to estimate the size of criminal markets or populations (Calderoni, 2014; Naylor, 2004; Reuter, 1997, 2013). The main points of criticism are that these estimates are built on certain highly disputable and in some cases untenable assumptions; and available data for proxy indicators are inaccurate, incomplete or unreliable to be used in advanced statistical analysis (Levi & Maguire, 2004; Savona, 2014). For instance, based on the assumptions required for the estimation of the 'relatively simple task' of estimating cocaine revenues, Naylor (2004) concludes that the 'reality is that no one has a clue how much illegal money is earned or saved or laundered or moved around the world, or how it is distributed among a host of malefactors.'

In general, the approaches for estimating the revenues of criminal markets are indirect, involving the identification of suitable proxies. Demand-based approaches use indicator data on specific use or consumption of goods or services (e.g. from household surveys). Supply-based approaches rely on data about the amount of goods or services traded or sold (e.g. from law enforcement records of seizures) (Eurostat, 2018). Such proxies involve many assumptions and associated uncertainties. Some of the general challenges in producing revenue estimates of this nature include:

- **There are no official statistics on the earnings of criminals** because the activities are hidden and there is no tax administration.
- **There is a lack of incentive for actors to provide information on their revenues or earnings, or to provide information that is accurate**. For instance, law enforcement may have an incentive to inflate data, whilst criminal actors have an incentive to understate.
- **The risk of double counting** because there is inherent overlap in both the actors and activities within criminal markets. With increasing poly-crime, this is likely to become an ever-present reality. These overlaps present challenges when generating revenue estimates, particularly when seeking to estimate the revenue of the SOC economy across all markets.

Additionally, the data commonly used for estimating criminal markets are prone to a range of biases that may result in over- or underestimation. The main sources of bias are summarised in Table 2.2. As far as possible, the approaches used to estimate the revenue from the nine criminal markets in this report have accounted for and acknowledged these limitations and biases. It is important that the estimations are interpreted with a high degree of caution. They may be better interpreted as an order of magnitude rather than point estimates. It is hoped that this study will provide a springboard for future research that seeks to continually improve upon the information that is available to support revenue estimations of this nature.

Table 2.2: Sources of bias in data commonly used for estimating criminal markets

Source of bias	Description
Selection bias	Occurs when the data is not representative of the target population. For example, law-enforcement data (such as seizure data) only represents crimes that have been detected and recorded, thus not capturing any information about those that occur without detection. Moreover, selection bias may manifest due to non-response to surveys. For example, it is known that some marginalised groups (e.g. people who inject drugs) are less likely to be represented in surveys.
Information bias	Derived from measurement error such as inadequate registration of official law-enforcement data or data reported to EU institutions by Member States, like Eurostat. There may be a lack of harmonisation, differences in national reporting of crime and a divergence between definitions and data collection that may contribute to these information biases.
Recall bias	Systematic differences in actors' ability to recall criminal activities or events. Self-reported data from surveys is particularly prone to this source of bias and self-reported answers might be exaggerated or underplayed. This is known to be particularly the case when being asked about criminal behaviours due to social desirability biases, where it is not deemed socially acceptable to admit to offending behaviour or victimisation.

Source: Adapted from EMCDDA (2019).

The analytical approach to producing revenue estimates in this study

Varying levels of data and information are available about different criminal markets and their sub-markets, and this influences the feasibility of producing reliable revenue estimates. In order to determine whether an estimate could be produced for each market, and the best method for doing so, a systematic approach was taken that involved the following steps:

1. Literature reviews to identify all prior revenue estimates produced since 2010 in the EU.
2. Assessment of each prior study for methodological rigour using a standardised quality appraisal tool (see **Annex 1**).
3. Design of methodological approaches for each market, which considered what was feasible considering the availability of secondary data, and which mitigated – to the best possible extent – potential biases, such as over- and underestimation.
4. Validation and refinement of the proposed methodological approach through stakeholder interviews.

This systematic process resulted in one of three outcomes for each market (and its sub-markets):

- **New or updated quantitative estimates of revenue** – due to sufficient data to do so. This was found to be the case for THB for sexual exploitation, smuggling of migrants, environmental crime (illicit waste and illicit wildlife), illicit firearms, illicit tobacco and road cargo theft (one sub-market of organised property crime).
- **The use of existing revenue estimates** from previous studies – because they represent the best available information and cannot be improved upon. This was found to be the case for illicit drugs, MTIC fraud, card payment fraud (one sub-market of cybercrime) and Automated Teller Machine (ATM) theft (one sub-market of organised property crime).
- **No estimates of revenue** – due to insufficient data and no reliable, prior estimates. This was found to be the case for IPR infringements (where estimates of cost prevail), food fraud, and cybercrime activities (other than card payment fraud).

Every market and sub-market – regardless of whether a quantitative estimate was produced – was subject to qualitative assessment through literature review and stakeholder interviews. Where possible, four research questions were addressed for each illicit market:

1. What is the annual revenue of each illicit market at the EU and Member State level?
2. What is the extent of OCG involvement in each market?
3. Who are the main actors involved in each market?
4. What are the future trends and dynamics of each market?

Aggregation of revenue estimates to produce an overall figure

Where possible, minimum, maximum and mid-level revenue estimates were produced for each market. This generally reflects the range of price information available. Revenue estimates were adjusted for inflation and updated to 2019 values using annual data from Eurostat on the Harmonised Indices of Consumer Prices (HICP) (Eurostat, 2020). Following this, the revenue estimates were aggregated to generate an overall figure of the revenues generated through SOC in the EU.

The aggregate estimate represents, where possible, revenues generated across the 28 EU Member States (including the UK). It was not possible to produce Member State-level estimates for every market, thus precluding an overall figure for each Member State.

Delineating the involvement of OCGs

In this study, market actors and the extent of involvement of OCGs have been explored qualitatively through literature review and stakeholder interviews. However, these interviews and literature reviews identified almost no estimates of the share of each market that is attributable to the activities of OCGs, as distinct from other actors. This reflects varying definitions of OCG and a general lack of data that would allow for a reasonable quantification to be made.

Thus, the revenue estimates made in this study might include some revenues generated by non-OCG actors, as well as by OCGs. For this reason, the revenue estimates that have been

produced should be interpreted as an overestimate of the revenues generated by OCGs, because other non-OCG actors are involved.

Headline revenue estimates and overall figure

The table below presents a summary of the headline revenue estimates produced for each market, along with the aggregated minimum, maximum and mid-point estimates. This study estimates that the annual revenues of the nine main criminal markets in the EU ranged from €92 to €188 billion (mid-point figure of €139 billion) in 2019. It is not possible to directly compare this overall revenue figure for all nine markets with that estimated in previous similar studies (such as that of Savona & Riccardi (2015)), because the markets examined are not the same.

It is useful to consider the relative scale of the markets examined in this study. The analysis shows that the largest markets in terms of revenue (from the lower boundary estimate) are MTIC fraud, illicit drugs, illicit tobacco (specifically cigarettes) and illicit waste.

Table 2.3: Headline criminal revenue estimates

	Criminal markets and areas	Revenues, adjusted for inflation, 2019 (€ million)			Source of estimate
		Mid	Low	High	
2.1	Illicit drugs	30,688.41	26,708.13	35,514.56	EMCDDA & Europol (2019)
2.2	THB for sexual exploitation	7,185.93	401.94	13,969.91	New estimate
2.3	Smuggling of migrants	289.37	215.60	363.15	New estimate
2.4	MTIC fraud	77,425.00	50,858.00*	103,991.67	Frunza (2019), EY (2015)
2.5	Illicit waste*	9,506.62	3,723.49	15,289.74	New estimate
	Illicit wildlife (European eels only)	18.05	4.71	31.39	New estimate
2.6	Illicit firearms	408.09	273.69	753.96	New estimate
2.7	Illicit cigarettes	8,309.15	8,012.62	10,087.48	New estimate
2.8	Card payment fraud	1,816.43	-	-	ECB (2018)
2.9	Cargo theft*	3,347.86	144.39	6,551.32	New estimate
	ATM physical attacks*	22.00	-	-	EAST (2020)
	Total	**139,016.91**	**92,181.00^**	**188,391.61^**	

Notes: Estimates have been adjusted for inflation using price index data from Eurostat (2020). The low and high estimates have been generated using different methodologies, with each described in the annexes that support the market analyses. A common example is the use of a range of price data. In most cases, the mid estimate represents the mid-point (median) between the low and high value. These mid-point estimates should be interpreted with a high degree of caution because the distributions are not necessarily normally distributed, but have nevertheless been provided here for illustrative purposes.
* Denotes that the estimate does not include all 28 EU Member States: **MTIC fraud** lower bound estimate excludes HR and CY. **Illicit waste** estimates exclude BE, CY, LU, MT, SI. Lower bound **cargo theft** estimates exclude AT, BG, HR, CY, EE, FI, EL, LT, LU, ML, PL. Upper bound estimates exclude MT. **ATM theft** estimates exclude BE, BG, HR, EE, HU, LV, LT, MT, PL, SI. ^ Lower and upper boundary aggregate estimates presume card payment fraud and ATM attacks are equivalent to mid-level estimate.

Changes in revenues earned over time

The data inputs and methodologies employed in this study for estimating the revenues of criminal markets are novel, and are thus not directly comparable to previous estimates that have been produced at the EU or Member State level. That said, it is worthwhile to consider the implications of these updated numbers for decision-makers who are tasked with considering where resources should best be targeted. Table 2.4 below provides a snapshot of possible trends in revenues earned across the criminal markets, along with considerations of how these trends should be interpreted.

The available evidence suggests:

- **upward trends** for illicit drugs, MTIC fraud and illicit waste; and
- **downward trends** for smuggling of migrants, illicit cigarettes, and cargo theft and ATM thefts.

There are several markets where previous estimates do not exist or are **not suitable for comparison**, even tentative ones. This study is intended to provide the groundwork for future estimations that might have the opportunity for monitoring over time.

Table 2.4: Revenue trends

Criminal market	Available evidence suggests	Notes for interpretation
Illicit drugs	Upward trend	Previous study methodology by EMCDDA/Europol is similar, so tentative comparisons can be made.
THB for sexual exploitation	Unclear	No previous reliable estimates at EU-level, precluding comparison.
Smuggling of migrants	Downward trend	Our estimate is lower than the previous ones, reflecting the lower number of irregular migrants seeking to enter the EU since the peak in 2015 (FRONTEX, 2020).
MTIC fraud	Upward trend	Frunza (2019) produced estimates for MTIC fraud revenue in 2013 to 2015 and showed an annual growth rate of 20%.
Illicit waste	Upward trend	Previous study methodology by Meneghini et al. (2017) is replicated, so direct comparisons can be made and are reliable.
Illicit wildlife	Unclear	No previous revenue estimates of the illicit wildlife market at the EU-level exist.
Illicit firearms	Unclear	Our estimate had a wider range than previous studies, so no clear trend can be discerned.
Illicit cigarettes	Downward trend	Methodology used to generate our estimate builds upon previous study methodology by Transcrime (2015a), so comparisons can be made and are reliable. The downwards trend is a reflection of a recent decrease in the volume of illicit trade reported by Project Stella, an annual industry-funded survey of the illicit market (KPMG, 2019).
Cybercrime	Unclear	No previous estimates.
Cargo theft	Downward trend	Our new revenue estimate is lower than an earlier estimate produced by FWI SCIC (2016), though methodologies and parameters differ so comparison should be made with caution.
ATM attacks	Downward trend	Data from EAST show a general tendency of decline in value of reported losses since 2015.

2.1. Illicit drugs

Emma Louise Blondes and Shann Hulme, RAND Europe

Key findings:

- According to estimates produced by the EMCDDA and Europol (2019) (adjusted for inflation to 2019 values), the annual revenues earned on the EU illicit drug markets were between €27 and €36 billion (mid-point figure of €31 billion).
- These estimates update the EMCDDA and Europol's previous estimates, which found that in 2013 the EU's overall illicit retail drug markets were worth €24 billion (EMCDDA & Europol, 2016). While comparing the figures suggests an overall increase in the revenue of the EU's drug markets, caution should be exercised because the methodologies between the two years are not directly comparable.
- Since they are highly profitable, the drug markets are particularly attractive for OCGs. Illicit drug markets in the EU are highly competitive, comprising a myriad of loose/horizontal networks acting across the supply chain (including importation, production, distribution and retail). OCGs involved in the EU drugs market are increasingly inter-ethnic and transnational. Nevertheless, these phenomena should not be overstated as some OCGs are still well established along some trafficking

routes.

- The size and composition of groups involved in the EU drug markets varies greatly, not least because no OCG holds a monopoly over drugs' supply chains. While some OCGs are well established along some trafficking roots, most actors involved in the drug markets are better characterised as loose criminal networks or small enterprises carrying out illicit profit-driven activities, rather than highly structured OCGs.
- Future trends and dynamics identified within the EU drug markets include the increasing production of herbal cannabis, synthetic drugs and precursors within the EU; growing online trade; and the use of cutting-edge technology to maximise production output.

The illicit markets for drugs involve the cultivation, manufacture, distribution, sale and purchase of substances that are subject to drug laws. For this study, the drug markets refer to cannabis, cocaine, heroin, synthetic drugs (including amphetamine, methamphetamine and MDMA/ecstasy) and new psychoactive substances (NPS). Excluded from this analysis are pharmaceutical and prescription drugs, as well as drugs used for medicinal purposes.

A comprehensive overview of the illicit drug markets in the EU, building upon the summary provided here, can be found in **Annex 2.1**.

2.1.1. Revenue estimates of the EU illicit drug markets

Table 2.5 presents the revenue estimates produced by EMCDDA and Europol (published in the EU Drug Markets Report and related technical report). According to these figures (adjusted for inflation to 2019 values), the revenues generated from retail markets in the EU for illicit drugs – including cannabis, cocaine, amphetamine, MDMA and heroin – was between €27 and €36 billion (€30 billion) (EMCDDA & Europol, 2019)[9].

- According to the EMCDDA/Europol's drug markets estimates, cannabis was the largest retail market at between €10 and €13 billion (€12 billion), followed by cocaine at between €8 and €11 billion (€9 billion), heroin at between €7 and €9 billion (€8 billion) and synthetic drugs (amphetamine and MDMA) at between €1.3 and €2 billion (€1.5 billion) (EMCDDA & Europol, 2019).
- The EMCDDA/Europol study does not provide disaggregated Member State-level estimates for confidentiality reasons[10]. However, Savona & Riccardi (2015)'s study (using a different methodological basis)[11] highlighted that the EU's four largest economies – namely Germany, France, the UK and Italy – recorded the highest retail revenues for illicit drugs. It is pertinent to note that in 2015, the UK recorded the highest revenue for cocaine and heroin in the EU. This finding suggests that the EU's overall revenue estimate of the EU retail illicit drug markets might differ after the UK has left the EU[12]. Notably, EMCDDA and Europol (2019) report that synthetic drugs are increasingly produced in the EU, both for domestic trafficking and exportation, with Belgium, the Netherlands, the Czech Republic and Poland recording the highest wholesale revenues for synthetic drugs.
- Importantly, Savona & Riccardi (2015) noted that the overall drug markets estimates and country-level estimates presented in their report are not directly comparable, given that they rely on a range of data sources provided by Member States (such as drug prevalence data), which are produced using different methodological approaches and estimated at different times. For this reason, Member State comparison should be done with caution. These results were consistent across the studies identified in the literature review (and discussed in **Annex 2.1**).

[9] EMCDDA & Europol's EU Drug Markets Report and related Technical report (2019) did not estimate the value of the EU's new psychoactive substances' market due to inconsistent consumption data for these drugs.
[10] Interview with EU-level stakeholder, 10 February 2020 (#1).
[11] The OCP project produced its own estimates for the EU cocaine and heroin retail markets, and aggregated existing estimates for the cannabis and synthetic drugs (amphetamine and ecstasy) markets, drawing from Kilmer & Pacula (2009) and Caulkins, Kilmer, & Graf (2013).
[12] In the absence of Member State level estimates, the study cannot deduce a revenue estimate of the EU27 retail illicit drugs markets.

Table 2.5: Revenue estimate of EU illicit drug markets

Drug type	Annual revenue, adjusted for inflation, 2019 (€ million)		
	Mid	Low	High
28 EU Member States	**30,688.41**	**26,708.13**	**35,514.56**
Cannabis	12,029.87	10,891.46	13,258.50
Cocaine	9,376.71	7,894.40	10,859.00
Amphetamine	1,041.89	859.08	1,327.06
MDMA	546.57	452.17	640.98
Heroin	7,693.36	6,611.02	9,429.02

Source: Estimates produced by EMCDDA and Europol are for 2017 (EMCDDA & Europol, 2019), which we updated to 2019 values using Eurostat's HICP (Eurostat, 2020). Estimates are not disaggregated at Member State level, so these estimates represent 28 EU Member States (including the UK).

Previous estimates of EU illicit drug markets

Previous estimates of the illicit drug markets in the EU are shown in the table below. The EMCDDA and Europol published estimates for 2013 and found that the revenues amounted to €24 billion (EMCDDA & Europol, 2016). The cannabis retail market was €9.3 billion, the cocaine retail market was €5.7 billion, the heroin retail market was €6.8 billion and the synthetic drug retail market was €2.4 billion (EMCDDA & Europol, 2016). While these figures suggest an overall increase in revenues, these results between the two years are not directly comparable due to changes in the methodology used to estimate revenues. Other studies have generated estimates of the revenues for specific drug markets, such as cannabis, cocaine and heroin.[13]

Table 2.6: Previous estimates of the EU illicit drug markets (2010 to present)

Member State	Revenue (€ million)			Sub-market	Year(s)	Source
	Mid	Low	High			
EU 28	9,313.4	8,405.6	12,851.2	Cannabis	2013	EMCDDA & Europol (2016)
	5,742.2	4,545.9	6,962.5	Cocaine		
	6,782.7	6,041.6	7,845.6	Heroin		
	2,494.2	1,817.3	3,220.4	Synthetic drugs (methamphetamine, MDMA)		
	24,332.5	20,810.4	30,879.6	**Total market**		
EU 27 (excluding HR)		6,700	9,800	Cannabis	2010	Caulkins, Kilmer & Graf (2013)
EU 24 (excluding CY, LU, MT and SE)	6,765	5,040	7,575	Cocaine	2014	Savona & Riccardi (2015)
EU 19 and Norway	7,996	6,395	10,656	Heroin	2014	Savona & Riccardi (2015)

2.1.2. Criminal actors and modus operandi

The 2017 EU SOCTA estimated that more than 35% of criminal groups active in the EU are directly involved in European drugs trafficking (Europol, 2017b). The drug markets are particularly attractive for OCGs as they are highly profitable and offer numerous business opportunities, given their large consumer base and the variety of products on offer (Savona & Riccardi, 2015). While each drugs market has its own characteristics, this study found that three overall trends characterise the European illicit drugs market:

[13] The research team notes that the Tops et al. (2018) study estimated that the revenue for synthetic drugs in the Netherlands for 2017 was €18.9 billion. While this study presents significant methodological limitations, it has been included in the table presented in the annexe for comparative purposes.

The EU drug markets are highly competitive, preventing any single criminal organisation from gaining a monopoly, even when the organisation is structured hierarchically. Revenues generated from drug trafficking are distributed across the supply chain (importation, production, distribution and retail), which suggests that different levels of OCG involvement should be considered at each stage[14] (Caulkins et al., 2016; Paoli et al., 2017; Savona & Berlusconi, 2015). Paoli et al. (2017) adds that OCG involvement in EU drug markets is characterised by a range of loose/horizontal criminal networks carrying out various illicit profit-driven activities, rather than monopolisation by a few mafia-type and highly structured organisations. Nevertheless, the increased competition within the market does not preclude the strong position of certain OCGs at some levels of the supply chain (Europol, 2017b).

European OCGs involved in the drug markets are becoming more inter-ethnic and transnational. Europol estimates that 70% of OCGs are multinational in their membership (Europol, 2013a). European OCGs are increasingly cooperating to facilitate trafficking across the continent. For instance, the EMCDDA and Europol report that Dutch OCGs are collaborating with traffickers of Turkish origin, resulting in two-way trafficking: Dutch OCGs send MDMA and other drugs from the Netherlands to Turkey in exchange for heroin and morphine (EMCDDA & Europol, 2017)[15]. However, the presence of inter-ethnic OCGs operating across the market should not be overstated, as evidence suggests that some ethnic groups have stronger presence in parts of the market (Saggers, 2019).

EMCDDA and Europol (2019) suggest that **two-thirds of OCGs involved in drug trafficking are also involved in other criminal activities**[16]. The principal overlapping criminal activity is THB and migrant smuggling, likely to result from shared trafficking routes (Saggers, 2019). Saggers reports that heroin is often used as a means of payment between OCGs involved in other drug markets (Saggers, 2019). Similarly, an interviewee claimed that cocaine from the Andean region is imported into the EU in exchange for synthetic drugs sent back to South America. However, these poly-criminality trends should not be overstated as there is limited substantive evidence to support these claims.

Modus operandi

Cannabis: The European **cannabis market** comprises resin and herbal cannabis, which are considered by Europol as two distinct markets regarding illicit trafficking (Europol, 2017b). **Herbal cannabis** consumed in Europe is primarily produced in the Netherlands, Belgium, Italy and Spain, though the EMCDDA reports that it is difficult to estimate the number of production sites in the EU (EMCDDA & Europol, 2019). Some herbal cannabis consumed in the EU is also produced in Albania (Europol, 2017b). The EU SOCTA 2017 reports that **cannabis resin** consumed in the EU mainly originates from Morocco, entering Europe through Spain, France and the Netherlands (Europol, 2017b). Libya has also emerged as an important transit hub for cannabis being transported to Europe (Europol, 2017b). Europol (2017b) reveals that the European resin and herbal cannabis markets are increasingly competitive and specialised, leaving room for more loosely organised OCGs to get involved along the supply chain. The growing level of competition within the European cannabis markets has reportedly led to increased violence (Europol, 2017b). Nevertheless, the EMCDDA reports signs of growing cooperation between some OCGs involved in the EU's cannabis market, though the dynamics that determine these inter-relationships are not currently well understood.

Cocaine: The EU's cocaine market is expanding as global production is increasing, particularly in the Andean region (Europol, 2017b). According to Saggers (2019) and Europol (2017b), a range of OCGs are involved in the EU cocaine market, and the drug is imported into the EU via various traditional means of transportation, including general aviation, as part of large shipments in containers – hidden among legal goods – or in smaller quantities by couriers. The EMCDDA notes an emerging trend, whereby European OCGs use national overseas territories – that are part of the European single market and European customs territory – located close to production countries, to smuggle cocaine into Europe (EMCDDA, 2018).

Heroin: Most of the heroin imported to Europe is produced in Afghanistan and trafficked into the EU via the Balkan route (UNODC, 2015). EMCDDA and Europol (2019) highlight that Turkish OCGs coordinate most of the European heroin importations, benefiting from well-established networks and infrastructure across the continent, although the distribution of heroin across

[14] Interview with EU-level stakeholder, 10 February 2020 (#1); Interview with EU-level stakeholder, 12 February 2020 (#3).
[15] Interview with EU-level stakeholder, 11 March 2020 (#14).
[16] Interview with EU-level stakeholder, 10 February 2020 (#1).

Europe is shared by a range of criminal organisations. Europol and stakeholder interviews revealed there has been evidence of laboratories starting to produce heroin precursors within EU for exportation (Europol, 2017b)[17].

Synthetic drugs: The EU SOCTA 2017 reports that the EU is a significant hub for the production and distribution of synthetic drugs, including amphetamine, MDMA and – to a lesser extent – methamphetamine (Europol, 2017b). Europol suggests that OCGs increasingly use online platforms to traffic synthetic drugs both within and outside of the EU, taking advantage of legitimate postal services to carry out their illicit activities. Europol signals that the European synthetic drugs market is highly flexible, with OCGs constantly exploring new avenues to expand and diversify this illicit market.

NPS: NPS continue to pose significant risks in Europe, despite a decrease in the number of first-substance detections. EMCDDA (2020b) report that over 790 NPS were reported to the EU Early Warning System, of which 53 were detected in 2019. An EU-level representative highlighted the significant knowledge gaps regarding NPS consumption and trafficking in the EU[18]. The interviewee stressed that NPS can be misleadingly sold as traditional drugs, making their detection particularly difficult for law enforcement, and significantly increasing health risks.

2.1.3. Future trends and dynamics

Cutting-edge technology has helped drug producers maximise their production outputs. Sophisticated technologies include climate-control systems to produce more herbal cannabis in the Netherlands, solar-powered tube wells to increase opium production in Afghanistan, or new technologies used for industrial-like synthetic drugs production in the EU. This phenomenon is leading to an increase in productivity and hence to a potential growth of production and trafficking volume. However, the large-scale productions are also making OCGs less agile.

Herbal cannabis, synthetic drugs and pre-precursors[19] are increasingly produced illegally in the EU, creating new business opportunities for OCGs. These drug markets are becoming even more profitable, as OCGs exploit regulatory loopholes and global commercial trafficking routes to reach a larger EU customer base and export substances outside of the EU. EMCDDA and Europol (2019) also warn that this increased production carries significant health and environmental harms.

Online trade is becoming more prevalent within Europe's drug markets (EMCDDA & Europol, 2017)[20]. Online platforms enable drug suppliers to improve their business models and increase profit margins, through encrypted technologies and by allowing suppliers to deliver drugs directly to consumers, with limited security risks. While studies confirm that the online drug markets are still relatively small compared to street-level drug markets, they show that online markets are predominately used for mid- and low-level transactions, though the models differ by drug type (EMCDDA & Europol, 2017; Kruithof et al., 2016). Although online drug markets appear to be proliferating, these trends should not be overstated, given the preliminary nature of these assessments.

2.1.4. Recommendations

This study finds that there are two principal ways in which data collection and estimation on the illicit drug markets could be improved in the EU:

- First, two stakeholders noted that the data gaps identified in the literature review could be filled by **encouraging Member States to consistently collect prevalence data on drugs on an annual basis**[21]. As such, estimates could draw from annual data rather than averages of annual data spanning four to five years.

[17] Interview with EU-level stakeholder, 12 February 2020 (#3); Interview with EU-level stakeholder, 11 March 2020 (#14).
[18] Interview with EU-level stakeholder, 12 February 2020 (#3).
[19] Amphetamine, methamphetamine and MDMA are produced from chemical starting materials called drug precursors. These drug precursors may also have legitimate uses and are strictly regulated at the global level to avoid diversion for illicit use. Yet, to bypass these regulations, OCGs producing illicit drugs in the EU have introduced alternative chemicals, which are then converted into drug precursors to produce synthetic drugs.
[20] Interview with EU-level stakeholder, 10 February 2020 (#1); Interview with National-level stakeholder, 25 February 2020 (#35).
[21] Interview with international-level stakeholder, 10 February 2020 (#2) and Interview with EU-level stakeholder, 12 February 2020 (#3).

- Second, two stakeholders highlighted the need to **better adjust prices for drugs' purity or potency levels**[22]. One interviewee suggested that improving forensic investigations on drugs could help collect robust data on drug purity level and retail price[23]. Further, the interviewee added that forensic investigations could provide more information about the origin of imported drugs, and pertinent data on the health implications of drugs consumed in the EU.
- The key findings, recommendations and actors for actioning or implementing these recommendations are summarised in the table below.

Table 2.7: Recommendations – Illicit drugs

Key findings	Recommendations	Key actors for recommendations
The EMCDDA and Europol produce demand-based estimates of the revenue of the retail illicit drug markets at the EU-level using routine data collections from Member States on prevalence of consumption and price and the European Web Survey on Drugs on quantities consumed. However, price data is not adjusted for purity and estimates at Member State level are not published. Of the markets examined in this study, the illicit drug markets represent the second most significant in terms of revenues generated in the EU.	Member States should collect annual prevalence data via general population surveys so that EU-level estimates can be updated annually. There should be continued efforts to harmonise the data collected by Member States. There should be efforts to improve forensic testing of drugs so that price data can be consistently purity-adjusted across Member States. The EMCDDA and Europol should share Member State disaggregated estimates with the European Commission. This will be particularly important going forward since the UK has left the EU, and the current estimates include the UK. The work of the EMCDDA and Europol in providing a factual overview of European drug problems, and a solid evidence base for informing drug policy should be further strengthened.	Member States European Commission EMCDDA Europol

2.2. Trafficking in human beings

Alexander Gerganov, Kamelia Dimitrova and Atanas Rusev, Centre for the Study of Democracy

Key findings:

- According to the new estimates produced in this study, the annual revenues derived from THB for sexual exploitation in the EU range between €0.4 and €14 billion (mid-point figure of €7 billion).
- This is the first time a reliable estimate at the EU-level has been produced for criminal revenues generated from THB for sexual exploitation, since all previous estimates referred to wider world regions.
- There is heavy involvement of OCGs in trafficking for sexual exploitation (including Nigerian OCGs), as well as in trafficking for forced criminality, for begging and for organ removal.
- The typical structure of criminal groups who are active in this market consists of loose networks, linked by family kinship or ethnic ties.
- Other key actors are various legitimate businesses involved in the trafficking chain who benefit from victims trafficked for sexual and labour exploitation and other exploitation, including companies in sectors such as transport, hospitality, agriculture, entertainment industry, construction and catering, etc.
- Criminals increasingly use the internet and technological advances to recruit, control and exploit their victims and hide the criminal proceeds.

[22] Interview with international-level stakeholder, 10 February 2020 (#2) and Interview with EU-level stakeholder, 12 February 2020 (#3).
[23] Interview with EU-level stakeholder, 12 February 2020 (#3).

- In addition to the traditional trafficking flow from Eastern Europe to Western Europe there are multiple and diverse flows of victims trafficked to the EU from all over the world. In terms of THB, Nigeria and China contribute the most.

The current study adopts the definitions of THB and exploitation as laid down in Directive 2011/36/EU: 'the recruitment, transportation, transfer, harbouring or reception of persons, including the exchange or transfer of control over those persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation'. The detailed definitions for exploitation, as well as the different forms of THB are provided in the **Glossary** at the beginning of this report.

A comprehensive overview of THB in the EU, building upon the summary provided here, can be found in **Annex 2.2**.

2.2.1. Criminal revenue estimates of trafficking in human beings for sexual exploitation in the EU

The table below presents the estimates produced for this project on THB for sexual exploitation in the 28 EU Member States. According to these figures, annual revenues derived from THB trafficking range between €0.4 and €14 billion (€7 billion mid-range estimate). THB for sexual exploitation is the most prevalent form of THB in the EU (European Commission, 2016c, 2020g).

- The results show that a conservative (lower bound) revenue estimate is €402 million (€274 million excluding the UK) just from trafficking for sexual exploitation. At the same time, a tentative estimate accounting for the much higher population of hidden victims of trafficking for sexual exploitation shows that the overall criminal revenue could be as high as €14 billion.
- Data on different Member States indicate a disproportionately large contribution of UK, France, Germany, Hungary, Italy and the Netherlands, which together account for 85% of the total market (UK alone accounts for 32% at €130 million of the lower boundary estimate). It should be noted though that the differences between Member States stem mainly from the number of registered victims, while the difference between average annual revenues per victim are much smaller. Therefore, the relative weight of particular Member States in the total revenue estimate produced should be interpreted with caution, since it likely stems not only from the actual number of victims, but also from the differences in collecting and providing information about victims of THB (as discussed in previous sections).
- The lower bound estimate of the criminal revenue generated by THB for sexual exploitation uses a supply-based approach, multiplying the number of victims by the average revenue per victim. Due to the unavailability of reliable methodologies to estimate the actual number of victims of THB in the EU[24], we multiplied the number of registered victims from the Commission data collection (European Commission, 2018b)[25] with the annual revenue per sex worker[26] as a proxy for the annual revenue per victim of trafficking for sexual exploitation. This approach provides a much lower estimate of the criminal revenue generated from THB for sexual exploitation.
- A tentative upper bound estimate for the whole EU was produced based on the much higher estimate of the International Labour Organisation (ILO)[27] for the victims of 'forced sexual exploitation', which also accounts for the hidden population. The upper bound estimate uses the same proxy values for the annual revenue per victim of trafficking for sexual exploitation, which was applied for the lower bound estimate.

[24] UNODC multiple-system estimation can be used to produce national-level estimates but has only been applied so far in a few EU Member States (UNODC, 2018c).
[25] The estimates were produced prior to the publication of the more recent data from the European Commission (2020g).
[26] The term 'sex worker' is used in Europol's report 'The THB Financial Business Model' (2015). It should be noted that prostitution and the sex industry are high-risk sectors for women and children trafficked for sexual exploitation. Sex workers and victims of THB for sexual exploitation cannot be conflated, and the approach uses only the earnings of sex workers as a *rough proxy* for the possible revenues generated by the victims of THB for sexual exploitation.
[27] The most recent estimate available for the EU is for 270,000 persons (ILO, 2012).

Despite the methodological caveats of producing such an upper bound estimate drawing on ILO data, such an approach is also in line with Europol practice of using ILO's estimates as a yardstick for the size of the criminal revenue deriving from THB for sexual exploitation (Europol, 2015c).

- It must be emphasised that while the ILO's definition of victims of forced sexual exploitation is broadly based on the Palermo protocol, it deviates significantly from Directive 2011/36/EU (which outlines the scope and focus of the current endeavour). In addition, the latest available ILO estimates for the EU (made for 2012) were published just after the Anti-trafficking Directive was adopted, and data collections in the EU on THB victims have been developed in relation to the Directive. Therefore, the upper bound estimate does not consider the social and economic developments since 2012, which have had an impact on the number of victims trafficked for sexual exploitation.

Table 2.8: Criminal revenue estimate of trafficking in human beings for sexual exploitation in the EU

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)		
	Mid	Low	High
28 EU Member States	**7,185.93**	**401.94**	**13,969.91**
27 EU Member States without UK		**273.70**	
Austria		9.05	
Belgium		2.46	
Bulgaria		6.30	
Croatia		0.44	
Cyprus		0.99	
Czech Republic		0.07	
Denmark		7.26	
Estonia		0.14	
Finland		1.96	
France		78.30	
Germany		30.00	
Greece		3.63	
Hungary		29.98	
Ireland		2.65	
Italy		50.10	
Latvia		0.55	
Lithuania		0.25	
Luxembourg		1.63	
Malta		0.07	
Netherlands		24.20	
Poland		1.92	
Portugal		0.91	
Romania		7.95	
Slovakia		0.41	
Slovenia		1.01	
Spain		7.16	
Sweden		5.01	
United Kingdom		129.73	

Note: Lower bound estimates were produced for 2016 and updated to 2019 values using Eurostat (2020) HICP. Upper bound estimates were produced for 2012 and updated to 2019 values using Eurostat (2020) HICP.

The lack of previous revenue estimates of trafficking in human beings in the EU

The UNODC employed a supply-sided approach to produce an estimate of annual revenues deriving from THB for sexual exploitation in **all European countries**[28] of €2.5 billion for the period 2007–2008 (UNODC, 2010). In a report from 2015, Europol provided estimates of the revenue of THB for sexual and labour exploitation in the **EU and developed economies**[29], which actually quoted earlier estimates produced by ILO (Europol, 2015c). According to the Europol report, the annual profits from THB for sexual exploitation in EU and developed economies amounts to €23.5 billion (Europol, 2015c).

The estimates provided by UNODC and Europol/ILO pertain to wider world regions, draw on different sources of data and use methodologies with various limitations (as discussed in the earlier section on the quality of prior estimates). Neither of the previous estimates are directly comparable to the current estimates produced specifically for the 28 EU Member States.

2.2.2. Criminal actors and modus operandi

THB networks can be characterised as small or medium sized, highly organised or individual domestic traffickers (UNODC, 2014). According to an expert[30] the proportion of OCG convictions related to THB are relatively higher than those in other criminal areas, such as drug trafficking and smuggling. OCGs are especially involved in THB for organ removal and THB for forced criminality. THB for sexual exploitation is conducted by both highly organised OCGs (such as Nigerian networks), as well as by independent traffickers.

THB heavily involves OCGs, but family ties are also abused (European Commission, 2020g). **Small or medium sized OCGs are often family- or clan-based and engage in sub-regional trafficking**. Highly organised, large-scale OCGs engage in sub-regional or trans-regional trafficking. By all accounts, these OCGs are more prevalent among non-EU actors, such as Nigerian and Chinese OCGs. These OCGs handle all phases of the trafficking process independently, and are able to hide their activities via legal businesses. Unorganised domestic traffickers are usually independent individual traffickers who deceive one or a couple of victims interpersonally, and tend to operate over short distances (UNODC, 2014).

Most traffickers originate from EU Member States. In 2015–2016, most people who were suspected (84%) or prosecuted (87%) in the EU for THB and had known citizenship were nationals of Member States. Some three-quarters of these were adult men. Bulgaria, Romania and Germany were among the top five citizenships in terms of suspects for both 2010–2012 and 2015–2016. When considering suspects, prosecutions and convictions together, Romania, Hungary, the Netherlands, Poland and Bulgaria were in the top five in 2015–2016 (European Commission, 2018c).

Modus operandi

Traffickers predominantly recruit victims for sexual exploitation via 'lover boy' methods, where victims are manipulated to become emotionally attached to their exploiters (Shentov et al., 2019). West African victims are often recruited and controlled via the abuse of cultural beliefs. Nigerian OCGs use psychological techniques related to *juju* folk magic for recruiting and keeping victims compliant. Contracts are made between exploiters and victims through the *juju* ritual, which is used to great effect in deterring victims from breaching the agreement because they believe bad omens, even death, will follow[31].

The internet is increasingly used for the recruitment, control and exploitation of victims. Traffickers increasingly use the internet and social networking tools to recruit victims, for logistics, to enable the exploitation of victims, and as a marketing platform for prostitution (European Commission, 2018c; 2020g). Exploiters use digital surveillance to monitor their

[28] This guesstimate included the 28 EU Member States in addition to Iceland, Liechtenstein, Norway, Switzerland, the Western Balkans and Turkey.
[29] EU-27, UK, Canada, USA, Australia, Gibraltar, Greenland, Isle of Man, Israel, Japan, New Zealand, San Marino, St. Pierre and Miquelon, Andorra, Iceland, Liechtenstein, Monaco, Norway and Switzerland.
[30] Interview with International-level stakeholder, 20 February 2020, #33; Interview with EU-level stakeholder, 26 February 2020, #36.
[31] Interview with Member State stakeholder (SE), 10 March 2020 (#43).

victims remotely and distance themselves from the scene of the crime. Traffickers increasingly rely on digital communication (i.e. social media, messaging apps, VoIP) in all phases of the THB process (European Commission, 2018c).

Victims of THB for labour exploitation are recruited through deception – either online or by word of mouth – and are controlled through manipulation. Victims are usually recruited via deception about the nature or conditions of the work, with promises of well-paid jobs with no requirement for qualifications. The recruitment is conducted by online advertisements, newspapers, word of mouth and local employment agencies (European Commission, 2020g; Europol, 2016b). Compliance is achieved less and less by the use of force, and more by subjecting victims to verbal manipulation, psychological pressure and threats. Victims are told that they have incurred significant costs for their transport, accommodation and arrangement of logistics, which they have to repay through long hours of labour (Europol, 2016b).

OCGs increasingly infiltrate and use legal business in their operations. OCGs infiltrate or create legal business structures to recruit workers, engage in a contractual relationship with them and move them to the country of exploitation (European Commission, 2020g; Europol, 2016b). This also serves as a facade for criminal activities because it gives an impression of legitimacy[32]. Cascade subcontracting is also used to conceal THB for labour exploitation (Davies & Ollus, 2019).

Traffickers recruit child victims from impoverished families, or target adults with physical and psychological disabilities for forced begging. Victims are controlled and exploited through exertion of pressure to beg (Europol, 2014a). Traffickers target impoverished families and push them into debt through targeting by complicit money lenders. The high interest rates prevent families from paying off their debt, and thus prompts them to put children in exploitative situations (Europol, 2014a). Roma, especially women and girls, are particularly vulnerable to THB for forced begging (Europol, 2016b). OCGs involved in THB for forced begging specifically target vulnerable people, such as adults with physical and psychological disabilities, or single mothers (Europol, 2014a).

OCGs capitalise on severe organ scarcity to meet demand for organ transplant and exploit impoverished people who are willing to sell their organs. The severity of organ scarcity leads to the functioning of the black market, where OCGs may act as a link between impoverished people who are willing to sell their organs, and those seeking transplants (UNODC, 2014). Trafficking networks involved in trafficking of persons for organ removal vary in size, division of tasks between the actors and geographical scope of the activities. Experts point to the predominant involvement of OCGs due to the transnational and highly profitable nature of the crime[33]. Typically, brokers, local recruiters, healthcare professionals and facilitators are involved in committing the crime (Bos, 2015). According to the latest data, 17 cases of trafficking for organ removal were reported in the EU by Member States during 2017 and 2018 (European Commission, 2020c).

THB for criminal activities is on the rise in the EU. THB for criminal activities illustrates the poly-criminality of THB. Victims are increasingly used by THB networks for criminal activities, such as begging, benefit fraud, identity fraud, credit fraud and insurance fraud (Europol, 2015c). Member States report an increase in trafficking for forced criminality (European Commission, 2018c; 2020g). Children are especially vulnerable to trafficking for criminal activities due to their dependency on adults (Europol, 2014a). Europol reports that victims of THB are often also exploited for the production and trafficking of drugs (Europol, 2016b).

2.2.3. Future trends and dynamics

To control victims, traffickers increasingly use psychological and emotional violence and threats, rather than physical abuse. There is increased targeting of people with developmental and physical disabilities (European Commission, 2018c; 2020g), and the age of identified victims is decreasing, with children constituting nearly a quarter (23%) of identified victims (European Commission, 2018c). Children from Eastern European countries and Roma communities continue to be particularly vulnerable, with traffickers exploiting kinship in order to organize recruitment and exploitation of the child. According to Europol, organised crime will continue to target vulnerable persons for exploitation, with an increasing targeting of EU citizens (Europol, 2017b).

[32] Interview with EU-level stakeholder, 12 March 2020 (#49).
[33] Interview with EU-level stakeholder, 26 February 2020 (#36); Interview with EU-level stakeholder, 20 February 2020 (#33).

Traffickers increasingly use legal businesses that can conceal exploitation, such as hotels, nightclubs and massage parlours. Legal business structures are expected to be targeted on an unprecedented scale, both for infiltration and for exploitation of the victims of trafficking (European Commission, 2020g; Europol, 2017b). Higher demand for cheap labour is expected to result in higher levels of THB for labour exploitation, especially in less regulated industries and those with seasonal demand of labour force (Europol, 2017b).

Traffickers continue to rely on the use of social media, VoIP and instant messaging applications at all stages of the THB cycle. A Europol report on the future of organised crime reveals that technological advances in robotics, nanotechnology, cryptocurrencies and digital surveillance – as well as the digitalisation of big data – could be enabling factors for traffickers to create new sophisticated strategies, and simultaneously reduce their chances of detection (Europol, 2015b). The ongoing outsourcing of data management to a few consolidated companies on a global level will create new opportunities for cyber-stealing of personal data (i.e. identities for victims) or information related to transportation and logistics (Europol, 2017b).

2.2.4. Recommendations

There are two principal ways in which data collection and estimation on THB (for various types of exploitation) could be improved in the EU:

- First, the Commission's data collection on THB provides a sound basis for establishing the number of identified and presumed victims, but an additional step is needed in order to account for the full extent of the phenomenon – **a reliable estimate of the hidden population which is not registered and therefore not included in the statistics** (European Commission, 2018c; 2020g).

  Various methods for estimation of hidden populations have been suggested and successfully applied in many other fields, such as problem drug-use (EMCDDA & Pompidou Group, 1997). Similar approaches might be discussed, agreed and eventually supported by the Commission for producing estimates of the hidden population of THB victims at Member State level, and ultimately at EU level. Reliable estimates of this population will eventually allow a more accurate estimate of criminal revenues, not only from THB for sexual exploitation, but also from the other forms of THB.

- Second, there is a clear lack of systematically collected data on the annual profit generated by victims for the traffickers involved in different forms of THB. **Collecting such data – especially for identified victims – could facilitate future estimation of the revenues deriving from THB**. Currently information on revenues generated by victims is collected within financial investigations related to THB cases, when police or judicial authorities trace finances and assets of perpetrators. The Commission might consider requesting that Member States mandate their police and/or judicial authorities to collect or report this data, along with the number of registered victims.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.9: Recommendations – Trafficking in human beings

Key finding	Recommendation	Actor
The European Commission collects data on the number of registered victims of THB, which provides the basis for the lower boundary estimate of THB for sexual exploitation at the Member State level. However, there is no agreement on how best to account for the hidden population of victims, and the only available proxy for monetising these estimates is the revenues generated through sex work. There are no secondary data sources available for reliably estimating the revenues generated through THB for reasons other than sexual exploitation (i.e. labour	Consideration to be given to how to best estimate the hidden population of THB victims at EU level by developing the range of methodologies currently available. This will improve estimation of potential number of victims for THB for various forms of exploitation, including for sexual and labour exploitation. Member States should systematically report to the European Commission information on revenues generated through THB, which is currently collected by police or judicial authorities in the course of their investigations.	Member States, particularly police and judicial authorities EU Anti-Trafficking Coordinator European Commission

Key finding	Recommendation	Actor
exploitation, forced begging, organ removal or participation in criminal activity).		

2.3. Smuggling of migrants

Quentin Liger, Optimity Advisors

Key findings:

- According to the estimates produced for this study, the annual revenues derived from the smuggling of migrants in the EU range from €165 to €278 million (€221 million).
- The estimate is lower than in previous studies, reflecting the lower number of irregular migrants seeking to enter the EU since the peak in 2015 (FRONTEX, 2020).
- A diverse range of actors within migrant smuggling networks perform a variety of roles, from small, local facility-based operations to larger criminal networks. Over time groups have become more structured and hierarchical, with a more developed use of new technologies including encrypted messaging systems (such as Telegram) or the dark net.
- The phenomenon of migrant smuggling is not expected to subside in the coming years. However, the number of migrants smuggled, their country of origin and the routes they have taken have evolved. While migration and smuggling routes change on a regular basis in response to external factors, hubs where the demand and supply of smuggling services meet, are rather more stable over time. These hubs are often important metropolitan areas.

According to the UNODC, smuggling of migrants is a crime involving the procurement for financial or other material benefit of illegal entry of a person into a State of which that person is not a national or resident (UNODC, 2011b).

A comprehensive overview of the smuggling of migrants in the EU, building upon the summary provided here, can be found in **Annex 2.3**.

2.3.1. Revenue estimates of smuggling of migrants in the EU

Table 2.10 below presents the estimates produced for this study for smuggling of migrants at the EU-level and for different smuggling routes. The results show that:

- The estimated revenue of the smuggling of migrants in the EU ranged from €213 to €363 million.
- The Eastern Mediterranean route constituted the largest market share, at between €81 and €122 million.

A sensitivity analysis shows that unsurprisingly, the figures vary proportionally if the assumption of migrants paying for their journey changes from 90% to 70%, providing a low, high and mid estimate of €165 million, €221 million and €278 million respectively.

At the time the research was undertaken, there were little data on secondary movements within the EU and to the UK. Furthermore, the methodology used does not allow for a granular assessment of the revenues for the smuggling of migrants along the Western Balkan routes.

Table 2.10: Revenue estimate of smuggling of migrants in the EU

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)		
	Mid	Low	High
28 EU Member States*	**287.97**	**212.78**	**363.15**
Western African route	1.03	0.69	1.38
Western Mediterranean route	68.40	49.07	87.73
Central Mediterranean route	70.53	45.60	95.46
Western Balkan route	33.56	24.45	42.66

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)		
	Mid	Low	High
Eastern Mediterranean route	101.72	81.34	122.10
Black Sea Route	0.00	0.00	0.00
Circular Route	4.18	4.18	4.18
Eastern European route	4.36	4.36	4.36

Notes: *While the smuggling routes do not provide a clear breakdown of estimates per Member State, they do include all detections at the external borders of the Union. Estimates were produced for 2018 and, for the 28 EU Member States, were updated to 2019 values using Eurostat's HICP (Eurostat, 2020). The estimates by route are the original 2018 estimates.

Previous revenue estimates of smuggling of migrants in the EU

Table 2.11 below shows previous estimates (published since 2010) of smuggling of migrants in the EU. According to the UNODC Global Study on Smuggling of Migrants, at the European level in 2016, the three Mediterranean routes (the main channels of irregular migration into the EU) stood at 375,000 migrants, for a total value of between $320 million and $550 million (USD). These estimates only relate to the crossing of the Mediterranean Sea into the EU. In order to have a more holistic picture, the volume and value of migrants smuggled within Africa to the north African shore was estimated at 480,000 migrants per year, for a total value of between $1.06 billion and $1.514 billion (USD) (UNODC, 2018). According to a joint Europol-INTERPOL Report, the annual turnover of the smuggling of migrants to the EU was worth an estimated $6.6 billion (USD) in 2015 alone (Europol-Interpol, 2016).

The differences between the current estimate developed for this study and previous one's stem from the reduction in the in number of migrants seeking to enter the EU which peaked in the autumn of 2015 and has been steadily dropping since (FRONTEX, 2020).

Table 2.11: Previous estimates of the smuggling of migrants in the EU (2010 to present)

Member State	Revenue (€ million)			Year(s)	Source
	Mid	Low	High		
EU 28	-	320 (USD)	550 (USD)	2016	UNODC (2018)
EU 28	-	320 (USD)	550 (USD)	2016	UNODC (2018)
EU 28	6,600	-	-	2015	Europol-Interpol (2016)
EU 28	190	-	-	2017	Europol (2018a)

2.3.2. Criminal actors and modus operandi

The smuggling of migrants is a complex field often involving different smugglers, facilitators and organisations who have a variety of motives. The concept and definition of a smuggler can be hard to pinpoint. Siegel provides an ethnographic assessment of the views migrants have of migrant smugglers, and the complexities of relationships between migrants and smugglers (Siegel, 2019).

The organisation and size of smuggling operations vary. According to UNODC, some smugglers provide limited small-scale services, whereas other smugglers belong to large and well-organised hierarchical criminal operations with transnational links and the capability of organising sophisticated smuggling passages (UNODC, 2018). According to Optimity, the business of smuggling usually functions as a network model of OCGs, with communication links between smaller groups of actors/facilitators to enable movement of people from one country to another, from source to destination. There may be multiple OCGs within a country, and networks can span borders or have links with other OCGs across borders. Networks cluster to form hubs where the intensity of smuggling activities is greatest (Optimity Advisors, 2015).

According to a study by Tiniti and Reitano (2016), there is a diverse range of actors within a network, who perform a variety of roles in the business of smuggling of migrants: *smuggler/top men*, *recruiters*, *guides*, *drivers* or *skippers*, *spotters/messengers*, *money collectors*, *forgers* (passports / formal documents), *suppliers* (boat makers, boat owners, car/bus owners), *corrupt policy officials* (immigration officials) and *corrupt service providers* (train conductors etc.), and

enforcers. Their role and function usually varies according to the type and scale of the smuggling network in which they are involved, and as to the range of services provided to migrants (Tiniti & Reitano, 2016).

The market for the smuggling of migrants is a flexible one due to low barriers to entry, low skills and (relatively) low capital requirements (Optimity Advisors, 2015). A study by Campana (2017) found that the costs to the smugglers of monitoring agents and clients are also likely to be modest, particularly in comparison with THB. Furthermore, given the low barriers to entry, the market entails low levels of organisational complexity. Independent operators often work on behalf of friends and family members, or are migrants themselves trying to reach a destination (Sanchez, 2018). A law enforcement representative interviewed highlighted how as migration enforcement and criminalisation increases, smuggling activities are increasingly facilitated by local operators, who specialise in the provision of specific tasks (such as Hawala, crossing a specific border, etc.)[34].

According to a law enforcement representative[35], **there has been an increase in the involvement of criminal networks over time**. Groups have become more structured and hierarchical, with a more developed use of new technologies, including encrypted messaging systems (such as Telegram) or the dark net. On the other hand, low profile facilitators – such as lorry drivers – who are part of the criminal chain work for different criminal organisations in a less structured way. Another trend is in the increasing use of violence and reckless techniques to extract a profit. A number of contributions from Member States to Europol highlighted behaviours that put the lives of migrants at risks.

When OCGs are involved in the smuggling of migrants, they are often also active in other crime areas, especially document fraud and THB. It is also possible that OCGs specialised in the smuggling of migrants cooperate with OCGs involved in other crime areas (Europol, 2018a).

Modus operandi

Optimity's study showed that from a supply-side perspective, smugglers (sellers) tend to advertise their business where migrants (buyers) can be easily reached, such as in neighbourhoods where diaspora communities live, in refugee camps or in various social networks online. The study suggested that smugglers' proactive recruitment and misinformation increased the number of migrants who were willing to buy smuggling services (Optimity Advisors, 2015).

From a demand-side perspective, evidence suggests that conflicts, civil unrest and security issues in countries of origin often result in a huge growth in the number of irregular migrants, and corresponding demand for smuggling services (Optimity Advisors, 2015).

According to the same source, the business of smuggling is best described as a **network model**, with a network of communication links between smaller groups of actors/facilitators to enable movement of people from one country to another, from source to destination (Optimity Advisors, 2015). There may be multiple networks within a country, and networks can span borders and/or have links with other networks across borders. Networks cluster to form hubs where the intensity of smuggling activities is greatest. Smuggling of migrants is different than THB. In the case of smuggling the person is seeking to cross a border willingly (and pays for the service). In the case of THB, people do not necessarily cross a border (but can be trafficked within their own country), and as victims of a criminal offence, their consent to such criminal act is irrelevant. This is not to say that smuggling is not dangerous. In 2016 alone, 4,581 people died at sea on the Central Mediterranean route (UNODC, 2018). This figure only reflects the human cost for one route, and does not consider the likely higher number of deaths on the routes from the countries of origin to the Mediterranean coast.

2.3.3. Future trends and dynamics

According to the International Centre for Migration Policy Development (ICMPD), given the situation in countries of provenance, **the phenomenon of the smuggling of migrants is not expected to subside in the coming years** (ICMPD, 2020). However, the number of migrants smuggled, their country of origin and the routes taken have evolved. This is expected to continue in the coming years. One prediction by the ICMPD is that the central Mediterranean route might lose importance if the peace process in Libya achieves an end to the conflict and brings political stability. On the other hand, Europol expects ongoing turmoil in Syria, Iraq and

[34] Interview with law enforcement representative, 19 March 2020 (#67).
[35] Interview with law enforcement representative, 19 March 2020 (#67).

Iran (which is still hosting over 2.5 million refugees from Afghanistan) to keep the eastern Mediterranean route as a focus of the smuggling of migrants (Europol, 2018a). Smuggling of migrants from Africa is expected to continue (Europol, 2018a).

Furthermore, the EU SOCTA report expects an increase in the number of fraudulent documents being used as part of a wider increase in the abuse of legal channels to get into the EU (Europol, 2017b). While migration and smuggling routes change on a regular basis in response to external factors, **hubs where the demand and supply of smuggling services meet are rather more stable over time** (UNODC, 2018). These hubs are often located in important metropolitan areas.

2.3.4. Recommendations

There are three principal ways in which data collection and estimation on smuggling of migrants could be improved in the EU:

- From the perspective of the number of migrants being smuggled, **data on detections at borders are generally considered to be of very high quality**. For reasons that range for the political to the humanitarian, border agencies are considered to have a high detection rate of irregular migrants crossing the external borders of the EU. Furthermore, these data are reported on a monthly basis by law enforcement authorities, as well as the high number of border and coast guards involved in data collection. The number of secondary and tertiary movements is much harder to assess, for reasons linked to the absence of border checks within the Schengen area.
- A more thorough assessment and compilation of the **price of smuggling operations** could be developed. Unlike other markets presented in the report, the supply of smuggling of migrant services involves many people. A migrant setting off from West Africa might use one network to cross the Sahel region, and another to cross the Mediterranean Sea for instance. As such, data on the price of smuggling could be collected as a useful resource to assess the size of the market more precisely. A more systematic collection of price data would allow for more granular analysis by transport type (and level of safety).
- A more granular analysis could also be undertaken by considering the **interplay between demand and supply** and the impact these factors have on the price of services offered to migrants. Given the relative stability of the hubs where smugglers operate, this could be done by increasing the data collection in these places.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.12: Recommendations – Smuggling of migrants

Key finding	Recommendation	Actor
Data from FRONTEX on illegal border-crossings detected provides a good basis for estimating smuggling of migrants by sea to Europe via different routes because detection rates are known to be high (even though not all irregular migrants are detected). However, the best available proxy for monetising these estimates is the price paid by migrants for smuggling services, which is known to be highly variable depending on demand (due to high price elasticity), safety and comfort of the journey, and available price data is sparse and cannot account for this variability.	Member States should systematically report to the European Commission information on price of smuggling services. Data collection at hubs where smugglers operate, which are relatively stable, may be a potential approach. Frontex and Europol have data on the price paid by smuggled migrants, but this information is not public.	Member States European Commission

2.4. Fraud

Fraud is defined as 'a deliberate act of deception intended for personal gain or to cause a loss to another party' (European Anti-Fraud Office, 2019). There are numerous types of fraud, including

excise fraud, Value Added Tax (VAT) fraud and MTIC fraud, payment fraud, food fraud, identity fraud and intellectual property right (IPR) infringements or counterfeit goods.

For the purpose of this study we have focused on three prominent types of fraud: MTIC fraud, food fraud and IPR infringements (counterfeit goods). Card payment fraud is examined separately in relation to cybercrime in **Section 2.8.**

2.4.1. MTIC fraud

William Phillips, RAND Europe

Key findings:

- According to estimates produced by EY (2015) and Frunza (2019) and adjusted for inflation to 2019 values, the annual revenues derived from the MTIC fraud market in the EU range between €51 billion and €104 billion.
- This is a wide range that reflects the difficulty in producing an accurate estimate in this market and hence, the resulting shortage of estimates. The Frunza (2019) estimate is the only known estimate that uses a top-down methodology, but is large compared to other estimates such as EY (2015), which uses a bottom-up approach.
- A high level of sophistication, organisation and cross-country co-ordination is required for MTIC fraud to take place; hence, OCG involvement is likely. There is evidence of both large OCGs, as well as local and small-scale initiatives.
- Some individual actors are involved, but tend to act as part of larger criminal networks. Legitimate businesses can also become involved in fraudulent activity.
- There is expected to be a movement towards less tangible goods and services, such as carbon credits, cloud computing and other online-based products, as well as rapidly consumed goods such as food. There is also expected to be movement into the green energy market, as this sector continues to grow.

Value added tax (VAT) fraud can be defined as the deliberate evasion of VAT, a form of consumption tax that is applied to the final consumer when they purchase a good or service. The most common form of VAT fraud is MTIC fraud (Europol, 2020d). When goods and services are traded from one EU Member State to another, they are VAT exempted in the Member State of departure. However, MTIC fraudsters take advantage of this by trading goods from one Member State to another, and subsequently do not pay VAT from final sales of those goods to the relevant tax authority. They then disappear; hence the notion of 'missing trader' (Poniatowski et al., 2019).

A comprehensive overview of the MTIC fraud market in the EU, building upon the summary provided here, can be found in **Annex 2.4.1**.

2.4.1.1. Revenue estimates of the EU MTIC fraud market

Table 2.13 below presents estimates of the MTIC fraud market in the 28 EU Member States. We have provided a lower bound estimate (obtained from EY, 2015) and an upper bound estimate (obtained from Frunza, 2019). According to these figures, adjusted for inflation to 2019 values, annual revenues derived from MTIC fraud range between €51 and €104 billion.

- The total annual revenue lost to MTIC fraud in the EU was as much as €104 billion (upper bound). The Commission estimated the VAT Gap to be €152 billion in the same year, suggesting that over 65% of the VAT gap could be attributed to MTIC fraud. However, the EY (2015) estimate of €51 billion suggests MTIC fraud is around a quarter of the VAT gap (calculated in 2011 to be €193 billion) (European Commission, 2013).
- The estimates differ substantially across Member States, according to Frunza's estimates. Italy has by far the highest amount of MTIC fraud at €28 billion, followed by Germany (€15 billion) and then Spain (€12 billion). Luxembourg has the lowest MTIC fraud (€37 million), followed by Malta (€47 million) and Slovenia (€56 million).
- The five most populous countries in the EU (Germany, UK, France, Italy, Spain) are responsible for MTIC fraud worth €69 billion – two-thirds of the total EU amount.

- To fully determine the extent of MTIC fraud within certain countries, it is also useful to consider how large the MTIC fraud is relative to the total VAT collected in the country, according to Frunza's Member States level estimates.
- Romania leads the way in this regard, with MTIC fraud losses comprising 43% of total collected VAT revenue. Italy, which has the highest absolute amount of MTIC fraud, has MTIC fraud losses making up 26.9% of VAT revenue. Central, Eastern and Southern European countries show a trend of having high MTIC fraud figures as a proportion of collected VAT.
- Whereas, Northern European countries such as Sweden (2.7%), Finland (1.9%), Luxembourg (1.0%) and the Netherlands (the lowest at 0.8%) tend to have lower proportions.

Table 2.13: Revenue estimate of the EU MTIC fraud market

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)	
	Low (EY, 2015)	High (Frunza, 2019)
28 EU Member States	**-**	**103,992**
27 EU Member States (excluding UK)	**-**	**96,767**
26 EU Member States (excluding HR, CY)	**50,858**	**103,271**
Austria		1,163
Belgium		824
Bulgaria		512
Croatia		457
Cyprus		264
Czech Republic		3,231
Denmark		1,119
Estonia		103
Finland		374
France		6,014
Germany		15,319
Greece		4,667
Hungary		3,322
Ireland		570
Italy		28,083
Latvia		359
Lithuania		1,190
Luxembourg		37
Malta		47
Netherlands		379
Poland		6,329
Portugal		1,687
Romania		5,962
Slovakia		1,304
Slovenia		56
Spain		12,240
Sweden		1,155

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)	
	Low (EY, 2015)	High (Frunza, 2019)
UK		7,225

Notes: Estimates updated to 2019 values using Eurostat's HICP (Eurostat, 2020).

Previous revenue estimates of the EU MTIC fraud market

Table 2.14 shows previous estimates of the EU MTIC fraud market produced by Frunza (2019). These estimates indicate that MTIC fraud is growing in the EU, with a growth rate of 20% over the period 2013–2015. Frunza attributes this in part to the fact that collected VAT is also growing in the EU. However, the estimates are also growing as a share of the VAT gap (increasing from 51.1% in 2013 to 65.4% in 2015).

Table 2.14: Previous estimates of the EU MTIC fraud market (2010 to present)

Member State	Revenue (€ million)			Source
	2013	2014	2015	
EU 28	82,484	93,531	99,037	Frunza (2019)

2.4.1.2. Criminal actors and modus operandi

OCGs are likely to play a significant role in the VAT fraud market. According to Savona & Riccardi (2015), VAT fraud can be carried out by a whole range of actors, from individuals to extremely structured criminal organisations. However, when it is scaled up to incorporate cross-border transactions, as is necessary for MTIC fraud, the very nature of the fraud is organised, since companies need to be set up in multiple countries (legitimate and bogus). Hence, according to an interview with a law enforcement representative[36], this means that OCGs are likely to play a significant role. A VAT fraud market expert[37] stated that since MTIC fraud is a cross-country scheme, it requires inter-country connections, involving several people to work together.

The size and composition of OCGs involved in MTIC fraud is believed to be mixed. A fraud market expert[38] interviewed stated that most VAT fraud is likely undertaken by local and small-time initiatives as opposed to traditional crime groups. The nature of VAT fraud does vary, with some forms of fraud primarily involving paperwork and requiring little people power. In this sense, it is very possible for a large amount of fraud to be carried out by a relatively small number of people. According to an MTIC fraud expert[39] the main leaders of MTIC fraud schemes sometimes only need to hire one or two people. However, sometimes large OCGs are involved. Savona & Riccardi (2015) identified the involvement of a wide range of OCGs, including Chinese, Italian and Eastern European OCGs.

The UK appears to be less affected by MTIC fraud compared to other countries, despite many MTIC fraud actors originating from the UK. All three VAT-fraud interviewees[40] identified the UK as prominent contributors of MTIC fraud actors within the EU. In terms of ethnicity, two interviewees[41] identified British nationals of Asian ethnic origin – such as British-Pakistani, British-Indian and British-Bangladeshi – as ethnic groups involved in this type of crime. According to a VAT fraud market expert[42], the countries where the fraud is planned and where the VAT is defrauded can differ. A report by de la Feria (2018) stated that in recent litigations where VAT fraud had been suspected, eastern Member States have been the most prominently involved, providing further evidence of high levels of MTIC fraud in Eastern Europe.

[36] Interview with law enforcement representative, 11 March 2020 (#15).
[37] Interview with private sector expert, 14 February 2020 (#6).
[38] Interview with private sector expert, 14 February 2020 (#6).
[39] Interview with National/Member State expert, 26 March 2020 (#62).
[40] Interview with market expert, 14 February 2020; Interview with National/Member State expert, 26 March 2020 (#62); Interview with law enforcement representative, 11 March 2020 (#15).
[41] Interview with private sector expert, 14 February 2020 (#6); Interview with law enforcement representative, 11 March 2020 (#15).
[42] Interview with private sector expert, 14 February 2020 (#6).

Modus operandi

MTIC fraud leaders who reside outside the EU may hire people inside the EU to carry out the fraud on their behalf. According to an MTIC fraud expert[43] the lead actors behind MTIC fraud schemes (also known as 'Directors') tend to hire people within the EU to run the fraudulent companies; organising the movement of goods, looking at invoices and signing tax declarations etc. The expert mentioned that young, vulnerable men who do not belong to an OCG and are seeking opportunities to make money are often identified. The 'Director' gives instructions on how to establish a company, and the targeted individual then operates as a front for the company. Another interviewee[44] also stated that Directors may reside outside the EU, opting to live in tax havens where their profits can be better protected from the authorities.

2.4.1.3. Future trends and dynamics

A trend is emerging towards intangible goods and rapid consumables. There is an emerging trend towards fraudulently trading intangible goods and services such as carbon credits and cloud computing, according to Lamensch & Ceci (2018). This may have come about because the intangible nature of these products requires less people-power to facilitate the trade and allows their transfer around Europe at a much faster rate, which also makes them increasingly harder to trace, hence they are more profitable at minimal risk. According to Borselli et al. (2015), trading over the internet minimises the risk of detection, makes any potential intervention significantly more challenging and makes it harder to trace the goods or to physically locate the organisations that are responsible. Further, Lamensch & Ceci (2018) reported evidence of VAT fraudsters moving towards goods that are consumed at a quicker rate, such as food, since their fast consumption also makes them difficult to trace.

Ultimately, MTIC fraudsters are opportunistic and will take advantage of any market. Fraudsters have proven themselves to be quick to react to the market, committing fraud on all sorts of types of goods when an opportunity has been presented – the carbon emissions market is a prime example. One interviewed MTIC fraud expert[45] expects to see more MTIC fraudsters moving into the 'green' certificate market, as EU countries continue to invest more heavily in greener energy, presenting more opportunities to MTIC fraudsters. However, Lamensch & Ceci (2018) noted that MTIC fraudsters appear to act opportunistically. They follow demand and economic trends, meaning all sectors are potentially vulnerable.

Brexit may displace MTIC fraud. KPMG (2016) noted that if the UK leaves the single market, the number of countries in which OCGs can trade goods VAT-exempt will be reduced. However, VAT fraud will likely be displaced into other countries, rather than be reduced overall (KPMG, 2016). There are further risks if the UK government attempts to boost international trade through possible changes in VAT and tax policy, since fraudsters may take advantage of this by developing new ways to set up VAT fraud schemes (KPMG, 2016).

2.4.1.4. Recommendations

There are two principal ways in which data collection and estimation on VAT / MTIC fraud could be improved in the EU:

- First, the evidence from the literature shows that details on estimation methods are scarce. Hence, the first area that could be improved is simply **to encourage more sources to release details of the methodologies used**. For example, the UK government conducts a thorough estimate of MTIC fraud every year, but do not disclose their methods. Being able to compare methods would allow other researchers and tax professionals to apply these methods to their own data, generating a wider pool of estimates to work with.
- Secondly, **access to more granular data could be improved**. This is an area in which there has already been some progress. In 2017, the Commission announced the launch of the Transaction Network Analysis (TNA) tool (European Commission, 2019e). National tax authorities can use the TNA tool to share VAT registration data on their domestic traders with other EU Member States. The hope is that this will enable authorities to more closely and accurately monitor intra-EU trade, helping to detect irregularities (UK Parliament, 2018). This can be done by summing up the intra-

[43] Interview with National/Member State expert, 26 March 2020 (#62).
[44] Interview with law enforcement representative, 11 March 2020 (#15).
[45] Interview with National/Member State expert, 26 March 2020 (#62).

Community acquisitions (ICAs) of the companies that go on to default on VAT payments (European Commission, 2018a). An ICA is declared by companies that import goods from another EU country, to both state that the initial trade is VAT-exempt and to register that further selling of goods is now subject to taxation.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.15: Recommendations – MTIC fraud

Key finding	Recommendation	Actor
Estimating the size of MTIC fraud in the EU is an incredibly complex task, hence there are relatively few methodologies and estimates in the literature. Several Member State tax authorities do estimate MTIC fraud for their own country, but details of methodologies are not publicly accessible.	Member States should publish their methodologies, to allow for replication. Member State tax authorities should systematically report VAT registration data of domestic traders to the Commission, enabling tax authorities to detect irregularities on an EU-wide basis. This will help EU-level authorities to more reliably identify and measure MTIC fraud.	Member State tax authorities European Commission

2.4.2. Intellectual property rights infringements

William Phillips, RAND Europe and Rajeev Gundur, Flinders University

Key findings:

- Estimates of the criminal revenues from intellectual property rights (IPR) infringements are limited and those that exist are susceptible to limitations and biases that result in an underestimate.
- In the IPR infringements market, estimates of loss to legitimate industry rather than criminal revenues prevail. Loss-based estimates are not the same as revenues, and therefore cannot be directly compared to other criminal markets examined in this study for which revenue estimates have been produced.
- The production, transportation and sale of counterfeit goods is a complex process, often undertaken by highly organised and hierarchically structured OCGs. Smaller actors are also involved, but often work as part of larger organisations via informal networks.
- Corrupt officials with inside knowledge of customs or original intellectual property rights have been known to be involved in IPR infringements, as are legitimate businesses who can be used to disguise illicit activity.
- Trade in counterfeits via the internet is expected to increase. Further, technological developments may make it easier and cheaper to manufacture counterfeits. Expanded railway connections between the EU and China may enable easier transportation.

IPR infringements can be broken down into four main categories:

- **Trade secret theft** – the theft of non-public technologies, methods, plans, processes or other sensitive information (CREATe & PwC, 2014).
- **Copyright infringement** – when copyrighted materials are distributed outside authorised channels and without payment to the copyright holder (CREATe & PwC, 2014).
- **Trademark infringement** – when a producer fabricates an item that simulates a brand to which they do not own the IPR (OECD-EUIPO, 2020).
- **Patent theft** – when a producer copies and sells a patented invention (i.e. counterfeits the invention) without the patent owner's permission or without paying a licensing fee (Levi et al., 2013).

Different types of IPR violations often overlap with one another and the term 'counterfeiting' is widely used to refer to general IPR violations (Bekhouche, 2018). **Counterfeiting** indicates the selling of products that are deceptive, including articles sold as a legitimate product when they are not, such as adulterated medications (EUIPO, 2016c; Hall et al., 2017; Lavorgna, 2014; Spink et al., 2013), and mislabelling or misrepresenting the origin of geographical indications (Cook, 2013; EUIPO, 2017e).

A comprehensive overview of the IPR infringements market in the EU, building upon the summary provided here, can be found in **Annex 2.4.2**.

2.4.2.1. Previous revenue estimates of the EU IPR infringements market

As shown in Table 2.16, several studies published since 2010 have estimated the criminal revenues from IPR infringements in the EU. As discussed further in Annex 2.4.2, the best available methodology is **demand-based**, as per Camerini et al. (2015) and Savona & Riccardi (2015). However, there are limitations of these approaches that cause an **underestimation of the market**:

- Consumer surveys, which are a key input of these estimates, are susceptible to self-reporting biases such as underreporting and recall problems. There are also questions around the representativeness of the samples (Camerini et al., 2015).
- These estimates have measured secondary markets in which purchasers of counterfeit goods are fully aware, as opposed to primary markets where the counterfeit products are sold to unsuspecting customers (Camerini et al., 2015).

Further, in the case of the approach taken by Camerini et al. (2015), the estimate only covers a subset of markets. Also, the market-specific propensity is calculated using the results of a survey from Spain, which is then applied to all other Member States.

Moreover, the approach to estimating counterfeit-goods markets employed by Calderoni et al. (2014) and Savona & Riccardi (2015) assumed that between 5% and 10% of the legal market is comprised of counterfeit goods. There is **little transparency** around the selection of these proportions and thus the estimates produced may have limited reliability.

A study by the OECD/EUIPO (2019) used customs seizure data to estimate the imports of counterfeit and pirated products into the EU. This study excluded domestically produced and consumed counterfeit and pirated products. Seizure data is not suitable for estimating the scale of criminal markets because it is not representative and substitution rates vary by product type, hence studies that rely on retail price or replacement value are not reliable.

For the reasons outlined above, these estimates are not used in this study. No new estimates are produced because there is a lack of available data to do so.

Table 2.16: Previous estimates of the EU IPR infringements market (2010 to present)

Member State	Sub-market	Revenue (€ million)			Year(s)	Source
		Mid	Low	High		
IT	Clothing, accessories of clothing, footwear, electrical equipment, IT equipment, CDs, DVDs, video tapes, toys, glasses, watches and jewels, perfumes and cosmetics	-	3,028	6,055	2008	Calderoni et al. (2014)
EU 28	Secondary markets (e.g. consumers are aware they are buying counterfeit goods) of clothing; footwear; food and non-alcoholic beverages; games, toys, and hobbies; information and communication technology; recorded media; household appliances; jewelry, clocks, and watches; perfumes and	9,000	-	-	2010	Camerini et al. (2015)

Member State	Sub-market	Revenue (€ million)			Year(s)	Source
		Mid	Low	High		
	articles for personal care; pharmaceutical products and medications					
EU 27	Retail sale of computers telecommunications, electrical household appliances; music and video recordings; games and toys; clothing; footwear and leather goods; cosmetic and toilet articles; watches and jewellery	-	21,356	41,353	2010	Savona & Riccardi (2015)
EU 27		42,711	-	-	2010	Savona & Riccardi (2015)
EU 28	Illegal internet protocol television	941			2018	EUIPO (2019b)
EU 28	35 product categories	121,000	-	-	2014–16	OECD/EUIPO (2019)

Loss-based estimates of the EU IPR infringements market

In the IPR infringements market, estimates of loss to legitimate industry rather than criminal revenues prevail. Loss-based estimates are not the same as revenues, and therefore cannot be directly compared to the criminal markets examined in this study for which revenue estimates have been produced. This is because the consumption of a counterfeit good does not necessarily represent reduced consumption of a legitimate alternative. In some counterfeit markets consumers may never have intended to purchase the legitimate good in the first place (Hoorens et al., 2012, p. vii). That is, the substitution rate of a good will vary greatly depending on the sector. Similarly, other estimates incorporating wider economic costs, potential health impacts, consumer surplus welfare gains of counterfeit good consumption and reputational effects are much higher than revenue estimates.

The table below shows eight estimates from EUIPO reports that state the revenue losses incurred by legitimate industries as a result of counterfeit activity.

Table 2.17: Prior estimates of revenue losses to legitimate industry

Sector	Revenue losses from IPR infringements (€ million)	EU Member States covered	Year of estimate	Reference
Toys and games	1,427	Data from 20 Member States used, but estimate has been scaled up to reflect EU 28	Annual estimate (based on data from 2007–2012)	EUIPO (2015)
Jewellery and watches	1,892	Data from 18 Member States used, but estimate has been scaled up to reflect EU 27 (excluding Croatia)	Annual estimate (based on data from 2007–2012)	EUIPO (2016b)
Handbags and luggage	1,581	Data from 20 Member States used, but estimate has been scaled up to reflect EU 28	Annual estimate (based on data from 2007–2012)	EUIPO (2016a)
Recorded music	170	19 Member States	2014	EUIPO (2017b)
Spirits and wine	1,260	Data from 19 Member States used for spirits and data from 24 Member States used for wine, but estimate has been scaled	Annual estimate (based on data from 2008–2013)	EUIPO (2016d)

Sector	Revenue losses from IPR infringements (€ million)	EU Member States covered	Year of estimate	Reference
		up to reflect EU 28		
Pharmaceuticals	10,188	Data from 19 Member States used, but estimate has been scaled up to reflect EU 28	Annual estimate (based on data from 2008–2013)	EUIPO (2016c)
Pesticides	1,313	Data from 24 Member States used, but estimate has been scaled up to reflect EU 28	Annual estimate (based on data from 2009–2014)	EUIPO (2017a)
Smartphones	4,212	26 Member States (excluding Malta and Bulgaria)	2015	EUIPO (2017c)
Tyres and batteries	2,426	Data from 24 Member States used for tyres, and data from 20 MS used for batteries, but estimate has been scaled up to reflect EU 28	2010–2015	EUIPO (2018)

2.4.2.2. Criminal actors and modus operandi

There is thought to be a high level of OCG involvement in the IPR infringements market, ranging from large, highly structured organisations, to groups of smaller, loosely structured groups who work together via informal networks.

EUIPO & Europol (2019) claimed that 'most criminal activity involving counterfeiting is undoubtedly performed by OCGs.' Due to the sophistication required to manufacture, transport and sell counterfeit products, large-scale sophistication and organisation is a prerequisite, therefore, OCG involvement is high. OCGs known to be active in IPR infringements have been identified as having a hierarchical structure, typically consisting of around 12 members, however, this varies by market (EUIPO & Europol, 2019). Smaller groups are also active, however, they tend to work together as part of less-structured networks (OECD-EUIPO, 2020).

Counterfeiting can be attractive to OCGs because it presents a profitable and low-risk way of making money. Treadwell (2012) found that increasingly complex supply chains make it hard to trace the origins of goods, and Papadouka & Haenlein (2017) reported that Free Trade Zones offer a cheap place to store goods, as well as having limited domestic authority presence. Savona & Riccardi (2015) noted that the legal penalties associated with counterfeiting are also relatively less severe, meaning they are failing to deter OCGs from engaging in counterfeiting. As reported by Europol-EUIPO, drug trafficking is the most common type of criminal activity to occur alongside IPR infringements (EUIPO, 2020b).

There is evidence of overlap with other illicit markets, such as drugs and fraud. IPR crime can be linked to other forms of crime in two main ways: other criminal activity can be used to facilitate IPR crime (or vice versa), or OCGs can engage in different criminal activities that are relatively independent of each other – known as 'parallel' activities (EUIPO, 2020b). The means to manufacture and transport both illicit drugs and counterfeit pharmaceuticals can be similar, and raids frequently find both illicit drugs and counterfeit pharmaceuticals in the same premises (EUIPO, 2020b)[46]. In addition, crimes such as VAT fraud and excise fraud are regularly undertaken in order to ensure counterfeit goods can be imported into the country where they are subsequently sold to the final consumer (EUIPO, 2020b).

Counterfeit goods are largely manufactured outside of the EU, then imported into the EU. Europol (2015a, 2017a) reported that OCGs often rely on manufacturers from outside the EU (predominantly China and other Asian countries) to produce counterfeit goods. OCGs can use their own transportation means or infiltrate the legitimate distribution chain; IPR-violating items

[46] Interview with European level stakeholder, 11 March 2020 (#16).

can be shipped along licit supply chains, concealed in licit shipments, or smuggled using traditional smuggling techniques (Godart, 2010; Hall et al., 2017).

Once in the EU, OCGs use other methods to distribute and sell their goods throughout the EU. According to Europol (2015a), a popular method used by counterfeiters is to import unbranded goods into the EU and then add IPR-infringing branding when inside the EU. A related technique is that of 'drop shipping' where goods are imported into an EU country with relatively fewer controls and then distributed onwards to EU countries with tighter borders. According to an expert stakeholder[47], there are four main ways that OCGs can get their products into the stores of retailers: by threatening to use violence or other coercive means, owning retail outlets whereby they can easily stock counterfeit goods in place of legitimate ones, engaging in loan sharking to ensure they have leverage over businesses who have borrowed money from them, and by infiltrating the logistics network supplying the goods.

2.4.2.3. Future trends and dynamics

The internet is facilitating the movement of counterfeit goods. Counterfeit goods are increasingly being ordered via the internet, where they are subsequently sent directly to the consumer through the postal system (European Union, 2019c). Further, the IP Crime Group (2019) found that counterfeiters are increasingly using e-commerce and other online platforms – such as Facebook, Instagram, Twitter, Gumtree, Amazon and Alibaba – to sell their products. EUIPO & Europol (2019) stated the trade in counterfeits is expected to increasingly take place online, and counterfeiters are expected to exploit this by using marketing strategies that will be 'better directed at the ever-increasing number of internet and particularly, social-media users'.

Advances in technology mean that it is easier to manufacture goods and fake branding from both inside and outside the EU. Technology improvements are making production methods less expensive and more accessible, allowing for more high-quality branding and packaging to be produced (Chaudhry & Zimmerman, 2012; EUIPO, 2020a). This could also enable more manufacturing to be done from inside the EU, which would then make exporting to the final consumer easier. Further, Europol (2017a) note future technology developments such as 3D printing may be able to produce more sophisticated counterfeits in the near future.

Improved rail connections will allow counterfeits manufactured in China to have easier and cheaper access to EU markets. Rail connections between Europe and China have been growing for years, and will continue to do so with the expansion of the China Belt and Road Initiative (Europol, 2017a). Rail freight is half the price of air freight and twice as fast as shipping, meaning rail is poised to be a 'logical choice for many counterfeit consignments' in the future (Europol, 2017a). This brings further opportunities for OCGs, as counterfeits can be sent from China and arrive at EU borders in Eastern Europe, where checks are less stringent, before making their way into the rest of Europe.

Ultimately, OCGs have demonstrated they are versatile and can take advantage of the latest market trends and economic climate. According to an expert interviewee[48], counterfeiters will ultimately follow market trends and use any opportunity to make money, leveraging the latest technological developments, consumer trends and economic conditions.

2.4.2.4. Recommendations

There are several ways in which data collection and estimation on IPR infringements could be improved in the EU:

- Chaudhry & Zimmerman (2012) argued that **more detailed market research on specific product categories is necessary**, due to the high level of distinction between different counterfeit sectors. For instance, studies need to be designed differently if they are estimating the amount of illegal movie streaming, compared to the demand for counterfeit pharmaceuticals. Substitution rates, ethical concerns and health and safety concerns all vary from market to market, hence the need for sector-specific research designs.
- More detailed surveys and studies on how consumers feel about counterfeited products in different contexts could be used to inform **more granular and accurate demand-based estimates**. The methodology used by Camerini et al. for estimating the propensity to consume counterfeit products utilised data from a Spanish survey, which

[47] Interview with EU-level stakeholder, 12 February 2020.
[48] Interview with international level stakeholder, 19 March 2020 (#24).

was extrapolated to all other EU Member States (Camerini et al., 2015). Using data from more detailed, country-specific surveys – such as EUIPO (2017d) and EUIPO (2019a) – could generate more accurate country-specific estimates of criminal revenues.

- Sullivan et al. (2017) argued that there needs to be a **more harmonised definition of what constitutes a counterfeit good**. Agreeing on a definition that is consistent across Member States will enable better data collection and more effective study of counterfeit markets by researchers.
- Further, law enforcement authorities of some Member States do not make their information on internal detentions available to the rest of the EU, creating **huge gaps in the available seizure data** (EUIPO, 2019c).
- In addition, seizure data is collected primarily for non-statistical purposes, by individuals with poor knowledge of statistics, meaning the **data is not as easy to use for statistical analysis purposes as it could be** (Butticè et al., 2018).

Table 2.18: Recommendations – IPR infringements market

Key finding	Recommendation	Actor
Estimates of the criminal revenues from IPR infringements are limited and those that exist are susceptible to limitations and biases that result in an underestimate. In the IPR infringements market, estimates of loss to legitimate industry rather than criminal revenues prevail. Loss-based estimates are not the same as revenues, and therefore cannot be directly compared to other criminal markets examined in this study for which revenue estimates have been produced.	Sector-, product- and country-specific research designs should be utilised to provide more accurate estimates (for example considering market-specific aspects, such as substitution rates and differences by demographics and countries). Consumer surveys conducted at the Member State level would improve demand-based estimates. A harmonised EU definition of a 'counterfeit good' may enable more standardised data collection and analysis.	Researchers Member States European Commission

2.4.3. Food fraud

William Phillips and Susie Lee, RAND Europe

Key findings:

- Due to a lack of available data, no revenue estimates have been produced for food fraud.
- OCG involvement is believed to be high in food fraud, however the available evidence suggests it mostly consists of legitimate food operators engaging in fraudulent activity. However, there are instances where large and well-known OCGs, such as the Camorra (Italy), have been involved in food fraud.
- In the future, growing amounts of trade in fraudulent food is expected to take place online. There is also evidence that specific fraud types – such as mislabelling of non-organic foods as organic, and halal fraud – will increase. Further, more advanced production and counterfeiting methods are expected to be developed.

Food fraud concerns the deliberate substitution, addition, tampering or misrepresentation of food/feed, food ingredients or food packaging, as well as false or misleading statements made about a product for economic gain (Spink & Moyer, 2011). For the purposes of this report, counterfeit food products are also included in this analysis.

A comprehensive overview of the food fraud market in the EU, building upon the summary provided here, can be found in **Annex 2.4.3**.

2.4.3.1. The lack of revenue estimates of the EU food fraud market

There is insufficient data in the literature to report on previous estimates of food fraud in the EU. This reflects the fact that estimating the revenues generated through food fraud is very difficult. There is a large amount of different types of food, all of which have different premiums associated with them when they are being fraudulently mislabelled. A food fraud expert interviewed as part of the study noted that estimating the revenue for food fraud is extremely difficult because of the complexity and hidden nature of the market. Estimation of revenues for particular sub-markets (olive oil, fish, eggs etc.) would be relatively easy; however, data is fragmented[49].

One study from the EUIPO (2016e) examined Geographical Indication (GI) infringements for wine, spirits, cheeses, fresh meat and meat products, beers, fruit, vegetables, cereals and other products in 17 EU Member States. The study estimated that these markets generated revenues of approximately €2.3 billion; however, given it only focuses on one type of fraudulent food (i.e. GI infringements) and covers only a proportion of Member States, it is an underestimate of the market as a whole.

A Europol and Interpol (2018) report covered many countries around the globe, but does not allow for disaggregation to the EU countries. These estimates relied on seizure data, which is known to fluctuate over time in response to law enforcement operations and effectiveness. Moreover, seizure data is influenced by the detectability of the product, and the location of the seizure may not be the final destination of the products. For food fraud, it is understood there are limited inspections and enforcement activity[50], meaning that the estimates produced are particularly likely to be considerable undercounts.

2.4.3.2. Criminal actors and modus operandi

Most food-fraud actors are legitimate food businesses and food business operators. The main actors in food fraud do not necessarily represent the typical conceptions of OCGs, such as hierarchical mafia-style groups (although they are also known to be involved to at least some degree). The evidence suggests that many of the market actors are legitimate business operators, who use fraudulent means to conduct their business. According to Lord and colleagues, fraudulent opportunities arise within the food system as a part of legitimate actors' normal behaviour (Lord et al., 2017). Many business operators engage in 'industrial drift', whereby fraudulent food items are introduced into the supply chain in order to cut costs. In these cases, there is little evidence to suggest actors are linked with other criminal activities or illicit markets.

However, there are incentives for traditional crime groups to participate in the food-fraud market. There is a relative lack of risk in the food-fraud market. Lord et al. noted that compared to other criminal markets such as drug trafficking, methods of detection in food fraud are less sophisticated and the penalties for being caught are less severe, meaning food fraud offers large potential reward at a lower level of risk (Lord et al., 2017).

The lack of traditional, mafia-type OCG involvement in food fraud means there is less of a connection to other illicit markets, however associations are still present. According to an expert interviewee[51], there is limited evidence of food fraud overlapping with other criminal markets. In part, this is because the lack of traditional, mafia-type OCG involvement in food fraud means there is naturally less of a connection with markets that have a higher level of OCG involvement. However, the interviewee[52] mentioned that some criminal organisations have been known to invest their profits from other criminal markets into some types of food crime, simply to make money. Further, the UK's National Food Crime Unit (NFCU) noted that a small number of food businesses are believed to have links to OCGs whose main activity is not in itself related to food fraud (NFCU, 2016). For example, OCGs may exploit infrastructure surrounding a food business to cover the importation of contraband, such as drugs or illegal wildlife (NFCU, 2016). In addition, OCGs may exploit national or EU funding available for the agri-food sector (Masini, 2018).

[49] Interview with EU-level stakeholder, 12 February 2020 (#5).
[50] Interview with EU-level stakeholder, 12 February 2020 (#5).
[51] Interview with EU-level stakeholder, 12 February 2020 (#5).
[52] Interview with EU-level stakeholder, 12 February 2020 (#5).

There may be a connection between food fraud and the wider counterfeiting market. According to an EUIPO report, law enforcement authorities who detect fraudulent food products regularly find links with the wider counterfeit goods market (EUIPO & Europol, 2019). Counterfeit car parts, clothing, cosmetics, electronic goods, pharmaceuticals, tobacco and toys have all been discovered in recent raids alongside counterfeit food products. This is because OCGs sometimes use the same production locations and distribution routes for both food and other counterfeit goods.

Modus operandi

Typically, food fraud actors will use misleading or fake packaging, and substitute cheap or dangerous ingredients. According to PricewaterhouseCoopers (PwC), product ingredients can be swapped for cheaper, lower quality alternatives; product packaging can contain false information; and the branding of legitimate and recognisable companies can be illegally copied (PwC, 2016). A common technique used in the counterfeit wine market involves placing low-quality wine inside bottles containing labels copying those of legitimate, expensive brands (EUIPO & Europol, 2019).

2.4.3.3. Future trends and dynamics

There is evidence that the motivation for food fraud may be growing. This is in part owing to the economic crisis in 2008, after which the estimated losses due to food fraud increased by 20% according to Gee & Button (2019). In addition, the structure of the legitimate food supply-chain is becoming increasingly complex, providing criminal actors with more opportunity for involvement in fraudulent activity (Codex Alimentarius Commission, 2017).

Increasing amount of trade in counterfeit food is expected to take place online. One of the interviewees[53] identified the online food market, especially for alcohol and food supplements, as an emerging platform. E-commerce may be attractive to criminals because opening new websites and temporary accounts is easy.[54]

Specific food-types and techniques are also seeing a rise in popularity. According to Food Fraud Advisors (2017), emerging trends in fraudulent activities in the agri-food sector include growing incidence of halal fraud, and counterfeiting middle-range foods rather than luxury foods. An expert interviewee[55] also commented that the mislabelling of non-organic foods as organic is a major trend, especially on food products imported from outside of the EU. This may also extend to the use of additives that are used to lower costs or enhance flavour etc., but are not disclosed on labelling due to their potential negative health implications or illegality[56]. Another expert interviewee[57] claimed that OCGs may move more into food types where there is **low awareness from authorities**. The interviewee spoke of a case whereby fraudulent tomatoes and potatoes were sold by OCGs across Italy and Germany, which went undetected due to the inconspicuous and low-priority nature of the goods involved.

There is also evidence that criminal actors are generally becoming more sophisticated and professional. Law enforcement authorities are increasingly reporting the use of counterfeit packaging materials, security rings and labels, as well as more sophisticated production methods. Authorities have seized infrastructure such as machines, corks and security rings that were used for fraudulent alcohol bottling. In the past, food fraudsters would refill the real packaging with fake products, however there is evidence that food fraudsters are now operating their own production lines. The EUIPO reports that up to one-seventh of all produce from some known legitimate alcohol production lines is fraudulent (EUIPO & Europol, 2019).

2.4.3.4. Recommendations

There are three principal ways in which data collection and estimation on food fraud could be improved in the EU:

- First, one interviewee[58] emphasised the need for **all 28 Member States consistently and systematically report the inspections that have been made within their country**, through the Administrative Assistance and Cooperation System (AAC) or by

[53] Interview with EU-level stakeholder, 12 February 2020 (#5).
[54] Interview with EU-level stakeholder, 12 February 2020 (#5).
[55] Interview with EU-level stakeholder, 12 February 2020 (#5).
[56] Communication with expert advisor to the study, 15 June 2020.
[57] Interview with international-level stakeholder, 19 March 2020 (#24).
[58] Interview with EU-level stakeholder, 12 February 2020 (#5).

other means. This will enable the creation of an EU-wide database of all records of food-fraud activity in one centralised place.

- Second, **advanced data-analytics techniques may be used to increase detection rates**. Marvin and colleagues built a Bayesian Network model that uses data on past food-fraud cases to predict future cases (Marvin et al., 2016). Using data from Rapid Alert for Food and Feed (RASFF) and some data from cases in the US, the model was able to predict the type of food fraud 91.5% of the time. The model only predicts the type of food fraud, but the authors state that given access to more data (such as monitoring and customs data), the model would be able to predict food fraud of any product imported from any country. The authors note that their model could be used to help authorities design monitoring and control measures to more effectively identify which food types are at increased risk of fraud, using data on the origin, price and demand of the food. This would improve the likelihood of detecting food fraud, generating more cases and data, allowing for better estimation of market size.
- Third, **EU-wide operations such as Operation OPSON should continue to be employed** (Europol, 2019b). The resulting enhanced cooperation and the vast amount of seized goods are further data points that can help in estimating the true size of the market. It is understood that there is relatively limited inspection and enforcement activity undertaken in food compared to other illicit markets[59], therefore increasing the number of operations targeting food fraud may also result in more cases being detected.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.19: Recommendations – Food fraud market

Key finding	Recommendation	Actor
The complexity of the market and a lack of data means it is not possible to come up with an accurate estimate of the market size. Food fraud is largely undertaken by legitimate food businesses seeking to cut costs, with traditional OCG involvement less common compared to other markets. There is evidence that food fraud will increasingly take place online and that counterfeit food manufacturing methods are becoming more sophisticated.	Member States should consistently and systematically report food inspections that have been made within their country, enabling the creation of an EU-wide database of all records of food fraud activity. Identifying more cases of food fraud will also allow for better estimation. Two ways this can be done are via advanced data analytics and by increasing the scope of large-scale operations, such as OPSON.	Member States European Commission

2.5. Environmental crime

The European Commission defines environmental crime as 'acts that breach environmental legislation and cause significant harm or risk to the environment and human health' (European Commission, 2020b). According to Europol, the most known offences of environmental crime are:

- **Illicit waste trafficking** involving the improper collection, transport, recovery or disposal of waste.
- **Illicit wildlife trafficking** involving the killing, destruction, possession or trade of specimens of protected wild fauna or fauna species.
- **Illegal operation of a plant** in which a dangerous activity is carried out or in which dangerous substances or preparations are stored.
- Production, importation, exportation, marking or use of **ozone-depleting substances** (Europol, 2020b).

This project focuses on illicit waste and illicit wildlife trafficking in the EU.

A comprehensive overview of the illicit waste market and illicit wildlife market in the EU, building upon the summary provided here, can be found in **Annex 2.5**.

[59] Interview with EU-level stakeholder, 12 February 2020 (#5).

2.5.1. Illicit waste

Shann Hulme and Susie Lee, RAND Europe and Lorenzo Segato, React Italy

Key findings:

- According to the original estimates produced in this study, the annual revenues derived from the illicit waste market in the EU range between €4 and €15 billion (mid-point figure of €9.5 billion).
- When comparing these estimates with the BlockWaste project, a previous Commission-funded study that used the same methodology, the study finds there has been a growth in the market for both hazardous and non-hazardous waste.
- There is known to be some OCG involvement in the illicit waste market, particularly small, loosely structured groups typically involved in the international shipment of waste from the EU.
- White-collar professionals are key actors in the illicit waste market, exploiting their awareness of the complex waste management system and loopholes in regulations.
- The illegal shipment of plastic waste, end-of-life vehicles and e-waste are expected to increase, and the overall size of the illicit waste market is also expected to grow in the context of a Chinese ban on waste imports from foreign countries.

The illicit waste market involves the illegal trading and disposal of waste outside of the regulatory frameworks set by national and international waste laws (Europol, 2013b). This can occur with other forms of waste crime, such as deliberate misclassification of waste or operation of illegal waste management sites.

2.5.1.1. Revenue estimates of the EU illicit waste market

Table 2.20: Revenue estimate of the EU illicit waste market presents the original estimates produced for this project of the illicit waste market in the 23 EU Member States for which sufficient data was available. According to these figures, annual revenues derived from illicit waste trafficking range between €3.7 and €15.3 billion.

- Annual revenues deriving from illicit **non-hazardous waste trafficking** (both within national boundaries and abroad) range between €1.7 billion and €12.9 billion. As similarly noted by previous research, the wide range obtained for non-hazardous waste may be due to the wide diversity of prices charged for illegal management of different types of waste (Meneghini et al., 2017).
- For **hazardous waste trafficking**, annual revenues range between €2.1 billion and €2.4 billion.
- There are **large fluctuations in the revenue estimates across Member States**. This is consistent with the findings of Meneghini et al. (2017) and reflects the information biases in Eurostat data collected from Member States on waste management. These limitations must be considered in interpretation of the results.
- Bearing in mind the limitations, the Member States with the highest volume of both hazardous and non-hazardous waste disappearing from the legal market are France, Italy, the UK and Germany. Those with the lowest volume of both hazardous and non-hazardous waste disappearing are Greece, Latvia and Croatia (for hazardous and non-hazardous). However, for non-hazardous waste, Austria ranks the lowest.
- When examining the **volume of hazardous waste disappearing as a proportion of waste generated**, the UK (64%), Slovakia (57%), Lithuania (54%) and Austria (54%) record the highest, whilst Bulgaria (1%), Estonia (1%) and Greece (3%) record the lowest. For non-hazardous waste, Latvia (30%), Portugal (29%), Lithuania (26%) and Slovakia (23%) record the highest, while Austria (1%), Romania (2%) and Bulgaria (3%) record the lowest.
- Consistent with previous research, **hazardous waste seems to be more exposed to the risk of illicit waste management than non-hazardous waste**. On average, between 2014 and 2016 around 33% of hazardous and 13% of non-hazardous waste disappeared from the legal market.

Table 2.20: Revenue estimate of the EU illicit waste market

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)								
	Hazardous			Non-hazardous			Total (hazardous and non-hazardous)		
	Mid	Low	High	Mid	Low	High	Mid	Low	High
23 EU Member States*	**2229.01**	**2065.29**	**2392.75**	**7277.61**	**1658.20**	**12896.99**	**9506.62**	**3723.49**	**15289.74**
22 EU Member States without UK	**1870.49**	**1733.10**	**2007.89**	**5057.41**	**1152.33**	**8962.45**	**6927.89**	**2885.43**	**10970.34**
Austria	64.47	59.74	69.20	31.00	7.07	54.94	95.47	66.80	124.13
Belgium	-	-	-	-	-	-	-	-	-
Bulgaria	11.24	10.41	12.06	155.76	35.49	276.03	167.00	45.91	288.09
Croatia	5.68	5.26	6.10	33.46	7.62	59.29	39.14	12.89	65.39
Czech Republic	51.35	47.57	55.12	108.39	24.69	192.08	159.74	72.27	247.21
Cyprus	-	-	-	-	-	-	-	-	-
Denmark	20.19	18.70	21.67	102.70	23.40	182.00	122.89	42.09	203.67
Estonia	10.14	9.40	10.89	118.83	27.07	210.59	128.97	36.48	221.48
Finland	13.73	12.72	14.74	-8.91	-2.03	-15.80	4.82	10.69	-1.05
France	524.29	485.78	562.80	777.10	177.06	1377.14	1301.39	662.84	1939.94
Germany	322.14	298.48	345.81	709.13	161.58	1256.69	1031.27	460.06	1602.49
Greece	1.11	1.03	1.19	96.19	21.92	170.45	97.30	22.95	171.64
Hungary	14.62	13.53	15.69	106.36	24.24	188.46	120.97	37.77	204.15
Ireland	16.02	14.85	17.20	132.52	30.19	234.85	148.54	45.04	252.05
Italy	452.64	419.40	485.88	937.78	213.67	1661.90	1390.42	633.07	2147.77
Latvia	3.93	3.65	4.22	31.62	7.21	56.03	35.55	10.86	60.26
Lithuania	8.94	8.28	9.60	70.47	16.05	124.89	79.41	24.33	134.49
Luxembourg	-	-	-	-	-	-	-	-	-
Malta	-	-	-	-	-	-	-	-	-
Netherlands	42.13	39.02	45.21	151.59	34.54	268.63	193.72	73.56	313.85

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)								
	Hazardous			Non-hazardous			Total (hazardous and non-hazardous)		
	Mid	Low	High	Mid	Low	High	Mid	Low	High
Poland	25.84	23.95	27.74	318.33	72.54	564.14	344.18	96.49	591.88
Portugal	30.02	27.82	32.23	164.05	37.38	290.74	194.08	65.20	322.97
Romania	16.53	15.32	17.74	123.63	28.17	219.07	140.16	43.49	236.82
Slovakia	23.37	21.65	25.08	91.31	20.81	161.82	114.68	42.45	186.90
Slovenia	-	-	-	-	-	-	-	-	-
Spain	97.61	90.44	104.78	583.91	133.04	1034.77	681.51	223.48	1139.56
Sweden	114.50	106.09	122.92	222.18	50.62	393.75	336.69	156.71	516.67
United Kingdom	358.53	332.20	384.86	2220.20	505.87	3934.53	2578.73	838.07	4319.40

Notes: Estimates were produced for 2014–2016 (mean) updated to 2019 values using Eurostat's HICP (Eurostat, 2020). *It was not possible to produce estimates for BE, CY, LU, MT, SI.

Previous revenue estimates of the EU illicit waste market

Table 2.21 shows previous estimates of the EU illicit waste market that have been published since 2010. The present study replicated the methodology employed by Meneghini et al. (2017), and found estimates – for both hazardous and non-hazardous waste – that were higher, suggesting some growth in the market. Consistent with previous research, our estimates found that hazardous waste seems to be more exposed to the risk of illicit waste management than non-hazardous waste.

Table 2.21: Previous estimates of the EU illicit waste market (2010 to present)

Member State	Revenue (€ million)			Sub-market	Year(s)	Source
	Mid	Low	High			
IT		304	507	Total	2007–2010	Calderoni et al. (2014)
		279	466	Non-hazardous		
		25	41	Hazardous		
23 EU MS (excluding BE, CY, LU, MT, SI)		3,288.4	13,528.1	Total	2010–2014	Meneghini et al. (2017); Suvantola et al. (2017)
		1,469.1	11,426.17	Non-hazardous		
		1,814.31	2,101.95	Hazardous		

Note: The aggregate figures presented here from Meneghini et al. (2017); Suvantola et al. (2017) were manually added up by the research team from the table of figures they provide in the report and accompanying technical annex.

2.5.1.2. Criminal actors and modus operandi

The demand for illegal waste management and disposal services is primarily driven by legitimate businesses seeking to minimise costs. With the increased requirement for proper disposal and management of waste, waste producers – especially those who generate large amounts of waste, such as corporates – are motivated to seek waste-management services at a low price.[60] This creates demand for cheaper services for managing waste, as well as opportunities for profit for criminal actors to undercut legal prices and illegally dispose of waste.[61] Previous research suggests that illegal waste prices can be between one-fifth and one-third the price of legal waste prices (Calderoni et al., 2014).

There is known to be some OCG involvement in the illicit waste market, particularly small, loosely structured groups typically involved in the international shipment of waste from the EU (Geeraerts et al., 2015; Noel, 2018). One expert interviewee[62] noted that perpetrators often have criminal backgrounds – such as previous sentences for drug-related crimes – and have been found to possess firearms. Many of the groups involved may be small, loosely structured and not centralised (Bisschop, 2012, 2017; Geeraerts et al., 2015; Massari & Monzini, 2004). With regard to illicit disposal of plastic waste, Interpol (2020) reported a link between OCGs and legitimate pollution management businesses, which are used as a cover for illegal operations.

White-collar professionals are central actors in the illicit waste market. Motivated primarily by the need to reduce the otherwise high costs of legal waste treatment, white-collar actors utilise their awareness of the complex waste-management system and loopholes in regulations to their benefit.[63]

Modus operandi

Disguising waste as second-hand goods is a frequent strategy used by criminal actors. Tyres taken from end-of-life vehicles (ELVs), for example, are sold to developing countries as second-hand even if they are too worn out to be safe and useful. Waste Electrical and Electronic Equipment (WEEE) may also be disguised as second-hand goods[64]. Such illegal activity takes

[60] Interview with an EU-level specialist in illegal waste market, 12 February 2020 (#04).
[61] Interview with an EU-level specialist in illegal waste market, 12 February 2020 (#04).
[62] Interview with a national-level specialist in waste crime intelligence, 8 April 2020 (#31).
[63] Interview with a national-level specialist in waste shipment, 3 March 2020 (#10).
[64] Waste Electrical and Electronic Equipment (WEEE) refers to electrical or electronic parts that have come to the end of their useful life, and covers a range of equipment that use electricity. Computers, TV sets, fridges and cell

advantage of the vague distinction between 'useful' and 'useless' parts of waste, especially in electronic waste (Rucevska et al., 2015). In this way, the actor profits three times: first, by receiving money in advance by a waste producer for recycling; second, by selling useful components from the waste; third, by illegally selling useless components as second-hand goods to non-EU countries[65].

Waste of different specialties may be mixed for concealment. Another mode of illegal shipment is to mix up waste of different degrees of speciality required for treatment (e.g. paper and hazardous waste) and to report the mixed-up shipment as only one lower priced / less protected category of waste (e.g. paper). For example, a storage site may mix toxic substances with domestic waste (Massari & Monzini, 2004). Illegal actors purchase lands or empty houses for waste storage and dispose of waste by burning the entire site[66]. The illegal shipment of waste is enabled through fraudulent documents and reporting.

2.5.1.3. Future trends and dynamics

Since the ban of solid waste import by China in January 2018, there has been a **re-routing of illegal waste shipments to emerging import countries**, primarily located in South and South-East Asian countries, and to a lesser extent Eastern Europe (INTERPOL, 2020).[67] This includes plastic waste, which has been identified as a growing problem with regard to illicit trafficking in the EU and globally. Interviewees shared cases such as an instant change in such international shipments after the Chinese ban, waste streams being shipped to other EU countries with less costs for creating illegal dumping/incineration sites which are often disguised as a recycling company in paperwork. The Chinese ban would entail a shift in not only the destination countries, but also different parties involved in the illegal trade of waste.

A report published in 2016 observed **ELVs and WEEE as emerging sub-markets** within the illegal waste market (EnviCrimeNet, 2016), which is consistent with remarks made by stakeholders interviewed for this study[68].

From a Delphi Study conducted as part of the BlockWaste project, experts expected **money-laundering and bribery to increase in frequency and significance** in the illegal waste market until 2030 (Suvantola et al., 2017). According to Interpol (2020), there has been an increase in fraudulent documents and misdeclaration of plastic waste.

2.5.1.4. Recommendations

There are two principal ways in which data collection and estimation on the illicit waste market could be improved in the EU. Notably, both limitations have been discussed in previous research by Meneghini et al. (2017) and Suvantola et al. (2017); however, little improvement seems to have been made.

- First, **systematically report information on price of illicit waste and revenues generated through illicit waste trafficking.** There is little systematic data on the price of illicit waste. Current and previous estimates rely upon information gathered from Italian judicial files and may have limited applicability to the illegal market in other Member States. Moreover, the price data has a large range – particularly for non-hazardous waste – thus the lower and upper estimates produced vary by over €10 billion, which calls into question the reliability of such estimates. Our enquiries revealed that there is little willingness to share price data for the purpose of estimation. Moreover, even where price data is available, there tends to be a misalignment between the unit of that data (i.e. the price of illegally trafficked plastics, tyres, end-of-life-vehicles, etc.) and the categorisation of the Eurostat data (i.e. hazardous and non-hazardous), which leads to challenges for estimation.
- Second, **address gaps and inconsistencies in reporting on waste generation and treatment.** The Eurostat data on waste generation and management is currently only

phones are examples. The Directive on WEEE 2002/96/EC and the Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment 2002/95/EC address the management of WEEE in the EU.

[65] Interview with an EU-level specialist in illegal waste market, 11 March 2020 (#20).

[66] Interview with a national-level specialist in waste crime intelligence, 8 April 2020 (#31).

[67] Interview with a national-level specialist in the shipment of waste, 3 March 2020 (#10); Interview with a national-level specialist in waste crime intelligence, 8 April 2020 (#31).

[68] Interview with a national-level specialist in the shipment of waste, 3 March 2020 (#10).

available up to 2016, and there remain gaps in reporting for some Member States, thus precluding an EU-wide estimate.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.22: Recommendations – Illicit waste market

Key finding	Recommendation	Actor
A gap analysis using Eurostat data on legal waste treatment, management and shipment provides the basis for estimating the amount of hazardousness and non-hazardous waste disappearing from the legal market, assumed due to illegal diversion. However, Eurostat data is only available for 23 of the 28 EU Member States (excluding BE, CY, LU, MT, SI) and data on the price of illegally traded waste – required for monetising the gap estimates – is only available for Italy.	Address gaps and inconsistencies in reporting by BE, CY, LU, MT, SI regarding waste generation and treatment. Member States should systematically report information on revenues generated through illicit waste trafficking, which is currently collected by police or judicial authorities in the course of their investigations, to the European Commission.	Eurostat Member States European Commission

2.5.2. Illicit wildlife

Susie Lee, RAND Europe

Key findings:

- The revenues from the European eel market range from €4.7 to a high of €31.4 million. However, there is insufficient data to enable an estimate of the illicit wildlife market as a whole in Europe, and this estimate is a vast underrepresentation of the extent of the phenomenon.
- Actors in the illegal wildlife trade have a heterogenous profile – varying by level of involvement in the supply chain and by species of wildlife trafficked.
- In order to effectively capture or poach, transport and ship wildlife for illegal sale, a certain level of skill and expertise is required. This means that actors in some wildlife markets include those who also operate in the legal trade.
- Transnational OCGs are known to be involved in the illegal trafficking of glass eels from Europe to Asia, and may work with established eel traders to facilitate diversion from the legal supply chain. There are also networks of poachers who covertly fish in order to supply the illegal market.
- The internet is likely to play an increasing role in facilitating the trade in illegal wildlife products, given the relative ease of connecting sellers to potential buyers.

Wildlife crime, or the illegal wildlife trade, refers to unlawful activities associated with illegal exploitation and trade of wildlife specimens, and encompasses the entire supply chain – from harvesting entire or parts from living organisms to processing, smuggling and selling ('t Sas-Rolfes et al., 2019; Interpol, 2018). Products range from wild, biological specimens of flora, fauna and fungi for purposes ranging from food to ornaments to construction (Phelps et al., 2016). Importantly, one species can provide multiple products that may be traded through different value chains. In addition, different forms or sources of a single product may be either legal or illegal, based on different contexts (e.g. caught within vs. outside of official quotas, farmed vs. wild-caught specimens, domestic vs. international trade, harvested within vs. outside of legally protected areas).

Europe is a major transit region for wildlife trade between continents (e.g. reptile skins), whilst also being a destination (e.g. live reptiles) and source region (e.g. glass eels, birds, falcons), and a location for manufacture of products from illegally smuggled wildlife (e.g. rhino horn and ivory which are sourced from African countries but are transformed and sold as antiques)

(Auliya et al., 2016; Bush et al., 2014; Interpol, 2018). Available seizure data indicate that the main commodity types seized in the EU in 2018 were medicinals (both animal and plant-derived), corals and reptile bodies, parts and derivatives (TRAFFIC, 2020). Of the total seizure records, 9% reported an estimated value of the commodities seized. In 2018, the top commodities with a reported value were European eels, live birds, live reptiles, mammal body parts and derivatives and ivory (TRAFFIC, 2020). Some of the main sub-markets are introduced in the box below. Interviewees noted that illicit wildlife trafficking has the potential to be a high-profit crime carrying relatively low risk, and it has received relatively little attention until recently[69].

Box 2.2: Illicit wildlife markets in the EU

European eels: European eels have been banned for trading beyond European external borders since 2010 (European Commission, 2014). Due to the high demand for eels in East Asian countries, European eel juveniles (also known as glass eels) are smuggled at much higher prices outside of Europe to Asian countries, where they are farmed and reared to adulthood for consumption (European Commission, 2017b). Illegal trade of glass eels occurs mainly from the four EU source countries (France, Spain, the UK and Portugal), but many other EU Member States (such as Germany, Bulgaria, Greece and Hungary – Sustainable Eel Group, 2018a) and neighbouring countries (Albania, Macedonia, Morocco and Russia – Stein et al., 2016) are believed to be used as transit countries.

Live birds: Illegal killing and taking of wild birds remains a continuing issue in Europe (Brochet et al., 2019). A recent assessment in 2019 indicated that motivations for illegal killing and taking of birds varies in Europe from food, sport and caged birds in Mediterranean Europe, sport and food in the Caucasus, and sport and predator control in Northern and Central Europe (Brochet et al., 2019). The EU is also a market for non-EU-native exotic birds, mainly parrots, that are kept as pets or caged birds (TRAFFIC, 2020).

Live reptiles: the EU comprises one of the largest live reptile markets (Auliya et al., 2016). Live reptiles imported from across continents are sold either as pets or as part of a collection. The illegal trade of live reptiles involves species regulated under the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), as well as species that are not CITES-regulated but are nationally protected in their country of origin, but which are often openly offered for sale in the EU (Auliya et al., 2016).

Ivory: Ivory has been banned for international trade since 1989 when African elephants were transferred from CITES Appendix II to Appendix I. China was one of the largest buyer markets for illegally traded ivory, however since introducing a ban on the ivory trade in 2017 there has been an observed decline in ivory demand (WWF, 2019). Until the 1980s, Europe was one of the leading importers and manufacturers of ivory globally (UNEP et al., 2013). Europe remains a key region for re-exporting illegal ivory products (UNEP et al., 2013). As of 2017, the export of raw ivory from the EU was banned, but domestic trade within the EU was permitted for worked ivory originally acquired before 1947 ('antiques') and for ivory produced between 1947 and 1989 with a government-issued certificate (European Commission, 2017a).

2.5.2.1. Revenue estimates of the EU illicit wildlife market

[69] Interview with an expert at NGO-level, 19 March 2020 (#23).

Table 2.23 presents original estimates produced for this project of the illegal European eel market in the EU. The results show that the value of the market ranges from €4.7 million to €31.4 million. Such a wide range is mostly due to the fluctuating price in response to the annual variations in the supply of glass eels[70].

70 Interview with an expert at NGO-level, 19 March 2020 (#23). For various reasons, the annual recruitment of European eels declined from the early 1980s to a low point in 2011 (Amilhat et al., 2019; Sustainable Eel Group, 2018b). Although the declining trend seems to have stopped, and some increase has been observed during 2011–2019, overall recruitment remains low (Amilhat et al., 2019). Supply of glass eels is also influenced by the availability of Japanese eels (the preferred type over the European eel). When Japanese eels are more abundant, there is likely a decline in the need for illegal trade of European eels.

Table 2.23: Revenue estimate of one species subject to illegal trade in Europe – European eels

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)			Sub-market	Source
	Mid	Low	High		
FR, ES, PT, UK [a]	18.05	4.71	31.39	European eels	New estimate

Notes: European eel estimates were produced for 2015–2017 (mean) and the estimates from TRAFFIC (2020) were for 2018. All estimates have been updated to 2019 values using Eurostat's HICP (Eurostat, 2020).
(a) European eel estimates are derived from gap estimates produced by the Sustainable Eel Group, representing the volume of eels disappearing from the legal market. In Europe, there are legal fisheries of European eels in four Member States: FR, ES, PT and UK – thus, these estimates are comprehensive as to the estimated amount being diverted from the legal supply chain.

Previous revenue estimates of the EU illicit wildlife market

Table 2.24 below presents previous revenue estimates of the EU illicit wildlife market that have been published since 2010. As can be seen, there are few revenue estimates – which reflects both the limited data available and the lesser focus on the wildlife trade when compared with other markets (e.g. illicit drugs). In addition to these monetised estimates, there have been a few attempts to estimate the volume of illicit wildlife trade. These estimates are presented in **Annex 2.5.2.**

It is not possible to draw explicit conclusions in relation to the change in market size overtime. While a comparison of our estimates of the European eel market with those produced by the Sustainable Eel Group (SEG) imply some growth in market size, it is important to note the differences between these studies that preclude such comparisons from being made. The SEG estimates use data on price of eels sold on Asian markets, thus reflecting revenues generated by actors operating in Asia, while this study uses the price of exporting from the EU, thus reflecting the revenues generated by EU criminal actors.

Whilst data to understand the extent of wildlife trafficking in the EU is limited, interviewees acknowledged the considerable harms resultant from the wildlife trade – such as extinction, introducing invasive species that then prey on or compete with native species, and threats to human health (UNODC, 2020; WWF, 2018).

Table 2.24: Previous estimates of the EU illicit wildlife market (2010 to present)

EU Member State	Revenue (€ million)			Sub-market	Year(s)	Source
	Mid	Low	High			
FR, ES, PT, UK		188	2,270	European eels	2016–2017	Sustainable Eel Group (2018b)
FR	0.77			Various	2017	IFAW (2018)
DE	1.25			Various	2017	
UK	0.98			Various	2017	

2.5.2.2. Criminal actors and modus operandi

The degree of OCG involvement differs by sub-markets of wildlife, and poly-criminality is little known. Various actors are likely involved at different stages of the supply chain for different wildlife products because the commodity (i.e. wildlife) is sourced from natural resources. So depending on the exact wildlife products, a heterogenous profile of actors may be required.

European eels: Existing information indicates the clear presence of transnational OCGs in the smuggling of eels out of Europe (TRAFFIC, 2020; UNODC, 2020)[71]. A market expert noted that Asian-based OCGs have been known to send 'fish mules' to smuggle eels by suitcases, and that these people could be ethnically Asian but possess European passports (UNODC, 2020)[72]. However, it is also important to note that legal traders may be involved at various points of the supply chain. For example, according to the market expert interviewee[73], preparing live glass eels for cargo shipping in good condition would require some degree of knowledge in fisheries,

[71] Interview with an expert at NGO-level, 19 March 2020 (#25).
[72] Interview with an expert at NGO-level, 19 March 2020 (#23).
[73] Interview with an expert at NGO-level, 19 March 2020 (#23).

suggesting the possibility that actors involved in legal trading of fish also participate in the trafficking of glass eels. According to UNODC (2020) networks of poachers can acquire glass eels through clandestine fishing, and on-supply to the illegal market.

Ivory: In a report published in 2017, Pro Wildlife et al. suggested that OCGs may be involved in ivory trading in Europe, given the trend of an unprecedented number of large seizures (e.g. as defined by the Elephant Trade Information System (ETIS), shipments of at least 800kg) in the EU since the end of 2015 (Pro Wildlife et al., 2017). However, larger seizures may also reflect increased enforcement efforts and awareness, especially given the growing attention on ivory issues linked to the increase in poaching in Africa and increased illegal trade and seizures globally (EIA, 2020).

Wild and exotic birds: Since 2005 there a trade ban on wild birds has been in place, to counter the spread of avian flu (Cardador et al., 2018). This resulted in a trade shift from wild-caught birds to captive-bred birds, and there is some evidence that the ban may have increased financial incentives for poaching or led to OCG involvement (Cardador et al., 2018; Ribeiro et al., 2019). In 2018, TRAFFIC (2020) reported one case involving the illegal trafficking of toucans, parrots and macaws in the European region. The 2019 study by Brochet et al. provided evidence for the continuation of the illegal killing of wild birds in Europe, but the magnitude of illegal trade involving these birds and information on main actors are still little known (Brochet et al., 2019).

Live reptiles: Market experts discussed the possibility of OCG involvement in supplying live reptile products for 'collectors', because the sourcing of exotic animals requires specialist knowledge of the animals and their ecology, as well as liaising with poachers in the country of origin and mules/couriers. Other actors in the illegal live reptile market in the EU involve reptile breeders[74].

Modus operandi

European eels: With regard to illegal poaching, UNODC (2020) indicated that poachers use hand nets, trap nets or small trawling nets to fish glass eels covertly at night. The market expert interviewed[75] described two main modes of smuggling eels that have been illegally poached or diverted from the legal supply chain. Firstly, transportation via airplanes by hiding the live glass eels in oxygenated, wet plastic bags, which are packed in suitcases and transported to Asia (Europol, 2018b; UNODC, 2020). For instance, OCGs operating as 'fish mules' have been observed concealing eels in suitcases and declaring them as other types of fish (Europol, 2019c; UNODC, 2020). Secondly, shipping in air cargo/freight, which is either declared as other seafood products or hidden under other seafood exports.

Ivory: Compared to other regions, Europe has notably low legal ivory prices. This might drive companies specialized in collecting ivory items to be involved in illegal re-exporting to Asia (Sosnowski et al., 2019). Internet sales are also considered to facilitate marketing of illegal ivory in the EU, with law enforcement facing difficulties in regulating the sale of illegal ivory on, for example, internet auction sites (UNEP et al., 2013).

Live reptiles: There are two main modes for the illegal trafficking of reptiles in the EU. First, a common mechanism for importing CITES-listed reptiles is to falsely report them as captive-bred reptiles, thus increasing the likelihood that a trade permit will be granted (Sina et al., 2016). Second, non-CITES listed reptiles may be imported into the EU after being illegally poached from their habitats, typically non-EU third countries. Because there is no legal instrument within the EU that would require operators placing these animals on the market to produce due diligence in relation to the original obtainment or harvesting, technically these reptiles then become 'legal' once they enter the EU.

2.5.2.3. Future trends and dynamics

Within each sub-market of the illegal wildlife market in the EU, information on emerging trends is relatively lacking. Two studies pointed to the **increased prominence of internet-based trade on illegal wildlife products** (IFAW, 2018; Sina et al., 2016). According to these studies, online advertisements via social media – such as Facebook[76] – are actively used for

[74] Interview with an EU-level enforcement on illegal wildlife, 11 March 2020 (#21).
[75] Interview with an expert at NGO-level, 19 March 2020 (#23).
[76] For example, wildlife-related foundations and NGOs have partnered with technology companies – such as eBay, Microsoft, Tencent, Facebook, Etsy and Instagram – to tackle the online illegal trade in threatened species (WWF, n.d.).

promoting wildlife products that may have been illegally sourced. Except for the Czech Republic, online sellers are not required by law to present supporting documentation on the legitimacy of a wildlife item. This situation exacerbates the existing difficulty of distinguishing legal from illegal wildlife trade over the internet. According to one of the two studies, conducted by the International Fund for Animal Welfare (IFAW), an emergent trend is **wildlife traffickers turning to the dark net in response to increased enforcement** mainly targeting the surface web (Interpol, 2017; Roberts & Hernandez-Castro, 2017). According to IFAW, even if trade occurs offline, the internet could facilitate the connection between sellers and buyers (IFAW, 2018).

2.5.2.4. Recommendations

The illegal wildlife market is one of the most difficult to estimate in terms of its size and value. This is evidenced by the lack of available secondary data and the limited number of studies that have attempted to do so. Current understandings of the market rely on seizure records (as reported by various agencies: Environmental Investigation Agency (EIA), 2020; TRAFFIC, 2020; UNODC, 2020)), which have high volatility, rendering them unsuitable for market estimates.

Future efforts to improve the measurement of the illegal wildlife trade in the EU are essential, through additional, primary data collection. One approach might be to **conduct comprehensive market 'occupancy' surveys for different species**, as described by Barber-Meyer (2009). Further dedicated research on this phenomenon is needed. The key findings from this study and the related recommendations are summarised in the table below.

Table 2.25: Recommendations – Illicit wildlife market

Key finding	Recommendation	Actor
There are no secondary data sources available for reliably estimating the revenues generated through the illegal wildlife trade in the EU. Current knowledge is predominantly reliant upon seizure data, which has high volatility rendering it unsuitable for market estimates. The revenues generated through the illegal trade of European eels – one sub-market of the illegal wildlife market in the EU – can be estimated by using gap analysis of the amount of eels disappearing from the legal market in the four source countries in the EU (France, Spain, Portugal and the UK).	Efforts should be made to improve the measurement of the illegal wildlife trade in the EU, through additional primary data collection. One approach might be to conduct comprehensive market 'occupancy' surveys for different species (Barber-Meyer, 2009).	Member States, including police and judicial authorities, and customs authorities European Commission

2.6. Illicit firearms

Quentin Liger, Optimity Advisors

Key findings:

- According to the estimates produced in this study, the annual revenues derived from the illicit firearms market in the EU range from €274 million to €754 million (€408 million).
- This estimate has a wider range than the previous estimate of between €370 million to €493 million.
- The illicit firearms market does not necessitate a high level of organisation, and therefore does not necessarily have to be undertaken by OCGs. There are two broad categories of actors involved in the supply of illicit firearms: single individuals involved in small-scale commerce, and large operators able to systematically and periodically move large quantities of arms and ammunitions (Savona & Riccardi, 2015).
- In line with the relatively low value of the overall market, illicit firearms trafficking does not generate high revenues, and is often a secondary source of income for traffickers.

- Flobert weapons are expected to continue being widely available in the European market. 3D-printed firearms are expected to increase, while current and former conflict areas (in particular the former Yugoslavia and the Donbass region) are expected to continue being important sources of firearms.

The revised firearms directive defines illicit trafficking as 'the acquisition, sale, delivery, movement or transfer of firearms, their essential components or ammunition from or through the territory of one Member State to that of another Member State if any one of the Member States concerned does not authorise it' (European Union & Council of the European Union, 2017).

A comprehensive overview of the illicit firearms market in the EU, building upon the summary provided here, can be found in **Annex 2.6**.

2.6.1. Revenue estimates of the EU illicit firearms market

The table below presents estimates of the illicit firearms market at the EU-level and for each of the 28 EU Member States. The results show that:

- The annual revenues of the illicit firearms market in the EU comprised between €274 million and €754 million (€408 million).
- Due to reporting inaccuracies, the estimates appear to underestimate the revenue of the market in some countries (such as France or Belgium), and overestimate that of others (as is the case of Austria).
- The range of estimates is very wide, even though the methodology only provides for a range linked to the price of firearms. This reflects how, in the overall assessment of the market, the revenue of firearms can vary between locations (up to a tenfold increase).

Given the lack of robustness surrounding the 10% factor used, we undertook a sensitivity analysis using a 5% and 20% factor. The figures vary proportionally to a mid, low and high estimate of €193.6 million, €129.9 million and €356.8 million respectively for 5%, and €774.2 million, €519.62 million and €1,417 million respectively for 20%.

Table 2.26: Revenue estimate of the EU illicit firearms market

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)		
	Mid	Low	High
28 EU Member States	**408.09**	**273.69**	**753.96**
27 EU Member States without UK	**324.555**	**219.174**	**528.571**
Austria	85.38	52.57	141.28
Belgium	5.11	3.22	9.62
Bulgaria	0.33	0.24	0.28
Croatia	25.88	12.82	23.88
Cyprus	0.29	0.20	0.51
Czech Republic	15.59	9.72	26.08
Denmark	9.17	6.32	16.36
Estonia	2.24	1.54	3.99
Finland	8.29	5.72	14.79
France	0.89	0.54	1.46
Germany	31.25	25.57	50.24
Greece	7.50	5.16	13.46
Hungary	6.60	4.11	11.03
Ireland	5.80	3.79	15.64
Italy	58.82	46.65	86.24
Latvia	3.27	2.25	5.83

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)		
	Mid	Low	High
Lithuania	4.77	3.29	8.52
Luxembourg	0.18	0.12	0.33
Malta	0.31	0.24	0.45
Netherlands	29.53	19.80	60.96
Poland	0.80	0.42	0.90
Portugal	3.88	2.68	6.98
Romania	4.94	3.08	8.27
Slovakia	2.81	1.46	3.12
Slovenia	0.21	0.15	0.19
Spain	3.35	2.47	5.04
Sweden	7.35	5.08	13.13
United Kingdom	83.54	54.51	225.38

Note: Estimates were produced for 2012–2018 (mean) and updated to 2019 values using Eurostat's HICP (Eurostat, 2020).

Previous revenue estimates of the EU illicit firearms market

The table below provides previous estimates (published since 2010) of the EU illicit firearms market. Existing estimates stem from two primary data sources: number of seizures and number of unregistered firearms. Studies seeking to assess the revenue of firearms trafficking have typically used the revenue of the legal firearms trade in order to estimate illegal trade.

To reach a figure of between €370 million to €493 million, Transcrime (2015b) used Italian seizure data and extrapolated it to the EU 28. This **supply-side estimate** was based on the revenue of seizures in Italy, and assumed that this represented between 8% and 10% of the total revenue of illicit firearms traded in the country.

Demand-side estimates were based on a range of between 10% to 20% of the revenue of firearms produced in – and net imports to – the country. Given data on legal firearms sales were available through Eurostat, the share of 10% to 20% was extrapolated to all other EU Member States. The source of the 10–20% assumption is not clear in the Transcrime study.

The estimate developed for this study provides a wider range than previous ones. This is mainly the result of increased granularity, and attempts to consider the different types of firearms and their prices in the different markets.

Table 2.27: Previous estimates of the EU illicit firearms market (2010 to present)

Member State included in estimate	Revenue (€ million)			Year(s)	Source
	Mid	Low	High		
IT	-	70	141	2010	Calderoni et al. (2014)
EU 28	-	247	493	2012	Savona & Riccardi (2015)

2.6.2. Criminal actors and modus operandi

In terms of supply, firearms trafficking does not necessitate a high level of organisation, and therefore does not necessarily have to be undertaken by OCGs. Transcrime identified two broad categories of actors involved in the supply of illicit firearms: single individuals involved in small-scale commerce, and large operators able to systematically and periodically move large quantities of arms and ammunitions (Savona & Riccardi, 2015). In line with the relatively low

revenues of the overall market, illicit firearms traffic is not very profitable, and is often a secondary source of profit for traffickers.

Modus operandi

Firearms are sourced via the following channels:

- The **Western Balkans** is a leading source of firearms in the EU. There is only speculation as to the exact size of the stock of firearms in the region, but evidence suggests it is an important source of firearms and other weapons (including rocket propelled grenade (RPGs) and hand grenades, etc).
- **Floberts** are weapons that are sold legally in some Member States (such as Slovakia or the Czech Republic). They can either be purpose-built alarm weapons, or genuine lethal weapons that have been deactivated to be sold legally. According to a Europol official, they can be reactivated 'in a matter of minutes' and are currently one of the main sources of firearms in the EU (Savona & Riccardi, 2015).
- **Postal services (fast parcels)** – including the illegal import of firearms originating from the USA in pieces – have limited risk of detection. This can also include non-finished pieces without markings, which are therefore untraceable, and the import of firearms that are 80% finished, only requiring final drilling and assembly by the buyers (Europol, 2017b).
- **Post-conflict countries** – many weapons are sent to Ukraine due to the conflict situation in the country. There is a high risk that this will be a future hotspot, similar to the Western Balkans. One Europol official mentioned that there are early signs that some groups involved in the selling of firearms in Ukraine are buying and converting Floberts, before selling them in the EU.
- **3D printing** represents few cases at present and is not currently viewed as a problem, but it is on the increase. The use of firearms using 3D printed parts in the far-right Halle synagogue shooting shows that it should not be taken lightly. Real additive manufacturing is still in its infancy, but this method is expected to increase in popularity as firearms become more difficult to procure.
- **The dark net** is an important, but not the main, way of trafficking. It provides a marketplace for those who are not connected to existing sources of firearms.

In non-war zones, including the EU, firearms trafficking is closely linked to other (transnational) criminal activities, including drug smuggling, other forms of trafficking and terrorism (Duquet, 2016). According to the EU SOCTA, 45% of OCGs are poly-criminal. Most of them require firearms, which suggests the firearms markets' importance is as an enabler rather than due to the revenues it represents.

2.6.3. Future trends and dynamics

The first trend relates to the **increased availability of Flobert weapons** on the market since the revision of the Firearms Directive (European Union & Council of the European Union, 2017). The Directive targets deactivated firearms and acoustic expansion weapons, but is less clear on Flobert firearms (which can either be purpose-built or converted). According to the Flemish Peace Institute (FPI), this presents arms dealers who own large stocks of firearms that were deactivated according to older standards with the choice of converting them into Floberts and selling them legally (Duquet & Goris, 2018). According to one law enforcement representative[77], this trend is likely to continue until there is a significant change in the legislation of Member States allowing the sale of Floberts.

While **3D printed firearms** do not currently represent many cases, with the price of printers falling, they will be easier to be manufactured. A related problem is that the technology has the potential to create firearms that cannot be detected at security portals.

The use of the **dark net** is another emerging trend that is likely to continue. A 2017 study by RAND investigated in detail the use of the dark net in the illicit firearms market. First, the dark net appears to allow individuals with no connection to OCGs to source firearms (as was the case in the 2016 Munich shootings). Online purchase of firearms is not expected to become an important source of firearms in the future, but it is likely to allow otherwise criminally 'unconnected' individuals to procure them (Persi Paoli et al., 2017).

[77] Interview with law enforcement representative, 28 April 2020.

Finally, **conflict areas** have traditionally been a source of illicit firearms. Twenty-five years after the Dayton Agreement ended the war in the former Yugoslavia and over 20 years after the 1997 pyramid crisis in Albania, the Western Balkans is still an important source of firearms in the EU. A Europol representative[78] highlighted the risk of the growing stock of weapons in Ukraine as a result of the war in Donbass: 'it could be the new Bosnia'.

2.6.4. Recommendations

Given the shortcomings and limitations in the method used to estimate the size of the illicit firearms market, several steps could be taken to improve data collection:

- **Data on seizures could be more robust**. As a follow-up to its 2015 study on firearms, the UNODC initiated systematic collection and publication of data on its online data portal. The number of Member States reporting data increase threefold to 16 for the 2020 study. Until countries systematically report data, this tool will only be partially useful. In our view, it is likely to become a key instrument for researchers in the future.
- **Production data is hard to come by and patchy**. 2012 is the last year from which data was available for a wide spectrum of Member States. In the past, the Norwegian Initiative on Small Arms Transfers (NISAT) provided a useful proxy (Norwegian Initiative on Small Arms Transfers, n.d.). NISAT data provided a comprehensive trade database aggregating several sources. Unfortunately, the database ceased being updated in 2017 due to lack of funding. Ensuring a source of information on firearms production or trade would be beneficial.
- **Information on the price of firearms has become more readily available**, mainly through research linked to terrorism. The Flemish Peace Institute is a valuable source that will soon be complemented by a project undertaken by Europol, which will provide greater insight.
- **The firearms market is very reactive**. As an example, Flobert firearms[79] first appeared on the market in 2016 and are now seen as one of the biggest firearms-related security problems in the EU (Duquet & Goris, 2018). Legally sold in countries such as Slovakia, manufacturers and dealers must register the sales of these firearms. One Europol official[80] mentioned that in the case of one seller, over 70% of sales were done using fake, stolen or lost IDs, which makes it very likely they were destined for the criminal market. A thorough analysis of these weapons registers would provide valuable insight into the illicit firearms market, including the share of legally sold firearms being used by criminals, the volume of these sales, and where they are sold.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.28: Recommendations – Illicit firearms market

Key finding	Recommendation	Actor
Data from Eurostat on the legal production of firearms, combined with information from the UNODC on seizure per type of firearm, provides the basis for estimating the illicit firearms market in the EU and its Member States. However, the estimate is reliant upon a tenuous assumption that 10% of firearms produced enter the illicit market. Production data is not up-to-date and there is no ongoing data collection. Price data is improving mainly due to terrorism-related research, but is not consistently available across all Member States.	Member States should systematically report on firearms seizures using the UNODC online data portal. Efforts to improve information on the price of illegal firearms should continue to be strengthened, such as by Europol and the FPI.	Member States UNODC Europol FPI

[78] Interview with law enforcement representative, 10 March 2020 (#65).
[79] Low calibre pistols that can be easily converted to fire live ammunition.
[80] Interview with law enforcement representative, 28 April 2020.

2.7. Illicit tobacco

Jirka Taylor, RAND Corporation and Fook Nederveen, RAND Europe

Key findings:

- According to estimates produced in this study, the annual revenues derived from the illicit cigarette market in the EU range between €8 billion and €10 billion (€8.3 billion). This is somewhat lower than previous EU-wide estimates.
- This estimate is highly sensitive to assumptions about the ratio between the price of licit and illicit products, and replicates parameters used in previous research. It is also limited to cigarettes. There are insufficient data to extend this market estimate to cover additional tobacco products, although the cigarette estimate can be assumed to express most of the total illicit market.
- It is widely assumed that OCGs play a dominant role in the illicit tobacco market. Typically, these groups are characterised as flexible, loosely structured, informal networks of criminals involved in production, transport, import, wholesale and retail.
- Other actors involved in the illicit trade include legitimate international transport and import/export companies, suppliers of materials needed to produce tobacco, and legitimate tobacco manufacturers.
- Ongoing trends that may affect the future include a move towards smaller shipment sizes and an increase in illicit domestic manufacturing. Products other than cigarettes are also expected to increase in market share.

According to the international Framework Convention on Tobacco Control, illicit tobacco trade refers to 'any practice or conduct prohibited by law and which relates to production, shipment, receipt, possession, distribution, sale or purchase including any practice or conduct intended to facilitate such activity' (WHO FCTC, 2014). While numerous definitions and characterisations can be offered, generally, there are five principal sources of illicit tobacco (Antonopoulos & Hall, 2016):

1. Counterfeiting, or the manufacture of fake branded tobacco products;
2. Bootlegging, which involves buying tobacco products in countries with low excise duties in volumes that exceed customs regulations;
3. Large-scale smuggling of untaxed tobacco products;
4. Diversion from legitimate supply chains; and
5. Illicit manufacturing of tobacco products.

A comprehensive overview of the illicit tobacco market in the EU, building upon the summary provided here, can be found in **Annex 2.7**.

2.7.1. Revenue estimates of the EU illicit tobacco market

Table 2.29 presents estimates produced for this project of the illicit tobacco market in EU Member States (and the UK). According to these numbers, the revenues of the illicit market from cigarettes in the 28 Member States ranged from €8 billion to €10 billion (€8.3 billion). Excluding the UK, the total value of the illicit tobacco market is approximately €6 billion. This estimate is very sensitive to assumptions about the ratio between the price of licit and illicit products and replicates parameters used in previous research (Transcrime, 2015b).

- The headline estimate covers only illicit trade in cigarettes. There are insufficient data to extend this market estimate to cover additional tobacco products, although the cigarette estimate can be assumed to express most of the total illicit market.
- There are substantial differences across individual Member States. The largest illicit market for cigarettes is in the UK, followed by France, Italy and Germany. Together these four countries account for two-thirds of the European illicit cigarette market by value.
- The updated headline revenue estimate is slightly lower than the 2012 estimate produced by Transcrime, which put the value of the EU cigarette market at €9.4 billion (ranging from €7.8 billion to 10.5 billion). This difference is broadly reflective of the estimated decrease in the illicit trade in cigarettes in recent years (KPMG, 2019).

Nevertheless, there is a large overlap between the ranges of the Transcrime and the updated headline estimates.

Table 2.29: Revenue estimate of the EU illicit tobacco market

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)		
	Mid	Low	High
28 EU Member States	**8309.15**	**8012.62**	**10087.48**
27 EU Member States without UK	**6190.19**	**5954.33**	**6985.64**
Austria	93.25	89.31	111.64
Belgium	101.20	94.67	113.60
Bulgaria	45.31	40.84	49.90
Croatia	41.22	28.90	50.65
Cyprus	14.49	12.86	16.59
Czech Republic	110.85	110.23	138.04
Denmark	30.59	27.62	34.12
Estonia	16.23	16.23	23.86
Finland	94.22	94.22	107.27
France	2038.49	2038.49	2117.91
Germany	514.29	488.82	601.62
Greece	513.51	513.51	605.67
Hungary	64.24	61.02	73.63
Ireland	257.38	255.60	311.83
Italy	635.81	534.29	734.65
Latvia	47.88	47.88	58.70
Lithuania	56.04	56.04	66.71
Luxembourg	1.56	1.42	1.80
Malta	10.67	9.95	11.17
Netherlands	134.89	131.43	153.33
Poland	440.97	428.53	554.32
Portugal	52.96	48.14	60.18
Romania	448.52	445.56	509.22
Slovakia	38.55	34.53	48.10
Slovenia	50.80	44.87	59.34
Spain	279.37	247.23	309.04
Sweden	56.93	52.12	62.76
United Kingdom	2118.95	2058.30	3101.84

Notes: Estimates were produced for 2018 and updated to 2019 values using Eurostat's HICP (Eurostat, 2020). Please note that for some, but not all, input parameters data are available for 2019. However, given the possible relationship between the model parameters, we opted to use 2018 values for all input data in order to achieve a unified reference year.

Previous revenue estimates of the EU illicit tobacco market

Table 2.30 shows previous estimates of the EU illicit tobacco market that have been published since 2010. The present study replicated the methodology employed by Transcrime (2015a), and lower estimates resulted. This is a reflection of a recent decrease in the volume of illicit trade reported by Project Stella, an annual industry-funded survey of the illicit market (KPMG, 2019), which is used as a key input to the revenue estimate. Further, one of the key parameters in the methodology is the relationship between the price of licit and illicit products.

The updated headline estimate used the same value as Transcrime, although it should be noted that the overall results are extremely sensitive to this value and there are no data on how this parameter may have evolved over time. Other existing estimates of the EU illicit tobacco market expressed their results as the proportion of illicit trade as a share of overall tobacco consumption.

Table 2.30: Previous estimates of the EU illicit tobacco market (2010 to present)

Member State	Revenue (€ million)			Sub-market	Year(s)	Source
	Mid	Min	Max			
25 EU countries (excluding LU, CY and MT)	77.3 billion cigarettes (12.2% of total consumption)	N/A	N/A	Cigarettes	2012	Prieger & Kulick (2018)
EU 28	Overall proportion of illicit packs: 8.6%	N/A	N/A	Cigarettes	2018	KPMG (2019)
EU 28	9,400	7,800	10,500	Cigarettes	2012	Transcrime (2015a)
17 EU countries[81] (and Albania)	Overall proportion of illicit packs: 6.5% (ranging from 0% in PT to 37.8% in LV)	N/A	N/A	Cigarettes and hand-rolled tobacco	2010	Gallus et al. (2014); Joossens et al. (2014)

2.7.2. Criminal actors and modus operandi

It is widely assumed that OCGs play a dominant role in the illicit tobacco market. Smuggling or bypassing customs agencies of countries through which the illicit tobacco is trafficked can be challenging, given the sheer size of and bulkiness of shipments, which may require participation of highly organised groups (Melzer & Martin, 2016). Transcrime (2015a) found that 94.8% of seized cigarettes were smuggled and distributed by large-scale actors who were typically part of transnational criminal networks. At the same time, these groups accounted for less than a quarter (23%) of all actors reported to be involved in illicit tobacco trade.

OCGs involved in the illicit tobacco market are typically described as flexible, informal and loosely structured. There is a lack of evidence for the presence of highly organised, hierarchical OCGs in the illicit tobacco market, which itself is viewed as fragmented and decentralised. Individual criminals and groups of criminals tend to operate in networks, with collaboration based on mutual benefit of individuals (Antonopoulos & Hall, 2016; CSD, 2015; Ellis, 2017; Interpol Office of Legal Affairs, 2014; KPMG, 2017; Transcrime, 2015a). The groups involved in the illicit trade of tobacco are often small OCGs or opportunistic, independent criminal entrepreneurs who co-exist and collaborate, often on an ad-hoc basis, to maximise their mutual profits (Antonopoulos & Hall, 2016; Interpol Office of Legal Affairs, 2014; Savona & Riccardi, 2015).

OCGs use established smuggling routes to trade different illicit goods. Smugglers often do not limit themselves to trafficking a single illegal commodity (Interpol Office of Legal Affairs, 2014). The Center for the Study of Democracy (CSD) also found that tobacco smugglers rarely switch to other commodities altogether, but rather invest in additional criminal activities (CSD, 2015). Illicit tobacco has sometimes been used by aspiring smugglers as a low-risk entry product to fund other, riskier illicit activities that require bigger financial investments (Ellis, 2017; Interpol Office of Legal Affairs, 2014). Transcrime found that the three main trafficking routes that tobacco smugglers use to traffic illicit tobacco into Europe are all known to be used

[81] The countries covered in the study were AT, BG, HR, CZ, UK (England only), FI, FR, EL, HU, IE, IT, LV, PL, PT, RO, ES, SE.

for other illegal products as well, including the trafficking of drugs and human beings (Transcrime, 2019).

Several other actors can be involved in the illicit trade of tobacco products. Tobacco trafficking commonly involves legitimate international transport and import/export companies. Their involvement is crucial in handling the sheer volume of the smuggled goods[82]. Other legitimate businesses that may be involved, knowingly or unknowingly, could be the suppliers of materials needed to produce tobacco, such as filters[83]. In addition to these actors, a number of publications in the peer-reviewed literature argued that legitimate tobacco manufacturers may also be directly and indirectly involved in the illicit tobacco market (ASH Scotland, 2016; CSD, 2015; Maftei, 2012; National Research Council, 2015; Tracit, 2019; US National Cancer Institute & WHO, 2016; WHO, 2015; WHO FCTC, 2014).

Modus operandi

Tobacco traffickers use increasingly diverse trade routes and modus operandi. Due to tax differences, it can be lucrative to smuggle legitimate products within the EU (i.e. tax evasion). Operators of established manufacturers may use their surplus tobacco-manufacturing capacity to create additional genuine but unregistered products, which can then be smuggled to other markets (OECD, 2008). Other methods include stealing shipments of legitimate products, e.g. from supermarkets, kiosks or other retail outlets; reselling legally produced tobacco products online, typically in a different market where excises are higher to maximise profits; and individuals or small groups of entrepreneurs purchasing small quantities of tobacco products abroad and then reselling these products on the black market of their home country (CSD, 2015). Trafficking tobacco from outside the EU usually involves shipping containers through legitimate distribution systems (L'Hoiry, 2012). Lastly, domestic illegal production in the EU appears to be on the rise, which reduces transport costs for the criminals and helps them avoid the heavy border controls at the EU's external border (KPMG, 2019).

2.7.3. Future trends and dynamics

Ongoing trends that may continue in the future are a move towards smaller shipment sizes and an increase in illicit domestic manufacturing. Areas of the illicit tobacco trade where changes have been recently observed include the size of shipments and the preferred modus operandi of criminals engaged in the trade (Borkowski & Twomey, 2019). Smuggling of legitimate products in large quantities seems to have decreased, and the presence of illicit tobacco factories with large production capacities operating on EU territory has increased.

Products other than cigarettes are expected to increase their market share. It is conceivable that the consumption of tobacco products other than cigarettes will increase in the future, with concomitant increases in their market share. This ongoing change in consumption patterns is expected to have implications for the illicit trade, which will need to react to the diversification of the tobacco market[84].

2.7.4. Recommendations

Based on the above, there appear to be three principal gaps in current data that hamper efforts to produce national and EU-wide estimates of the illicit tobacco market:

- First, **the only EU-wide data on the extent of illicit consumption of tobacco products are produced in a manner that is not free of conflicts of interest**, due to its reliance on funding from tobacco manufacturers, which precludes the verification and replication of its results. This makes the key input data impossible to scrutinise, and by extension, problematic to use. The Commission is currently in the process of exploring possibilities to conduct independent market estimates that would potentially draw on a combination of methods and make use of newly available tracking and tracing (T&T) data[85], which would go a long way towards plugging this first gap.
- Second, **there is little systematic data on the price of illicit products at various stages of the illicit supply chain**. As a result, it is impossible to develop a good understanding of how the proceeds from the illicit trade accrue to various types of

[82] Interview with EU-level representative, 18 March 2020 (#28).
[83] Interview with academic expert, 19 February 2020 (#7); Interview with academic expert, 11 February 2020 (#13).
[84] Interview with EU-level representative, 18 March 2020, (#28).
[85] For more information, see: https://ec.europa.eu/health/tobacco/tracking_tracing_system_en

participants, including OCGs. It also necessitates the use of broad assumptions, the appropriateness of which is currently impossible to assess. Sparse and limited individual data points on this topic can be found in existing literature; however, these are wholly insufficient to capture both the variety of contexts in which illicit tobacco products are sold, and the variety of factors that influence the price of illicit products.

- Lastly, while several studies have been conducted on illicit trade in cigarettes, **much less is known about illicit trade of other tobacco products**. Some existing studies, for instance those based on a tax gap methodology, include other tobacco products in their scope due to their inability to distinguish individual tobacco products, but very little research and data collection has been dedicated specifically to illicit trade in tobacco products other than cigarettes. This is perhaps understandable as cigarettes represent the lion's share of tobacco consumption and will continue to do so for some time. However, the share of other tobacco products (as well as other smoking products not containing tobacco) is projected to grow in the future, and data collection and research efforts should reflect this trend.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.31: Recommendations – Illicit tobacco market

Key finding	Recommendation	Actor
The basis for estimates of the illicit tobacco market is industry-sponsored discarded-pack surveys, combined with data on the legal sale and prices of tobacco from the European Commission. However, the estimates rely upon assumptions about the illicit-to-licit price ratio, for which there is currently limited evidence available. There are currently no good-quality large-scale data on the extent of the illicit consumption of tobacco products other than cigarettes, precluding the construction of a robust estimate for additional tobacco products.	The European Anti-Fraud Office (OLAF) should continue to explore possibilities for independent market estimates that could potentially draw on a combination of methods and make use of newly available T&T data. These estimates should attempt to cover a range of tobacco products, and not be limited to cigarettes. Member States should systematically report to OLAF information on the price of illegal tobacco and its determinants, which is currently collected by police and judicial authorities in the course of their investigations.	Member States OLAF European Commission

2.8. Cybercrime activities

Fook Nederveen and Erik Silfversten, RAND Europe

Key findings:

- The absence of commonly agreed definitions and taxonomies of cybercrime hinder the identification, reporting and monitoring of cybercrime trends, and make it difficult to understand the true scope of the phenomenon.
- There are severe challenges associated with estimating the revenues from the cybercrime market. No prior estimates of the total revenue of the EU cybercrime market were identified in this study.
- Reliable EU-wide data on card payment fraud is collected by the European Central Bank, which includes both online and offline fraudulent activity. The data shows that card payment fraud amounts to at least €1.8 billion. Card-not-present fraud, which is more likely to be conducted by online or virtual means, accounts for 73% of this revenue, and this share is growing.
- Groups of cybercriminals operate in varying structures, depending on the crime they are committing. Cybercriminals increasingly specialise, commercialise and collaborate in their operations, creating a more complex cybercrime supply chain. The level of OCG involvement is very difficult to establish in this market.
- Future trends may include more offerings, more diverse products and services, increased specialisation and more integrated/comprehensive packages of cybercrime-

as-a-service.

The concept of cybercrime encompasses a vast range of crimes, and cybercrime taxonomies are as plentiful and contested as the definition of cybercrime. This complicates understanding the true scope of the phenomenon. Within the context of this study, the analysis of the illicit cybercrime market included two components: card fraud (card present and card not-present (CNP)), and Cybercrime-as-a-service (CaaS).

Card fraud refers to a broad set of activities, including:

- Counterfeit, lost and stolen, and mail-not-received fraud (intercepted cards);
- Identity (ID) fraud (theft of card credentials and account takeover);
- False ATM Fraud;
- Phishing, pharming, hacking and carding[86];
- 3D-Secure fraud;
- Device manipulation, including point-of-service (POS) terminal and ATM breaches, and manipulation of consumers' Personal Computers (PCs) and mobile phones; and
- Data breaches of processing or card-data-storage infrastructure (Nets, 2019).

Within the context of this study, attention has been placed on **CNP** fraud, which is more likely to be conducted by online or virtual means. **CaaS** refers to the offer for sale of tools, resources or services to conduct or engage in cybercrime, either through direct contacts between sellers and buyers or through organised marketplaces (often found on the dark net).

Further explanations and reflections on definitions of cybercrime and which activities it usually encompasses, how our conceptualisation of this market relates to the other markets considered in this study and why we focus on card fraud and CaaS – and what these consist of – can be found in **Annex 2.8**.

2.8.1. Revenue estimates of the EU card-payment fraud market

The literature review identified no studies that contained estimates of the revenues generated through cybercrime in the EU. However, for the purposes of this study, we present the estimates from one report by the European Central Bank (ECB) that explicitly included an estimate of the total value of card-payment fraud in the EU (ECB, 2018). Due to ECB's role in the oversight of card payment schemes, providers such as Visa Europe are obliged to report volumes and values of (fraudulent) transactions on a country-level, using common definitions and templates, to the ECB (ECB, 2018). Full details of the methodological approach are presented in **Annex 2.8.**

The table below presents estimates of card payment fraud derived by the ECB, as well as the share of CNP fraud, at the EU-level and for each Member State. The results show that **CNP fraud makes up 73%** of the €1.8 billion total value of card fraud in the EU, making it the largest category of card fraud. The ECB's 2018 card-fraud report noted CNP fraud was the only form of card fraud that had seen an increase in absolute and relative terms since its previous report (ECB, 2018). Representatives at the ECB underlined that overall card-fraud levels were stable over the past five years, but that the share of CNP is growing and is expected to increase further in future iterations of the report[87]. As card-present fraud becomes more complicated due to the implementation of regulatory requirements, and the adoption of fraud prevention and detection security tools, CNP fraud is increasingly seen as easier to commit[88].

The table below also shows that there is quite some **difference country by country**. The share of CNP fraud ranges from 41% of all card fraud in Portugal to 84% in Lithuania. This can partly be explained by differences in card usage, such as the number of cards and the number and value of transactions per inhabitant. Countries with a large market for online transactions, such as the UK, France, Spain and Scandinavian countries, tend to face larger CNP fraud shares,

[86] Carding is a form of credit-card fraud where a stolen credit card is used to charge prepaid cards.
[87] Interview with private sector representatives, 6 May 2020, (#91).
[88] Interview with private sector representatives, 6 May 2020, (#91).

as there are more attack vectors[89]. Indeed, in the 2018 Card Fraud Report the ECB observed that in countries where card usage was limited, the levels of fraud were relatively low.

Table 2.32: Revenue estimate of the EU card payment fraud market

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)			Proportion CNP
	Mid	Low	High	%
28 EU Member States		**1,816.43**		**73%**
27 EU Member States without UK		**1,015.81**		
Austria		21.40		81%
Belgium		38.71		75%
Bulgaria		2.99		61%
Croatia		1.53		71%
Cyprus		1.52		76%
Czech Republic		4.26		66%
Denmark		56.74		72%
Estonia		1.24		63%
Finland		22.26		62%
France		442.96		73%
Germany		149.95		66%
Greece		3.81		77%
Hungary		2.78		74%
Ireland		46.04		82%
Italy		75.74		69%
Latvia		1.44		66%
Lithuania		0.76		84%
Luxembourg		3.70		69%
Malta		1.47		71%
Netherlands		32.13		74%
Poland		6.69		56%
Portugal		20.92		41%
Romania		3.61		67%
Slovakia		1.71		79%
Slovenia		1.25		62%
Spain		63.09		66%
Sweden		43.12		70%
United Kingdom*		764.62		77%

Notes: Estimates were produced by the ECB (2018) for 2016 and updated to 2019 values using Eurostat's HICP (Eurostat, 2020).

The lack of previous revenue estimates of the EU cybercrime market

An estimate of cybercrime revenues specifically focused on the EU was not found in the literature. Estimates that do exist commonly have a global or national-level focus. There are also studies estimating the size of sub-sections of markets. However, these estimates have significant caveats and should be approached with caution as to their accuracy and validity. The severe challenges and limitations associated with estimating revenues from cybercrime and the total annual revenue generated by OCGs include:

[89] Interview with private sector representatives, 6 May 2020, (#91).

- Contested or varying definitions;
- Inconsistent research approaches and results;
- Methodological weaknesses and overreliance on survey data;
- Insufficient, incorrect or biased data;
- Questionable assumptions;
- Revenues that may be significantly lower than costs; and
- The global and border-agnostic nature of cyberspace.

Measurements of the costs (rather than revenues) of cybercrime are faced with the same challenges and are equally controversial (Lewis, 2018). In fact, the estimates found in the literature are predominantly focused on costs (which are likely to be an order of magnitude higher than the revenues generated by cybercrime).

2.8.2. Criminal actors and modus operandi

The anonymised and cryptographic nature of the cybercrime market makes it very complicated to obtain information about the characteristics of the perpetrators, their organisation and their modus operandi. At the same time, some have found cybercrime is becoming more attractive as a lucrative profession for able hackers (Ablon et al., 2014; Choo & Smith, 2008; Grabosky, 2007; Huang et al., 2018; McGuire, 2018; Nets, 2019; Williams, 2001).

Cybercriminals increasingly specialise, commercialise and collaborate in their operations, creating a more complex cybercrime supply chain. The cybercrime market is easily accessible, anonymous and fast-paced. Through the division of labour, organised cybercriminal operations become increasingly complex. Online forums play an important facilitating role for communications and networking (Huang et al., 2018). Groups of cybercriminals operate in varying structures, depending on the crime they are committing. Networks of criminals are hierarchical in nature and adopt clear roles based on their skillset. The FBI, for example, identified 10 specialisations that (groups of) individuals adopt in a typical cybercrime: 'coders or programmers', 'distributors or vendors', 'technical experts', 'hackers', 'fraudsters', 'hosters', 'cashers', 'money mules', 'tellers' and 'leaders' (Chabinsky, 2010). According to Huang et al. (2018) the cybercrime ecosystem can be seen as 'a complete cyber-threat capability supply chain', consisting of vulnerability discovery, resistance operation (avoiding detection), delivery of cyber-attacks, marketplace support, repurposing gains to enable further attacks, human resources and technological support. Nonetheless, these networks of collaborating cybercriminals seem to lack the structure and hierarchy of conventional OCGs (Nagy & Mezei, 2016). Rather, organised groups involved in cybercrime are perceived as flexible networks of diverse, high-skilled individuals who rarely meet outside of cyberspace.

The level of OCG involvement in the cybercrime market is very difficult to establish. Methodological challenges include, for example, disagreement about what 'organised' crime refers to in the cybercrime context, whether organisation equals organised crime, the assumed convergence between cybercrime and organised crime without strong empirical evidence, and the lack of attribution and understanding of motivations of perpetrators.

Cybercrime services and platforms are utilised by and support other forms of criminality, resulting in a platform economy for criminality online (McGuire, 2018). Takedowns of illicit online markets have shown that these platforms also offered goods from other illegal markets, such as illegal drugs, firearms, counterfeited goods, identity and other formal documents, and toxic chemicals. Other types of fraud in which cybercriminals are involved include fake lotteries, unlawful gambling operations, stock scams and advance-fee frauds (Moore etal., 2009; Nagy & Mezei, 2016). In addition, cybercrime facilitates more traditional forms of criminal activities such as extortion and the distribution of imagery of sexual abuse of children (MONEYVAL, 2012).

2.8.3. Future trends and dynamics

On top of ever-increasing internet penetration around the world and, as a result, more prevalent exploitable vulnerabilities, cybercriminals can leverage technological advances to perpetrate their crimes. Levels of anonymity, complexity of operations and speed may all increase in the future. Progress in automation may also reduce the manpower necessary to undertake a certain criminal activity. Emerging technologies such as artificial intelligence and machine learning, autonomous devices and systems, Internet of Things (IoT), blockchain (and distributed ledger

technologies), privacy-enhancing technologies, and developments in computing and data-storage technologies, may offer opportunities or vulnerabilities that cybercriminals may attempt to exploit (more) in the future.

Cybercriminals increasingly work together to maximise profits. This could result in more offerings, more diverse products and services, increased specialisation and more integrated/ comprehensive packages of CaaS. Further specialisation could also mean that fewer skills are needed to participate in the market, lowering the threshold to criminal activities in cyberspace, and could deepen the trend towards a more complex cybercrime supply chain. This could take the shape of a 'cybercriminal service composition as a service' – a one-stop-shop combining the services of various hackers and illicit marketplaces (Huang et al., 2018). Increased specialisation, commercialisation and collaboration would also further complicate determining the criminals' identities and, ultimately, lower the barriers to the access to cybercrimes even further to increase demand and revenues.

Cybercrime could become a more viable career for able hackers, and cybercriminals could be driven deeper underground. If (international) criminal justice responses cannot keep up with the increasingly difficult prosecution of cybercriminals, cybercrime may become more attractive to able hackers. McGuire concluded that 'both the legitimate and illegitimate economies come together within an increasingly cyber-criminogenic world; one where the tools and cultures of information crime become blurred and interchangeable with the tools and cultures of an information society, and vice versa' (McGuire, 2018).

2.8.4. Recommendations

Many previous studies concluded that a comprehensive estimate of revenues from cybercrime is not feasible, and perhaps not productive to attempt. Previous efforts to develop comprehensive estimates of global cybercrime have been considered misleading[90]. Having said this, others who have explored these issues have highlighted good practice and potential considerations for future research into the revenues and costs generated by cybercrime, such as:

- Adopting systematic research methodologies and approaches;
- Clearly defining and scoping the market segment to be estimated;
- Using the best available data and ensuring buy-in from data holders; and
- Leveraging good practice by estimating other illicit markets.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.33: Recommendations – Cybercrime market

Key finding	Recommendation	Actor
Estimates of the revenues from cybercrime do not exist. However, card-not-present (CNP) fraud is included in the European Central Bank's (ECB) reporting of card payment fraud (both online and offline).	Focus future research efforts on specific cybercrime sub-markets using tailored methodological approaches. Partnerships with industry may be strengthened in order to access data for deriving estimates, as well as police and judicial authorities for accessing case information.	Member States, particularly police and judicial authorities Industry

2.9. Organised property crime

Alexander Gerganov, Mitch Legato and Atanas Rusev, Centre for the Study of Democracy

Key findings:

- Cargo thefts and ATM physical attacks are the only organised property crimes for which reliable revenue estimates can be provided, although they remain rather niche crimes in the EU when compared to other forms of organised property crime.

[90] Interview with cybercrime academic expert, 12 February 2020 (#12).

- According to the estimates produced in this study, the annual revenues derived from the cargo theft market in the EU range between €0.1 billion and €7 billion for 2019. ATM physical attacks account for another €22 million in annual revenues.
- The data availability does not allow for the generation of an estimate of revenues for other organised property crime types, such as burglaries, robberies and motor vehicle theft. However, upper bound estimates of losses incurred by households and businesses from the motor-vehicle theft market are as high as €2.5 billion, €3.4 billion from domestic burglary, and €0.5 billion from the robbery market.
- Comparison of revenue estimates for both cargo theft and ATM physical attacks show a decreasing trend over the period 2015 to 2019.
- Organised property crimes are frequently carried out by mobile organised crime groups (MOCGs), which systematically commit a significant number of property crimes over large areas across Europe, and often originate from Eastern European countries.
- Each organised-property crime sub-market has unique actor characteristics, which include differing levels of organised crime involvement and skill level. Organised crime involvement is highest in motor vehicle thefts, cargo thefts and ATM physical attacks.
- A growing trend faced by law enforcement in combating organised property crime is the increasing use of technology to facilitate and abet in criminal activities.

Organised property crimes – or the theft or destruction of property (Europol, 2020e) – range from widespread crimes such as burglary, motor vehicle theft and robbery to more niche crimes such as cargo theft and trafficking in cultural goods (Angelini et al., 2015).

A comprehensive overview of the organised property crime market in the EU, building upon the summary provided here, can be found in **Annex 2.9**.

2.9.1. Revenue estimates of the EU cargo-theft and ATM physical attacks markets

Cargo thefts and ATM physical attacks are the only organised property crimes for which reliable revenue estimates can be provided, given the general lack of prior methodologies and datasets for most of the organised property crimes. Estimates of costs or losses from organised property crime are presented in Box 2.3. Table 2.34 presents the estimates produced for this project of cargo theft and ATM physical attacked. The following estimates have been produced:

- The estimates of the cargo theft market in 2019 at the EU-level and for each of the EU Member States (without Malta) can be as large as €6.5 billion, despite the much smaller sum of €144 million based on reported incidents (used as a lower bound).
- ATM physical attacks account for €22 million in revenues (cash stolen) in 2019. The data is collected and reported by the European Association for Secure Transactions (EAST) on annual basis (EAST, 2020).
- An incidence-based approach was used for all estimates provided below and the number of incidents was multiplied by the average loss per incident. For the cargo-theft and ATM physical attacks markets, estimates show the value of the corresponding market, while for motor vehicle theft, domestic burglary and robbery only annual losses are calculated as a broad indication of the direct cost of these crimes. The estimate of the value of the losses for these crimes reflects only the value of the stolen property and does not include any additional costs related to the crime incident (e.g. cost of other damages resulting from the crime, possible health costs, etc.).

Table 2.34: Revenue estimate of the EU cargo theft and ATM physical attacks markets

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)			
	Cargo theft*			ATM physical attacks**
	Mid	Low	High	Low

EU Member State	Annual revenue, adjusted for inflation, 2019 (€ million)			
	Cargo theft*			ATM physical attacks**
28 EU Member States	**3,347.85**	**144.39**	**6,551.32**	**22**
27 EU Member States without UK	**2,970.26**	**49.87**	**5,890.70**	
Austria		-	168.96	
Belgium		1.37	64.00	
Bulgaria		-	58.20	
Croatia		-	34.04	
Cyprus		-	13.20	
Czech Republic		0.45	267.10	
Denmark		0.14	57.76	
Estonia		-	9.06	
Finland		-	85.76	
France		2.57	685.84	
Germany		6.84	1,517.43	
Greece		-	150.83	
Hungary		0.36	93.62	
Ireland		0.76	71.71	
Italy		5.87	356.40	
Latvia		0.66	25.29	
Lithuania		-	41.80	
Luxembourg		-	19.07	
Malta		-	-	
Netherlands		18.52	307.18	
Poland		-	663.46	
Portugal		0.25	68.65	
Romania		8.72	110.27	
Slovakia		0.83	139.51	
Slovenia		-	39.51	
Spain		1.24	641.06	
Sweden		1.29	200.97	
United Kingdom		94.52	660.63	

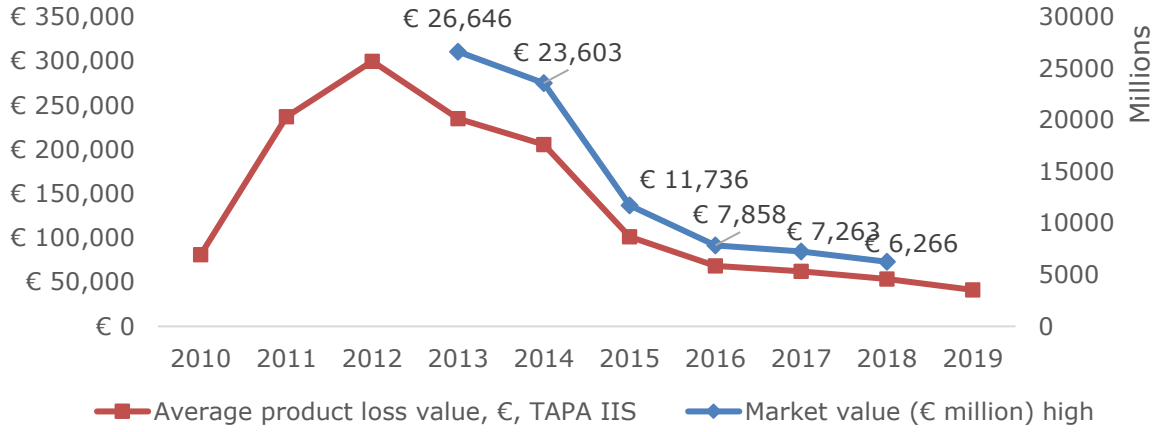
Notes: *Cargo thefts do not include MT. **Included Member States are AT, CY, CZ, DK, FI, FR, EL, IE, IT, LI, LU, NL, PT, RO, SK, ES, SE, CH, UK.

Previous revenue estimates of the EU cargo theft and ATM physical attacks markets

Previous revenue estimates are available only for cargo theft and ATM physical attacks. The revenue estimate of cargo theft presented in Table 2.34 for 2019 (€6.5 billion) is lower than the previous most-recent estimate for 2013 (€11.6 billion) (FWI SCIC, 2016). It should be noted that FreightWatch used its own more conservative estimate of €91,000 loss per incident for its 2013 estimate, which differs from the average loss value based on the incidents registered in the Transported Asset Protection Association (TAPA) Incident Information Service (IIS) database used for the estimate in this report. Since this previous estimate used different assumptions to the current approach, the estimates are not directly comparable with the ones produced in this study.

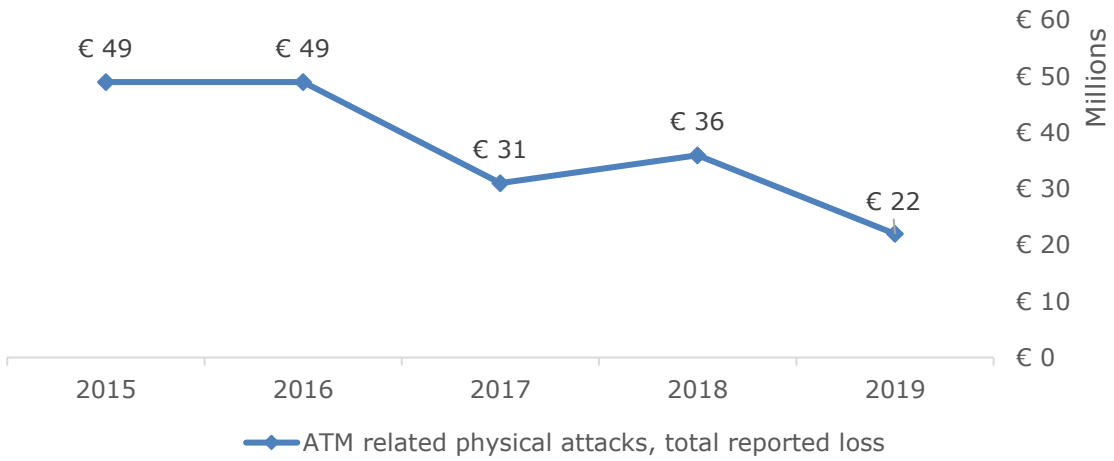
TAPA IIS is the best and only source of structured information on cargo theft, and it contains information on number of incidents and average loss per incident for the period 2013–2018. The available data allows production of revenue estimates and reconstruction of the trend on the market, which shows a steady downward tendency (see figure below).

Figure 2.1: Average product loss value (TAPA IIS) and total market value (2010 to 2019)



The current study has not produced a new estimate for ATM attacks, but draws on the cash stolen reported by EAST. Data from EAST show a general tendency of decline in value of reported losses since 2015 (see Figure 2.2).

Figure 2.2: ATM related physical attacks, total reported loss (2015–2019)



Source: EAST (2020).

Box 2.3: Estimates of the costs of organised property crime in the EU

Tentative loss-based estimates for motor vehicle theft, domestic burglary and robbery can be calculated, but should be used with great caution due to multiple methodological limitations of the estimates. Loss-based estimates are not the same as revenues, and therefore cannot be directly compared to other SOC markets for which revenue estimates have been produced.

- Motor vehicle theft losses (different from revenues) are estimated to be as high as €2.5 billion (an upper bound estimate).
- Domestic burglary losses (different from revenues) are estimated to be as high as €3 billion (an upper bound estimate).
- Robbery market losses (different from revenues) are estimated to be as high as €462 million (an upper bound estimate).

EU Member State	Losses from organised property crimes (€ million)		
	Motor vehicle theft	Domestic burglary*	Robbery

	High	High	High
28 EU Member States	2,526.27	3,389.86	461.91
27 EU Member States without UK	2,093.81	2,674.05	369.47
Austria	29.23	31.87	3.05
Belgium	54.19	179.21	22.12
Bulgaria	8.65	11.97	1.82
Croatia	3.12	12.24	1.01
Cyprus	3.51	2.49	0.14
Czech Republic	77.97	19.53	1.85
Denmark	0.80	109.06	2.38
Estonia	1.24	2.61	0.23
Finland	22.27	12.88	1.91
France	589.75	651.24	116.79
Germany	197.59	314.66	45.34
Greece	124.24	59.52	4.98
Hungary	11.59	54.79	0.98
Ireland	17.90	-	2.55
Italy	532.23	528.72	36.37
Latvia	3.95	3.86	0.70
Lithuania	3.65	6.99	1.27
Luxembourg	6.22	5.73	0.53
Malta	1.21	2.30	0.24
Netherlands	92.93	134.44	9.32
Poland	45.46	57.02	9.47
Portugal	37.44	33.21	13.87
Romania	10.69	39.09	3.69
Slovakia	5.56	4.44	0.55
Slovenia	1.97	7.84	0.28
Spain	120.11	283.77	77.94
Sweden	90.34	104.58	10.09
United Kingdom	432.46	715.81	92.44

*Domestic burglary estimates do not include Ireland

2.9.2. Criminal actors and modus operandi

Organised property crimes are frequently carried out by MOCGs. These groups systematically commit a significant number of property crimes over large areas across Europe, and often originate from Eastern European countries (Van Daele & Vander Beken, 2010). An interview with a law enforcement representative[91] noted that this is due in part to EU enlargement and the subsequent increase in free movement that has provided new opportunities for MOCGs to commit a number of crimes in a region over a short duration before moving on (UNODC, 2010).

The type of goods targeted depends on both the crime and the organisation's skill level. Expert interviewees noted that highly structured organisations have the skills to carry out more lucrative but riskier property crimes, such as stealing a specific container from a

[91] Interview with Spanish national-level expert, 22 April 2020 (#72).

warehouse or pieces of art from a museum[92]. In contrast, loosely structured groups are often involved in more opportunistic property crimes, such as domestic burglaries, where they can steal jewellery, electronics and other items containing gold which can easily be sold at pawnbrokers or 'Cash for Gold' shops (Wollinger et al., 2018, p. 17).

Each organised property crime market has unique actor characteristics, which include differing levels of OCG involvement and skill level. It is estimated that 60–80% of burglaries in the EU are now carried out by MOCGs comprised of small groups of men aged between 30 and 50 from Eastern Europe[93]. Conversely, the average robber is between 20 and 30 years old, and those who carry out physical ATM attacks closely resemble MOCGs involved in both burglary and robbery[94]. (Cornelius et al., 2017; HM Government, 2018). For motor vehicle theft, anti-theft protections such as electronic tracking systems have resulted in a market that requires skills or tools that are too expensive for the common criminal (Savona & Riccardi, 2015). The vast majority of cargo thefts are carried out by OCGs, although with differing levels of organisation[95]. Actors who traffic cultural goods operate within a legal, finite and niche market, and require a certain level of skills and knowledge of locating, looting and later transporting and selling illicit cultural goods internationally (Campbell, 2013).

Modus operandi

The modus operandi for organised property crime varies based on the type of organised property crime. Burglaries most commonly occur when criminals simply break into homes while the owners are away, often after surveillance or casing the property and surrounding areas (Van Daele & Vander Beken, 2010). While targets for robberies are increasingly more random, traditional targets, such as banks, have better security and less cash, so are no longer targeted by risk-adverse criminals[96]. Europol & EUCPN note that gas and explosive attacks are the most common physical ATM attacks, followed by in-situ attacks and rip-out/ram-raid attacks (Europol & EUCPN, 2019, p. 4). Some stolen vehicles are used as a means to commit other crimes, with high-performance cars used as getaway cars in other organised property crimes or vans and trucks used in ram attacks on ATMs (Savona & Riccardi, 2015). Alternatively, in other thefts the car is stolen for its resale value.[97]

Methods of cargo theft differ based on the criminals involved. Some operations involving pre-planned measures to carry out thefts and protect the criminals from being identified include using stolen cars or fake license plates, GPS and mobile phone jammers, and communication through walkie-talkies (Boerman et al., 2017, p. 210). According to Gruber (2019), actors involved in cultural goods trafficking often rely on the ignorance of buyers to obfuscate an item's provenance in addition to creating fake export documents, import licenses or certificates of authenticity to mask the illegal origins of cultural goods. This has created ambiguity on the legality of pieces, creating difficulties for buyers to verify that pieces are legal (Shea, 2018).

2.9.3. Future trends and dynamics

Trends indicate that domestic burglary, robberies and cargo theft will rise slightly or – like motor vehicle theft – stabilise, while profitability and incidences of cultural goods trafficking will likely continue to grow (Europol, 2017b). Domestic burglary remains a lucrative market but is impacted by improvements in home security and law enforcement becoming more accustomed to how to stop or deter burglars (De Stercke et al., 2014). Increasing rates of robberies can be partially attributed to improvements in police recording, despite security measures taken to curb robberies (Home Office, 2018b). While motor vehicle theft rates have stabilised, the number of recovered cars has decreased (Europol, 2020e). With cross-border travel and trade an integral component of the EU, the cargo theft market will remain profitable and easily accessible for criminals[98]. Trafficking of cultural goods will continue to grow as a profitable, recession-proof market in which supply and demand will continue to increase in the future (Shea, 2018).

[92] Interviews with cargo theft experts and cultural goods trafficking experts, 26 February 2020 (#38) and 27 February 2020 (#39).
[93] Interview with law enforcement representative, 8 April 2020 (#61).
[94] Interview with expert from non-profit organisation, 27 April 2020 (#74).
[95] Interview with cargo theft expert, 27 February 2020 (#39).
[96] Interview with law enforcement representative, 12 March 2020 (#50).
[97] Interview with law enforcement representative, 22 April,2020 (#72)
[98] Interview with law enforcement representative, 12 March 2020 (#50).

One growing trend faced by law enforcement in combating organised property crimes is the increasing use of technology to facilitate and abet in criminal activities[99]. Both social media and GPS have allowed thieves across all organised property crimes to monitor the comings and goings of targets and plan routes without ever coming into contact with victims (Profiling, 2015). This has allowed OCGs to carry out crimes more effectively and efficiently while simultaneously lowering their criminal profile to police[100]. Another trend is the continued and increased reliance on the use of online platforms for selling loot anonymously to remain undetected by law enforcement (Wollinger et al., 2018). This is universal across organised property crime markets, as the internet is often the easiest and safest way to sell stolen goods, with sellers able to sell goods both within the EU and internationally (Aniello & Caneppele, 2017).

2.9.4. Recommendations

The current study suggests two possible ways in which data collection and estimations of the organised property crime market could be improved (although both would be costly and difficult to implement):

- First, Eurostat currently reports numbers of incidents for robbery, motor vehicle theft, domestic burglary and commercial burglary. If **incidence rates for the sub-types of these crimes were also collected/reported**, this would facilitate estimates of organised property crimes for specific sub-markets – such as distraction burglary, plant theft, theft of cash, valuables in transit and others. Given the differences in legislation between Member States, however, this is rather unlikely to be feasible, since even current more general crime types – like robbery and motor vehicle theft – are not considered completely reliable for comparisons between Member States (van Dijk et al., 2014).
- Second, conducting **large-sample harmonised cross-country victimisation surveys among populations, and especially businesses** could be a much better source of data for estimating OCG markets, albeit a costly one. Such surveys would allow collection of detailed information about losses and rates of reporting to the police for different organised property crime types, and other relevant details through which revenue estimates could be produced for more of the organised property crime sub-markets.

The key findings from this study and the related recommendations are summarised in the table below.

Table 2.35: Recommendations – Organised property crime

Key finding	Recommendation	Actor
Criminal statistics on registered property crime collected by Eurostat do not provide disaggregated data on incidents for the different sub-types of organised property crimes (e.g. plant theft, theft of cash and valuables in transit), which would allow better differentiation of crimes with high OCG involvement from high-volume crime. All identified methodologies account for the unreported crime and rely on input data from crime victimisation surveys. Such surveys are available only for a few Member States. There is a lack of data on the ratio between monetary value of stolen property and revenue of criminals, which makes it impossible to estimate revenues of organised property crime.	Collect incident rates for specific types of organised property crimes, especially the ones known for high involvement of OCGs. Conduct large-sample harmonised cross-country victimisation surveys among populations, and especially businesses in all EU Member States on a regular basis. Such surveys should collect detailed information about losses per incident and rates of reporting to the police for different organised property crime types. Member States should systematically report information on revenues generated through property crimes (which is currently collected by police or judicial authorities in the course of some of their investigations) to the European Commission.	Eurostat Member States European Commission

[99] Interview with cargo theft expert, 27 February 2020 (#39).
[100] Interview with law enforcement representative, 8 April 2020 (#61).

3. Serious and organised crime investment and infiltration in the legal economy

The previous chapter estimated that the revenues generated across the nine criminal markets in the EU ranged from €92 to €188 billion (mid-point estimate of €139 billion) in 2019. These considerable criminal earnings may subsequently be **invested** by OCGs in the legal economy for a range of reasons, such as to maximise profit, influence politics and industry, and conceal ongoing illicit activities. Moreover, OCGs may **infiltrate** legal businesses and industries, which means investment of not only financial but also human resources for the purpose of participating in or influencing decision-making of the business (Savona & Riccardi, 2018).

SOC investment and infiltration in the legal economy is cause for concern, as it may create unfair market competition and economic uncertainty, and can lead to corruption and the deterioration of politics and public administration (Ferrante et al., 2019; Operti, 2018; Savona & Riccardi, 2015). An organisation infiltrated by an OCG may be more likely to engage in unlawful conduct and be non-compliant with regulatory frameworks, thus exposing the public and state to harms. Reputational damage to the infiltrated occupation or industry may also occur (Victorian Law Reform Commission, 2020).

In light of these harms it is imperative that efforts to tackle SOC focus not only on the generation of criminal proceeds (which we explored in Chapter 2), but also on their subsequent investment and infiltration in the legal economy. This chapter of the study is intended to inform policy efforts in this regard, and is structured as follows:

- **Section 3.1** examines the main categories of assets and business sectors in which OCGs make investments in the EU, and the frequent modus operandi for transferring proceeds.
- **Section 3.2** focuses on the freezing and confiscation of criminal proceeds in the EU – one mechanism for tackling the investment of criminal proceeds by OCGs in the legal economy.
- **Section 3.3** offers novel analysis on risk factors that facilitate SOC infiltration of companies and public procurement in the EU.
- **Section 3.4** explores the vulnerabilities within legal sectors that may be exploited by OCGs, using the conceptual framework of the underground (or shadow) economy.
- **Section 3.5** considers to what extent NPMs, such as cryptocurrencies, are exploited by OCGs for the purposes of investment, money-laundering and the furthering of criminal activities.
- **Section 3.6** describes some possible emerging threats with regard to SOC investment and infiltration in the legal economy.

3.1. Investment by organised crime groups in the legal economy

Shann Hulme, RAND Europe

Key findings:

- The predominant sectors of known investments by OCGs in the legal economy are property/real estate, transportation and construction. However, there is a lack of robust data to quantify such investments, and it is likely that current understandings are not representative of the phenomenon.
- Cash couriers are used by OCGs for transferring proceeds generated through cash-based markets like illicit drugs, THB and illicit tobacco.
- Electronic funds may be transferred by OCGs through money muling or 'smurfing'.
- Cryptocurrency exchange services and mixing or tumbler services are used for transferring cryptocurrencies and funds earned through cybercrimes.

Literature review	Interviews	Surveys	Proven cases
			

Additional information supporting the analysis presented in this chapter can be found in **Annex 3.1**.

3.1.1. Business sector and type of assets

Available evidence from prior literature on investments by OCGs in the legal economy by business sector, type of asset and drivers of investment is summarised in the table below. The predominant sectors of known investments are property and real estate, hospitality, environment, construction, transportation, wholesale and retail, and finance. There are various types of assets within each sector and the drivers of investment tend to differ across sectors.

Table 3.1: Investments by organised crime groups in the legal economy

Business sector	Type of assets	Drivers of investment
Property/real estate	Land Houses Industrial or commercial buildings Companies that buy and sell real estate Shops Hotels Parking lots	Residential use Symbolic and social status for OCG members Business use Properties operate as logistical base for illicit activities – particularly important for THB, smuggling of migrants and drugs trafficking Profit maximisation and earning of legal revenues through renting Control over a territory or area – such as through territorially specific assets, like hotels
Hospitality	Bars and restaurants Casinos and gambling establishments	Concealment of illicit proceeds by laundering funds through cash-intensive businesses
Environment	Waste management Renewable energy	Utilising public subsidies on renewable energy to maximise profits Facilitating illicit activities – e.g. using service providers for illegal waste disposal
Construction	Public procurement	Rent-seeking behaviour to finance illegal activities and gain political consensus and social control This sector is attractive to OCGs for the following reasons: high territorial specificity; low levels of innovation; labour intensive and not fully open to market competition Exploiting inefficient control systems
Transportation	Cars Boats Motorcycles Cargo ships Trucks Luxury cars, yachts, jets, helicopters	To facilitate illicit activities by using vehicles to transport illicit goods from one place to another Status symbol and prestige
Wholesale and retail trade	Food products Flowers Oil products Medicines High-value goods like jewellery, diamonds, precious metals	Facilitate illicit activities To launder illicit proceeds and used as currency – once purchased, commodities can be sold locally or transported overseas to meet demand of a market in exchange for payment
Finance	Financial instruments Bank accounts Hawala Prepaid cards Cryptocurrencies Corporate shares	Money-laundering

Source: Research team's analysis and synthesis of existing literature on investments by OCGs in the legal economy in the EU (Antonopoulos & Hall, 2016; Dugato et al., 2015; Ferwerda & Kleemans, 2019; Gilmour & Ridley, 2015; Kruisbergen et al., 2015; Levi, 2015; Ravenda et al., 2019; Riccardi, 2014; Savona & Riccardi, 2018; Terziev et al., 2018; Transcrime, 2015b).

Frequency of investment by sector and asset type

While it is difficult to precisely quantify the sectors and assets of OCG investment, some general insights can be drawn through triangulation of the prior literature, surveys and proven cases:

- In the prior literature, the most heavily cited business sector for investment by OCGs was the property and **real estate** sector, and cash-intensive sectors like **hospitality** (bars, restaurants and gambling establishments).
- Of the 81 proven cases examined, 55 contained information on investments by OCGs in the legal economy. The breakdown of investments by business sector is shown in Table 3.2 below, demonstrating that consistent with the literature, the **real estate** sector is the most prominent for investment. **Transportation** also featured prominently, typically as a means by which to facilitate the movement of illicit goods.
- The four AROs that were able to provide statistical data on the type of asset frozen or confiscated over the period 2017 to 2020 similarly indicated that **real estate** represented most cases. This was followed by **cash and financial instruments, luxury goods and vehicles**. The AROs reported a small number of cases involving **cryptocurrencies**. Interviewees involved in asset seizure and recovery in the EU indicated that cases involving cryptocurrencies were growing in prominence; however, they were still low in number overall[101].

Table 3.2: Sectors of investment by organised crime groups

Business sector	Number of cases
Real estate	20
Transportation	23
Construction or manufacturing	20
Wholesale or retail trade	14
Financial instruments	9
Hospitality	8
Environment	6

Source: Research team's database of proven cases of SOC investment and infiltration in the legal economy (n=81).

The prior literature and interviews with experts revealed some patterns of investment type by actors operating across different illicit markets.

In illicit markets that are predominately cash-based – that is, illicit drugs, THB, smuggling of migrants, intellectual property right (IPR) infringements and illicit tobacco – prior research and interviews with stakeholders showed that it is common for OCGs to buy **luxury, high-value movable goods** such as jewellery, watches, motor vehicles, designer clothing and gold (CSD, 2015; Petrunov, 2011)[102]. These investments may be acquired for personal consumption and to **enhance the living standards** of OCG members[103]. These goods are also **used as currency** and may be sold or traded[104]. In the EU, OCGs take advantage of freedom of movement of goods in the Schengen area to convert criminal proceeds into legal goods that are then traded across international borders (ALEFA, 2019). Two interviewees explained how OCGs may increasingly favour investments in assets that are not monitored, such as luxury goods like jewellery and watches in lieu of cash, so as to avoid the risks associated with physically transporting cash[105].

Several examples were provided in the literature of proven cases, supported by interviewee remarks, of OCGs investing in the legal economy to **facilitate the logistics of criminal activity**.

- According to the EMCDDA and research by Savona & Riccardi, it is common for OCGs involved in **illicit drugs trafficking** to buy boats and lorries to move drugs across Europe (EMCDDA & Europol, 2016; Savona et al., 2016).

[101] Interview with Member State representative, 27 April 2020 (#74).
[102] Interview with an academia representative, 25 February 2020 (#35).
[103] Interview with National/MS-level expert, 2 April 2020 (#30).
[104] Interview with law enforcement representatives, 11 March 2020 (#14); Interview with Member State representative, 28 April 2020 (#77).
[105] Interview with Member State representative, 28 April 2020 (#77).

- One interviewee mentioned that OCGs involved in **IPR infringements** may invest in bars and restaurants, supermarkets chains and transportation networks to control the distribution and sales of their own products[106]. Examples included OCGs involved in the production and supply of counterfeit goods investing in the manufacturing industry through the purchase of machinery, factories or legitimate manufacturing or wholesale companies to aid in the production of counterfeit goods.
- In the case of **food fraud**, a market expert interviewee[107] mentioned a case study in Italy where the Camorra bought an entire supermarket chain and controlled the local delivery network, allowing them to have total control of the food products being delivered to – and sold by – the supermarkets.
- A study by the CSD (2015) found that OCGs involved in **Missing Trader Intra-Community (MTIC) fraud** invested in businesses that could facilitate fraud – such as logistical companies in order to transport goods – or companies that handle a lot of cash for money-laundering purposes, such as nightclubs, hotels and restaurants. A Value Added Tax (VAT) fraud expert[108] confirmed this, revealing that real estate is often purchased, and legitimate companies from a variety of sectors are bought to be used for money-laundering purposes.

3.1.2. Modus operandi of transferring funds for investment of criminal proceeds in the legal economy

Strategies for investment by OCGs in the legal economy are focused on minimising the risk that the illegal origin of the proceeds will be detected. As noted by several interviewees[109], investments might be made abroad and there is a range of strategies for moving money – either physically or electronically – in order to conceal investments across the business sectors and assets described above.

[106] Interview with International-level stakeholder, 19 March 2020 (#24).
[107] Interview with international-level stakeholder, 19 March 2020 (#24).
[108] Interview with private sector expert, 14 February 2020 (#6).
[109] Interview with law enforcement representative, 11 March 2020 (#15); Interview with National/Member State expert, 26 March 2020 (#62); Interview with National/Member State expert, 2 April 2020 (#30).

Table 3.3 provides a summary of the main strategies employed by OCGs in the EU identified during interviews and a review of the literature. As shown, there are clear links between the strategy employed and the illicit market through which the proceeds were generated. This is typically related to whether the criminal activity generates predominately cash or non-cash. Indeed, there are specific modus operandi for transferring cryptocurrencies generated through cybercrimes such as phishing, ransomware and the sale of illicit goods and services on dark-net marketplaces.

Stakeholders identified a persistent trend of OCGs employing the services of **criminal entrepreneurs** who have specialised and technical knowledge of transferring and placing proceeds of crime for reinvestment. Two stakeholders reported that European OCGs increasingly hire criminal entrepreneurs to launder their illicit drugs-trafficking proceeds[110]. According to a report by the EMCDDA and Europol, such 'crimes as a service' have become more widespread within the European drugs market, particularly for money-laundering (EMCDDA & Europol, 2017). Moreover, a study by CSD (2015) showed that criminal proceeds may be invested in the services of accountants, lawyers and similar professionals who can help advise the creation and dissolution of front and shell companies, and give financial and tax advice.

[110] Interview with law enforcement representatives, 11 March 2020 (#14); Interview with EU-level representative, 12 February 2020 (#3).

Table 3.3: Strategies for laundering and investment of illicit proceeds

Strategy employed	Illicit market links
Cash couriers are persons that physically transport cash across borders. OCGs often recruit people as cash couriers to transport illegally generated cash across an international border on their person, often concealed in clothing, on the body or in luggage (FATF & MENAFATF, 2015).	Commonly used for transferring proceeds generated through cash-based markets like **illicit drugs, THB and illicit tobacco**. Regarding THB, there is evidence that victims themselves may be used for carrying money (Europol, 2015c).
Micro-transfers (or micro-laundering) is where large sums of money are moved in small amounts through thousands of electronic transactions (Richet, 2013). The benefit of this approach is that AML transaction limits can be evaded, and it is difficult for law enforcement to trace.	Commonly used for transferring illicit proceeds generated electronically – such as via **MTIC fraud, card-payment fraud, cybercrime** and the **online sale of illegal goods and services (e.g. drugs, IPR infringements and counterfeit goods).** McGuire (2018) found that in 20% of the **cybercrime cases** sampled in his research, the main money-laundering tools were PayPal and other digital payment systems. Cybercrime profits are diverted through multiple PayPal accounts to distribute the profits, often in combination with fraudulently opened bank accounts and Western Union transfers (Richet, 2013). In relation to **IPR infringements**, a report from the EUIPO & Europol (2019) noted that micro-transfers were a common strategy, in addition to the use of prepaid cards. Prepaid cards are used because certain Member States do not allow their seizure, creating an added level of security for offenders.
Money muling or 'smurfing' is where a person receives money from a third party in their bank account, then transfers it to another account or withdraws it in cash to give to someone else, obtaining a commission for it (Europol, n.d.).	According to Europol, more than 90% of money mule transactions identified through the European Money Mule Actions are linked to **cybercrime** (Europol, n.d.). For example, money mules are the preferred means for draining compromised financial accounts obtained via **phishing attacks** (Florêncio & Herley, 2010). Money-laundering networks in the country of origin of the perpetrators are often exploited by phishing networks[111]. For example, in one case described in the literature, a German-based cybercriminal network used the services of members of an outlaw motorcycle club to manage money mules (Leukfeldt et al., 2017). In another case, a Latvian phishing network applied a traditional money-laundering scheme by bringing money mules to the Netherlands, making them open bank accounts and withdraw the money, before returning to their country of origin[112]. The risks of tracing the money mules to the perpetrators is minimised by the use of facilitators who recruit and coordinate the money-mule network[113]. In addition, cybercriminals often used additional layers of security (e.g. installing proxy server, VPNs, and encryption of the traffic network) in their communication with facilitators[114].
Mixing or tumbler services combine identifiable (or 'tainted') cryptocurrency funds with untainted pools of funds, to obfuscate the origin, possession and movement of illicitly obtained	Commonly used for transferring proceeds earned in cryptocurrencies through **cybercrimes like ransomware** (Liao et al., 2016) and the **sale of illegal goods and services on dark net**

[111] Interview with an academia representative, 25 February 2020, #35.
[112] Interview with an academia representative, 25 February 2020, #35.
[113] Interview with International organisation representative, 22 April 2020, #73; Interview with an academia representative, 25 February 2020, #35.
[114] Interview with International organisation representative, 22 April 2020, (#73).

Strategy employed	Illicit market links
cryptocurrencies. The extent to which they do so is a function of the process of tumbling, both in terms of encryption and mixing strategy (Chohan, 2017).	**markets**.
Cryptocurrency exchange services facilitate the buying and selling of cryptocurrency units in exchange for fiat currencies or other cryptocurrencies (European Commission, 2016a). There is reportedly an emerging trend to convert bitcoins into more privacy-oriented cryptocurrencies like Monero (EUIPO & Europol, 2019). Such exchange services are based on both a service and an output platform. An output platform – a bank or service such as PayPal – is used to make sure the exchanged currency ends up in the possession of a client. The bank transfers can be made to money mule accounts, but also to the bank accounts of the perpetrators, if the layering in the cryptocurrency ecosystem is sufficient[118]. A substantial number of mixing and exchange services are offered on dark-net websites (Van Wegberg et al., 2018).	An interview with law enforcement representatives indicated that the use of a combination of money-laundering tools in the cryptocurrency ecosystem could be more cost-efficient than traditional cash-out schemes.[115] While costs for the money mules and their coordinator could reach 40% of revenues, the layering and cash-out through several cryptocurrency tools might cost only 6%[116]. Furthermore, the overall cash-out process takes less time, as cryptocurrency mixing and exchange could be carried out in just a couple of hours and without any logistical constraints[117].
Straw ownership is a strategy whereby a person owns a legal enterprise on behalf of an OCG, usually for a fee, to conceal the identity of the beneficial (i.e. effective) owner.	Where OCGs acquire ownership of a legitimate company or financial instrument, particularly in order to facilitate the logistics of illicit activities or to launder money, it is a common strategy for 'straw men' to be involved. As reported by Hall et al. (2017) the ownership of legitimate companies via straw men provides a shield of legitimacy for money transfers. Our review of proven cases identified several examples where OCGs involved in **IPR infringements** and **counterfeiting**, **illicit tobacco**, as well as **tax and MTIC fraud** used 'straw men' to open bank accounts or set up legitimate companies. For example, one case in the Czech Republic involved two active OCGs, with some overlapping personnel. The first group manufactured counterfeit identity documents pertaining to real and fictitious individuals. The second group used these documents to place their own personnel (via straw owners) in decision-making positions in over 400 commercial entities. These entities reported substantial fictitious activities and turnover to provide cover for illegal sales of goods to avoid VAT liability.
Offshore accounts and tax havens are used for transferring criminal proceeds outside the EU, where the traceability of the money becomes more difficult, and as an alternative to increasingly controlled banking systems (ALEFA, 2019).	

3.1.3. Geographical trends in investment by organised crime groups in the legal economy

Data availability is insufficient to quantify geographical trends in investment by OCGs in the legal economy.

[115] Interview with Europol representatives, 12 March 2020, (#48).
[116] Interview with Europol representatives, 12 March 2020, (#48).
[117] Interview with Europol representatives, 12 March 2020, (#48).
[118] Interview with law enforcement representatives, 12 March 2020, (#48); Interview with representatives from an international organisation, 25 February 2020, (#73).

A lack of data means that it is not feasible to offer a reliable and comprehensive quantification of the types of assets and business sectors in the legal economy across different geographical areas that OCGs are known to investment in.

Presented in Table 3.4 below is information from our survey of AMOs. Based on the data that was available to AMOs and reported to us, it provides some indication of the types of assets managed by AMOs between 2017 and 2020. While these data provide some useful and current insights about the types of assets seized from OCGs in different Member States, the overview should not be considered to be representative of investment by OCGs in the legal economy. This is because while European law requires Member States to make use of freezing and confiscation measures, in practice – due to high costs of identifying the proceeds and in managing them once they are confiscated – the authorities apply the provisional measures mainly in serious crime cases, usually those that are high income and high liquidity, such as drug trafficking (European Commission, 2012). Thus, in addition to undetected investments, the absence of indications from a Member State that they were managing foreign OCG assets does not mean these assets were not invested in by OCGs in that country.

Table 3.4: Assets managed by Asset Management Offices (2017–2020)

EU Member State	Cash	Bank accounts	Financial instruments	Crypto currency	Property	Luxury goods	Vehicles	Metals	Old coins	Watches	Companies	Electronic devices	Animals
Belgium	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	-	-	-
France	Y	Y	-	Y	Y	-	-	-	-	-	-	-	-
Ireland	Y	Y	-	Y	Y	-	Y	-	-	Y	-	-	-
Italy	Y	-	-	-	Y	-	-	-	-	-	Y	-	-
Netherlands	Y	Y	-	Y	Y	Y	Y	-	-	-	Y	-	Y
Portugal	-	-	-	Y	-	-	-	-	-	-	-	-	-
Romania	-	-	Y	Y		-	-	-	-	-	-	-	-

Source: Research team's survey of AMOs (2020).
Notes: '-' = no statistics available. 'Y' = assets that were managed by the relevant Member State.

Investments are often made in the country of origin of the OCG. Research by Kruisbergen et al. (2015) examined 150 cases involving 1,196 investments in the legal economy by OCGs operating in the Netherlands. They found that 63% of all assets were located in the country of origin or 'home country' of the offender.

Our analysis of 81 proven cases of infiltration reached a similar conclusion. In the 75 cases where the country, origin or ethnicity of the OCG was known, 61 cases (81%) involved investments in their country of origin. For example, an Irish family-based OCG involved in unknown illicit activities purchased a range of family residences and vehicles in Ireland. In another case a Hungarian OCG involved in the pirating of digital materials invested in a property in Hungary to store the computer servers that were used to commit the crime.

Sometimes investments are made in foreign countries, although this typically occurs to facilitate the logistics of the illicit activity. In 14 cases (19%) in our study, investments were made by OCGs in a country other than their 'home country'. For example, in one case an OCG involving actors from 'former Soviet Union states' invested in transportation companies in multiple European countries, primarily in Central and Eastern Europe. These transport companies were used for attracting customers who would then have their cargo stolen. In another case, four family-based OCGs operating in Italy were involved in the trafficking of counterfeit goods. They invested in cash-intensive businesses in Italy for the purpose of money-laundering, as well as companies in China to facilitate further production of the goods. In another case, a Thai-based OCG operating in Denmark invested in a business in Denmark, which served as a front for an illegal brothel. Evidently, in most of these cases investments were made in the country where the illicit activity was taking place.

3.1.4. Recommendations

The key findings stemming from this part of the study and the related recommendations are summarised in the table below.

Table 3.5: Recommendations – Investment in the legal economy

Key findings	Recommendation	Key actors for recommendation
To date, analysis of investments by OCGs in the legal economy has been based upon limited case information available from public sources – such as legal databases and media archives – resulting in a non-representative understanding across Member States. Data on asset seizure and recovery is also a source of information, though this too suffers data limitations. The predominant sectors of known investments by OCGs in the legal economy are property/real estate, transportation and construction.	Initiate a coordinated effort that would allow prosecutors, police and judicial authorities, AROs, AMOs, FIUs, researchers and others to share and collate case examples of OCGs investing in or infiltrating the legal economy. The UNODC SHERLOC database offers a useful model, which may be adapted to specifically capture financial aspects of SOC.	European Commission, in particular through the ARO and FIU platforms Member States, particularly police, judicial authorities and prosecutors

3.2. The freezing and confiscation of assets from organised crime groups

Laura Lica-Banu, EY

Key findings:

- There remain considerable gaps in the collection and availability of statistical data on assets frozen or confiscated in the EU. Data collection is not centralised and is still largely undertaken manually, and there is no systematic collection of information about seized assets linked to SOC.
- Considering the ongoing limited availability of data, it is not possible to reliably ascertain the overall number and value of assets frozen or confiscated at the EU-level.
- Attention should be paid to improving systems for data collection, to enable a more robust understanding of the extent of asset recovery in the EU.

Literature review	Interviews	Surveys
		

Additional information supporting the analysis presented in this chapter can be found in **Annex 3.2**.

Recovering criminal assets is a legal process whereby instrumentalities or proceeds from crimes are identified in order to cover damages, compensate the victims for the losses caused by the commission of crimes and deprive the criminal of the benefit. While there are differences between Member States, the recovery of criminal assets is generally undertaken in phases, involving:

- Asset identification and tracing;
- Preservation during the investigation (by execution of freezing or seizure orders);
- Confiscation ordered by a court;
- Enforcement by the national agencies; and
- Returning the assets to the State, deprived communities or victims.

The freezing and confiscation of criminal proceeds is an essential component of the fight against SOC, since it deprives criminals of their financial gains (European Commission, 2020a). For a detailed discussion of the EU legal framework relevant to the freezing and confiscation of assets and how the recovery process works in each EU Member State, see a recent report by the European Commission (2020a). The present section of this report provides a current overview of the availability of data on assets frozen or confiscated in the EU, followed by a discussion of what is known about the number and value of assets frozen or confiscated from OCGs.

3.2.1. Statistical data on assets frozen or confiscated in the EU

Previous research

In 2015, Transcrime assessed the availability of data on confiscated assets in Europe as part of Project Organised Crime portfolio (OCP) (Savona & Riccardi, 2015). Their assessment revealed:

- There was no systematic information on the amount or value of criminal assets seized, frozen or confiscated across Europe.
- Methods and criteria to collect data on confiscated assets varied widely across EU countries.
- In the same country, data may be collected by different agencies, who adopted different data-collection methods.
- Available databases provide a very partial picture and it is hard to determine how many assets seized are ultimately confiscated.
- Few data-recording processes have been automated.

In 2016, Europol published a report that reaffirmed the lack of harmonisation of data collected on asset-seizure and recovery in the EU (Europol, 2016a). Europol noted that improving the collection of data was necessary for assessing the impact of the asset-recovery regime in the EU. They recommended that a central database be established to increase efficiency of the management of frozen and confiscated assets at a national level (Europol, 2016a).

Insights from this study

Our study finds that there has been little improvement in statistical data collection on asset-freezing and confiscation in the EU. Based on interviews and surveys of AROs, AMOs and FIUs we conclude that there remain considerable gaps in the availability of data on asset-seizure and confiscation in the EU.

Data collection is not centralised, resulting in gaps, fragmentation and inconsistencies. Consistent with Transcrime's 2015 analysis, interviewees in this study explained that data collection on asset-seizure and recovery is not centralised. There is no single authority for collecting data in most Member States and various organisations are involved in the process[119].

The lack of centralisation means that various types and formats of statistical data are kept both within and between countries. The formats of data vary from one year to another; there are discrepancies in terms of number of cases (hundreds of thousands versus tens of cases); and the number of cases and values differ also due to the modalities in which authorities provide information.

Data collection processes are not automated. Interviewees explained that data collection processes are mainly manual, and IT systems or electronic databases are rarely used (this is consistent with Transcrime's assessment). This means that data collection is slow and reliant upon the accuracy of manual extraction from hard-copy case files. While progress appears to have been slow in this regard, some interviewees mentioned that projects to upgrade to electronic systems are currently underway. This is expected to improve not only the speed and accuracy for which data can be aggregated, but also data sharing between agencies[120]. Data sharing is important for linking asset-seizure with the legal outcome, and whether or not a confiscation ultimately took place.

[119] Interview with ARO, 23 April 2020 (#68); Interview with ARO, 24 April 2020 (#69); Interview with ARO, 27 April 2020 (#74).
[120] Interview with AMO, 30 April 2020 (#81).

There is limited systematic collection of information about seized assets linked to SOC. The information about seized assets linked to SOC is not systematically collected at national level. While in some instances it is possible to identify SOC cases by using a keyword search in national case-management systems, FIUs and AROs do not specifically cluster the statistics based on criterion 'organised crime', nor is this required under the EU legislative regime[121].

The approach to data collection is not harmonised across the EU. Several interviewees[122] declared that the statistical data their institutions keep is segmented on type of offence, amounts and/or type of assets. Limited information is kept on which provisional measures were applied, and on whether the case is linked or not to organised crime. Moreover, there are differences between and within Member States as to what behaviours are classified as SOC.

3.2.2. Number and value of assets frozen or confiscated in the EU

Previous research

Bearing in mind the complex regulatory framework and limitations of statistical data on asset-freezing and confiscation in the EU, previous research has only been able to draw tentative conclusions about the number and value of assets frozen and confiscated.

Previous research suggesting that the number and value of assets frozen and confiscated has been growing over time in some EU Member States should be interpreted with caution.

Transcrime's Project OCP analysed data on asset-seizure and recovery for seven EU Member States: Italy, Spain, France, Ireland, UK and the Netherlands (Transcrime, 2015b). The study found that the number of seizures and confiscations of SOC assets has been increasing over time (Transcrime, 2015b). The longest time-series of data were available for Ireland, Italy and Spain, and these showed an overall upward trend in the number of confiscated assets over the period 2005 to 2012. The study also found that several Member States have recorded a reported increase in the value of assets confiscated.

Europol produced an updated summary of statistical information on asset-freezing and confiscation in the EU for the period 2014 to 2016, informed by a survey of AROs across the EU (Europol, 2016a). Consistent with Transcrime's findings, the analysis showed that for many of the respondent countries the value of assets frozen and confiscated was growing. There are some important considerations when interpreting findings on the number and value of assets frozen and confiscated in the EU, as summarised in the box below.

Box 3.1: Considerations when interpreting data on the number and value of assets frozen and confiscated in the EU

- Different definitions and criteria are used for 'value' of assets across Member States. Some Member States define value as the benefit to the offender, whereas others refer to damage to the claimant.
- Methods for estimating 'value' of non-cash assets differ by Member State and over time.
- Increases in the number of assets frozen or confiscated may reflect improved practices in asset recovery, new investigative techniques, improved reporting or increased law enforcement funding and capacity.
- Decreases in the number or value of assets frozen or confiscated may reflect more sophisticated modus operandi of criminals, or different strategies employed by asset-management agencies (Europol, 2016a).

Bearing in mind the data limitations, previous research suggests that only a small proportion of assets from criminal proceeds are frozen and confiscated.

In addition to examining trends, Europol (2016a) made the first attempt to estimate what proportion of proceeds of crime were subject to freezing or confiscation. Referring to Transcrime's estimate that SOC in the EU generated revenues of €110 billion, Europol[123]

[121] Interview with ARO, 28 April 2020 (#77).
[122] Interview with ARO, 27 April 2020 (#74); Interview with AMO, 30 April 2020 (#81); Interview with ARO, 28 April 2020 (#77).
[123] To generate this estimate, Europol extrapolated survey findings from 15 Member States to the non-responding countries, by calculating the ratio between average value of seized/frozen or confiscated assets and the average

estimated that 2.2% (around €2.4 billion) of this was provisionally seized or frozen; however only 1.1% (around €1.2 billion) was finally confiscated at EU-level.

Insights from this study

Considering the ongoing limited availability of data, it is not possible to reliably ascertain the number and value of assets frozen or confiscated at EU-level.

Table 3.4 summarises the results from data provided by the 10 AROs who responded to our survey, and who provided statistics on freezing and confiscation measures. Most Member States reported the number and value of assets subject to seizure/forfeiture as a whole, so the statistics presented below do not disaggregate freezing from confiscation.

- Across the 10 Member States, the annual value of orders from 2017 to 2019 averaged around €513 million.
- In Ireland, Latvia and Sweden, there were increases in the number of freezing and confiscation orders over the period 2017 to 2019.
- In Estonia, Finland and Ireland there were increases in the total value of orders over the period 2017 to 2019.
- In Ireland, despite there being only one additional order in 2019 compared with 2018, there was a dramatic increase in the total value of orders from around €8 million to over €60 million. According to the annual report of the Irish Criminal Assets Bureau, this was due to the granting of a freezing order over cryptocurrency to the value of €53 million (Criminal Assets Bureau, 2019).
- The value of assets for most Member States tends to fluctuate, which may reflect whether high- or low-ranging assets are targeted, as well as changes in reporting practices.
- For Member States where the number and value of freezing and confiscation orders could be disaggregated, the findings are consistent with previous literature that only a proportion of assets subject to freezing are ultimately confiscated. For example, in Estonia in 2019 there were assets frozen to the value of €9.6 million, of which €3.96 million was ultimately confiscated.

From the available data it seems that a small proportion of the estimated €139 billion revenues from SOC in the EU (our estimate from Chapter 2) are ultimately frozen or confiscated. This is consistent with previous research. It should be noted that the data currently available on asset recovery in the EU is flawed – it is not representative across all Member States, it is collected by a range of organisations in a non-centralised manner, and the level of granularity required for a robust analysis is not available.

Table 3.6: Data on freezing and confiscation measures in the EU

EU Member State	Number of orders			Total value of orders (€ million)		
	2017	2018	2019	2017	2018	2019
Bulgaria	-	-	-	14.2	6.7	4.2
Croatia	900	892	-	40.4	24.0	-
Denmark	-	-	-	8.6	2.2	10.5
Estonia	177	152	136	7.4	9.0	9.6
Finland	-	-	-	20.9	36.5	44.9
Ireland	28	30	31	7.0	8.4	64.995
Latvia	97	98	105	0.91	0.8	0.9
Netherlands	2,306	2,167	1,928	359.7	400.9	258.2
Slovenia	94	129	97	-	-	132.6

GDP of the responding countries for the period analysed. This percentage of GDP is assumed as also valid at the EU-level (Europol, 2016a).

EU Member State	Number of orders			Total value of orders (€ million)		
	2017	2018	2019	2017	2018	2019
Sweden	652	817	857	39.0	10.3	17.15
Total	**4,254**	**4,285**	**3,154**	**498**	**499**	**543**

Source: Research team's survey of AROs (2020) (n=10 responded).

Note: '-' = no data.

In addition to collecting data directly from AROs, we also compiled available statistics from the literature – mainly FATF Mutual Evaluation Reports. This data – presented in **Annex 3.2** – was available for the value of assets seized in money-laundering cases for 18 EU Member States.

- It is not possible to compare overall value over time because each year includes data for a different number of Member States.
- For the majority of countries, the value of assets frozen or confiscated fluctuated over time, which may reflect changes in valuation methodology or reporting practices, as well as practices targeting high- or low-valued assets.
- The extraction of this data may be useful for future data-collection efforts.

Challenges in asset recovery

Given the assumption that only a small proportion of assets funded by SOC are frozen and confiscated, it is worthwhile to consider some of the challenges that Asset Management Organisations face in carrying out freezing and confiscation orders. The Eurojust Report on Casework in Asset Recovery (published in February 2019) indicated a series of practical difficulties that were identified by the competent authorities during the execution of freezing and confiscation orders (Eurojust, 2019). These were:

- Differences among Member States in implementing the Framework Decision 2003/577/JHA, which often create obstacles in executing freezing/confiscation orders.
- Issues in identifying the competent authority to which asset-freezing/confiscation orders should be addressed, when the assets are situated in different locations in the executing/requested State; there were also issues with respect to the place of prosecution that had an impact on the confiscation measures.
- Difficulties in the communication of the execution of a Letter of Request (LoR), especially when simultaneous requests go through parallel channels or in cases where the execution involves third-party ownership.
- Issues that appeared during the sale of the confiscated assets, for example, when assessing the estimated value of the property, reaching the asset-sharing agreement and covering asset-management-related costs.
- Issues that appeared at the restitution of confiscated assets to the victims, for example, obstacles with the transfer of assets in cases involving both Member States and third countries.

Surveys with AROs and AMOs in this study revealed a number of further difficulties. The most commonly identified themes were:

- Tracing assets in foreign jurisdictions, particularly in so-called tax havens where contact with relevant authorities is more difficult[124].
- Identifying the beneficial owner of targeted assets[125].
- Identifying the owner of a property held in trust[126].
- Identifying the source of funds for the initial purchase of cryptocurrencies (especially since the introduction of anonymisation tools, such as cryptocurrency mixers)[127].
- Lack of resources and the need for additional staff and financial investigators[128].

[124] Reported in two Member States: DK, CZ.
[125] Reported in three Member States: SE, EE, HR.
[126] Reported in one Member State: IE.
[127] Reported in two Member States: EE, CZ.

3.2.3. Recommendations

The key findings stemming from this part of the study and the related recommendations are summarised in the table below.

Table 3.7: Recommendations – Asset recovery

Key finding	Recommendation	Key actor
There remain considerable gaps in the collection of data on asset-seizure and confiscation in the EU. Data collection is not centralised, resulting in gaps, fragmentation and inconsistencies. Data collection processes are still largely undertaken manually, and use of IT systems or electronic databases is rare. There are differences between and within Member States as to what behaviours are classified as SOC.	Accelerate efforts by AROs and AMOs to automate systems for data collection. Findings of this study should be viewed considering other studies underway on asset seizure and confiscated in the EU. In particular, the Commission funded study: "Freezing, confiscation and asset recovery in the EU: What works and what does not work."	Member States, particularly AROs, AMOs, FIUs European Commission

3.3. Risk factors for serious and organised crime infiltration of companies and public procurement

Mihaly Fazekas and Yuliia Kazmina, Government Transparency Institute and Clément Fays, RAND Europe

Key findings:

- Our analysis of individual financial and ownership risk indicators does not support the claim of the literature that SOC-infiltrated companies have a significantly different financial (e.g. share of current assets) or ownership (e.g. network centrality) profile than their non-infiltrated peers.
- When considering multiple dimensions (e.g. share of current assets, standard deviation of assets, standard deviation of revenue and EBITDA margin), the analysis revealed that companies infiltrated by SOC have a distinct profile.
- Extrapolations across the EU identified that corruption, high cash-intensity and weak legal frameworks are positively associated with the level of SOC infiltration in the economy.
- Regarding infiltration of public procurement, single bidding, number of contracts awarded by the procuring entity in the year, the share of a supplier in a buyer's annual spending, and relative price are all associated with higher probabilities of SOC infiltration.
- The extrapolations to the whole EU revealed a rich and diverse picture that only partially overlap with existing perceptions of where SOC infiltration is high. For example, some regions of France or Finland have a non-negligible infiltration risk.
- Our analysis demonstrates that it would be both feasible and fruitful to build large-scale SOC risk-assessment tools – based on micro-level databases describing companies and public procurement contracts – that would allow frequent monitoring rather than one-off reports.

Literature review	Secondary data	Proven cases
		

This section of the report identifies and analyses the risk factors of SOC infiltration of the legitimate EU economy. The analysis involved identifying and analysing risk factors for: (1) companies, and (2) public-procurement contracts. The analysis of risk factors for companies and transactions used micro- and macro-level data.

- **Micro data** is individual-level information, in this case companies and contracts.
- **Macro data** is information at the level of countries, regions and business sectors.

[128] Reported in three Member States: PT, IT, HR.

This section first presents the results of the analysis on risk factors that facilitate SOC infiltration of companies, followed by risk factors of transactions. Both sub-sections include a brief mapping of risk factors that have been identified in the prior literature, and a summary of the methodological approach.

A comprehensive overview of the literature review, methodological approach and findings of this analysis can be found in **Annex 3.3**.

3.3.1. Risk factors that facilitate serious and organised crime infiltration of companies[129]

Risk factors identified in the prior literature

There is a large body of literature on risk factors that facilitate SOC infiltration of companies. A considerable scholarly debate has arisen among various authors with diverse positions regarding what level of measurement (micro-, meso- or macro-) and what indicators (qualitative, quantitative or a combination of both) to employ for the most precise measurement of SOC infiltration in the legal economy.

A large number of studies are based on single, micro-level indicators – such as a firm's cash-intensity, profitability or balance sheet structure as compared to its peers in an industry – while others combine a set of financial metrics with more aggregated information on the sectoral or country level, to provide a more comprehensive picture than each individual red flag (e.g. Savona & Riccardi (2018) and Ferwerda & Kleemans (2019) – for more details see **Annex 3.3**).

A comprehensive study by Savona & Riccardi (2018) presented a wide-ranging list of potential risk factors that facilitate SOC infiltration of companies. Some of these risk factors – which might indicate an infiltrated organisation – include:

- **Lower financial debt** and **higher proportion of shareholder loans**. Due to illicit revenue streams or shareholders' support, infiltrated companies will not require other external funding as compared to peers in their sector or geographical region.
- **Less cash on hand** and **fewer liquid assets** due to fear of them being confiscated. Thus, other types of assets prevail in the balance sheet of such companies.
- **Variance of total assets**, suggesting unusual movements of large sums of money unrelated to usual economic activities.
- **High revenues not supported by market conditions**, potentially signalling illegal or non-market income channelled through the company.

More recent research into SOC infiltration has employed network theory to analyse interconnected business ownership networks, networks of financial facilitators and geospatial networks. Such studies use **ownership links with secrecy countries**, as well as the overall **complexity of business ownership structure** for measurement of SOC infiltration (see for example, Ferwerda and Kleemans (2019)). The complexity of the ownership structure has been discussed in the literature in both qualitative and quantitative measures. Qualitative studies point out that the use of legal instruments – such as numbered trusts of various secrecy levels, and International Business Corporations – could be red flags of SOC infiltration.

Developing big data methods also resulted in a new approach to SOC studies, employing social-media analysis in combination with formal concept analysis and Natural Language Processing techniques to detect the presence of corroborated SOC threats. An exhaustive list of indicators of SOC infiltration in the legal economy is presented in **Annex 3.3**.

A closer look at the literature on risk factors of SOC infiltration, however, reveals several gaps and shortcomings. Despite a great variety of indicators, most studies have relied on merely theoretical or qualitative indices with no or very limited potential for implementation on a large scale, due to a lack of empirical data. Only a few studies in the field demonstrate a comprehensive analysis of quantitative measures of SOC infiltration. However, even these studies typically analyse indicators of SOC infiltration in isolation, without considering how they interact (see for example, Savona & Riccardi (2018)). Therefore, in this report we build upon and complement the existing body of literature and expand the analysis of SOC infiltration

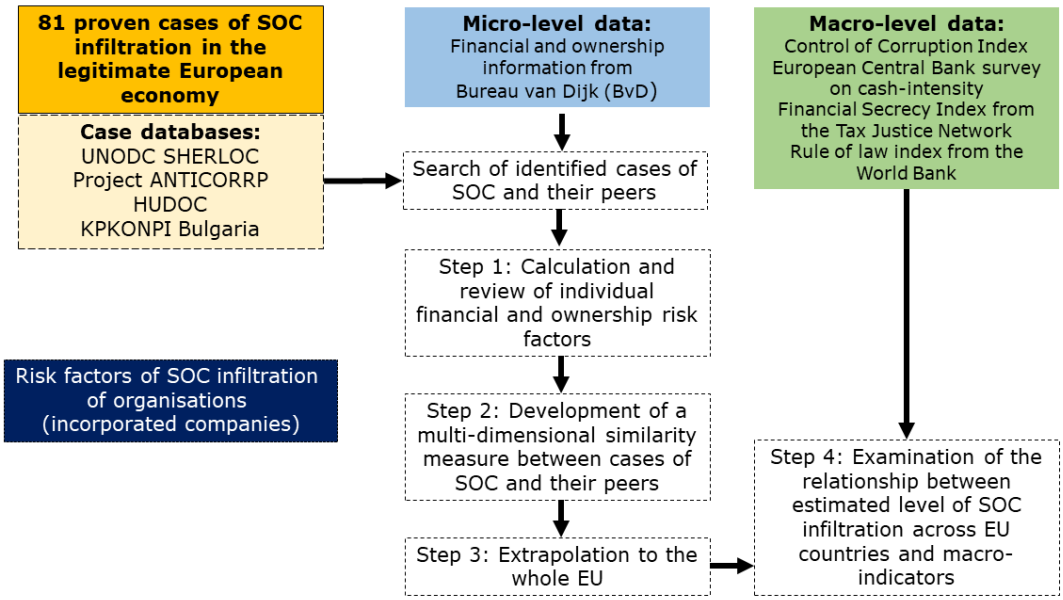
[129] This section draws extensively on the technical paper: 'Investments by organised crime groups in the legal economy' (Fazekas et al., 2020).

indicators by using proven cases and exploring combinations of risk factors, rather than looking at them in isolation.

Methodological approach

Our methodological approach and data sources for identifying and analysing risk factors of SOC infiltration of companies are schematically illustrated in Figure 3.1.

Figure 3.1: Methodological approach and data sources for analysing risk factors that facilitate SOC infiltration of companies



First, **we collected a sample of 81 cases of SOC infiltration** of companies in the legitimate European economy. These proven cases covered 14 EU Member States – mostly Bulgaria and Italy – and the construction, finance, real estate and car manufacturing markets. The source and search process for identifying and extracting these cases is provided in **Annex 3.3**.

Second, **we searched the micro-level dataset** – Bureau van Dijk (BvD) – which contains financial and ownership information for more than 796,000 companies in Europe, for these companies. Despite identifying 81 cases, overall the data remained sparse (particularly regarding disclosure of full names of legal entities), which constrained our search capacity. Ultimately, the BvD database contained 14 cases that could be used in this analysis. Most of the cases in the filtered subset are Bulgarian and Italian firms, with several cases from Romania and Croatia, as shown in the table below. The limitations of the small sample size are discussed below.

Table 3.8: Cases of serious and organised crime infiltration of companies available for this analysis

Member State	Industry
Italy	Other professional, scientific and technical activities
Bulgaria	Construction of buildings Civil engineering Specialised construction activities
Bulgaria	Advertising and market research
Romania	Construction of buildings
Italy	Manufacture of other non-metallic mineral products
Italy	Construction of buildings
Italy	Construction of buildings Civil engineering Specialised construction activities
Croatia	Advertising and market research
Italy	Specialised construction activities
Italy	Construction of buildings Civil engineering Specialised construction activities
Bulgaria	Financial service activities (except insurance and pension funding) Food and beverage service activities Gambling and betting activities
Bulgaria	Other professional scientific and technical activities
Romania	Human health activities
Italy	Wholesale trade (except motor vehicles and motorcycles) Retail trade (except motor vehicles and motorcycles)

Analytical steps

Once the proven cases were identified in the BvD dataset, four analytical steps were followed (refer to **Annex 3.3** for additional detail):

- **Step 1**: Calculate and review **individual micro-level risk indicators** of SOC infiltration (i.e. financial profile, ownership network structure, ownership links with secrecy countries). In this step, we calculated risk indicators for available proven cases of SOC and compared the results with the overall distributions of these indicators in the respective markets using the BvD dataset. This simple review of individual indicators was designed to show to what extent the proven cases are different from other companies in the same sector and country. If a proven case appears to be average or near average in a sector for one of the indicators, we conclude that such measures will not be a particularly useful indicator of SOC infiltration on its own.
- **Step 2**: Combine individual micro-level indicators into a single, multi-dimensional similarity measure to analyse **combinations of risk factors** and how widespread they are. In this case, we looked at similarity to proven cases across all known indicators at once. The reliability of measurement of SOC infiltration greatly increases if multiple indicators are triangulated against each other. Even if each indicator on its own is an imprecise measure of SOC infiltration, taken together they may offer a precise measurement, as their combinations may be highly unusual.
- **Step 3**: Using the developed similarity measure from Step 2, we were able to **extrapolate the assessment of SOC-infiltrated companies to all EU countries**. We focused on four industries in which at least three proven cases of SOC infiltration were present: wholesale and retail of motor vehicles, construction activities, real estate activities, and financial service activities.

- **Step 4:** We use the predicted SOC infiltration scores based on the similarity metrics built in Step 3 to assess the external validity of our complex indicator using macro-risk factors discussed in the literature (e.g. corruption, cash-intensity, financial secrecy). We used the share of companies flagged as being at high risk of infiltration as a proxy for SOC infiltration in a country, and disaggregated this analysis by business sector.

Limitations of the analysis

There are several caveats to the analysis of risk factors that facilitate SOC infiltration of organisation, given the overall low number of proven cases of SOC infiltration of companies:

- First, the available data could be subject to selection bias given that there can be systematic differences between the characteristics, business profiles and strategies of those SOC-infiltrated companies that were discovered, and those companies that were infiltrated by SOC and continued to operate undetected.
- Second, the identified pool of proven cases of SOC infiltration is not large enough to draw conclusions for the whole population of SOC-infiltrated businesses in Europe. To address these issues, this chapter does not generalise to all SOC-infiltrated companies in Europe, but instead compares how business profiles of firms in Europe are similar to the companies identified in the proven cases. Furthermore, we made extrapolations only within sectors for which a minimum of three proven cases were present.

Results of the analysis

Step 1: Calculation and review of individual financial and ownership risk factors

Financial profile

Prior studies have highlighted that infiltrated companies tend to have less cash and other liquid assets on hand[130] due to a fear of their confiscation, thus other types of assets prevail in the balance sheet of such entities (Savona & Riccardi, 2018). Contrary to the prior literature, our analysis showed that the infiltrated companies in our dataset are evenly distributed in terms of liquidity of assets.

There is no significant difference between infiltrated companies in our sample and their peers in terms of liquidity of assets.

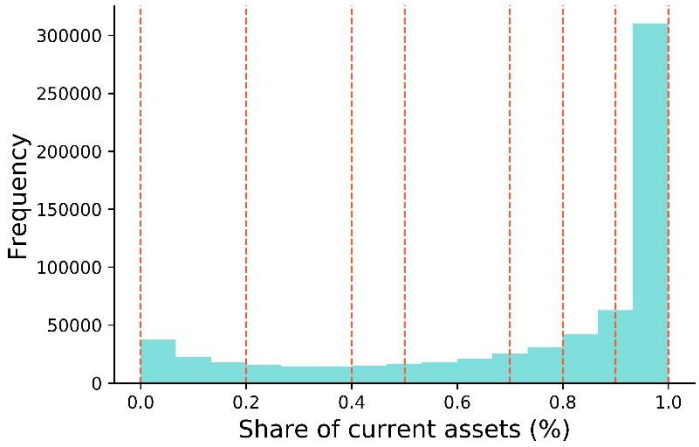
The graph below visually depicts these findings. As shown, the distribution of the share of current assets[131] in the sample ranges from 0 to 1.

- Companies with share of current assets at 0 represent only fixed or highly illiquid asset profiles that contain assets that cannot be readily convertible to cash.
- Companies with share of current assets at 1 represent highly liquid asset profiles that contain a large share of cash or other assets that can be easily converted into cash.

The figure below shows that the distribution is highly skewed, with most of the firms having a relatively high (>0.8) share of current assets. Red vertical lines on the graph represent estimates of share of current assets for proven cases of SOC infiltration in our dataset. These are relatively evenly distributed over the 0 to 1 range. The sample of proven cases includes companies with no or minimal current assets, as well as highly liquid asset profiles. This means that no clear pattern such as that suggested by the literature emerges.

[130] Liquid assets can easily be converted into cash in a short amount of time. Liquid assets include things like cash, money market instruments, and marketable securities.
[131] Current assets include liquid assets that can be sold or used over a year.

Figure 3.2: Distribution of share of current assets in markets with proven cases of serious and organised crime infiltration

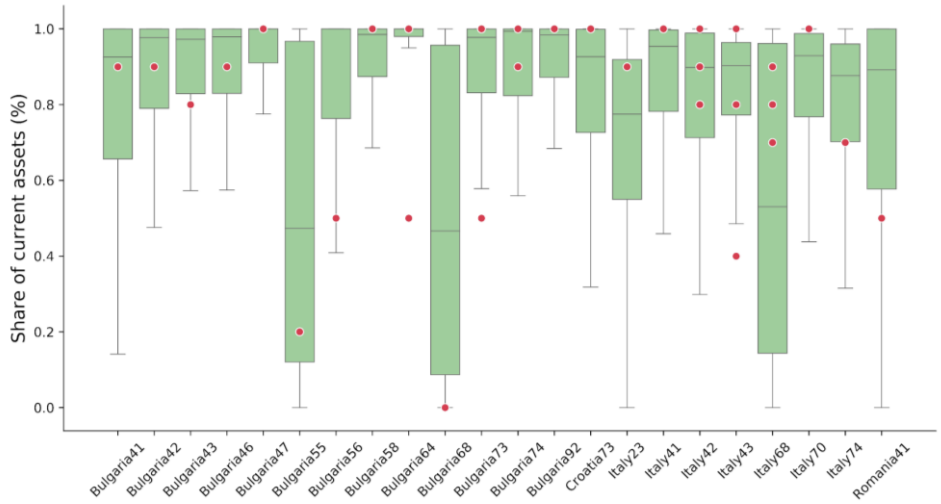


Note: Blue bars represent all companies in respective markets (n = 796k companies), red vertical lines indicate proven SOC cases.
Source: Analysis of BvD data and research team's proven cases of SOC infiltration.

Infiltrated companies are also broadly similar to other companies with regard to share of current assets, when examined by business sector.

To identify further indicators of infiltration, we narrowed the analysis to specifically look at country-sector groups. As mentioned previously, all cases of SOC infiltration in this study were collected from four countries – Italy, Bulgaria, Croatia and Romania. Most cases were involved in construction or related activities, with the rest in retail, finance, healthcare and other professional, scientific and technical activities. When comparing each case to its own country-sector group using the full range of financial indicators identified, the picture remained the same: the cases are only rarely drastically different from the broader markets they sit in. These findings are illustrated in the figure below, which compares the share of current assets for the overall market distributions as per the BvD dataset, with those of the proven cases of SOC infiltrated companies. Such a comparison demonstrates to what degree the proven cases are outliers in their own sector and country. As shown, most proven cases fit in the interquartile range (middle 50%) of distributions (represented by a green box) of the share of current assets in each market, hence they cannot be classified as outliers. Nevertheless, there are several exceptions: the accommodation sector (market 55) in Bulgaria and the real estate sector in Bulgaria and Italy (market 68) tend to have a wider score distribution with lower averages. These markets have a wider range of the box as well as a lower level of the grey line, which indicate mean values.

Figure 3.3: Distribution of share of current assets in markets with proven cases of serious and organised crime infiltration, by country-sector groups



Note: Green boxes represent middle 50% of a distribution; grey lower and upper bounds show minimum and maximum of 99.3% of distribution, leaving out outliers. Identified cases are represented by red dots. The following 2-digit Nomenclature of Economic Activities (NACE) codes are used on this figure: 41 Construction of buildings; 42 Civil engineering; 43 Specialised construction

activities; 46 Wholesale trade except of motor vehicles and motorcycles; 47 Retail trade except of motor vehicles and motorcycles; 55 Accommodation; 56 Food and beverage service activities; 58 Publishing activities; 64 Financial service activities, except insurance and pension funding; 68 Real estate activities; 70 Activities of head offices, management consultancy activities; 73 Advertising and market research; 74 Other professional scientific and technical activities.
Source: Analysis of BvD data and research team's proven cases of SOC infiltration.

Ownership network structure

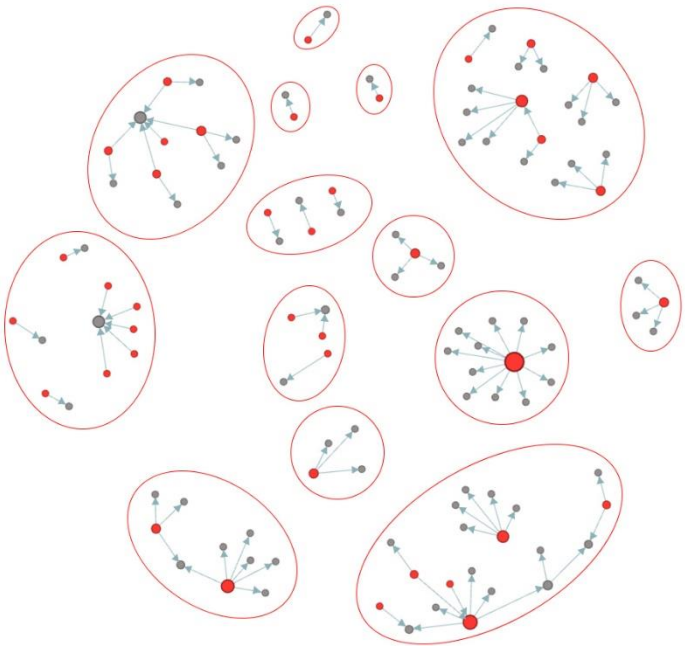
We focused on two network structure indicators: the degree of an entity and its centrality measures, both of which are described below.

- The **degree of an entity** (hereafter, 'degree') is the number of links connected to the company, or the number of shareholders and subsidiaries a company has.
- The **degree centrality** (hereafter, 'centrality') indicates the normalised number of ties a node (i.e. an organisation) has. The degree centrality of an organisation in a market network can be interpreted as an immediate risk/chance of a node (organisation) receiving and capturing any signal or event flowing through the network.

Both degree and centrality demonstrate a company's exposure to the ownership network, the opportunity and the extent to which it can directly influence other companies.

The literature suggests that high centrality of a company in an ownership network is associated with a higher level of SOC infiltration, while it also suggests that infiltrated companies have a more extensive ownership network (Gurciullo, 2014). In order to test this hypothesis, we examined ownership networks of companies that featured in proven cases of infiltration, as well as the distribution of centrality measures of proven cases of SOC infiltrated businesses and other businesses in the respective markets. The findings are depicted in Figure 3.4 below.

Figure 3.4: Ownership networks of proven cases of serious and organised crime infiltration of companies



Note: Red nodes represent proven cases of SOC, grey nodes are related companies. The arrow shows a relationship from a shareholder to a subsidiary. Entities placed in the same oval belong to one proven criminal case. Source: Analysis of BvD data and research team's proven cases of SOC infiltration.

Box 3.2: Interpreting the ownership networks displayed in Figure 3.4

- Red nodes represent proven cases of SOC infiltration of companies.
- Grey nodes represent their related companies – shareholders and subsidiaries.
- An arrow shows a direction of a relationship: from a shareholder to a subsidiary. While half of the cases were not found to have any shareholders or subsidiaries (those entities are excluded from the graph), the rest have a sparse, partially interconnected network of ownership.

Infiltrated companies in the available sample have sparse ownership networks and low degree and centrality measures.

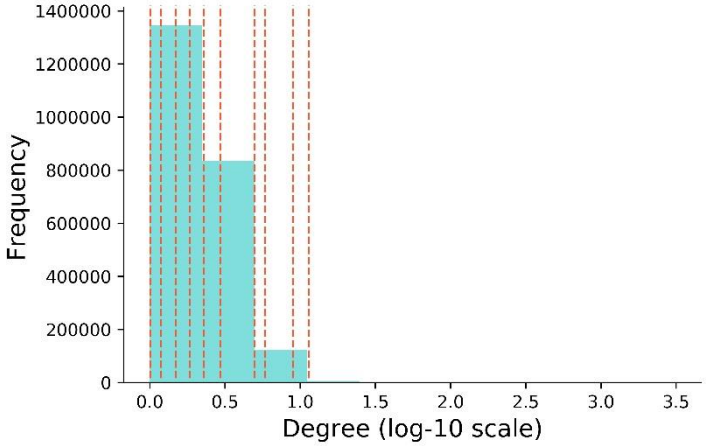
The figure above illustrates the ownership network for proven cases of SOC. The degree of each node or organisation (the number of links from the node to the deepest layer) is – on average – 2. The highest degree in the observed sample of cases is 11 for an Italian construction company, all of which are the company's subsidiaries. The rest of the cases have a degree in the range of 1 to 5. Other companies in the sample are independent firms with no shareholders or subsidiaries, contrary to previous literature that has assumed that SOC-infiltrated companies tend to have extensive ownership networks and high centrality. Interestingly, proven cases of SOC that were convicted in one case (placed in the same oval above) were not necessarily linked in terms of ownership.

The degree and centrality of proven cases of SOC are broadly similar to other companies in their respective markets.

Figure 3.5 compares the degree and centrality of proven cases with market peers, by presenting the degree of distribution in markets with identified cases alongside proven cases of SOC infiltration. The blue histogram represents all companies in respective markets from the BvD dataset, while the red vertical lines correspond to proven cases of SOC infiltration.

In the observed sample of companies, the distribution of degree is wide and highly skewed, with a long right tail representing that most of the firms have low centrality, while there are several outliers in a network having the highest degree. This means that contrary to previous literature, which has found that SOC-infiltrated businesses have high centrality, our analysis suggests that none of the observed cases of SOC infiltration have a high degree. Conversely, the majority of cases of infiltration are depicted on the left-hand side of the distribution, with the lowest centrality measures.

Figure 3.5: Distribution of degree in markets with identified cases of serious and organised crime infiltration of companies



Note: Blue histogram represents all companies in respective markets, red vertical lines correspond to proven cases of SOC. Degree was rescaled to a logarithmic (log-10) scale.
Source: Analysis of BvD data and research team's proven cases of SOC infiltration.

Ownership links with secrecy countries

Many attempts have been made to identify or develop quantitative measures for the complexity of business ownership and its links with black-listed jurisdictions. The reviewed literature suggests that the use of legal instruments – such as numbered trusts of various secrecy levels in various jurisdictions, including tax havens and black-listed jurisdictions – could be risk factors for SOC infiltration (e.g. Blum et al., 1998). Some authors describe a positive relationship between ownership links and investment-based visas in jurisdictions of high secrecy and a large scale of offshore – potentially SOC infiltrated – financial activities (e.g. Scherrer & Thirion, 2018).

As of February 2020, the list of black-listed jurisdictions included 12 countries/territories: American Samoa, Cayman Islands, Fiji, Guam, Oman, Palau, Panama, Samoa, Seychelles, Trinidad and Tobago, US Virgin Islands and Vanuatu (Council of the European Union, 2020). Despite the legal importance of the EU list, it is not comprehensive enough for the purposes of our analysis, given that it lacks some of the well-known tax havens such as Malta, Cyprus, Bahamas, British Virgin Islands, etc.

To ensure the most comprehensive analysis of links between EU Member States and black-listed jurisdictions and other tax havens, in addition to the official EU list, we used the Financial Secrecy Index (FSI) from the Tax Justice Network (Tax Justice Network, 2020). The indicator is based on the level of secrecy provided to non-resident investors, and has four different dimensions: knowledge of beneficial ownership, corporate transparency, the efficiency of tax and financial regulation, and international standards and cooperation. We considered the aggregated FSI score for defining jurisdictions with high secrecy. From the whole FSI-2020 ranking list, we considered the top-30 jurisdictions but excluded large countries because large countries are likely to have a host of legitimate businesses, in spite of their lax financial and company laws (e.g. USA, Japan, the Netherlands, Germany, etc.).

Our analysis found no ownership links with black-listed jurisdictions in the sample of proven cases of SOC infiltration of companies.

In our sample, all the shareholders and subsidiaries of companies with proven SOC infiltration were domestic firms. Contrary to the assumption outlined in the literature, the available pool of proven cases of SOC infiltration was found to have no links with high-secrecy jurisdictions. Given the small sample of proven cases in our study, further analysis of ownership links to secrecy jurisdictions of a larger sample of companies is warranted.

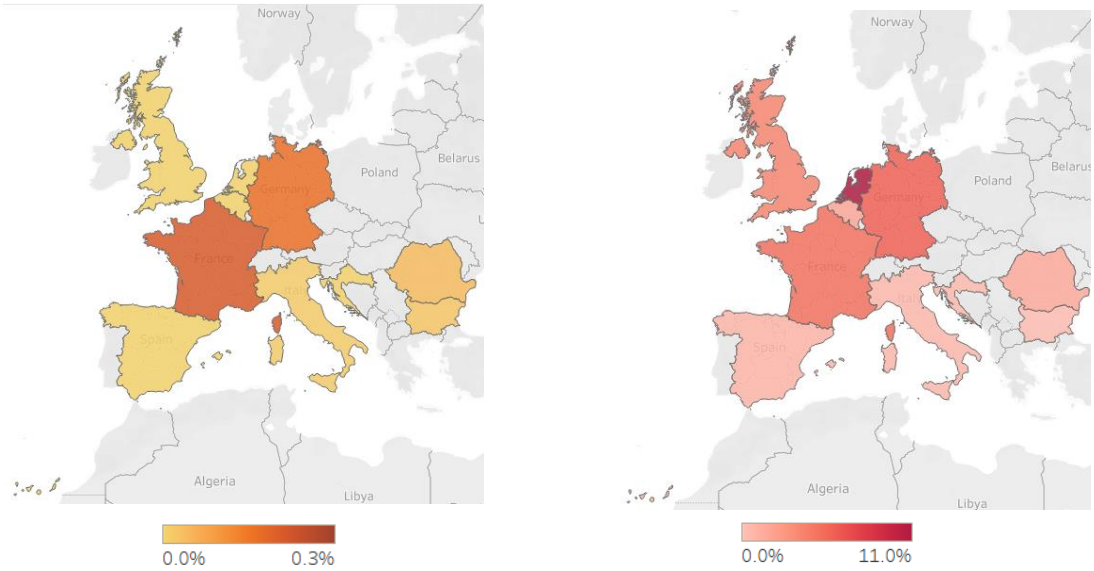
The share of ownership links between European firms and black-listed or high-secrecy jurisdictions is very low.

According to the EU-list, the proportion of ownership links between European firms and black-listed jurisdictions is less than 1%. If defined more broadly using the FSI, the share of ownership links between European firms and high-secrecy jurisdictions reaches a maximum of approximately 10%.

The distribution of the share of ownership links between European firms and black-listed or high-secrecy jurisdictions is presented in Figure 3.6. As shown, according to the EU-list the range of the estimated indicator barely reaches 0.5% in France and Germany. The FSI ranking has a higher estimate, and France and Germany are still at the top of the ranking, but the highest share of links with high-secrecy jurisdictions is estimated in the Netherlands (11%).

Figure 3.6: Distribution of the share of ownership links between European companies and black-listed or high-secrecy jurisdictions

A) As defined by the EU list **B) As per FSI ranking**



Note: The sample of EU firms used in this analysis is limited to countries with satisfactory ownership data quality. Source: Analysis of BvD data (n=796k) and the European Commission (2020) list of black-listed jurisdictions and the Tax Justice Network (2020) FSI.

Step 2: Development of a multi-dimensional measure of similarity

After reviewing potential indicators of SOC infiltration individually (Step 1), next we evaluated their combinations. We used the sample of proven cases and a set of risk factors of SOC infiltration from the literature (i.e. share of current assets, standard deviation of assets, Standard deviation of revenue, and EBITDA margin) to classify all firms in markets with identified cases of SOC infiltration into relative groups, based on their similarity. For this task we employed cluster analysis techniques that are described at length in **Annex 3.3**.

Box 3.3: What is cluster analysis?

Cluster analysis aims to classify a sample of observations – on the basis of a set of measured variables – into a number of different groups, such that similar subjects are placed in the same group. Here, the set of measured variables is the SOC infiltration risk factors: financial and ownership network indicators.

Companies with proven SOC infiltration were assigned to three groups or clusters. This suggests that companies that have been infiltrated have a distinct profile when considering multiple risk factors at once.

Companies with proven infiltration ended up in the three largest clusters of the six identified. We examined the similarities between infiltrated companies and companies that were grouped into the same cluster. A similarity measure was developed based on closeness of the financial profile in a respective country or market group. An important feature of these observations is that they were not associated with a particular reason that would trigger law enforcement intervention – thus the indicators are not simply reproductions of policing choices, but genuinely new combinations of indicators. The distribution of the developed similarity measure in markets with identified cases of SOC infiltration is presented in **Annex 3.3**.

Step 3: Predictions and extrapolations to all EU countries using the best model

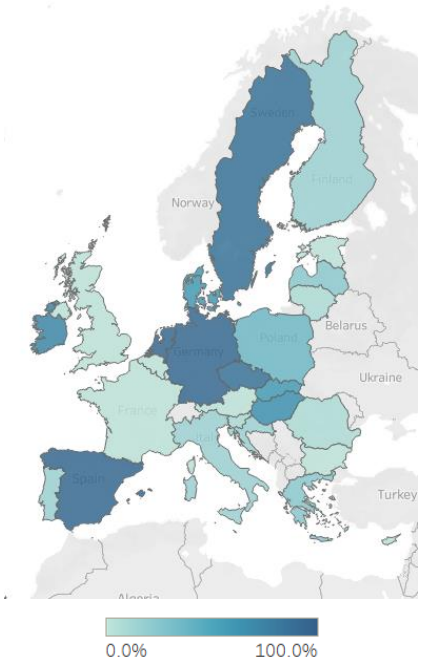
The cluster analysis approach and the multi-dimensional similarity measure from Step 2 allowed us to extrapolate the assessment of SOC-infiltrated companies to all EU countries. We did this by focusing on four industries for which at least three proven cases of SOC infiltration were recorded: wholesale and retail of motor vehicles, construction activities, real estate activities, and financial services activities. We developed a new, aggregated macro-measure of SOC infiltration – the share of companies within an industry with business profiles highly similar to SOC-infiltrated companies.

The results of the analysis for wholesale and retail trade and construction are presented in Figure 3.7. Figures for the real estate and finance sectors are presented in **Annex 3.3**. The darker colour corresponds to a higher share of companies with a similar business profile to infiltrated companies. All four industries have significantly different country rankings, both from each other and from perceptions of country rankings based on macro indicators or the literature. These highlight the value of the analysis to deliver new insights:

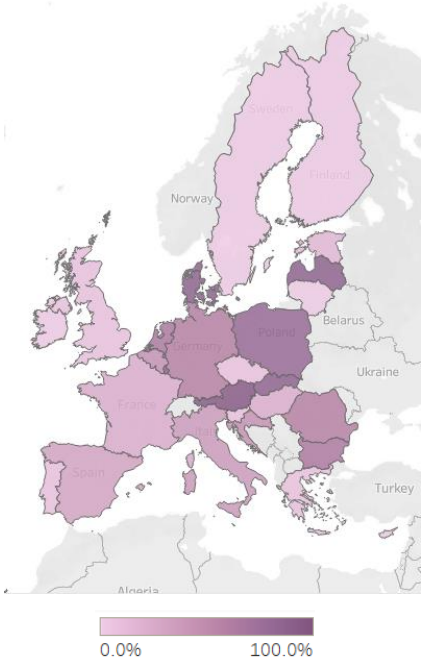
- Countries with the highest share of businesses that are highly similar to SOC cases in the **motor vehicles** sector are Spain, Sweden, Czech Republic, Germany and Netherlands.
- In the **construction market**, the leading countries are Poland, Latvia, Slovakia, Austria and Denmark.
- For the **real estate market**, UK, Romania, Austria and Belgium have the highest share of flagged companies.
- In the **finance sector**, Cyprus, Croatia, Germany, Portugal and Spain present the top five countries with the highest percentage of potentially SOC-infiltrated businesses.

Figure 3.7: Distribution of share of companies with high similarity measure as compared to infiltrated companies across Europe

A) Wholesale and retail trade of motor vehicles



B) Construction



Note: The figure presents the distribution of the share of companies with a high similarity measure (as developed in the previous section of our analysis). A similarity measure was developed based on closeness of the financial profile in a respective country or market group with the employment of cluster analysis. Source: Analysis of BvD data (n=796k) and authors' own calculations.

Step 4: Examining the relationship between estimated levels of SOC infiltration across EU countries and macro-indicators

We used the infiltration estimates derived in Step 3 and macro-data on risk factors identified in the literature (e.g. corruption, cash intensity, financial secrecy, quality of rule of law) to compare the risk of infiltration across EU countries. We used the share of companies flagged as being at high risk of infiltration as a proxy of SOC infiltration in a country, and disaggregated this analysis by business sector.

Corruption

According to the literature, the main sentinel crime of SOC infiltration is corruption, as it indicates that OCGs have lobbied to infiltrate public procurement, avoid control and facilitate the takeover of legal businesses (Savona & Riccardi, 2018). We examined correlations between infiltration risk for companies and corruption, using the Control of Corruption Index (CCI) in the Worldwide Governance Indicators produced by the World Bank. This index is intended to reflect the extent to which public power is captured by private interests[132]. For the purpose of our analysis, we rescaled the index from 0 (weak control) to 5 (strong control).

Box 3.4: A note on the interpretation of corruption indices

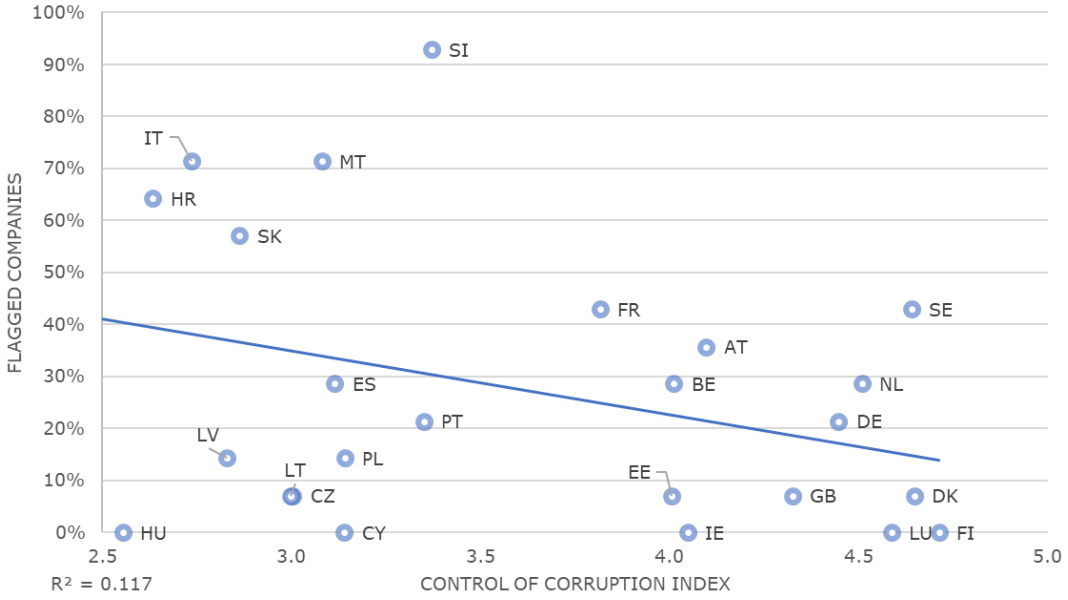
It is important to note that the CCI indicator of corruption is mostly based on individuals' perceptions, and can therefore differ from the actual level of corruption within a country. For instance, it is possible that intensified action against corruption could increase the perception of corruption in a country in the short term. Other popular corruption indicators, such as the Corruption Perception Index measured by Transparency International, suffer from the same limitation.

[132] The CCI is built using many different sources into a consistent and comparable annual index ranging from -2.5 (weak control of corruption) to 2.5 (strong control), and uses an unobserved components model to aggregate the different sources of information.

In the construction industry, countries with a lower level of corruption exhibited a relatively low share of companies at risk of SOC infiltration, compared to highly corrupt countries.

As shown in Figure 3.8, we observed a negative correlation between the CCI and the percentage of companies in the construction industry flagged as being at risk of infiltration. The coefficients of correlation are low, indicating a weak relationship, but this is expected given the small sample size (28 observations, one for each Member State) and the fact that corruption would only be one of many explanatory factors of infiltration in a predictive model. A negative correlation was also observed between the CCI and the percentage of companies flagged as being at risk of infiltration in the motor vehicle trade industry (figure presented in **Annex 3.3**). No significant correlation was identified for the other sectors where infiltration data is available (real estate and financial services).

Figure 3.8: Correlation between Control of Corruption Index and share of at risk of infiltration in the construction industry



Source: Research team's analysis.

Cash-intensity

To assess whether cash-intensity of a country indicates vulnerability to SOC infiltration of companies, we used a 2017 EU-wide survey from the European Central Bank (ECB) (Esselink & Hernandez, 2017). Respondents were surveyed on many aspects of their use of cash, including the share of the value of their spending, which was made using cash[133].

In the construction and motor vehicle trade industries, countries with a higher cash intensity exhibited a relatively high share of companies at risk of infiltration compared to countries with lower cash-intensity.

Our visualisations of the correlations between cash-intensity and share of flagged companies in certain sectors are presented in **Annex 3.3**. There are some clear outliers among those countries where cash usage is high. For instance, zero percent of Austrian companies in the motor vehicle trade industry are flagged as at risk of being infiltrated, even though nearly 70% of all transactions are made using cash in the country. In contrast, all countries exhibiting low cash usage have a low share of flagged companies.

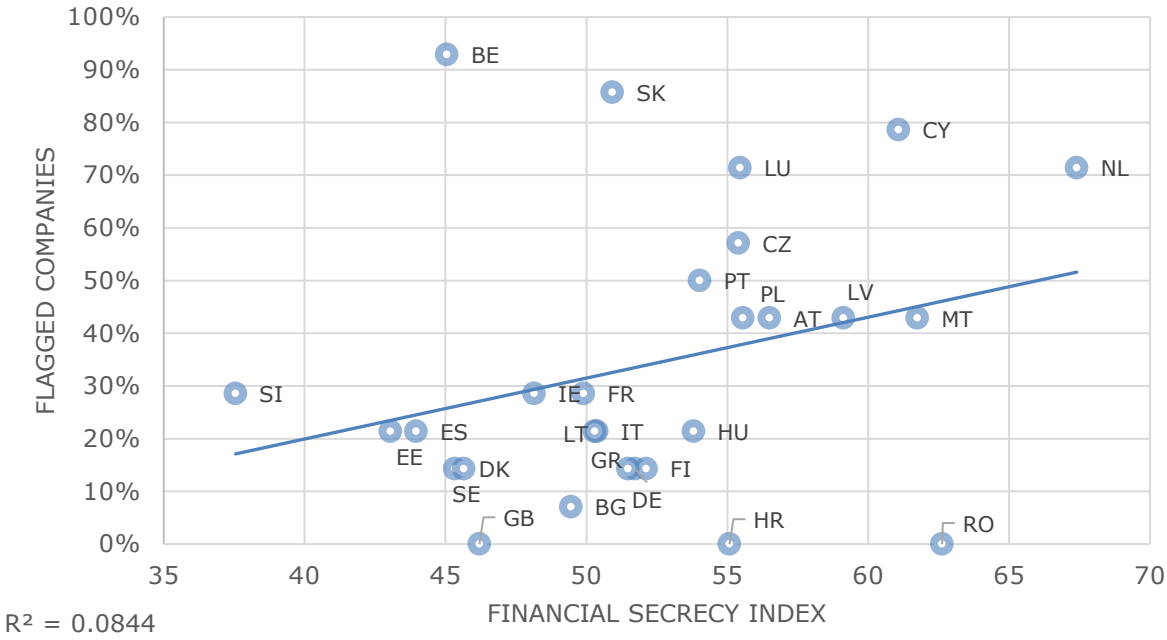
[133] Some EU countries were included in this survey. Data is missing for Bulgaria, Czech Republic, Denmark, UK, Croatia, Hungary, Poland, Romania and Sweden.

Financial secrecy

Building upon the analysis in Step 3 – which used micro-data from BvD and proven cases to generate predictions of SOC infiltration scores – we analysed the correlation between the FSI ranking[134] and the share of companies in the financial sector at risk of infiltration by country.

In the financial sector, countries with a higher FSI ranking exhibited a relatively high share of companies at risk of infiltration, compared to countries with a lower FSI ranking. As shown in the figure below, we observed a positive correlation between the FSI and the share of companies flagged as being at risk of infiltration in the financial sector.

Figure 3.9: Correlation between the Financial Secrecy Index (FSI) ranking and share of companies at risk of infiltration in the financial sector



Source: Research team's analysis.

Quality of the rule of law

At the macro-level, one source of data that we can use as a proxy for the quality of legal framework across EU Member States is the Rule of Law index provided by the Worldwide Governance Indicators produced by the World Bank (World Bank, 2019). Rule of law is defined by the 'perceptions of the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, property rights, the police, and the courts, as well as the likelihood of crime and violence' (World Bank, 2019). It is an index ranging from -2.5 (worst governance) to 2.5 (perfect governance). For the purpose of our analysis, we rescaled it from 0 (worst) to 5 (perfect).

Countries with a higher rule of law index exhibit a relatively lower share of companies at risk of infiltration, compared to countries with lower rule of law index. Our visualisations of the negative correlations between rule of law and share of flagged companies in the two usual sectors are presented in **Annex 3.3**. As expected, higher ability to enforce the rule of law seems to crowd out infiltration, as OCGs are less able to conceal their illicit activities in legitimate businesses.

[134] To reiterate, the Financial Secrecy Index (FSI) is developed by the Tax Justice Network (Tax Justice Network, 2020) and is based on knowledge of beneficial ownership, corporate transparency, the efficiency of tax and financial regulation, and international standards and cooperation.

3.3.2. Risk factors that facilitate serious and organised crime infiltration of public procurement

Risk factors identified in the prior literature

While there is no dedicated literature discussing risk factors for SOC infiltration in public procurement, there is a large body of international evidence of risk factors for corruption in public procurement. Such studies examine tendering corruption risks, political connections and company risk profiles in various contexts such as elections, high-level politics, welfare services and redistributive politics. Drawing on these studies enabled us to derive a set of potentially relevant indicators that can be tested empirically in the context of SOC infiltration of public procurement.

Studies examining the risk of corruption in public procurement have identified missing stock (in infrastructure projects) and single bidding as potential indicators of risk.

A prominent study by Olken (2007) commissioned independent engineers to review road projects and calculate the amount and value of missing inputs, which it used as an indication of corruption during contract implementation. Another approach to assess the amount of missing procurement outputs in infrastructure was proposed by Golden and Picci (2005), who examined the difference between the stock of infrastructure and cumulative public spending on it, using two independent data sources. Other authors used indicators characterising the bidding process on the micro-level: the use of exceptional procedure types (Auriol et al., 2016), negotiated procedures (Chong et al., 2016), explicit scoring rules (Hyytinen et al., 2018) or single bidder auctions (Klašnja, 2016). In addition to such quantitative measurement exercises, a wealth of qualitative studies has documented the nature and logic of diverse corrupt practices in public procurement. These studies cover many countries – both from Organisation for Economic Co-operation and Development (OECD) and non-OECD groups – from a more journalistic, government-centred or legalistic approach (David-Barrett et al., 2018; OECD, 2007; Transparency International, 2006; World Bank, 2009).

Personal political connections and political influence over public procurement – established through political party donations – have also been identified as potential risk factors in the literature.

Academic papers have considered short- as well as long-term direct benefits accruing to connected companies (1 to 4 years) (Goldman et al., 2013; Luechinger & Moser, 2014), while others considered ties either to specific individuals or parties as a whole (Straub 2014).

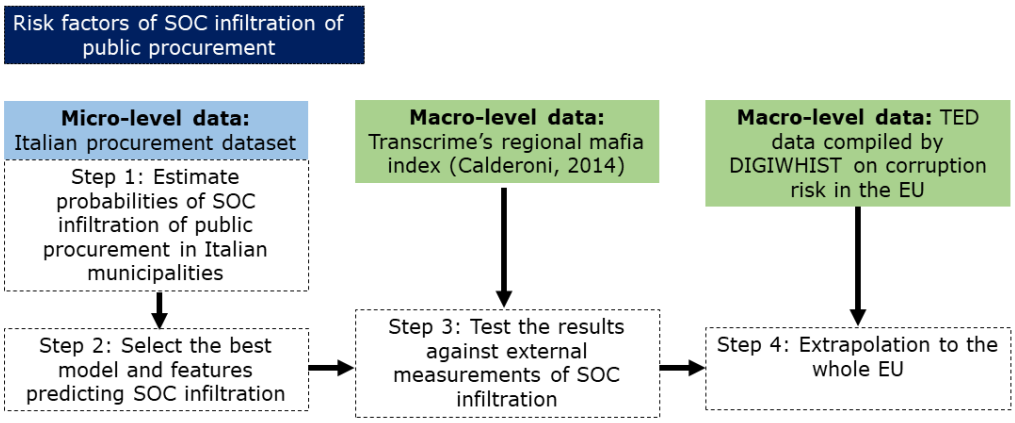
Some studies have examined how corruption can alter the financial performance of companies, which leads to signs of corrupt corporate behaviour.

Using diverse analytical techniques, company turnover is often found to increase due to corruption (see for example, Cheung et al., 2006; Cingano & Pinotti, 2012; Dávid-Barrett & Fazekas, 2016). Previous research has identified a strong relationship between government turnover and company success in economies with high corruption, rather than those with lower corruption (Dávid-Barrett & Fazekas, 2016). Quantitative studies and case studies have shown that company-registry characteristics – such as tax haven registration or very young company age at the time of winning public procurement contracts – have been found to be associated with a range of other risk factors (Fazekas & Kocsis, 2015; Fazekas & Tóth, 2017).

Methodological approach

The methodological approach and data sources for identifying and analysing risk factors of SOC infiltration of public procurement are depicted in Figure 3.10.

Figure 3.10: Methodological approach and data sources for analysing risk factors that facilitate SOC infiltration of public procurement



Data sources

As the main input to this analysis, we constructed a micro-level dataset that contained yearly observations for more than 1,500 Italian municipalities over the period 2008 to 2014. Detailed information on each open-tendered public contract was taken from a national dataset managed by ANAC, the Italian anti-corruption agency, which holds information about all contracts with a reserve price higher than €150,000. The data was gathered, cleaned and republished by the EU-funded research project DIGIWHIST[135]. The dataset provides information on the auction ID, number of bidders, bidders' names, bids, contract-awarding procedure, reserve price of the contract, categories of work involved in the contract, the final price paid by the contracting authority and the timing for the completion of the project. For the main analysis, we restricted the set of municipalities to those that were dissolved by the central government due to proven mafia infiltration into the municipal administration (data collected from the Italian Ministry of Interior)[136]. In addition to this dataset, we also used an Italian regional-level mafia index (Calderoni, 2014) and Tenders Electronic Daily (TED) data on public procurement tenders across the EU, as compiled by DIGIWHIST.

Analytical steps

We followed three analytical steps (refer to **Annex 3.3** for additional detail):

- **Step 1**: The probability of SOC infiltration of public procurement in Italian municipalities was estimated. A binary variable was created:
    - SOC infiltration of the contract or supplier was coded as 1, and applied if the contract was awarded in a municipality that was dissolved up to 3 years after the award of the contract.
    - Non-infiltration of the contract or supplier was coded as 0, and applied if the contract was awarded in a dissolved municipality 3 years after the dissolution.

  The set of predictors used included, among others, contract value, number of bids, CPV division, selection criterion, contract delivery is local, or relative price (for the full list see **Annex 3.3**). The set of predictors was restricted in order to allow for EU-wide extrapolation. That is, the variables only available in the Italian public procurement dataset, but not in TED[137], were removed from the analysis.
- **Step 2**: A set of predictive models weas estimated, and the best method selected based on prediction accuracy.

[135] Available at: www.opentender.eu/it
[136] The municipal dissolution power of the central government is based on Law no. 164/1991. It allows the national government to dissolve any local government whenever direct or indirect links emerge between local elected politicians and criminal companies, or when there are such pressures that compromise the normal functioning of the local administration.
[137] Tenders electronic daily (TED) is the online version of the 'Supplement to the Official Journal' of the EU, and is dedicated to European public procurement.

- **Step 3**: The results for the infiltration score were validated using Transcrime's Italian region-level mafia index (Calderoni, 2014). This was for the whole of Italy and not just for the municipalities infiltrated.

Box 3.5: A note on the predictive models we estimated

We compared three groups of predictive models: (1) logistic regression; (2) random forest; and (3) gradient boosting machines. The models were built to predict the binary outcome variable on the contract level, where 1=SOC infiltration of the contract/supplier; and 0=SOC non-infiltration of the contract/supplier. Models were compared based on the percentage of contracts that were correctly classified on the test dataset, with 70% of the sample used for training the models and 30% used for testing accuracy.

Limitations of the analysis

The main limitation of the analysis is that it only considers extreme forms of SOC infiltration of municipal public procurement, i.e. cases when the municipal administration was, by and large, under mafia control. There are other, less invasive or more insidious forms of SOC infiltration in local or national public procurement, which the assessment cannot capture due to the different traces they leave in administrative datasets. In addition, the peculiarities of the Italian context may present limitations to the generalisability of the findings.

Results of the analysis

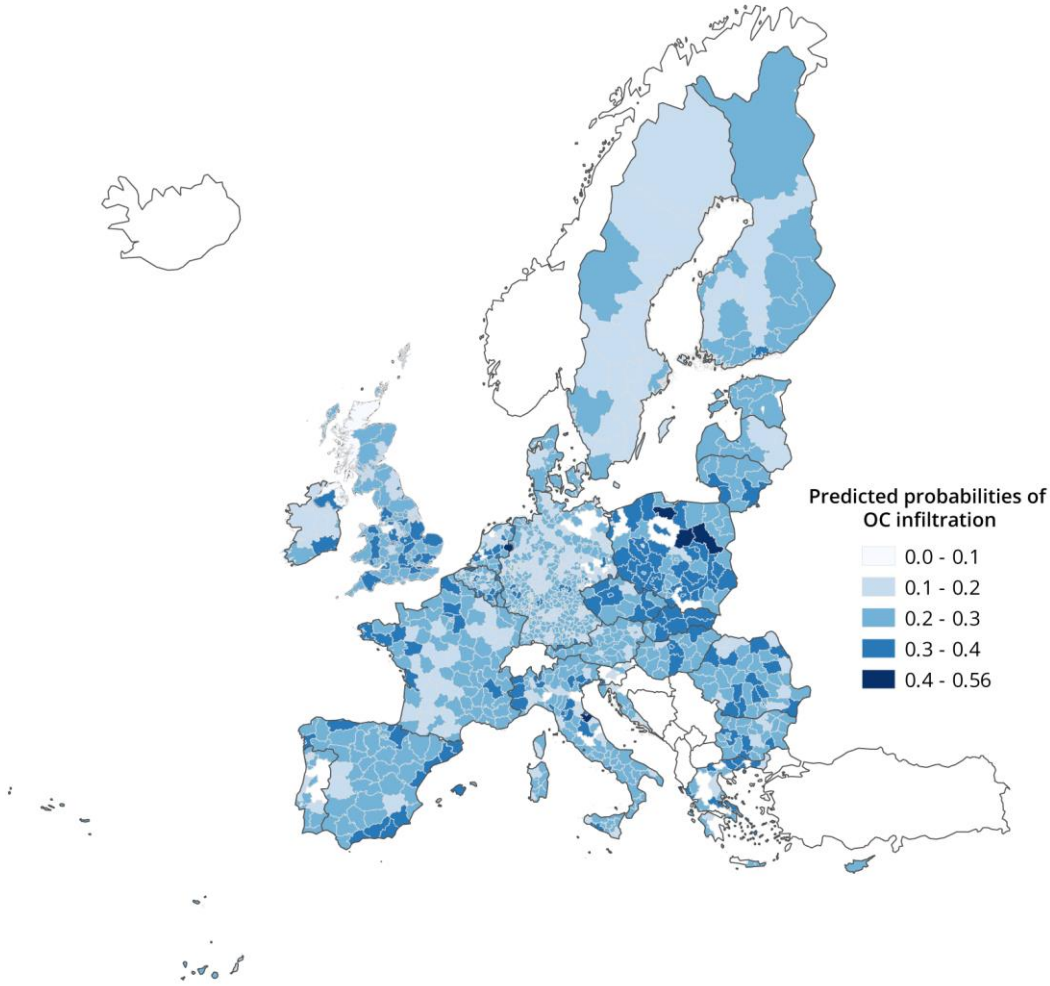
Steps 1 to 3 allowed us to conclude that the random forest model is most reliable for identifying SOC infiltration of municipal procurement contracts. (The details of the analytical process for arriving at this conclusion are provided in **Annex 3.3**.) The best random forest model showed that, among others, the following actionable red flags were the most influential in predicting SOC infiltration: number of contracts, buyer's spending concentration, relative price of a contract, and missing information.

The random forest model was thus used to estimate the probabilities of the SOC infiltration of public procurement across the whole of Italy and for the rest of the EU. Each country or region received an aggregate score based on the average predicted probability of SOC infiltration for all its municipal contracts. Crucially, from the perspective of using this indicator for further analysis, most contracts had a low estimated probability of SOC infiltration, while a substantial minority of contracts had a predicted probability above 50%. The distribution of predicted SOC infiltration probabilities for the whole Italian public procurement dataset is presented in **Annex 3.3**.

Figure 3.11 presents the results of the extrapolation for the European data aggregated by NUTS3 regions, with darker colours indicating higher infiltration risk.

- Countries with the **highest** predicted probabilities of SOC infiltration of public procurement are Italy, Poland, Spain, Hungary, Greece and Romania.
- Countries with the **lowest** predicted probabilities of SOC infiltration of public procurement are Germany, France, Norway and Sweden.
- The model predicted higher average probabilities of SOC infiltration for the Eastern regions and Southern regions of the EU.

Figure 3.11: Mean value of predicted probability of SOC infiltration of public procurement for European NUTS3 regions



Source: Extrapolations using the best model, based on contract-level TED data compiled by DIGIWHIST.

3.3.1. Recommendations

Risk factors for SOC infiltration of companies

Our analysis of financial and ownership risk indicators does not support the claim of the literature that SOC-infiltrated companies have a significantly different financial or ownership profile than their non-infiltrated peers, when considering individual features. The findings of our analysis showed:

- There is no significant difference between infiltrated companies and their peers in terms of **presence of liquidity of assets**.
- Infiltrated companies are also broadly similar to other companies with regard to **share of current assets**, when examined by business sector.
- Infiltrated companies in the available sample have **sparse ownership networks and low degree and centrality measures**.
- The **degree and centrality of proven cases of SOC** are broadly similar to other companies in their respective markets.
- Our analysis found **no ownership links with black-listed jurisdictions** in the sample of proven cases of SOC infiltration of companies.

Nevertheless, this analysis revealed that companies infiltrated by SOC have a distinct profile when considering multiple dimensions at once.

Building on these findings, we extrapolated the results across the EU and identified a modest but positive correlation between the level of corruption and the share of companies infiltrated in both the construction and the motor vehicle trade sectors. Similarly, we found positive correlations with cash intensity, rule of law and financial secrecy.

The table below presents a list of valid indicators of SOC infiltration of companies, as established by this study.

Table 3.9: Valid indicators of serious and organised crime infiltration of companies

Factors associated with SOC infiltration	Level of indicator	Indicator
Share of current assets	Micro	Company's current assets as a percentage of total assets.
EBITDA margin	Micro	Company's operating profit as a percentage of its revenue.
Volatility of total assets	Micro	Standard deviation of reported annual total assets.
Volatility of reported revenues	Micro	Standard deviation of reported annual revenues.
Corruption	Macro	Control of Corruption Index (Worldwide Governance Indicators).
Cash-intensity	Macro	The share of cash present in relation to other factors of production to produce a good or service.
Legal framework	Macro	Rule of Law index (Worldwide Governance Indicators) and FSI (tax Justice Network).

Risk factors for SOC infiltration of public procurement

In line with theoretical expectations, our study validates the finding that procurement risk indicators – single bidding, number of contracts awarded by the procuring entity in the year, the share of a supplier in buyer's annual spending, and relative price – are associated with higher probabilities of SOC infiltration. Therefore, **the empirical analysis in this study confirmed that tendering risks serve as a risk factor of SOC infiltration**. Extrapolation to the EU as a whole revealed a rich and diverse picture that only partially overlaps with perceptions of where SOC infiltration is high.

The table below presents a list of valid indicators of SOC infiltration of public procurement, as established by this study.

Table 3.10: Valid indicators of serious and organised crime infiltration of public procurement

Factors associated with SOC infiltration	Level of indicator	Indicator
Number of contracts	Micro	Number of contracts awarded by the procuring entity in the year.
Buyer's spending concentration	Micro	Share of supplier in the buyer's total annual public-procurement spending.
Relative price of a contract	Micro	Estimated price of the tender divided by the awarded contract value.
Missing information	Micro	Share of key fields that are empty in the public record (e.g. contract value).

Cross-cutting findings and recommendations stemming from the analysis of risk factors for SOC infiltration are presented in Table 3.11.

Table 3.11: Recommendations – Risk factors for serious and organised crime infiltration

Key findings	Recommendations	Key actors for recommendations
To date, analysis of infiltration risk has been based upon limited case information – available from public sources such as legal databases and media archives – resulting in a non-representative understanding across Member States.	Initiate a coordinated effort that would allow prosecutors, police and judicial authorities, AROs, AMOs, FIUs, researchers and others to share and collate case examples of infiltrating the legal economy. The UNODC SHERLOC database offers a useful model, which may be adapted to specifically capture financial aspects of SOC.	European Commission, particularly through ARO and FIU platforms Member States, particularly police, judicial authorities and prosecutors
Our analysis demonstrates that it would be both feasible and fruitful to build large-scale SOC risk-assessment tools based on micro-level databases describing companies (incorporated companies) and transactions (public procurement).	Consider the development of a (quasi-) real-time monitoring system, which would be able to better support policy decisions rather than one-off reports.	European Commission

3.4. The exploitation of the underground economy for serious and organised crime

Jirka Taylor, RAND Corporation, Shann Hulme, Clément Fays and Fook Nederveen, RAND Europe and Kamelia Dimitrova and Rositsa Dzhekova, Centre for the Study of Democracy

Key findings:

- There is no agreed definition of the underground economy. Some definitions include both legal and illegal activities, while others strictly exclude illegal activities. This creates problems in measuring and comparing estimates of the size and extent of the underground economy.
- The relative size of the underground economy is, according to estimates by Medina & Schneider (2019), larger in Eastern and Southern Europe than in Western and Northern Europe.
- The literature on the exploitation of the underground economy by OCGs remains limited.
- OCGs are in a particularly good position to exploit underground-economy practices in sectors that are closely connected to many economic activities, and have a relatively centralised position in existing economic networks.
- In the case of THB for labour exploitation, the underground economy and SOC intersect and drive one another.

Literature review	Interviews	Secondary data	Case study
			

Additional information supporting the analysis presented in this chapter can be found in **Annex 3.4**.

The underground (or informal or shadow) economy refers to 'legal activities that are deliberately concealed from public authorities for the following kinds of reasons: to avoid payment of income, value added or other taxes; to avoid payment of social security contributions; to avoid having to meet certain legal standards such as minimum wages, maximum hours, safety or health standards' (OECD, 2002). Among all economic activities that are hidden from government oversight, an important distinction is made between:

- **Unrecorded legal activities** that would contribute to the national GDP if they were recorded – e.g. employees in legitimate sectors without a formal contract (Hassan & Schneider, 2016).
- **Illegal or criminal activities** that do not overlap with legitimate sector activities – e.g. drugs or weapon trafficking.

- **Informal economic activities** that are not supposed to be accounted for in the national GDP. Unlike the two other categories, these are not typically considered part of the underground economy.

The literature features two competing definitions of the underground economy. Neither of these include the third type of activity on the list above (DIY/household), while both include the first activity (unrecorded legal activities). The difference relates to the second activity. One definition excludes illegal activities and only focuses on legal economic activities that are not reported to the government (Deviatov, 2009). The other includes illegal activities as part of the underground economy (Herwartz et al., 2015). **As stated above, for the purposes of this study, we adopted a definition excluding illegal activities**, which were examined distinctly in 2.

3.4.1. The extent and characteristics of the underground economy in the EU

Table 3.12 provides an overview of the relative size of the underground economy across the EU from 2010 to 2017 (based on Medina & Schneider (2019), whose study adopts the same definition as described above). Underlying considerations on this and other methods to measure the underground economy are presented in **Annex 3.4**.

Table 3.12: Underground economy as a proportion of GDP (%)

Member State	2010	2011	2012	2013	2014	2015	2016	2017
Austria	7.6	6.9	7.0	7.0	6.6	7.3	7.4	7.1
Belgium	16.9	16.0	16.7	16.6	15.9	17.2	16.9	16.5
Bulgaria	26.2	24.4	24.5	24.8	24.2	24.9	24.0	22.9
Croatia	24.6	23.7	24.6	24.0	23.8	24.7	23.6	22.7
Cyprus	26.0	26.2	27.1	27.0	25.6	26.6	26.7	25.2
Czech Republic	13.5	12.4	12.5	12.7	12.1	12.2	12.3	11.7
Denmark	13.0	12.0	12.4	11.9	11.1	12.0	12.1	11.7
Estonia	22.7	20.1	20.0	19.6	19.3	21.0	20.9	20.1
Finland	11.1	10.6	11.1	11.1	10.6	11.5	11.4	10.8
France	11.8	11.1	11.7	11.6	11.4	12.2	12.2	11.7
Germany	10.6	9.5	9.9	9.9	9.2	10.2	10.7	10.4
Greece	23.1	23.0	24.3	23.7	23.6	25.3	25.4	24.8
Hungary	20.7	19.7	20.4	19.9	19.8	20.8	20.5	19.8
Ireland	12.3	12.0	12.0	11.7	11.0	9.5	9.7	9.6
Italy	20.8	18.9	20.0	20.0	19.7	20.9	20.6	19.8
Latvia	20.8	19.3	18.7	18.4	17.9	19.1	18.8	18.0
Lithuania	24.1	22.0	21.5	20.5	20.0	21.3	21.0	19.7
Luxembourg	8.8	8.4	9.0	8.7	7.9	8.5	8.7	8.8
Malta	23.5	23.1	23.8	22.6	21.9	21.5	20.1	18.6
Netherlands	9.4	8.9	9.1	9.0	8.6	9.0	9.1	8.8
Poland	21.5	20.0	20.3	19.9	19.4	20.2	20.4	19.9
Portugal	18.6	17.6	17.7	17.5	16.7	17.4	17.1	16.1
Romania	26.5	24.4	25.1	23.7	23.2	23.7	23.8	23.0
Slovakia	13.9	12.9	13.1	12.9	12.9	13.6	13.2	13.1
Slovenia	21.9	20.9	21.7	20.8	19.7	20.7	20.2	19.0
Spain	21.3	20.6	21.3	21.1	20.9	21.9	21.3	20.3
Sweden	10.3	9.5	10.2	10.2	10.1	10.7	10.9	10.7
United Kingdom	10.3	9.9	9.7	9.5	8.7	9.2	9.7	9.4

Member State	2010	2011	2012	2013	2014	2015	2016	2017
EU average*	17.6	16.6	17.0	16.7	16.1	16.9	16.7	16.1
Weighted EU average**	14.2	13.2	13.5	13.3	12.8	13.5	13.7	13.3

Notes: * Unweighted average ** Average weighted by contribution to EU's GDP. Source: Medina and Schneider (2019).

3.4.2. The exploitation of the underground economy by organised crime groups

Previous research has shown that (1) the formal and underground economy are intertwined and boundaries between the two are often blurred; and (2) opportunities for OCG infiltration of the formal economy tend to arise in circumstances where this blurring occurs (Ponsaers et al., 2008). This is because under such circumstances, there are often weak or poorly enforced regulations and 'legal loopholes' that mean illegal activities may be more likely to go undetected. As stated by Ponsaers et al. (2008), 'where regulation is less present or less enforced, it [SOC infiltration] seems to be more likely to flourish.'

Our literature review and interviews with experts identified five legal sectors with predominant vulnerabilities that produce a grey or underground aspect that, as a result, may be subject to exploitation by OCGs. These include the following sectors: transportation, entertainment, construction, finance, and labour. Each of these sectors and the factors facilitating OCG exploitation are explored below. The labour sector is examined via an in-depth case study focusing on the use of undeclared work by OCGs for THB in Bulgaria and Romania (see Box 3.6 and **Annex 3.4**).

Transportation sector

The transportation sector comprises companies that provide services to move people or goods, and consists of several industries including air freight and logistics, airlines, marine, road and rail, and transportation infrastructure (Hayes, 2020). The transportation sector is used by OCGs for the **trafficking of illicit goods such as drugs, tobacco, counterfeit products, THB and migrant smuggling, and MTIC fraud**; and is also subject to **theft of cargo and attacks involving firearms and explosives** (Confederation of European Security Services (CoESS), 2017). According to the EU SOCTA, OCGs in the EU are becoming increasingly cross-border in their operations, and are thus heavily reliant upon the transport industry to move goods for supply and distribution (Europol, 2017b). It is typical for OCGs to use the services of legitimate transport companies to (consciously or unconsciously) aid in their pursuits (Klima, 2011). Investing in transport companies and types of transport – like motor vehicles, lorries and boats – is also common practice for OCGs. This section briefly explores some of the vulnerabilities within the transport sector that present opportunities for exploitation by OCGs.

Inadequate screening. Cargo and freight companies have a responsibility to arrange customs papers and approve containers for transport. However, research has shown that such companies are becoming increasingly unaware of the goods they transport, meaning that illicit goods can be easily concealed. One researcher, Klima (2011), analysed 26 case files and conducted interviews with law enforcement in Belgium and found that transport operators expedite jobs for entrepreneurial reasons, often at the jeopardy of adequate due-diligence. Klima's research found that if the paperwork of their customers appears legitimate and payment is made, typically no further enquiries are made (Klima, 2011). To appear legitimate to entrepreneurs, OCGs may use 'straw men' to conceal their identity as well as fraudulent documentation, such as fake identity documents and customs declarations (Hall et al., 2017). The transport sector is highly competitive, and operators are often under financial pressure due to high overhead costs (Slack & Rodrigue, 2020). Security inspections of cargo adversely affect efficiency and competitiveness, thus transport companies may seek to minimise the overall number of inspections carried out (Yin, 2006). Moreover, the implementation of adequate security and crime-prevention measures (such as GPS tracking) is cost-prohibitive, particularly for small- and medium-size enterprises (Klima, 2011). The large and increasing volume of global trade has meant that it is impractical for operators to carry out thorough manual inspections and currently, screening and detection equipment are not widely used (Slack & Rodrigue, 2020). Consistent with this, the Confederation of European Security Services (CoESS) noted that cargo ships and their freight are difficult to monitor and scan entirely, and these inadequate screening processes further increase opportunities for criminal activity and OCG exploitation (Confederation of European Security Services (CoESS), 2017).

Insider threats. Interviews with stakeholders highlighted that transport companies may be incentivised to accept bribes from OCGs in return for aiding criminal activities, such as by not carrying out inspections or 'turning a blind eye' to illegal cargo[138]. A report by CoESS identified that this insider threat is apparent across the aviation and maritime industries, serving to weaken existing security measures (Confederation of European Security Services (CoESS), 2017). Cost is the major factor for determining whether to employ security providers in the airport and maritime industries, and there is no mandatory minimum criteria for recruitment, vetting and training (Confederation of European Security Services (CoESS), 2017).

New technologies and digital infrastructures. The transport sector is increasingly utilising new technologies and digital infrastructures in its operations. For example, as one interviewee described, land-transport companies may now bid for loads through online systems, and as a result there is diminishing likelihood that operators 'know their customer'[139]. This increases the anonymity of OCGs and other criminal actors. Moreover, such online systems are known to be subject to high levels of fraudulent activities, such as false identity documents (Europol, 2015b). According to Europol, 'as transportation and logistics infrastructures rely more and more on online systems and automated remote management, OCGs will increasingly rely on intrusion into these systems to manipulate transport routes, infiltrate supply chains and gather valuable and sensitive data' (Europol, 2015b).

Entertainment sector

Another set of economic sectors that offers an opportunity for OCGs to take advantage of underground economic practices falls under the umbrella term 'entertainment industry'. This term encompasses, but is not limited to, prostitution, gambling and hospitality. A number of entertainment sectors, such as prostitution and gambling, are **subject to a variety of possible regulatory regimes** – ranging from complete legality and official regulation to complete prohibition – which determines the scope and susceptibility of a given sector to underground economy practices (Ponsaers et al., 2008). Taking prostitution as an example, Sanders (2008) recognized four distinct regulatory regimes: 1) legal formal, with legitimate businesses and registration; 2) legal informal, with no express prohibition on sex work, but no legal provisions for businesses or workers; 3) illegal informal, with unofficial tolerance of sex work, although official prohibition; and 4) illegal criminal, with official prohibition and enforcement.

SOC involvement is strong in illegal criminal systems where THB and exploitation of individuals are common (Kilvington et al., 2001)[140]. From the perspective of taking advantage of underground economic practices, it is the middle two regimes – straddling the grey boundary between the legal and illegal zone – that offer the most opportunities for SOC, and are thus most in line with our definition of the underground economy (although even countries with a legalised framework for sex work will have some informal sex economy alongside the formal one) (Sanders, 2008).

A critical feature of sex markets in the grey zone is that while the sex work itself is not illegal or is at least tolerated, **other aspects that would normally accompany commercial activities, such as advertising and procurement, remain illegal**. This may render it necessary to rely on informal practices to manage a business in the sex industry and to obtain input from related sectors that may be necessary to run a business in the sex industry, particularly at scale (Sanders, 2008). Sanders (2013) identified several such 'ancillary' industries that facilitate and provide support to sex markets: real estate services to find premises, security, transportation, hospitality, cleaning, styling and advertising. Frequently, these services and other commodities are sourced as part of an effort to integrate sex work with the broader tourism and hospitality economies. The need to ensure the provision of these services leaves room for the involvement of OCGs.

As with other sectors discussed in this chapter, the extent of SOC involvement in sex markets can differ across contexts, as some sex work can and does take place without much organisation. In a study on sex markets in selected cities of the USA, Dank et al. (2014) found that street-based and web-based sex trade were not commonly associated with OCG networks, although participants may maintain a close social network, e.g. informing each other about law enforcement activities. In contrast, venues and forms that were typically linked with more ancillary services, such as massage parlours and strip clubs, were – according to police

[138] Interview with cargo theft expert, 27 February 2020 (#39).
[139] Interview with transport industry representative, 27 February 2020 (#39).
[140] Interview with an academia representative, 13 March 2020 (#19).

testimonies – more likely to be run as part of hierarchical structures, which would indicate the involvement of OCGs (Dank et al., 2014). Although the aforementioned study was conducted in the United States, similar differentiation may also apply in Europe[141].

Similar to prostitution, gambling operations can also straddle the boundary between legal and illegal markets, depending on national legislative frameworks[142]. One example is regulatory regimes that allow for the operation of private gambling, but the holders of the gambling license organise activities that exceed or are in violation of what they are authorised to undertake (Nagy & Mezei, 2016). Similarly to at least some forms of sex work, running a gambling venue is a complex undertaking requiring input from a variety of ancillary industries and specialised staff, including dealers, maintenance, security, as well as people (e.g. 'cappers') to find customers and encourage them to bet (Ferentzy & Turner, 2009). This diversity of tasks to be overseen and staff to be managed again presupposes a level of organisation that OCGs can fulfil (Markovska & Zabyelina, 2016).

In addition to profits to be made in the sex industry and gambling, these sectors are also attractive to criminal organisations due to the fact that in 'vice' industries and potential related offenses such as these, **both supplier and consumer are interested in keeping the transaction hidden**, making this type of activity difficult to uncover by law enforcement[143]. Further, as a highly cash-intensive activity (Markovska & Zabyelina, 2016; Unger et al., 2006), legal gambling operations are among the most popular forms of money-laundering, due to the ability to convert large values of dirty cash into winning chips or tickets that could subsequently be cashed in as a clean cheque or a bank deposit (Schneider, 2017). One interviewee added that in some casinos it may be possible to have winnings paid out in cryptocurrencies, which makes investigations and tracking of suspicious transactions more difficult[144]. This observation was seconded by another interviewee who noted the widespread use of virtual currencies in sports betting[145].

Construction sector

Construction has been frequently recognized in the existing literature – as well as in our expert interviews – as a sector that is attractive to SOC (Gurciullo, 2014; Morselli et al., 2012; Richards, 2018)[146]. OCGs find the construction sector appealing because of the potential for large profits (Kenny, 2007), as well as the relatively high degree of business concentration in the industry (Gurciullo, 2014).

The construction sector has been noted as being permeated by underground economic practices (Gottschalk, 2010; Williams, 2015). Undeclared work is recognized as a frequent practice, and relatedly, in numerous instances construction work is performed by individuals who are not authorized to do so, e.g. due to immigration rules[147] or lack of appropriate qualification or certification (Richards, 2018). Underground construction work is also frequently performed in violation of workers' rights and in conditions that do not conform to existing health and safety standards[148]. Relatedly, construction work can be performed using substandard materials in contravention of existing regulations or contractual obligations (Richards, 2018). Labour unions can serve as a vehicle to mitigate the risk of abusive practices and non-conformities, although they can also be a conduit for underground practices.

Factors that facilitate underground work practices in the construction sector and OCG exploitation thereof include **high levels of staff turnover and workforce mobility**, as well as the **time-limited nature of the work** (Chartered Institute of Building (CIOB), 2016). For instance, a study examining the construction sector in Sicily noted that the considerable grey area surrounding contracting arrangements created room for OCGs and colluding individuals to

[141] See, e.g. Huisman and Kleemans (2014).
[142] Interview with an academia representative, 13 March 2020 (#19).
[143] When discussing the willingness of participants to engage in hidden commercial transactions in the context of the sex industry, it is necessary to recognise that coercion is a notable feature of sex markets and that, though some sex workers may see their job as a rational economic option, the notion of 'choice' more widely is very problematic with respect to individual sex workers (see, e.g. Simmons, 2018). Thus, this discussion primarily applies to those who organise the transactions.
[144] Interview with a Belgium national-level expert, 27 March 2020 (#59).
[145] Interview with European level stakeholder, 11 March 2020 (#16).
[146] Interview with an academia representative, 13 March 2020 (#19).
[147] Interview with an academia representative, 13 March 2020 (#19); Interview with National/MS-level expert, 2 April 2020 (#30).
[148] Interview with National/MS-level expert, 30 March 20 (#60); Interview with National/MS-level expert, 25 February 20 (#34).

work together (Tenti, 2012). Further, **construction work involves complex operations that vary from one assignment to another**. As a result, the production processes are not always standardized and may involve one-off or rare activities, the execution of which may be difficult to monitor and assess by a third party (Kenny, 2007). The **completion of construction work also requires drawing on a range of professions and types of expertise**, further exacerbating the sector's complexity and its accountability difficulties (Morselli et al., 2012). This connectedness to other sectors and the centrality of the construction sector to existing economic networks is in turn considered by observers as a precondition to infiltration by organised crime (Gurciullo, 2014). Further, the construction industry is inextricably tied with the real estate sector, which in its own stead attracts large legitimate as well as illegitimate investments (Nelen, 2008). The real estate sector offers OCGs an opportunity to launder proceeds from illicit activities[149], for instance via the creation of successive real estate transactions with artificial fluctuations in the valuation of the new or existing construction (Maillette, 2015; Ritzen, 2011).

In this context, OCGs can take advantage of prevalent underground economic practices by supplying cheap, and at times forced, labour. Personnel provided by OCGs does not have to be limited to construction workers but can also include security staff for construction sites (Chartered Institute of Building (CIOB), 2016). Other tactics employed by OCGs to take advantage of underground practices to infiltrate the sector include providing fake certificates and qualifications to individual workers and forging documentation that workers may need to access construction sites (Chartered Institute of Building (CIOB), 2016). The precarious position many undocumented construction workers find themselves in leaves them vulnerable to exploitation[150]. In financial terms, this exploitation could manifest itself via irregular pay or unclear discrepancies in how much workers are supposed to be paid, and how much they are paid in reality (Focus on Labour Exploitation (FLEX) Shaky Foundations, 2018). This in turn only increases the profits flowing to OCGs and raises the attractiveness of the sector as an infiltration target.

An important qualification to the discussion above is that OCG involvement is not necessary in order for collusive behaviour to emerge in the construction sector. A system with vulnerabilities and specificities such as those described earlier often develops profiteering schemes on the part of participants without any external organisation (Morselli, 2012). Relatedly, one interviewee noted that the use of underground practices by one market participant puts pressure on others, who may have intended to stay above board but may have no choice but to participate in such practices due to the competitive advantages they confer[151].

Financial sector

The financial services industry, including such institutions as banks and FinTech, provides services that OCGs may wish to have access to, such as processing transactions, issuing loans and accepting deposits (amongst many other services). In the context of the underground economy, of particular interest are **NPMs** because they are less regulated and offer enhanced anonymity (although Section 3.5 observes that the use of NPMs by OCGs is still overshadowed by cash as the prevalent payment method). When OCGs utilize NPMs in their operations, it often occurs in addition to cash payments, rather than as a substitution. Despite the absence of empirical evidence for the extensive use of NPMs, experts have frequently acknowledged their potential for exploitation by OCGs.

Interviewees identified cybercriminals and OCGs active in other markets as being among those using NPMs[152]. Due to their anonymous, fast and global nature, **virtual currencies** offer a cheap vehicle to transfer and launder large amounts of illicit funds. One interviewee explained that NPMs are more cost-efficient than traditional cash-out schemes[153], and employees of financial institutions, governments and companies often lack the expertise required to tackle misconduct in NPMs[154]. They are **complicated to regulate, and regulatory interventions are hard to enforce, as transactions have a high degree of anonymity** (complicating attribution and determination of liability) and move between jurisdictions all over the world in

[149] In an older study by Unger et al. (2006), the authors concluded that the Dutch real-estate sector was the conduit for most money-laundering efforts in the country.
[150] Interview with National/MS-level expert, 30 March 20 (#60).
[151] Interview with National/MS-level expert, 2 April 2020 (#30).
[152] Interview with European-level stakeholder, 11 March 2020 (#16).
[153] Interview with EU-level stakeholder, 12 March 2020 (#48).
[154] Interview with UK cybersecurity company expert, 25 March 2020 (#56).

an instant[155]. The legal status of virtual currencies – which are often not subjected to taxation – varies widely across the world (Frunza, 2018). **Regulatory uncertainty** can be exploited by OCGs, which in this context is more acute as innovations commonly precede the regulations that are introduced in response to them[156]. Legal services that were highlighted as areas of particular concern in relation to OCG exploitation (see Section 3.5) are: 1) the role of virtual currency exchangers, which may facilitate money-laundering by converting illicit revenues from virtual currencies into cash; 2) custodian wallet providers, which may facilitate money-laundering by simplifying criminal transactions; 3) 'mixer' or 'tumbler' services, which facilitate money-laundering by obscuring transactions; and 4) the access to privacy-focused virtual currencies, which offer even more extensive anonymisation of criminal transactions than other virtual currencies.

In addition to cash, NPMs have found their way into the underground economy as a means for transactions. Their usage has become customary in cybercrime (particularly – almost by definition – in crypto markets), but to a far lesser extent in THB and in most of the other markets considered in this study. In fact, OCGs may not feel they have a need for NPMs, since their established methods have worked well for them. For example, a system of favours or exchanging expensive gifts may be very effective in places where corruption levels are high[157]. Exploring new financial tools that enhance the secrecy of their operations may not be the highest priority if prosecution can be avoided through other means. Overall, **OCGs appear to maintain a strong preference for using cash** in their transactions, which is already difficult to trace[158]. The use of financial services in the underground economy is therefore an exception rather than a rule.

Hawala (and other informal value-transfer systems) is another example of a non-bank payment method. According to Van de Bunt (2008) hawala is 'unmistakably part of the informal economy', as financial transactions are not always certified or regulated by governments. **Transactions are hard to trace**, regardless of whether the funds are licit or illicit, as there is often no identification of the client and no record-keeping. The total value and volume of transactions are unknown, and estimates are next-to-impossible to carry out. It follows that investigations by law enforcement are complicated and that there is limited evidence with regard to the extent to which OCGs utilise Hawala[159]. Hawala bankers, or Hawaladars, can participate knowingly or unknowingly in the money-laundering of proceeds generated through illegal activities (as well as in terror finance, which lies outside this brief). Interviewees underlined the potential risks associated with Hawala and similar alternative payment methods[160], but simultaneously warned against overemphasising its role in the money-laundering operations of OCGs[161].

Illustrating the use of the underground economy for SOC in the labour sector

In order to better understand the links between SOC and underground economic structures – and the modus operandi of OCG exploitation of such structures – we undertook a case-study analysis focusing on the use of undeclared work by OCGs involved in THB for labour exploitation in Bulgaria and Romania. We focused on THB because there is known to be heavy organed crime involvement and there is a known intersection with the labour sector (as discussed in Section 2.2), and we focused on Bulgaria and Romania because they are among the top-five EU countries for registered victims of trafficking (European Commission, 2018b).

The full case-study is provided in **Annex 3.4**, which covers the extent of THB in Bulgaria and Romania, the characteristics of victims, the mechanisms for exploitation of the grey areas between the licit and illicit economy, and the role of intermediaries, as well as revenues,

[155] Interview with European-level stakeholder, 11 March 2020 (#16); Interview with UK cybersecurity company expert, 25 March 2020 (#56); Interview with a Belgium national-level expert, 27 March 2020 (#59).
[156] Interview with a EU level expert, 12 March 2020 (#17); Interview with national-level stakeholder, 25 February 2020 (#35); Interview with UK cybersecurity company expert, 25 March 2020 (#56); Interview with a Belgium national-level expert, 27 March 2020 (#59).
[157] Interview with an academia representative, 13 May 2020 (#89).
[158] Interview with national-level stakeholder, 25 February 2020 (#35); Interview with Swedish national-level stakeholder, 14 February 2020 (#43).
[159] Interview with a Belgium national-level expert, 27 March 2020 (#59).
[160] Interview with cargo theft expert, 27 February 2020 (#8); Interview with Bulgarian national-level stakeholder, 13 March 2020 (#51).
[161] Interview with a EU level expert, 12 March 2020 (#17); Interview with Bulgarian national-level stakeholder, 13 March 2020 (#51).

financial flows and money-laundering. The findings from this case study are summarised in the box below.

Box 3.6: The use of undeclared work by OCGs engaged in THB for labour exploitation in Bulgaria and Romania

OCGs revert to different **undeclared work practices** and fraudulent schemes throughout the different phases of labour trafficking, in order to avoid government detection, reduce costs and increase profits, at the expense of the human rights of victims.

The analysis of 11 proven cases of labour exploitation of Bulgarian and Romanian nationals in other EU destination countries shows a high level of infiltration by OCGs in the legal economy, notably the use of **legal companies** for the purpose of recruitment and exploitation of victims.

In the **recruitment** stage, victims are often offered contracts by intermediaries that are legitimate business entities acting as recruitment agencies, although without being licensed as such. When contracting victims, perpetrators use a variety of **underground economy practices** for tax evasion, such as abuse of EU posted workers' regulations and bogus self-employment.

In the **exploitation** stage, letter-box companies are used as sub-contractors (often deliberately creating a cascade of sub-contractors) in order to conceal the exploitation of victims and the evasion of due taxes, social insurance and health contributions.

When it comes to **returning the proceeds** of trafficking, money-laundering mechanisms include the purchase of properties in both countries of origin and destination, and registering of legal companies in the countries of destination.

Thus, OCGs increasingly employ legitimate companies yet revert to grey-economy practices in the course of THB for labour exploitation. This blurs the line between the formal and informal economy and poses further challenges.

Cross-cutting themes

Drawing on lessons from the sectors discussed above – as well as on findings from existing literature and interview more broadly – presented below are a series of cross-cutting and overarching observations addressing the research questions on the exploitation of the underground economy by OCGs.

OCGs are in a particularly good position to exploit sectors with close connections to many economic activities, and enjoy a centralised position in existing economic networks.

For instance, as discussed above, in sectors such as the entertainment and construction industries at least part of the input provided by OCGs seems to come in the form of providing 'ancillary' services that support the execution of the main activity (Gurciullo, 2014). These ancillary services are not necessarily illegal in their own right, but are undertaken on an informal basis due to the circumstances in which they are provided (Ponsaers et al., 2008). Based on similar principles, the transportation industry is also of key interest to OCGs as it relates to many types of economic activity and directly impacts many other sectors due to the relyiance on shipments of goods and transportation of people. After all, transportation and logistics are invariably included in any businesses that are considered as ancillary to sectors including manufacturing and entertainment.

OCGs and underground economic practices can coexist, but the presence of one is not a precondition for the existence of the other.

Underground economic practices can be exploited for criminal activities, and individuals engaging in the 'grey' (i.e. informal) economy can be recruited for activities in the 'black' (i.e. illegal) economy. However, it is important to recognize that many OCG activities in the sectors discussed above take the form of strictly illegal activities, and as such do not meet the definition of underground economy for the purposes of this study. By contrast, many underground economic practices take place without the involvement of OCGs, and can develop independently of the presence of OCGs (Morselli et al., 2012). Underground practices frequently take the form of 'good guys going dirty', i.e. legitimate businesses adding underground activities to their

otherwise above-the-board portfolios[162]. This observation also sheds light on definitional issues and ambiguity in this area (Walle, 2008). Using a narrower definition of underground economy leaves out a raft of OCG activities that are commonly referred to as 'informal', but are illegal by their very criminal nature and not due to the fashion in which they are carried out (Morselli et al., 2012; Nagy & Mezei, 2016).

Exploitation of underground economy by OCGs is inextricably linked with corruption.

Corruption has been identified as a strong facilitator of OCG activities, including those that straddle the boundary between legitimate and illegitimate domains (Markovska & Zabyelina, 2016). Environments where both public officials and the general population incorporate informal norms in their daily behaviour, circumventing existing regulations, create an opening for OCG involvement and exploitation (Dobovšek, 2008). For instance, exploitation of the underground economy is particularly attractive when perpetrators are able to collude with public officials and control the schedule/character of inspections, or at least be given advance warning. Elsewhere, OCGs may be able to influence police and prosecutorial decisions. All these mechanisms serve to decrease the risks of participating in the underground economy[163]. Relatedly, exploitation schemes are frequently reliant on cash or benefit from the cash-heavy nature of infiltrated industries. However, as both existing literature and interviewees revealed, trading influence and the ability to provide non-monetary benefits to business partners – such as preferential access to certain goods or services, or support in other underground schemes, which in turn may be dependent on collusion with public authorities – is another important currency (Dobovšek, 2008)[164].

There is a relative paucity of evidence on OCG exploitation of the underground economy.

There is a substantial body of literature on both OCGs and on the underground economy. However, there is a relative paucity of evidence bringing these two components together and exploring how they interact[165]. A possible contributing factor has been the divergence in the focus of the two respective fields, as well as definitional issues. The underground economy has historically been the object of studies by sociologists and economists, who focus on areas such as the conditions that give rise to the underground economy or its size, interaction and effect on the legal economy. More recently, insights from other disciplines have contributed to the field, though these new interdisciplinary approaches lag behind the traditional lines of inquiry[166]. By contrast, organised crime has typically been the domain for legal scholars and criminologists, with supplemental contributions by anthropologists and sociologists[167]. A large body of existing research in this area focuses on illicit activities and groups' modus operandi in contexts that do not meet a narrower definition of the underground economy or limit their scope to traditional mafia-like groups. This difference between the two academic fields also gives rise to definitional issues and possible disagreements over the conceptualisation and theoretical placement of the underground economy, which skirts the boundary between legal and illegal activities.

3.4.3. Recommendations

Cross-cutting findings and recommendations stemming from our analysis of the exploitation of the underground economy for SOC are summarised in the table below.

Table 3.13: Recommendations – Underground economy

Key finding	Recommendation	Actor
There is no agreed definition of the underground economy. Some definitions include both legal and illegal activities; while others strictly exclude illegal activities. This creates problems in measuring and comparing estimates of the size and extent of the underground	Improve understanding at EU-level of the nature of OCGs operating across and between illicit markets. This will be important for informing targeted policy at the strategic level and operations by law enforcement.	Eurostat Member States European Commission

[162] Interview with EU-level stakeholder/academic, 19 February 2020 (#53); Interview with academia representative, 11 February 2020 (#13).
[163] Interview with academia representative, 13 May 2020 (#89).
[164] Interview with academia representative, 13 May 2020 (#89).
[165] Interview with academia representative, 11 May 2020 (#88).
[166] For a brief historical narrative of research on informal economy, see Walle (2008).
[167] There are notable exceptions, exemplified by the work of Peter Reuter, an economist involved in the study of OCGs (see Reuter & Tonry, 2020, for a recent example).

Key finding	Recommendation	Actor
economy.		
The exploitation of the underground economy by OCGs remains an under-examined topic in the existing literature.	Facilitate further research on the unique ways OCGs infiltrate the underground economy. Specifically: • Improve understanding of the benefits accruing only to OCGs and not to other actors involved in the underground economy. • Strengthen the economy analysis of OCG involvement in the underground economy. • Expand the scope of current underground-economy research to cover OCGs. • Conduct supporting research involving criminal actors (e.g. people currently imprisoned in connection with OCG involvement).	European Commission
OCGs are in a particularly good position to exploit underground economi**c** practices in sectors that are closely connected to many economic activities, and have a relatively centralised position in existing economic networks. There are structural 'loopholes' across a number of sectors – transport and logistics, entertainment, construction, financial, and labour **–** that are susceptible to OCG exploitation.	Conduct vulnerability analyses across each of the identified sectors with a view to understanding the specific asymmetries that may produce an underground-economy structure, particularly for exploitation by OCGs, with a particular emphasis on understanding differences in legislative frameworks across Member States.	European Commission
The underground economy and SOC intersect and thrive on each other in cases of THB for labour exploitation.	The European Union could consider proposing a common definition of labour exploitation as part of the Directive on preventing and combatting THB, in order to foster cross-border investigations on labour THB.	European Commission European Parliament European Council

3.5. The exploitation of new payment methods and non-bank payment methods by organised crime groups

Atanas Rusev, Kamelia Dimitrova and Maria Karayotova, Centre for the Study of Democracy

Key findings:

- The use of new and non-bank payment methods for money-laundering purposes is observed in practically all Member States, and there are indications that it is growing – although with different intensity across countries and criminal markets.
- Cryptocurrencies are regularly used in both cyber-enabled and cyber-dependent crimes, in illicit trade via dark-net markets and in money-laundering linked to these types of crime.
- Prepaid cards are rarely used by OCGs, compared to cash and other methods.
- Digital or mobile wallets are moderately used in certain cybercrimes – such as phishing and child sexual exploitation material – but rarely used in IPR infringements and money-laundering compared to traditional payment methods.
- Other innovative and mobile-payment services are rarely used compared to cash and bank transfers.
- Money-transfer services are regularly used, particularly for THB, smuggling of migrants, cybercrime and money-laundering, but less often than cash.
- Hawala and similar informal transfer systems are regularly used for migrant smuggling and rarely for other types of crimes, except where OCGs are of particular nationalities (i.e. of Nigerian, Chinese or Afghani origin).
- Overall, OCGs still rely more on cash than on new and non-bank payment methods.

Literature review	Interviews	Case study
		

Additional information supporting the analysis presented in this chapter can be found in **Annex 3.5**.

The first supranational assessment of the risks of money-laundering in the EU prepared by the Commission emphasised that NPMs are vulnerable to exploitation by OCGs for money-laundering, although not all NPMs present same the level of risk (European Commission, 2017b).

The term 'new payment methods' is defined by the FATF (2010) as 'payment innovations that gave customers the opportunity to carry out payments directly through technical devices such as personal computers, mobile phones or data storage cards.'

The main forms of NPMs and other non-bank payment methods include:

- cryptocurrencies and services related to cryptocurrencies (cryptocurrency exchangers, custodian wallet providers, cryptocurrency mixers);
- e-money and e-money products and services (prepaid cards and digital/mobile wallets);
- other innovative mobile- and internet-based payment systems (money remittances, payment-initiation services, execution of payment transactions, cash deposit and withdrawal services);
- official money-remittance services (such as Western Union, Money Gram);
- informal value-transfer services, also known as hawala.

The use of NPM for money-laundering purposes can include one or more stages of the money-laundering process, i.e. transfer or conversion of illicit funds, which may or may not lead to full integration of these illicit funds in the legal economy (Levi & Soudijn, 2020).

This section focuses on the use of NPMs and non-bank payment methods by OCGs. It discusses intensity of use, criminal markets and associated risks for each of the covered NPMs, followed by an overview of factors that influence their use. It includes excerpts from two case studies,

illustrating the use of NPMs in the context of cybercrime and THB. The full texts can be found in **Annex 3.5**.

3.5.1. Cross-cutting themes

Interviews conducted with EU-level and national-level stakeholders provided evidence that use of NPMs for money-laundering purposes is observed in practically all Member States, and there are indications that it is growing, although with different intensities across countries and criminal markets.

Against this background, Europol and interviewed stakeholders noted that despite the important role that NPMs play in some SOC criminal activities, **OCGs still rely more on cash than on NPMs; even in cybercrimes, cash plays a crucial role in the laundering of the proceeds**. In this sense the trend over recent years has not been of NPMs supplanting cash, but rather NPMs being used in conjunction with cash (Europol, 2015d, 2020a).

3.5.2. Cryptocurrencies and related services

Cryptocurrencies are virtual currencies, which are defined by the Commission as digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically (European Commission, 2017b).

The use of cryptocurrencies in the context of SOC is reportedly related to criminal markets, such as illicit drugs, counterfeit goods, illicit firearms, stolen and fraudulent identity documents that are traded on dark-net markets (Europol, 2018c). Cryptocurrencies are also closely linked to cybercrime activities such as identity theft, account takeovers, phishing and card fraud (wherein stolen credit card data are sold on the dark net), ransomware, and sale of cybercrime tools and services – including the provision of bulletproof hosting, counter anti-virus services, Denial-of-Service (DDoS) services and malware (Europol, 2018c). As well as the sale of illicit goods and services on dark-net markets and use in the context of cybercrimes, Europol also reports on the use of cryptocurrencies for money-laundering purposes (Europol, 2018c).

Three cryptocurrency services are especially prone to money-laundering risks and abuse by organised crime (Sat et al., 2016):

- **Privacy-focused cryptocurrencies** such as Dash, Zcash and Monero are renowned for privacy-preserving features – such as mixing and stealth addresses – that make de-anonymisation and tracing of transactions particularly difficult (Europol, 2018d).
- **Cryptocurrency exchangers** are described as the 'bureau de change' of the virtual currency world (European Commission, 2017b). Some exchangers can be considered as professional facilitators who willingly provide financial services to criminal actors (Leukfeldt et al., 2019). Peer-to-peer exchanges are recognised as a particularly big challenge[168] with regard to investigation by both Europol and the FATF (Europol, 2018c; FATF, 2015). Similarly, so-called 'coin swap' services, which provide exchange of cryptocurrencies from one type to another (crypto-to-crypto) and are currently not covered by the 5th Money Laundering Directive, have been identified as posing high risk of money-laundering abuse[169].
- **'Mixer' or 'tumbler' services** mix identifiable (alternatively known as 'tainted') cryptocurrency funds with untainted pools of funds to obfuscate the trail behind the cryptocurrencies. They are often used to facilitate money-laundering of cryptocurrency funds originating from cybercrime activities (Chainanalysis, 2020; Europol, 2019a; Silfversten et al., 2020). Although some of the biggest centralised tumbling service-providers have been shut down in recent years, decentralised mixing services have started to gain popularity (Chainanalysis, 2020).

[168] Interview with national-level stakeholder, 27 March 2020 (#58); Interview with EU-level stakeholder, 12 March 2020 (#48).
[169] Interview with UK cybersecurity company expert, 25 March 2020 (#56); Interview with EU-level stakeholder, 12 March 2020 (#48).

Extent of use for criminal and money-laundering purposes

There is an ongoing debate about the extent of use of cryptocurrencies for criminal purposes, so currently it is hard to establish with certainty the actual degree of this use.

Research exploring links between cryptocurrencies and illicit activities has focused on bitcoin being the most commonly used cryptocurrency, and some experts[170] contend that bitcoin is extensively used for criminal purposes (Chainanalysis, 2020). Foley et al. (2019) argued that approximately 25% of bitcoin users and 50% of bitcoin transactions are associated with illicit activity. This amounts to around $72 billion (USD) of unlawful activity per year involving bitcoin (Foley et al., 2019). A slightly more conservative estimate is provided by Yin Sun & Vatrapu (2017), who suggest that the number of bitcoin users involved in illegal activities ranges between 11% and 30% of all users.

These estimates have been contested by other studies, which argue that cryptocurrency use for criminal purposes is lower than suggested by Foley et al (2019). A recent study by the Centre on Sanctions and Illicit Finance and Elliptic on the flow of bitcoins from previously identified illicit activities to various cryptocurrency exchange and mixing services established that about 1% of all transactions can be attributed to illicit activities (Fanusie & Robinson, 2018). Chainanalysis, one of the leading blockchain-analysis companies, also reports that their analysis of illicit transactions with 16 different cryptocurrencies (including bitcoin) established that 1.1% of all transactions are related to illicit activities (Chainanalysis, 2020).

The existing research and interviewed experts[171] point out that a major part of cryptocurrencies used for illicit purposes is linked to dark-net markets (Chainanalysis, 2020; Fanusie & Robinson, 2018). One of the identified studies pointed out that between 80% and 99% of illicit transactions with bitcoins in the period 2013–2016 were related to dark-net markets, wherein Europe hosted a disproportionate amount of illicit activity – ranging between 38% and 57% of all illicit transactions (Fanusie & Robinson, 2018). Although law enforcement agencies around the world successfully shut down many of the most popular dark-net markets, apparently new ones continue to mushroom and fill the void, and even manage to increase the overall volume of sales (Chainanalysis, 2020).

Apart from dark-net markets, **cryptocurrencies are commonly employed in various cybercrime activities**. The Chainanalysis study reported a surge in the number and the value of cryptocurrency transactions related to cyber scams – such as Ponzi schemes, blackmail scams, online investment scams and phishing – which in the period 2017–2019 outweighed dark-net markets in the share of overall illicit transactions, and now constitute the overwhelming majority of cryptocurrency-related crime (Chainanalysis, 2020). According to their analysis, over 2.4 million individual transfers were related to six individual Ponzi schemes in 2019. The use of cryptocurrencies in the context of various cybercrimes (e.g. ransomware, crypto jacking, phishing and fraudulent cryptocurrency investment schemes) was also confirmed by interviews conducted with experts[172].

Box 3.7: Use of cryptocurrencies in ransomware attacks

Ransomware attackers use cryptocurrencies as a preferred payment method, since the blockchain system and decentralised nature of cryptocurrencies provide a level of anonymity and are typically not subject to banking regulation or oversight. Malicious actors prefer to request ransoms in bitcoins, since it is the cryptocurrency with the highest liquidity and is easier to hide high volumes of funds inside the network[173]. In addition, bitcoin is still the most publicly known cryptocurrency and it might be easier for victims to obtain it in order to pay the ransom. Nevertheless, cryptocurrencies are new to many of victims and it takes some effort and time to make and verify an account on cryptocurrency exchangers. A study suggested that a low pay-out ratio might be caused exactly by this complexity of complying with the cybercriminals' demands (Kshetri & Voas, 2017).

As ransomware payments are predominantly made in bitcoins, perpetrators use money-laundering tools in the bitcoin ecosystem – or a combination of these tools – to launder the proceeds and cash-out[174]. A substantial number of bitcoin mixing and exchange services, or overall cryptocurrency money-laundering

[170] Interview with an UK cybersecurity company expert, 25 March 2020 (#56).
[171] Interview with UK cybersecurity company expert, 25 March 2020 (#56).
[172] Interview with academic expert, 25 February 2020 (#35); Interview with UK cybersecurity company expert, 25 March 2020 (#56); Interview with EU stakeholder, 12 March 2020 (#48); Interview with EU stakeholder, 22 April 2020 (#73).
[173] Interview with law enforcement representatives, 12 March 2020, #48.
[174] Interview with Europol representatives, 12 March 2020, #48; Interview with International organisation representative, 25 February 2020, #73.

services, are also offered on dark-web websites. An interview with law enforcement officers suggested that the use of a combination of money-laundering tools in the cryptocurrency ecosystem could also be more cost-efficient than traditional cash-out schemes[175].

3.5.3. E-money and related services

Electronic money or e-money is a digital representation of a fiat currency, and is used to electronically transfer value denominated in the fiat currency. This is also the main difference between e-money and cryptocurrencies – the latter are also a digital representation of value, but are not issued nor guaranteed by any jurisdiction (FATF, 2014). According to the Commission the defining characteristic of e-money is its prepaid nature, since a card, mobile device or online account needs to be credited with a monetary value for that value to constitute e-money. E-money and related services include two main types of NPM: prepaid cards and digital and mobile wallets. These two types of e-money products differ by the way e-money is stored – the first can be classified as 'hardware-based' and the latter as 'server-based' (European Commission, 2017b).

Prepaid cards

The ECB defines prepaid cards as cards on which a monetary value can be loaded in advance and stored either on the card itself, or on a dedicated account on a computer (European Central Bank, 2020). Prepaid cards have been reported to be misused for criminal purposes in relation to drug trafficking, THB, prostitution (European Commission, 2017b) and cashing out in cases related to cybercrime (Europol, 2018c; Sat et al., 2016).

Extent of use for criminal and money-laundering purposes

Although our desk research identified no estimates about the extent of use of prepaid cards for criminal and money-laundering purposes, all the identified reports indicated widespread use. Thus, Commission reports about multiple cases reported by FIUs across Member States and Europol noted an increasing use in the context of cybercrime (European Commission, 2017b; Europol, 2018c). Bulanova-Hristova et al. (2016) also stated that prepaid cards and vouchers are widely used for money-laundering in the context of cybercrime. One of the interviewed national-level law-enforcement experts in Belgium also outlined the growing popularity of prepaid vouchers that allow payment of various services online in the context of various cyber frauds[176].

Digital and mobile wallets

Digital and mobile wallets are electronic applications that offer customers easy access to funds – through cards or other payment instruments, and other data – in order to make payments for goods or services, in stores or online over the internet (EBA, 2018). Abuse of digital and mobile wallets has been documented in certain cybercrimes such as phishing, online child sexual exploitation, as well as for money-laundering purposes (Europol, 2018c; McGuire, 2018). Additionally, an interviewed national-level expert reported that these services are commonly abused in IPR infringement crimes[177].

Extent of use for criminal and money-laundering purposes

Since both mobile and electronic transactions are highly vulnerable to social engineering schemes (e.g. phishing), they are often used as a point of infiltration for potential abuse for criminal and money-laundering purposes (US Payments Forum, 2018). Although the existing research is inconclusive about the extent of this use, sources suggest that it is substantial, especially in regard to cybercrimes. Europol reports that perpetrators in child online sexual exploitation cases generally use such online payment systems (Europol, 2018c). The Anti-Phishing Working Group reports that in 2016 PayPal was one of the top four targets of global phishing attacks (Aaron & Rasmussen, 2017). Compromised accounts are subsequently sold on the dark net and/or used for money-laundering purposes. McGuire (2018) argues that in nearly 20% of cybercrime cases digital payment systems – such as Paypal, Skrill, Dwoll, Venmo, Xoom, Popmoney and Square Cash – and mobile-payment systems – like Kenya's M-Pesa – are used for money-laundering purposes. According to an interviewed UK cybersecurity expert, cybercriminals usually target digital services that are popular and have a large customer base,

[175] Interview with Europol representatives, 12 March 2020, #48.
[176] Interview with Belgian national-level stakeholder, 27 March 2020 (#59).
[177] Interview with Swedish national-level stakeholder, 10 March 2020 (#43).

therefore some of the new products and services have yet to experience such attacks or abuse for criminal purposes[178].

Common money-laundering schemes involving mobile and digital wallets are the so-called micro-laundering schemes, whereby large sums are broken down and transferred via numerous low-value transactions (McGuire, 2018; Richet, 2013). Digital and mobile wallets can also be abused for money-laundering purposes through high-value purchases on online trade platforms, which are then resold on the black market (McGuire, 2018). Such schemes often involve use of money mules, who transfer funds through their accounts or are used to withdraw the money in cash (McGuire, 2018; Mikhaylov & Frank, 2016). Europol reports that such money-mule networks that transfer money or 'cash-out' from such compromised digital accounts or compromised bank-card accounts comprise the most common modus operandi with regard to cybercrime (Europol, 2015d).

Box 3.8: Use of new payment methods in phishing attacks

Digital payment systems and forms of electronic cash are used as a target in the perpetration of phishing attacks and to launder the proceeds from the commission of cybercrimes (McGuire, 2018). Digital payment providers are a preferred target of phishing attacks as they usually communicate with their customers via email and telephone messages, which creates an opportunity for perpetrators to effectively deceive users.

Once the user's credentials are stolen, the cybercriminal could either use the digital payment accounts themselves to withdraw available balance, buy goods and services and/or sell the credentials on the online underground markets (Trend Micro, 2011). PayPal accounts obtained through phishing are one of the common commodities on the dark net (McGuire, 2018). Such packages of accounts obtained on the dark net could be used in PayPal micro-laundering schemes. The low prices of such stolen credentials have also led authors to suggest that making use of the stolen data is either very difficult or fails frequently (Florêncio & Herley, 2010; Franklin, 2007).

The selection of a payment service as a target of a phishing campaign depends to a great extent on the **payment culture in the victims' country of origin**[179]. If a particular payment service is popular and profitable among the general population in a Member State, there is a higher probability that a phishing campaign might be organised[180]. The specific target of a phishing campaign could also depend on the **origin, growth and technical expertise of the criminal network**.

3.5.4. Other innovative internet and mobile payment services

Along with digital and mobile wallets there are also several innovative online or mobile-based payment services that are regulated under the EU payment service legal framework (European Parliament, 2015). In many cases these services are integrated and complement e-money products, such as digital and mobile wallets. Others enhance or automate traditional banking products and services (e.g. debit or credit cards, bank accounts) – known as third-party payment-initiation services – providing services related to opening and operating an online (non-bank) payment account or services related to money transfers to physical persons.

Although e-money and payment services are often provided as integrated FinTech products, it should be noted that not all payment-service providers are e-money institutions as per the definition of the e-money directive (European Commission, 2009). Therefore, not all internet and mobile payment services necessarily involve provision of digital or mobile wallets to their users. The first payment-service directive adopted in 2007 allowed payment services to be delivered not only by banks and e-money institutions, but also by the so called 'payment institutions'. Some of these payment institutions are licensed to operate only in the country where they are registered. Payment institutions can provide payment services but are not allowed to take deposits or issue e-money (European Commission, 2017b). Examples of such FinTech service providers in the EU are Trustly, iDEAL, Oxlin and Transferwise, among many others.

Extent of use for criminal purposes and money-laundering

The review of literature did not identify any research papers that have examined abuse of such internet and mobile-payment services by OCGs in Europe, apart from those related to e-money products. Although Europol has discussed these innovative payment services in its Internet Organised Crime Threat Assessment (IOCTA) reports (Europol, 2014b, 2018c), they were marked as possible targets for abuse by cybercriminals and OCGs, with no accompanying

[178] Interview with UK cybersecurity expert, 30 April 2020 (#85).
[179] Interview with academia representative, 25 February 2020 (#35).
[180] Interview with Europol representatives, 12 March 2020 (#48).

indication of registered cases. The few identified papers mostly referred to other world regions, such as Africa, where mobile payment systems are widely used and regulations are weak (Hunter, 2019; Oyoo, 2020). Similarly, the interviews conducted with stakeholders rarely mentioned use of such services in the context of OCGs. An example was provided in Bulgaria, where services of a licensed payment-service provider were abused in a case related to MTIC fraud for transfer of funds between various shell companies[181]. Another example was provided in Romania, where services of a licensed payment-service provider were abused for money-laundering of funds originating from cybercrime[182].

3.5.5. Other non-banking fund-transfer methods

Among the other non-banking fund-transfer methods commonly employed by OCGs are legitimate money-transfer services – such as Western Union, Money Gram and RIA Money Transfer – as well as various informal value-transfer systems (also known as hawala). Both methods are not novel and have a long history of use. They also both involve cash-to-cash funds transfers.

Money remittance services

Money remittance (also known as wire transfer) is a **non-bank financial service that predates the FinTech revolution, where the payer gives cash to a payment service-provider's agent to make it available to the payee through another agent**. In this case the transfer of the funds occurs without any payment accounts being created in the name of the payer or the payee (European Commission, 2017b). Over the years these services have often been reported as being abused by OCGs for money-laundering purposes. In a report from 2010, FATF and Moneyval reported a variety of OCG activities related to money-remittance services, including 'drug trafficking, fraud (mainly IT-fraud like phishing); economic crimes (document forgery, malfeasance, tax evasion, etc.); THB, smuggling of migrants; theft (credit card fraud, currency theft, etc.) and smuggling (e.g., tobacco, alcohol, arms)' (FATF/Moneyval, 2010). More recent studies confirm that money remittance services are still widely used in the context of smuggling of migrants (UNODC, 2018), THB (ALEFA, 2019; CSD, 2015) and a variety of cybercrimes (McGuire, 2018; Mikhaylov & Frank, 2016).

Extent of use for criminal purposes and money-laundering

Existing reports and studies do not provide any estimates about the exact extent of the exploitation of money remittance services for criminal purposes or money-laundering. The EU supranational risk assessment of the risks of money-laundering concludes that these services are recurrently used to launder money. Considering this, the report notes that the level of money-laundering threat related to money remittance services is considered as very significant (European Commission, 2017b). The exploitation of remittance services is more pronounced in certain cross-border crimes such as smuggling in migrants and THB and various cyber scams and internet fraud, such as lottery scams, online romance and dating frauds, and family emergency scams (ALEFA, 2019; McGuire, 2018; UNODC, 2018). This was also reiterated by the interviewed EU-level and national-level experts, who also detailed that these services are used for a variety of purposes – such as to layer funds in order to obfuscate a money trail, to repatriate proceeds to countries of origin or to settle transactions between different actors in a given OCG or network[183].

[181] Interview with national law-enforcement expert, 13 March 2020 (#51).
[182] Interview with EU-level stakeholder, 22 April 2020 (#73).
[183] Interview with EU-level expert, 12 March 2020 (#44); Interview with EU-level expert, 22 April 2020 (#73); Interview with national-level expert, 10 March 2020 (#43); Interview with national-level expert, 27 March 2020 (#59).

Box 3.9: Wire transfers used by OCGs from Southeast Europe

Proceeds from THB for sexual exploitation are typically gathered in cash. Southeast European OCGs stockpile the amounts and break them down into small sums to be transferred to the countries of origin. When money remittance services – such as Western Union – are used, traffickers use 'smurfing techniques' to wire the money (ALEFA, 2019)[184]. This practice refers to breaking up significant amounts of cash into smaller amounts. These amounts are typically transmitted by several persons. The money transferred is thus below the threshold requiring an in-depth identification of the customer. Using multiple senders and/or receivers, large sums of cash can be transferred to the countries of origin of perpetrators without raising suspicion (Europol, 2015c).

Members of the OCG rarely make the wire transfers. Rather, victims send the money to relatives or relatives of the traffickers. The sale of personal identities for the use of wire transfers by traffickers is also reported by law enforcement. Typically, the persons selling their personal identities are from impoverished groups with low levels of literacy, and are not aware of the THB operation[185]. As money-remittance services located in the EU are required to identify their customers, but any form of photographic identification is sufficient to transfer amounts below a specified threshold, traffickers use this method to avoid detection by law enforcement.

Due to heightened attention by law enforcement on money transfer operations, and cooperation from key money transfer service providers, previous research and interviews conducted for this study revealed that Bulgarian and Romanian traffickers decreasingly use money transfer services for the return of proceeds, in lieu of more intensive forms of cash smuggling (Raets & Janssens, 2019; Shentov et al., 2019)[186].

Informal value-transfer systems (hawala)

Informal value-transfer systems – such as hawala, hundi, padala and fei-chien – are used in many regions of the world for transferring funds, both domestically and internationally, and they operate outside the 'regulated' financial system (European Commission, 2017b). They are deeply rooted in historical, cultural and economic backgrounds. Informal value-transfer systems, also commonly denoted as hawala networks, appear to be susceptible to SOC abuse, and some hawala networks are particularly created to serve criminal needs (European Commission, 2017b). FATF classifies hawala networks in three general categories: pure traditional (legitimate); hybrid traditional (often unwitting); and criminal (complicit) (FATF, 2013). Use of hawala services has been reported in relation to organised crime activities such as THB and migrant smuggling (European Commission, 2017b; FATF, 2011), illicit tobacco trade (FATF, 2012) and drug trafficking (FATF, 2013). Specialised criminal hawala networks also enable other offences including tax fraud, currency offences and corruption (FATF, 2013).

Extent of use for criminal purposes and money-laundering

Despite the concerns of EU and national authorities that hawala is often exploited for criminal purposes and money-laundering, not much empirical material on the misuse of hawala banking has been published to date, and little is known about the extent of its exploitation by OCGs (European Commission, 2017b; Van de Bunt, 2008). FATF reports that rough estimates from several countries show that hawala remittances range from 10% to 50% of the total remittance market, although they also note that these estimates are based on anecdotal or partial information, and should not be taken as representative. Moreover, hawala and similar service providers also serve legitimate demand from financially excluded migrant workers, and it is not known what the ratio is between remittances for legitimate purposes and for criminal purposes (FATF, 2013).

The presence of hawala banking also differs from country to country, and in some countries regulated money-transfer agents are reportedly also used to conduct illegal transactions in addition to their regulated activities. This further complicates the task of formulating even a rough estimate of the volume of criminal money flows associated with hawala. However existing research shows that the use of hawala services is more pronounced in certain criminal markets. Thus, hawala is one of the most-used methods by OCGs involved in smuggling of migrants to the EU (Campana, 2018; Optimity Advisors, 2015; UNODC, 2018). CSD and ALEFA also report common use of hawala for transferring illicit funds in the context of THB by Nigerian and Chinese OCGs (ALEFA, 2019).

[184] Interview with EU stakeholder, 10 March 2020 (#44).
[185] Interview with national stakeholder BG, 13 March 2020 (#51).
[186] Interview with national stakeholder BG, 13 March 2020 (#51).

Box 3.10: Use of informal value-transfer systems by Nigerian OCGs

Nigerian OCGs use hawala systems to return the proceeds of THB to the country of origin (Europol, 2019d). A large part of the money transferred via the hawala systems is for the repayment of debts incurred by the families of the THB victim. Nigerian victims are often recruited in their own home, sometimes by a relative or family friend (UNODC, 2010). The victims' family is asked to pay money for their transportation and living costs. Previous studies assess that the fee demanded by traffickers can range between $35,000 and $70,000 (USD) (Campana, 2016). An interviewed law enforcement expert from Sweden referred to an amount reaching €70,000 for transfer to Sweden, a country considered a highly profitable destination[187]. These fees are thus returned to the victim's country of origin through the hawala system.

An informal value-transfer system utilised by Nigerian networks in Italy, also known as 'euro-to-euro', involves the parallel money transfer through grocery stores and other retailers. The system is based on the credibility of the intermediary within a widespread network of intermediaries located mainly in Nigeria, and with money collected in Italy. According to a recent study, the fee for transferring money through this informal system is 1–2% of the total (Shentov et al., 2019). Another recent case study on THB for sexual exploitation of Nigerian women in Oslo indicated that the hawala customers were required to pay a transaction fee of 10% (FATF, 2011).

3.5.6. Factors that influence the use of new and non-banking payment methods for criminal purposes

Anonymity of payment transactions and lower risk of tracing are attractive to criminals. Our review of literature and interviews suggested that the use of NPMs and non-banking payment methods is largely driven by several major factors – level of (perceived) anonymity and traceability of transactions, cost of transactions, global reach of transactions, regulatory gaps and constraints for law enforcement (European Commission, 2017b). For some of the NPMs and non-banking payment methods, other specific factors are also suggested to come at play. These factors are discussed in more detail below.

Table 3.14: Overview of factors influencing use of new and non-banking payment methods by organised crime groups

Factor	New and non-banking payment method	Driving (D) or Inhibiting(I) effect	Description
General factors			
Anonymity / risk of tracing	Cryptocurrencies	D/I	Cryptocurrencies provide a far higher level of anonymity than traditional non-cash payment methods – such as payments with debit and credit cards or digital wallets – although it remains still incommensurable to cash (Butler, 2019; FATF, 2014). Certain privacy-oriented cryptocurrencies are renowned for anonymity (Silfversten et al., 2020). New regulatory measures have obliged crypto exchangers to apply customer due-diligence and report suspicious transactions[188]. Extent of anonymity varies across currencies.
	Prepaid cards	D	Criminals can buy and load multiple cards just below the legally prescribed threshold that would require customer identification (European Commission, 2017b).
	Digital/mobile wallets; Other internet/mobile payment services	I	E-money issuers are regulated and obliged to perform customer identification and monitoring of suspicious transactions (European Commission, 2017b)[189].
	Money remittance	I	Regulatory measures have been introduced in

[187] Interview with national stakeholder SE, 10 March 2020 (#43).
[188] Interview with Luxembourg national-level stakeholder, 27 March 2020 (#58).
[189] Interview with Belgium national-level stakeholder, 27 March 2020 (#59); Interview with Luxembourg national-level stakeholder, 27 March 2020 (#58).

Factor	New and non-banking payment method	Driving (D) or Inhibiting(I) effect	Description
	services		many jurisdictions around the world, limiting anonymity (Western Union, 2020).
Speed and global reach of transactions	Cryptocurrencies	D	Average transaction time for cryptocurrency transaction of 10 min. to 1 hour, whereas banks require 3–4 working days for international transactions (Butler, 2019). Global reach (Mikhaylov & Frank, 2016).
	Digital/mobile wallets Other innovative and mobile payment services	D	Transactions typically occur in real time, allowing for rapid transaction layering. Global reach (Di Castri et al., 2015; FATF, 2013; Mikhaylov & Frank, 2016).
	Money remittance services	D	Varies but is generally faster than bank payment methods. Global reach (European Commission, 2017b; FATF/Moneyval, 2010).
	Hawala and similar services	D	Generally, transactions can be settled in a few hours, or at the most in one or two days (FATF, 2013; Soudjin, 2015).
Cost of transactions and cost for circumvention of existing regulatory constraints	Cryptocurrencies	D	Most cost-efficient compared to other traditional methods for money-laundering and cross-border transactions (Bryans, 2014; Dabrowski & Janikowski, 2018)[190]. Bitcoin transaction cost in 2019 was as low as $0.35 (Butler, 2019).
	Digital/mobile wallets Other innovative and mobile payment services	D/I	Generally lower than bank fees, although regulations limit the balance and frequency of e-money transactions and eventually raise overall costs for criminals (Chatain et al., 2011).
	Money remittance services	D/I	Generally lower than bank fees, although regulatory restrictions additionally raise costs for money-laundering (Western Union, 2020).
	Hawala and similar services	D	Providers usually charge 25–50% of the equivalent bank charge (depending on destination) and offer better exchange rates than banks (FATF, 2013b; Soudjin (2015)).
Regulatory gaps, customer due-diligence	Cryptocurrencies	D	New regulatory measures for exchangers provide monitoring and tracing capabilities to police and have increased the perceived risks for criminals (Butler, 2019; Fanusie and Robinson, 2018).[191]
	Prepaid cards	D/I	Limits on the maximum amounts stored, transferred and withdrawn are often complemented by fraud prevention and consumer-protection controls (European Commission, 2017b; HM Treasury and Home Office, 2017).
	Digital/mobile wallets Other innovative and mobile payment services	D	Start-ups and smaller FinTechs lack the capacity to implement customer due-diligence policies (European Commission, 2017b).
	Money remittance services	I	Many countries around the world have increased their regulatory oversight on money remittance services and introduced new AML measures, such

[190] Interview with EU stakeholder, 12 March 2020 (#48).
[191] Interview with UK cybersecurity expert from the private sector, 25 March 2020 (#56).

Factor	New and non-banking payment method	Driving (D) or Inhibiting(I) effect	Description
			as additional requirements for customer due-diligence and suspicious transaction reporting (Western Union, 2020).
	Hawala and similar services	D	Not subject to any regulatory control, and disregards official banking obligations for identification of clients, record keeping, and the disclosure of unusual transactions (ALEFA, 2019; European Commission, 2017b; FATF, 2013; FATF/Moneyval, 2010).
Capabilities of law enforcement agencies and jurisdictional constraints	Cryptocurrencies	D	Attractive to perpetrators due to constraints in jurisdictional power, information exchange, national differences in regulatory frameworks, and technological challenges (requires equipment and expertise to use it)[192].
	Prepaid cards	D	Prepaid cards fall outside cash regulation in many jurisdictions and are not subject to customs declarations (Europol, 2015d).
	Digital/mobile wallets Other innovative and mobile payment services	D	Jurisdictional constraints and differences in legal frameworks can severely limit police investigations (Di Castri et al., 2015; FATF, 2013; Mikhaylov & Frank, 2016)[193].
	Money transfer services	I	Increased scrutiny from law enforcement authorities has decreased use of money remittance services by OCGs (CSD, 2015).
	Hawala and similar services	N/A	No data.
Specific factors			
Need for technical expertise	Cryptocurrencies	I	Lack of technical knowledge has been attributed as a primary inhibiting factor for criminals (European Commission, 2017b; Silfversten et al., 2020).
Volatility of (cryptocurrency) markets	Cryptocurrencies	I	Most of the widely used cryptocurrencies are well known for the volatility of their value (European Commission, 2017b; Silfversten et al., 2020)[194].
Risk of fraud by hackers and managers of crypto exchangers	Cryptocurrencies	I	Europol reports increasing attacks and frauds targeting cryptocurrency services (Europol, 2018d).
Sale of compromised accounts	Digital/mobile wallets	D	Compromised accounts are sold on the dark net – for example 100 PayPal accounts can be bought for $100 on average (McGuire, 2018).
Wide acceptance in society	Prepaid cards	D	The possibility to use prepaid cards for payment of goods and services in the EU is relatively high (European Commission, 2017b).
Simplicity to use	Prepaid cards	D	Do not require specific knowledge (European Commission, 2017b).
	Money transfer services	D	Money transfers do not require specific knowledge or planning in order to use (European Commission, 2017b; FATF/Moneyval, 2010).

[192] Interview with EU-level stakeholder, 12 March 2020 (#48); Interview with national-level law enforcement stakeholder, 27 March 2020 (#59).
[193] Interview with Belgian national-level expert, 27 March 2020 (#59).
[194] Interview with EU-level stakeholder, 12 March 2020 (#48).

Factor	New and non-banking payment method	Driving (D) or Inhibiting(I) effect	Description
Cash-to-cash character of transactions	Money transfer services	D	Particularly convenient for cross-border crimes, such as THB that generate cash proceeds in small amounts on a regular basis[195].
	Hawala and similar services	D	Criminal hawala networks often offer services such as collection, hoarding, transportation and safe-keeping of cash (FATF, 2013; Soudijn, 2019).
Ability to transfer large sums	Hawala and similar services	D	Transfer of tens or even hundreds of thousands of euros are carried out for criminal clients (Europol, 2017c; Soudjin, 2015; Van de Bunt, 2008).
Additional financial services	Hawala and similar services	D	Offers additional banking services such as currency exchange, changing smaller denominations into €500 notes – which are no longer printed, but still in circulation – (and vice-versa), holding escrow accounts and trade guarantees, short-term lending and even safe-keeping of funds (FATF, 2013b; Soudijn, 2019).
Smooth illegal transactions	Hawala and similar services	D	Hawala service-providers often act as a trusted third party and guarantee illegal transactions (Van de Bunt, 2008; FATF, 2013b; Optimity Advisors, 2015).
Cultural preference	Hawala and similar services	D/I	Some areas in Central and South Asia, the Middle East and North Africa use these services predominantly, to the point where they become part of financial culture (FATF, 2013b; Soudjin, 2015)[196].

3.5.7. Recommendations

Key findings and related recommendations stemming from this part of the study are summarised in the table below.

Table 3.15: Recommendations – New and non-bank payment methods

Key finding	Recommendation	Actor
Cryptocurrencies are regularly used in most types of cybercrime, particularly the illicit trade through dark-net markets. Institutions providing novel internet/mobile payment services are often less aware of money-laundering risks and have insufficient knowledge of AML rules, especially start-ups and smaller FinTech companies.	Continued enforcement of the regulations governing the conversion of virtual to fiat currencies since the 5th AMLD. Ensure support for FATF in pursuing worldwide adoption and implementation of regulations governing the virtual currency service providers. Enlarging the scope of 5th AMLD regarding cryptocurrency service providers and cryptocurrency exchangers, to include service providers that provide crypto-to-crypto exchange. Member States should further enhance their law enforcement capabilities for analysis and investigation of illicit cryptocurrency transactions. Member States should further	Member States (law enforcement and judicial authorities, FIUs) European Commission, FATF European Parliament

[195] Interview with EU level stakeholder, 12 March 2020 (#44).
[196] Interview with an EU level expert, 12 March 2020 (#17); Interview with a Swedish national level expert, 10 March 2020 (#43).

Key finding	Recommendation	Actor
	increase regulatory oversight and provide additional AML training to staff of start-ups and smaller FinTech companies.	

3.6. Possible emerging threats

Emma Louise Blondes and Sam Cole, RAND Europe

Key findings:

- Brexit might entail money-laundering risks due to regulatory gaps.
- Golden visa schemes continue to vary in their requirements across the EU, presenting opportunities for illicit investments.
- Cash and high-value goods will continue to pose a threat to anti-money-laundering efforts.
- The green economy could be exploited by OCGs as it continues to grow.
- SARS-CoV-2 (Covid-19) may present opportunities for OCGs, particularly with regard to the volatile economic condition, the increasing number of non-cash payments, and increased risk of corruption.
- FinTech services are predicted to be a new target for OCGs, with new payment methods facilitating the laundering of illicit funds.

Literature review	Interviews
	

This section considers some emerging threats that may be exploited by OCGs to manage and transfer criminal finances. Our analysis sought to identify key external factors shaping the future management of criminal finances by OCGs over the next five years (2020 to 2025), as distinct from identified market trends and the modus operandi of investments discussed in preceding sections. The table below summarises the trends identified using the Political, Economic, Social, Technological (PEST) framework. This is not an exhaustive futures analysis, but offers some emerging insights gleaned from the literature and interviews with experts.

Table 3.16: Summary of PEST trends and sources

	Future trend shaping management of criminal finances by OCGs 2020–2025	Sources				
		Stakeholder interviews	Academic published literature	Grey literature	News sources	Blog posts & practitioner commentary
Political	Brexit	X	X	X	X	X
	Golden visas	X		X	X	
Economic	Cash and high-value goods	X		X		
	Green economy	X	X	X		
Social	COVID-19 pandemic			X		
Technological	FinTech & NPMs	X		X		

3.6.1. Political

Brexit might increase money-laundering risks due to regulatory gaps

Given the backdrop of political uncertainty leading up to the final Withdrawal Agreement in 2019 (European Union, 2019a), the perceived impact of a 'no deal' Brexit was predicted to **leave gaps or inconsistencies in criminal justice enforcement that could be exploited by OCGs** (National Audit Office, 2019). Despite declarations seeking 'comprehensive, close, balanced, and reciprocal law enforcement and judicial cooperation in criminal matters' (European Union, 2019b), the possibility remains that an agreement on such matters may not be reached by the end of the current transition period; without an extension, this would mean cooperation would be conducted through alternative regional instruments, such as the 1957 European Convention on Extradition and the 1959 European Convention on Mutual Assistance in Criminal Matters (Plachta, 2020).

- It is evident that the UK will seek some divergence from EU harmonisation measures. Whilst the UK government confirmed it would implement measures of the 5th AMLD[197] (including key innovations relating to virtual currencies), the UK government decided not to be bound by the 6th AMLD, stating that domestic UK legislation was already 'largely compliant' (Home Office, 2018a). Such exclusion from measures facilitating swift recognition of asset freezing and confiscation orders between Member States could possibly have a **detrimental impact upon the UK's priorities to 'deny the most dangerous and determined criminals access to their money and assets'** (Grimes, 2019). Given the transactional nature of trade-based money-laundering, many blog posts and commentary from industry and policy experts highlight the importance of swift information exchanges in disrupting such capital flows (Keatinge, 2016); without this the UK may make 'London's dirty money fight harder' (Vincent, 2020). Despite structures such as the FATF and membership of the Egmont Group of FIUs existing outside of EU membership, they are identified as being focused on policy rather than on the operational realities of disrupting such crimes (Keatinge, 2016).
- Other writers submit that whilst the UK is already largely compliant with the 6th AMLD, one area of divergence may be with regards to the corporate offence of failing to prevent money-laundering (Binns, 2019). If it does not implement such legislation, the UK could become an outlier for money-laundering through legitimate businesses. Divergence in the UK context also has a much wider reach, given the number of UK Crown Dependencies and Overseas Territories already identified as 'among the worst offenders for enabling secrecy company ownership' (Young, 2016). Leaving the EU may therefore create a 'cordon sanitaire where nobody questions the financial secrecy of Britain's offshore territories', existing outside of the EU AML framework and without answer to the Commission (Young, 2016).
- Predicted changes to SOC trends are also evident outside of the UK–EU cooperation in criminal matters. With the UK government stating that it will no longer be a part of the EU single market (HM Government, 2020b), this is suggested to reduce the risk of MTIC fraud being carried out in the UK. Rather than reducing overall levels, **such fraud will likely be driven elsewhere in the EU** (KPMG, 2016).
- One aspect of the UK's future economic policy is to increase the number of operational Freeports by creating up to 10 such ports across the UK (HM Government, 2020a). Freeports are designated areas that, while located geographically within a country, exist outside of its border for tax purposes; companies operating within them can therefore defer or avoid the payment of taxes on goods brought in for storage or manufacture on-site ahead of subsequent export (Partingdon, 2019). The UK government recently published a consultation paper outlining its proposals, in which it recognised concerns about the links between Freeports and illicit cross-border activities (Partingdon, 2019). In light of known risk factors associated with freeports – including assessments of the potential for illicit trade in counterfeits, money-laundering, tax evasion and customs duties evasion – RUSI identified that the UK's proposals lack provision for assessing existing criminal risks in the areas where freeports will be established (RUSI, 2020). Whilst the legislative AML regimes were unlikely to differ from those operating in the rest of the UK, concerns remained that a light-touch authorisation approach could mean freeport operators are not risk-assessed on their ability to carry out security-related responsibilities (RUSI, 2020). The extent to which this is a future investment trend

[197] Anti-money-laundering (AML) – Directive (EU) 2018/843.

depends upon the freeports' success and consequent use; if successful however, they are said to appeal to both legitimate businesses and criminals alike (RUSI, 2020). Such concerns were echoed by one interviewee, who identified that Freeports would significantly affect the illicit trade of tobacco[198].

- One interviewee noted that the UK's withdrawal and divergence from EU waste directives (European Commission, 2020e) could make it more attractive to white collar criminal actors in the waste market[199].

Golden visa schemes continue to vary in their requirements across the EU, presenting opportunities for illicit investments

Most EU Member States have either a citizenship by investment or residency by investment scheme. The European Parliament noted an 'increasing trend' in marketizing citizenship for wealthy individuals (European Parliament, 2019). In the 10 years prior to 2018, the EU welcomed 6,000 new citizens and close to 10,000 new residents through such 'golden visa' schemes (Transparency International, 2018). With such growth recognised, evidence suggests that this may present opportunities for illicit investments, with due-diligence checks in some Member States identified as insufficient. However, understanding the scale of golden visa misuse, rather than use, is difficult – despite a suggested increase in public interest, Transparency International state that 'secrecy continues to enshroud the most basic information about golden visas' (Transparency International, 2018). Media reports evidenced by 'leaked documents' have linked individuals accused of bribery and large-scale corruption to citizenship and residency investments in Portugal (Pegg, 2017) and Cyprus (Farolfi et al., 2017).

- The European Commission created a Group of Member State experts on Investor Citizenship and Residence Schemes in the EU to collaboratively address this issue. The expert group published a comprehensive report in January 2019, which outlined its concerns that **investor citizenship and residence schemes create risks to the security of Member States and the Union**, with the possibility of infiltration from non-EU OCGs, money-laundering, corruption and tax evasion (European Commission, 2019b). The expert group also put forward recommendations to mitigate some of the risks presented in the report.
- Member State schemes vary in their investment criteria, with some requiring a low physical presence in the country, facilitating only passive investments (European Parliament, 2019). Cyprus and Portugal have been identified as operating insufficient due-diligence checks and failing to take account of an applicant's source of funds or wealth when analysing applications (Transparency International, 2018). Maltese officials were also identified as having wide discretion when assessing an applicant's eligibility (Transparency International, 2018). The Hungarian Investment Immigration Programme was terminated in 2018, with Transparency International identifying it as a 'unique example of mismanagement, discretionary decision-making and opaque governance' (Transparency International, 2018). **Without a clear criteria and due-diligence checks, golden visa programmes are therefore said to be at higher risk of misuse by individuals investing proceeds of crime** (Transparency International, 2018).
- The 5th AMLD introduced an amendment requiring enhanced due diligence for third-country nationals who apply for residency rights or citizenship in Member States in exchange for capital transfers, or investments in corporate entities. However, the Commission notes that these obligations apply only to economic operators, not governmental organisations or agencies – identified as the authorities responsible for investor citizenship (European Commission, 2019b). One interviewee noted that without the political will in Member States to implement preventative measures, **golden visas will continue to be a persistent, rather than emerging, illicit investment trend**[200].
- Global estimates suggest that **the broad demand for golden visas will continue to increase**, with wealthy individuals and investors viewing residency and citizenship as alternative assets (Henley and Partners, 2020). Henley and Partners – who advertise themselves as a 'global leader in residence and citizenship planning' – identified that

[198] Interview with academic stakeholder, 19 February 2020 (#7).
[199] Interview with national-level stakeholder, 3 March 2020 (#10).
[200] Interview with EU-level stakeholder, 26 February 2020 (#8).

some 36% of ultra-high net worth individuals hold an alternative passport, up from 34% in 2018. Cyprus, Greece, Malta and Portugal were identified as smaller nations welcoming high-net worth individuals in large numbers, partly due to their membership of the EU (Henley and Partners, 2020).

- In the context of COVID-19, Henley and Partners revealed that **applications for 'pandemic passports' increased 42% compared with 2019** (Aldridge, 2020).

3.6.2. Economic

Cash and high-value goods will continue to pose a threat to anti-money-laundering efforts

According to Europol's 2015 analysis and our assessment in Section 2.5, **cash remains the preferred method used to launder** proceeds of crime (Europol, 2015d). In 2019, the EU's Supranational Risk Assessment Report signalled that dealers in high-value goods accepting cash payments continue to pose a threat for AML efforts (European Commission, 2019c). The Supranational Risk Assessment Report also reported that cash-like assets – such as gold or diamonds or easily tradable 'lifestyle' goods, such as cultural artefacts, cars or jewellery – are commonly used to launder money due to weak controls (European Commission, 2019c). One interviewee explained that OCGs purchase high-value goods because they are difficult to trace, and are less suspicious than large amounts of cash, specifically when crossing borders[201]. They can also be easily sold in exchange for cash as required.

Despite measures to increase the legal limits of cash payments and the 5th AMLD's efforts to expand the range of high-value goods transactions subject to regulations, two stakeholders emphasised the ongoing risks associated with high-value goods, cash-like assets and easily tradable 'lifestyle' goods[202]. The difficulties in regulating the flow of cash and high-value goods across the EU look likely to persist over the next five years.

- One interviewee specifically mentioned the growing practice of buying second-hand car garages, high-value watches and expensive clothing for money-laundering purposes[203]. Transparency International also stressed that many high-value retailers operating in the luxury sector fail to comply with due-diligence and reporting obligations, creating opportunities for money-launderers (Transparency International, 2017).
- Another interviewee stressed that gold was still frequently used to move money outside of Europe. However, the interviewee warned that OCGs are likely to exploit other loopholes in the system as gold becomes more strictly regulated[204].

The green economy could be exploited by OCGs as it continues to grow

According to the desk research and stakeholders interviewed in the context of this study, the growing European green economy – marked notably by the von der Leyen Commission's European Green Deal, which set out a roadmap to address climate and environmental challenges by making Europe's economy more sustainable (European Commission, 2019a) – could present risks for the placement and transfer of criminal finances by OCGs specifically in the absence of harmonised regulations:

- Two stakeholders highlighted the risk of **OCGs further exploiting the European Carbon credits market** for money-laundering purposes[205]. Recent investigations demonstrated that OCGs penetrated the European carbon-trading market at a time when authorities were unprepared, taking advantage of the markets' weak regulations[206]. While Carbon Trading Crime includes a range of criminal activities, including Value Added Tax (VAT) Fraud, Interpol notes that OCGs have also infiltrated this market to launder proceeds of crime (Interpol, 2013). One interviewee suggested

[201] Interview with EU-level stakeholder, 11 March 2020 (#14).
[202] Interview with national-level stakeholder, 28 April 2020 (#77). Interview with EU-level stakeholder, 11 March 2020 (#14).
[203] Interview with national-level stakeholder, 28 April 2020 (#77).
[204] Interview with national-level stakeholder, 28 April 2020 (#77).
[205] Interview with EU-level stakeholder, 11 March 2020 (#15); Interview with EU-level stakeholder, 26 March 2020 (#62).
[206] Interview with EU-level stakeholder, 26 March 2020 (#62).

that OCGs would continue resorting to such tactics until harmonised measures are implemented across all EU Member States[207].

- Three studies suggested that **some OCGs are investing in wind farms across Italy** to penetrate the legitimate economy and launder proceeds of crime (Caneppele et al., 2013; Di Natala, 2013). Interpol also signalled this trend at a global scale (Interpol, 2013). According to Caneppele et al. (2013), such practices were facilitated in part by loosely regulated government incentives to promote the green economy. Whilst evidence of OCG investments in windfarms have only been uncovered in Italy, law enforcement has increasingly shed light on carbon credit money-laundering schemes, creating uncertainty around the continuation of this trend over the next five years.
- **In July 2020, the EU adopted a recovery plan to respond to the economic and social damages caused by the COVID-19 pandemic, which could be exploited by OCGs** (European Commission, 2020f). The plan includes a temporary recovery instrument, Next Generation EU, which will provide €750-billion of grants and loans to boost EU economies. Through this fund, the von der Leyen Commission seeks to support projects aligned with the EU's green transition. Thus, as suggested above, there is a risk that OCGs will take advantage of these emergency funding schemes to manage and transfer proceeds of crime. Further, the EU's potential use of green bonds as part of its recovery plan could present money-laundering opportunities for OCGs (Khan, 2020).

3.6.3. Social

COVID-19 may present opportunities for OCGs

The COVID-19 pandemic, which developed as of December 2019, rapidly resulted in a global health crisis that brought severe socio-economic challenges. In a report dated 20 April 2020, Europol analysed how some of these challenges might be exploited by OCGs in Europe (Europol, 2020a). The analysis included predictions on the placement and investment of criminal finances by OCGs, which are detailed below:

- Europol predicted that OCGs may **take advantage of the current volatile economic situation to launder money using onshore financial systems**. According to Europol, OCGs could shift their money-laundering practices to countries outside of the EU, where AML frameworks are weaker and financial systems are less resistant to introducing large amounts of capital originating from dubious sources at times of precarious economic stability (Europol, 2020a).
- Recent evidence suggests that the COVID-19 emergency has led to an increasing use of digital payments, including mobile and online payment methods, due to a push towards online trade (PWC & Strategy, 2020). Europol stipulates that the **mounting number of non-cash payments** experienced during the COVID-19 crisis could be sustained in the future (Europol, 2020a). As such, Europol expects OCGs to increasingly seek new laundering practices using non-cash payments, alongside traditional investments in cash-intensive businesses (Europol, 2020a).
- Additionally, the Council of Europe's Group of States against Corruption (GRECO) published a statement in April 2020 warning Member States about corruption risks in the light of the pandemic (Council of Europe, 2020). GRECO suggested that recent emergency responses to the crisis, such as economic relief and research and development funding schemes could present **money-laundering risks linked to corruption**. This statement echoes the threat mentioned above, concerning OCGs exploiting the EU's recovery plan to address the COVID-19 pandemic's economic and social effects.

There are also some emerging trends due to Covid-19 in relation to specific criminal markets:

- **Illicit drugs**: In November 2020, Europol stated that although the supply of some European drug markets was disrupted at the onset of the pandemic, the overall impact of the crisis appears to have been limited (Europol, 2020c). However, Europol indicates that the initial disruptions might have led to fluctuations in drug prices in EU drug markets. Lockdown measures also reportedly affected demand for certain drugs, such as MDMA, which is usually consumed in recreational settings. The EMCDDA's preliminary analysis of the impact of Covid-19 pandemic on selected online markets highlighted that

[207] Interview with EU-level stakeholder, 26 March 2020 (#62).

online cannabis sales increased on selected dark-net platforms between January and March 2020 (EMCDDA, 2020a). Nonetheless, these trends should not be overstated given the preliminary nature of the assessments.

- **THB**: Due to the economic, social and financial impacts of Covid-19, Europol refers to increased demand for trafficking of people for sexual and labour exploitation (Europol, 2020a).
- **Smuggling of migrants**: It is likely that the increasing limitation in cross-border travel will have lasting effects on the market. According to the Global initiative against transnational organised crime (2020), difficulties may stem from increased pressure on smugglers to cease operations in their communities in order to reduce the risk of contagion, and increased vulnerability as 'tested' routes are closed and alternatives must be found. The report provides the example of the weekly convoy between Agadez and Dirkou in Niger, which was cancelled due to the pandemic. This drives up both the price and risk of the operations. A temporary increase in the stationary migrant population. Those migrants caught by border closures during their journey will be forced to remain where they are until the restrictions are eased. This links to a high risk of humanitarian disaster if the virus, or indeed other illnesses spread in camps.
- **IPR infringements**: The Anti-Counterfeiting Group (2020), EUIPO (2020a) and Europol (2020c) noted the growing supply of counterfeit face masks, hand sanitisers, testing kits, thermometers, cleaning products, indoor sports equipment and even Covid-19 treatment drugs. The illicit sales of such products have predominately been on the surface web, and targeted advertisements have been used to drive up sales (Europol, 2020c). Europol (2020c) noted that OCGs have demonstrated adaptability in their business model in the face of the pandemic.
- **Food fraud**: The economic crisis in 2008 increased motivation for food fraud (Gee & Button, 2019) and similar trends may be observed due to Covid-19.
- **Cybercrime**: Europol (2020c) reported that cybercriminals have exploited individuals' reliance on digital solutions during Covid-19. Some emerging trends include phishing emails through spam campaigns with specific reference to Covid-19, and the growth in malware, ransomware and malicious apps using Covid-19 as a lure (Europol, 2020c).

3.6.4. Technological

FinTech services are predicted to be a new target for OCGs, with NPMs facilitating the laundering of illicit funds

In its 2019 risk assessment, the European Bank Authority identified FinTech as a potential challenge for AML efforts[208]. There is strong growth in the availability and cheapness of FinTech remittance transfers in the Global North and South; however, OCGs are still said to rely more on cash than NPMs to launder proceeds, with these new methods recognised as being supplementary at present (see also Section 3.5). Europol & Eurojust (2019) report that ineffective international cooperation with some countries could result in **emergence of 'online criminal hot spots and (virtual) safe havens'**.

- **Interviewees noted that NPMs represent both opportunities and risks for money-laundering**: NPMs will allow law enforcement to trace all the transactions, but because of their speed and accessibility criminals will use them frequently[209]. This will also be driven by poor access to banking services in other parts of the world like Africa, where more and more people rely on mobile payment services.[210] One interviewee noted that OCGs will likely target the most popular FinTech products and services, since in these crimes scale is very important[211].
- **Europol suggests that the use of cryptocurrencies by SOC perpetrators will generally continue to grow**, eventually allowing OCGs to anonymously exchange and use financial resources on an unprecedented scale without the need for complex and cost-intensive money-laundering schemes (Europol, 2015b). Cryptocurrencies are

[208] Joint Opinion of the European Supervisory Authorities on the risks of money-laundering and terrorist financing affecting the European Union's financial sector, JC2019 59, 4 October 2019.
[209] Interview with EU-level stakeholder, 12 March 2020 (#48).
[210] Interview with Luxembourg national-level stakeholder, 27 March 2020 (#58).
[211] Interview with UK private-sector cybersecurity expert, 4 May 2020 (#75).

expected to change the criminal landscape, since they enable individuals to act as freelance criminal entrepreneurs operating on a crime-as-a-service business model, receiving payment in cryptocurrencies and negating the need for a sophisticated criminal infrastructure to receive and launder money. This tendency is suggested to make the role of freelancers even more prominent and allow OCGs more easily to outsource specialised activities at little risk to themselves (Europol, 2015b).

- There is a growing tendency towards the **proliferation and use of automated decentralised cryptocurrency exchanges**, which does not require know-your-customer on the part of users, allowing them to remain anonymous (Europol, 2018c). Europol further suggests that implementation of the 5th AMLD – which requires cryptocurrency platforms and custodian wallet providers to apply full customer due-diligence and report suspicious transactions – may result in an **increase in criminal exchange services operating on the dark net**, as the criminal community respond to regulatory developments (Europol, 2019a). Europol identified a likely increase in exchanging fiat and cryptocurrencies given that these fall outside of the regulated sector (Europol, 2019a). The exchanger that maintains the platform only collects fees for linking the two parties – a model that is structured in such a way that it falls out of the scope of the 5th AMLD[212].
- Chainalysis – a company providing compliance and investigation software to banks, businesses and governments – suggests that anonymous, decentralized (peer-to-peer) exchange services will continue to gain popularity with criminals, gradually replacing the current centralised mixing services ('third party custodial mixers') (Chainanalysis, 2020). **Criminals will begin to favour cryptocurrency swapping services** ('chain-hopping') as an alternative to third-party mixing (Chainanalysis, 2020).
- **A pronounced shift towards more privacy-orientated currencies** is likely, which will additionally provide faster transaction times, lower transaction fees and less price volatility compared to bitcoin. Chainalysis highlights that privacy-focused currencies such as Monero could eventually become the main currency of choice for criminals in the coming years (Chainanalysis, 2020). Europol also expects the shift towards privacy-focused currencies to lead to the **gradual decline of existing cryptocurrency mixing services** (Europol, 2018c).
- **Growth is expected in targeting of cryptocurrency exchangers and other cryptocurrency depositories by hackers**, since the profits of a successful hack can be comparably profitable and inherently easier to launder (Europol, 2018c).
- **New ways for cryptocurrency users to avoid regulatory interference might evolve** (Paesano, 2019). The recent development of 'lightning network' technology for bitcoin allows transactions that have taken place to not be published on the blockchain (Paesano, 2019).

[212] Interview with Luxembourg national-level stakeholder, 27 March 2020 (#58).

References

Aaron, G., & Rasmussen, R. (2017). 'Global phishing survey: Trends and domain name use in 2016'.

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). 'Markets for cybercrime tools and stolen data: Hackers' bazaar'. Santa Monica, CA: RAND Corporation.

Aldridge, J. (2020). 'The Ultra-Rich Are Now Buying "Pandemic Passports" So They Can Move to Safer Countries'. *Robb Report*, 4 May. Retrieved from: https://robbreport.com/travel/destinations/super-rich-buying-pandemic-passports-multiple-nationalities-2918500/

ALEFA. (2019). *Trafficking in human beings (THB). Financial investigations handbook*. Retrieved from: http://www.alefa.eu/ckeditor_uploads/files/165804-ALEFA-E-Publication-updated-14%2003%2019%20v%20edit%20with%20NO%20contacts.pdf

Amilhat, E., Basic, T., Beaulaton, L., Belpaire, C., Bernotas, P., Briand, C., . . . Dekker, W. (2019). 'Joint EIFAAC/ICES/GFCM Working Group on Eels (WGEEL)'.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J. G., Levi, M., . . . Savage, S. (2013). 'Measuring the cost of cybercrime'. In Bohme, R. (Ed.), *The economics of information security and privacy*, 265–300: Springer.

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., . . . Vasek, M. (2019). 'Measuring the changing cost of cybercrime'. Retrieved from: http://orca.cf.ac.uk/122684/

Angelini, M., Camerini, D., Giommoni, L., Soriani, C., & Standridge, P. (2015). 'Organised crime portfolio: Illicit revenues and criminal investments in Europe'. *European Law Enforcement Research Bulletin*(12), 4–12.

Aniello, S., & Caneppele, S. (2017). 'Selling stolen goods on the online markets: an explorative study' *Global Crime*, 1–21.

Antonopoulos, G. A., & Hall, A. (2016). 'The financial management of the illicit tobacco trade in the United Kingdom'. *British Journal of Criminology, 56*(4), 709–728.

Armbrüster, C., Beauvais, P., Chedouki, J., Cornu, M., Fortis, É., Frigo, M., . . . Renold, M. (2011). 'Study on preventing and fighting illicit trafficking in cultural goods in the European Union'.

ASH Scotland. (2016). 'Illicit tobacco'. Retrieved from: https://www.ashscotland.org.uk/media/591209/illicit-tobacco.pdf

Auliya, M., Altherr, S., Ariano-Sanchez, D., Baard, E. H., Brown, C., Brown, R. M., . . . Henningheim, E. (2016). 'Trade in live reptiles, its impact on wild populations, and the role of the European market'. *Biological Conservation, 204*, 103–119.

Auriol, E., Straub, S. & Flochel, T. (2016). 'Public procurement and rent-seeking: the case of Paraguay', *World Development*, 77: 395-407.

Barber-Meyer, S. (2009). 'Dealing with the clandestine nature of wildlife-trade market surveys'. *Conversation Biology 24*(4), 918–923.

Bekhouche, I. E. (2018). 'Copyright and trademark offences which might infringe the consumer's rights'. *ATHENS LJ, 4*(243).

Belev, B. (2002). 'The informal economy in the EU Accession countries: size, scope, trends and challenges in the process of EU enlargement'. Retrieved from: http://home.cerge-ei.cz/hanousek/INFOREC%20PART%20II-6.pdf

Binns, J. (2019). 'The UK's anti money laundering laws post Brexit'. Retrieved from: https://www.bcl.com/uks-anti-money-laundering-laws-post-brexit/

Bisschop, L. (2012). 'Is it all going to waste? Illegal transports of e-waste in a European trade hub'. *Crime, Law and Social Change, 58*(3), 221–249.

Bisschop, L. (2017). 'Transnational environmental crime: exploring (un) charted territory'. In White, R. (Ed.), *Transnational Environmental Crime* (3–32). London: Routledge.

Blum, J.A., M. Levi, R.T. Naylor, and P. Williams. (1998). Financial havens, banking secrecy and money-laundering (UN).

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). '2017 National Threat Assessment'. Retrieved from: https://www.politie.nl/binaries/content/assets/politie/algemeen/nationaal-dreigingsbeeld-2017/2017-national-threat-assessment-organised-crime.pdf

Borkowski, F., and C. Twomey. (2019). European Union: Confronting Illicit Tobacco Trade: An Update on EU Policies (World Bank).

Borselli, F., Fedeli, S., & Giuriato, L. (2015). 'Digital VAT carousel fraud: a new boundary for criminality?'. *Tax Notes International*, 77(8). Retrieved from: https://www.researchgate.net/publication/273131335_Digital_VAT_Carousel_Fraud_A_New_Boundary_for_Criminality

Bos, M. (2015). 'Trafficking in human organs'. *Policy Department, Directorate General for External Policies, European Union, 20*(21), 22–23.
Brochet, A. L., Van Den Bossche, W., Jones, V. R., Arnardottir, H., Damoc, D., Demko, M., . . . Ghasabyan, M. (2019). 'Illegal killing and taking of birds in Europe outside the Mediterranean: assessing the scope and scale of a complex issue'. *Bird Conservation International, 29*(1), 10–40.
Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., de Poot, C., . . . Korsell, L. (2016). 'Cyber-OC-Scope and manifestations in selected EU member states'. Bundeskriminalamt Wiesbaden.
Bush, E. R., Baker, S. E., & Macdonald, D. W. (2014). 'Global trade in exotic pets 2006–2012'. *Conservation Biology, 28*(3), 663–676.
Butler, S. (2019). Criminal use of cryptocurrencies: a great new threat or is cash still king? *Journal of Cyber Policy, 4*(3), 326-345.
Butticè, V., Caviggioli, F., Franzoni, C., Scellato, G., & Thumm, N. (2018). *Impact of counterfeiting on the performance of digital technology companies*. Retrieved from: https://www.econstor.eu/bitstream/10419/202232/1/jrc-dewp201803.pdf
Bryans, D. (2014). 'Bitcoin and money laundering: mining for an effective solution'. *Ind. LJ, 89*, 441.
Calderoni, F. (2014). 'Mythical numbers and the proceeds of organised crime: estimating mafia proceeds in Italy'. *Global Crime, 15*(1–2), 138–163.
Calderoni, F., Favarin, S., Garofalo, L., & Sarno, F. (2014). 'Counterfeiting, illegal firearms, gambling and waste management: an exploratory estimation of four criminal markets'. *Global Crime, 15*(1–2), 108–137. doi:10.1080/17440572.2014.883499
Camerini, D., Favarin, S., & Dugato, M. (2015). 'Estimating the counterfeit markets in Europe'. Transcrime.
Campana, P. (2016). 'The Structure of Human Trafficking: Lifting the Bonnet on a Nigerian Transnational Network'. *The British Journal of Criminology, 56*(1), 68–86.
Campana, P. (2017). 'Macro trends in the smuggling of migrants into Europe: An analytical exploration'. *European Law Enforcement Research Bulletin*(16), 57–64.
Campana, P. (2018). 'Out of Africa: The organization of migrant smuggling across the Mediterranean'. *European Journal of Criminology, 15*(4), 481–502.
Campbell, P. B. (2013). 'The Illicit Antiquities Trade as a Transnational Criminal Network: Characterizing and Anticipating Trafficking of Cultural Heritage'. *International Journal of Cultural Property*(20), 113–153.
Caneppele, S., Riccardi, M., & Standridge, P. (2013). 'Green energy and black economy: mafia investments in the wind power sector in Italy'. *Crime, Law and Social Change, 59*(3), 319–339.
Cardador, L., Tella, J. L., Anadon, J. D., Abellan, P., & Carrete, M. (2018). 'The European trade ban on wild birds reduced invasion risks'. *Conservation Letters.*
Carnevale, S., Forlati, S., & Giolo, O. (2017). *Redefining Organised Crime: A Challenge for the European Union?* Oxford: Bloomsbury Publishing.
Carrera, S., Guild, E., Vosyliūtė, L., Scherrer, A., & Mitsilegas, V. (2016). 'The cost of non-Europe in the area of organised crime'. *CEPS Paper in Liberty and Security in Europe* (90).
Caulkins, J. P., Disley, E., Tzvetkova, M., Pardal, M., Shah, H., & Zhang, X. (2016). 'Modeling the structure and operation of drug supply chains: The case of cocaine and heroin in Italy and Slovenia'. *International Journal of Drug Policy, 31*, 64–73.
Caulkins, J. P., Kilmer, B., & Graf, M. (2013). 4. Estimating the size of the EU cannabis market. Further insights into aspects of the EU illicit drugs market, 27.
Chabinsky, S. (2010). 'The Cyber Threat: Who's Doing What to Whom?'. Retrieved from: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom
Chainanalysis. (2020). 'The 2020 state of cryptocrime. Everything you need to know about darknet markets, exchange hacks, money laundering and more'. Retrieved from: https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf
Chartered Institute of Building (CIOB). (2016). Crime in the construction industry. Retrieved from: https://policy.ciob.org/wp-content/uploads/2016/02/Crime-in-the-Construction-Industry.pdf
Chatain, P.-L., Zerzan, A., Noor, W., Dannaoui, N., & de Koker, L. (2011). 'Protecting Mobile Money against Financial Crimes. Global Policy Challenges and Solutions'. Retrieved from: https://openknowledge.worldbank.org/bitstream/handle/10986/2269/600600PUB0ID181Mobile09780821386699.pdf?sequence=1

Chaudhry, P. E., & Zimmerman, A. (2012). *Protecting your intellectual property rights: Understanding the role of management, governments, consumers and pirates*. Springer Science & Business Media.
Cheung, Y.-L., Rau, P. R., & Stouraitis, A. (2006). Tunneling, propping, and expropriation: evidence from connected party transactions in Hong Kong. *Journal of Financial Economics*, 82(2), 343-386.
Chohan, U. W. (2017). 'The Cryptocurrency Tumblers: Risks, Legality and Oversight'. *Discussion Paper Series: Notes on the 21st Century*.
Chon, S., & Broadhurst, R. (2014). 'Routine Activity Theory and Cybercrime: What about Offender Resources?'. Retrieved from: https://ssrn.com/abstract=2379201
Chong, E., Klien, M., & Saussier, S. (2016). 'The use and abuse of discretionary procurement procedures: Evidence from the European Union', Working Paper. Chaire EPPP.
Choo, K. K. R., & Smith, R. G. (2008). 'Criminal exploitation of online systems by organised crime groups'. *Asian Journal of Criminology, 3*(1), 37–59.
Cingano, F., & Pinotti, P. (2012). Trust, firm organization and the structure of production. Paolo Baffi Centre Research Paper (2012-133).
Codex Alimentarius Commission. (2017). *Codex committee on food import and export inspection and certification systems – discussion paper on food integrity and food authenticity*. Retrieved from: https://ec.europa.eu/food/safety/international_affairs/standard_setting_bodies/codex/ccfics_en
Confederation of European Security Services (CoESS). (2017). *Best practices in transport s*ecurity Retrieved from: https://www.coess.org/download.php?down=Li9kb2N1bWVudHMvcGItY29lc3MtYmVzdC1wcmFjdGljZXMtaW4tdHJhbnNwb3J0LXNlY3VyaXR5LTIwMTctMTAucGRm
Cook, T. (2013). 'Revision of the European Union regime on customs enforcement of intellectual property rights'. *Journal of Intellectual Property Rights, 18*, 485–490.
Cornelius, C. V. M., Lynch, C. J., & Gore, R. (2017). *Aging out of crime: exploring the relationship between age and crime with agent based modelling*. Paper presented at the SpringSim-ADS 2017, Virginia Beach.
Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime (2008).
Council of Europe. (2020). 'Corruption risks and useful legal references in the context of COVID-19'.
Council of the European Union (2020). 'Taxation: EU list of non-cooperative jurisdictions'. Retrieved from: https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/
CREATe, & PwC. (2014). 'Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats'. Retrieved from: https://www.innovation-asset.com/hubfs/blog-files/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf
Criminal Assets Bureau. (2019). 'Annual Report 2019'. Retrieved from: https://www.cab.ie/wp-content/uploads/2020/07/2019-Annual-Report-English.pdf
CSD. (2015). 'Financing of Organised Crime'. Retrieved from: http://old.csd.bg/artShow.php?id=17317
Dabrowski, M., & Janikowski, L. (2018). 'Virtual currencies and central banks monetary policy: challenges ahead'. Retrieved from: https://blockcointoday.com/wp-content/uploads/EU-virtual-currencies-report.pdf
Dank, M. L., Khan, B., Downey, P. M., Kotonias, C., Mayer, D., Owens, C., . . . Yu, L. (2014). 'Estimating the size and structure of the underground commercial sex economy in eight major US cities'.
Dávid-Barrett, E., & Fazekas, M. (2016). Corrupt contracting: Controlling Partisan Favouritism in Public Procurement.
Dávid-Barrett, E., Fazekas, M., Hellmann, O, Mark, L. & McCorley, C. (2018). 'Controlling Corruption in Development Aid: New Evidence from Contract-Level Data'.
Davies, J., and N. Ollus. (2019). 'Labour exploitation as corporate crime and harm: outsourcing responsibility in food production and cleaning services supply chains'. Crime, Law and Social Change, 72: 87-106.
de la Feria, R. (2018). 'Tax Fraud and the Rule of Law'. Retrieved from: https://wayback.archive-it.org/org-467/20200808042212/http://eureka.sbs.ox.ac.uk/7281/1/WP1802.pdf
De Stercke, J., Liagre, F., & Stove, A. (2014). 'An integral methodology to develop an information-led and community-orientated policy to tackle domestic burglary'. Retrieved from:

Deviatov, A. (2009). 'Cash, Money Laundering, and the Size of Underground Economy'. Retrieved from: https://www.nes.ru/dataupload/files/programs/econ/preprints/2009/Deviatov.pdf
Di Castri, S., Grossman, J., & Sihin, R. (2015). 'Proportional risk-based AML/CFT regimes for mobile money. A framework for assessing risk factors and mitigation measures'.
Di Natala, L. (2013). 'Italy: Sicilian's Casa Nostra interests in "Green economy" and its low profile strategy'. *ESISC Briefing*.
Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), (2015).
Dobovšek, B. (2008). 'Economic organized crime networks in emerging democracies'. *International Journal of Social Economics, 35*(9), 679–690.
Dugato, M., Favarin, S., & Giommoni, L. (2015). 'The risks and rewards of organized crime investments in real estate'. *British Journal of Criminology, 55*(5), 944–965.
Duquet, N. (2016). 'Armed to kill: An exploratory analysis of the guns used in public mass shootings in Europe'. Flemish Peace Institute.
Duquet, N., & Goris, K. (2018). 'Firearms acquisition by terrorists in Europe: Research findings and policy recommendations of Project SAFTE'. Brussels: Flemish Peace Institute.
Dyson, S., Buchanan, W. J., & Bell, L. (2019). 'The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime'. Retrieved from: https://arxiv.org/pdf/1907.12221.pdf
EAST. (2020). 'European Payment Terminal Crime report 2019. Period: January - December''. Non-public EAST report (disclosed to research team upon request to use for the study).
EBA. (2018). 'EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech'. Retrieved from: https://fintechireland.com/uploads/3/5/4/5/35459745/report_on_prudential_risks_and_opportunities_arising_for_institutions_from_fintech.pdf
ECB. (2018). 'Fifth report on card fraud, September 2018'. Retrieved from: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html
Economic Declaration. (1989). Retrieved from: http://www.g8.utoronto.ca/summit/1989paris/communique/index.html
Ellis, C. (2017). 'On Tap Europe: Organised Crime and Illicit Trade in Tobacco, Alcohol and Pharmaceuticals'. Retrieved from: https://rusi.org/sites/default/files/201703_rusi_whr_2-17_on_tap_europe_updated_low-res.pdf
EMCDDA. (2018). 'Recent changes in Europe's cocaine market: results from an EMCDDA trendspotter study'. Retrieved from: https://www.emcdda.europa.eu/system/files/publications/10225/2018-cocaine-trendspotter-rapid-communication.pdf
EMCDDA. (2019). 'Estimating the size of the main illicit retail drug markets in Europe: an update'. Retrieved from: https://www.emcdda.europa.eu/system/files/publications/12174/TD0219965ENN.pdf
EMCDDA. (2020a). 'COVID-19 and the drug supply chain: from production and trafficking to use (UNODC)'. Retrieved from: https://www.emcdda.europa.eu/drugs-library/covid-19-and-drug-supply-chain-production-and-trafficking-use-unodc_en
EMCDDA. (2020b). 'European Drug Report 2020: Trends and Developments'. Retrieved from: https://www.emcdda.europa.eu/system/files/publications/13236/TDAT20001ENN_web.pdf
EMCDDA & Europol. (2016). 'EU drug markets report: In-depth analysis'. Office of the European Union.
EMCDDA & Europol. (2017). 'Drugs and the darknet: perspectives for enforcement, research and policy'. Retrieved from: http://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf
EMCDDA & Europol. (2019). 'EU drug markets report: In-depth analysis'. Office of the European Union.
EMCDDA & Pompidou Group. (1997). 'Estimating the prevalence of problem drug use in Europe'. Retrieved from: https://www.emcdda.europa.eu/html.cfm/index34027EN.html_en
ENAA. (2020). 'European Network on the Administrative Approach tackling serious and organised crime'. Retrieved from: https://administrativeapproach.eu/
EnviCrimeNet. (2016). 'Report on Environmental Crime in Europe'. Retrieved from: http://www.envicrimenet.eu/images/docs/envicrimenet%20report%20on%20environmental%20crime.pdf

Environmental Investigation Agency (EIA). (2020). 'Illegal trade seizures: large-scale elephant ivory seizures'. Retrieved from: https://eia-international.org/wildlife/wildlife-trade-maps/large-scale-elephant-ivory-seizures/
Esselink, H., & L. Hernandez. (2017). "The use of cash by households in the euro area." In Occasional Paper Series European Central Bank.
EUIPO. (2015). 'The economic cost of IPR infringement in the toys and games (4th sectorial study)'. Retrieved from: https://euipo.europa.eu/ohimportal/en/web/observatory/ipr_infringement_toys_and_games?utm_source=hootsuite
EUIPO. (2016a). 'The economic cost of IPR infringement in handbags and luggage (6th sectorial study)'. Retrieved from: https://euipo.europa.eu/ohimportal/en/web/observatory/ipr_infringement_handbags_and_luggage
EUIPO. (2016b). 'The economic cost of IPR infringement in jewellery and watches (5th Sectorial study)'. Retrieved from: https://euipo.europa.eu/ohimportal/en/web/observatory/ipr_infringement_jewellery_and_watches
EUIPO. (2016c). 'The economic cost of IPR infringement in the pharmaceutical industry: Quantification of infringement in Manufacture of pharmaceutical preparations (NACE 21.20)'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study9/pharmaceutical_sector_en.pdf
EUIPO. (2016d). 'The economic cost of IPR infringement in the spirits and wine (8th sectorial study)'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study8/wines_and_spirits_en.pdf
EUIPO. (2016e). 'Report on Infringement of Protected Geographical Indications for Wine, Spirits, Agricultural Products and Foodstuffs in the European Union'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Geographical_indications_report/geographical_indications_report_en.pdf
EUIPO. (2017a). 'The economic cost of IPR infringement in the pesticides sector (10th sectorial study)'. Retrieved from: https://euipo.europa.eu/ohimportal/en/web/observatory/ipr-infringement-pesticides-sector
EUIPO. (2017b). 'The economic cost of IPR infringement in the recorded music industry (7th sectorial study)'. Retrieved from: https://euipo.europa.eu/ohimportal/en/web/observatory/ipr_infringement_music
EUIPO. (2017c). 'The economic cost of IPR infringement in the smartphones sector (11th sectorial study)'. Retrieved from: https://euipo.europa.eu/ohimportal/en/web/observatory/ipr-infringement-smartphone-sector
EUIPO. (2017d). 'European citizens and intellectual property: Perception, awareness and behaviour'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/2017/european_public_opinion_study_web.pdf
EUIPO. (2017e). 'Infringement of protected geographical indications for wine, spirits, agricultural products and foodstuffs in the European Union'. Alicante, Spain: European Union Intellectual Property Office.
EUIPO. (2018). 'The economic cost of IPR infringement in the tyres and batteries sectors (12th sectorial study)'. Retrieved from:
EUIPO. (2019a). '2019 intellectual property and youth scoreboard'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IP_youth_scoreboard_study_2019/IP_youth_scoreboard_study_2019_en.pdf
EUIPO. (2019b). 'Illegal IPTV in the European Union: Research on online business models infringing intellectual property rights - phase 4'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf
EUIPO. (2019c). 'Report on the EU enforcement of intellectual property rights: Results at EU borders and in Member States 2013–2017'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Rep

ort_on_Enforcement_of_IPR_at_EU_borders_and_in_MS_2013_2017/2019_Report_on_enforcement_of_IPR_at_EU_borders_and_in_MS_2013_2017_Full_en.pdf
EUIPO. (2020a). '2020 status report on IPR infringement: Why IP rights are important, IPR infringement, and the fight against counterfeiting and piracy'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Status_Report_on_IPR_infringement/2020_Status_Report_on_IPR_infringement_en.pdf
EUIPO. (2020b). 'IP crime and its link to other serious crimes: Focus on Poly-Criminality'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_IP_crime_and_its_link_to_other_serious_crimes/2020_IP_crime_and_its_link_to_other_serious_crimes_Full.pdf
EUIPO & Europol. (2019). 'Intellectual Property Crime Threat Assessment 2019'. Retrieved from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf
Eurojust. (2019). 'Report on Eurojust's casework in asset recovery'.
European Anti-Fraud Office. (2019). 'Report fraud'. Retrieved from: https://ec.europa.eu/anti-fraud/olaf-and-you/report-fraud_en#:~:text=Fraud%20is%20a%20deliberate%20act,Communities'%20financial%20interests%2C%201995)
European Central Bank. (2020). 'All glossary entries'. Retrieved from: https://www.ecb.europa.eu/home/glossary/html/glossa.en.html
European Commission. (2009). 'E-money - Directive 2009/110/EC'.
European Commission. (2012). 'Commission Staff Working Paper Accompanying document to the Proposal for a Directive of the European Parliament and the Council on the freezing and confiscation of proceeds of crime in the European Union - Impact Assessment (SWD/2012/0031 - COD/2012/0036/)'.
European Commission. (2013). 'Study to quantify and analyse the VAT Gap in the EU-27 Member States: Final Report'. Retrieved from: https://ec.europa.eu/taxation_customs/sites/taxation/files/docs/body/vat-gap.pdf
European Commission. (2014). 'Economic impact of eel trade ban – general trends. Study in support to the STECF'.
European Commission. (2015). 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions'. Strasbourg.
European Commission. (2016a). 'Commission Staff Working Document: Technical assessment of the experience made with the Anti-Contraband and Anti-Counterfeit Agreement and General Release of 9 July 2004 among Philip Morris International and affiliates, the Union and its Member States'. Retrieved from: https://ec.europa.eu/anti-fraud/sites/antifraud/files/technical_assessment_pmi_24022016_en.pdf
European Commission. (2016b). 'Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending directive 2009/101/EC'. Retrieved from: http://europeanmemoranda.cabinetoffice.gov.uk/files/2016/09/EM_on_4AMLD_Amendments_(002).pdf
European Commission. (2016c). 'Study on the gender dimension of trafficking in human beings. Final report'. Retrieved from: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._final_report.pdf
European Commission. (2017a). 'Commission introduces new measures to fight poaching and to end trade in raw ivory'. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1308
European Commission. (2017b). 'Commission Staff Working Document - Accompanying the document: Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations'. Retrieved from: http://europeanmemoranda.cabinetoffice.gov.uk/files/2017/07/10977-17-ADD-2.pdf
European Commission. (2018a). 'The concept of Tax Gaps - Report III: MTIC Fraud Gap estimation methodologies'. Retrieved from: https://ec.europa.eu/taxation_customs/sites/taxation/files/tax_gaps_report_mtic_fraud_gap_estimation_methodologies.pdf

European Commission. (2018b). 'Data collection on trafficking in human beings in the EU - Final report'. Retrieved from: https://eprints.lancs.ac.uk/id/eprint/138015/1/20181204_data_collection_study.pdf
European Commission. (2018c). 'Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims'. Retrieved from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181204_com-2018-777-report_en.pdf
European Commission. (2019a). 'A European Green Deal'. Retrieved from: https://ec.europa.eu/info/priorities/european-green-deal_en
European Commission. (2019b). 'Investor Citizenship and Residence Schemes in the European Union, Com(2019) 12 final', p.14.
European Commission. (2019c). 'Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. SWD(2019) 650 final'.
European Commission. (2019d). 'Security Union: A Europe that protects'.
European Commission. (2019e). 'VAT Fraud: New tool to help EU countries crack down on criminals and recoup billions'. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2468
European Commission. (2020a). 'Asset recovery and confiscation: Ensuring that crime does not pay'. Retrieved from: https://ec.europa.eu/home-affairs/news/20200602_commission-adopts-report-asset-recovery-confiscation-ensuring-crime-does-not-pay_en
European Commission. (2020b). 'Combating environmental crime'. Retrieved from: https://ec.europa.eu/environment/legal/crime/
European Commission. (2020c). 'Data collection on trafficking in human beings in the EU'.
European Commission. (2020d). 'EU Security Union Strategy: connecting the dots in a new security ecosystem'. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1379
European Commission. (2020e). 'Notice to stakeholders. Withdrawal of the United Kingdom and EU Rules in the Field of Industrial Products'. Retrieved from Brussels: https://ec.europa.eu/info/sites/info/files/notice_to_stakeholders_industrial_products_0.pdf
European Commission. (2020f). 'Recovery plan for Europe'. Retrieved from: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/recovery-plan-europe_en
European Commission. (2020g). 'Report from the Commission to the European Parliament. Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims {SWD (2020) 226 final}'. Retrieved from https://data.consilium.europa.eu/doc/document/ST-12280-2020-INIT/en/pdf
European Commission. (n.d.). 'Internal Security Fund - Police'. Retrieved from: https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police_en
European Parliament. (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
European Parliament. (2019). 'Citizenship by Investment (CBI) and Residency by Investment (RBI) schemes in the EU'.
European Union. (2019a). '2019/C 384 I/01 Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Community, Official Journal of the European Union, 62, 12 November 2019'.
European Union. (2019b). '2019/C 384 I/02 Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom, 12 November 2019'.
European Union. (2019c). 'Report on the EU customs enforcement of intellectual property rights: Results at the EU border, 2018'. Luxembourg: Publications Office of the European Union.
European Union, and Council of the European Union. (2017). Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons, (2017).

Europol. (2009). 'Cargo theft report: Applying the brakes to road cargo crime in Europe'. Retrieved from: http://www.transportschaden.biz/html/documents/Cargo_Theft_Report.pdf
Europol. (2013a). 'Serious and Organised Crime Threat Assessment (SOCTA)'. Retrieved from: https://www.europol.europa.eu/activities-services/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013
Europol. (2013b). 'Threat Assessment 2013: Environmental Crime in the EU'. Retrieved from: https://www.europol.europa.eu/publications-documents/threat-assessment-2013-environmental-crime-in-eu
Europol. (2014a). 'Intelligence notification: Child trafficking for forced criminal activities and forced begging'.
Europol. (2014b). 'The Internet Organised Crime Threat Assessment (iOCTA)'. Retrieved from: https://www.europol.europa.eu/iocta/2014/
Europol. (2015a). '2015 Situation Report on Counterfeiting in the European Union'. Europol and the Office for Harmonization in the Internal Market.
Europol. (2015b). 'Exploring tomorrow's organised crime'. Retrieved from: https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime
Europol. (2015c). 'The THB financial business model. Assessing the current state of knowledge'.
Europol. (2015d). 'Why is cash still a king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering'. Retrieved from: https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering
Europol. (2016a). 'Does crime still pay? Criminal asset recovery in the EU - Survey of statistical information 2010–2014'.
Europol. (2016b). 'Situation report: trafficking in human beings in the EU'. Retrieved from: http://www.respect.international/situation-report-trafficking-in-human-beings-in-the-eu/
Europol. (2017a). '2017 Situation Report on Counterfeiting in the European Union'. Europol and the Office for Harmonization in the Internal Market.
Europol. (2017b). 'European Union Serious and Organised Crime Threat Assessment: Crime in the age of technology'. Retrieved from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017
Europol. (2018a). 'European Migrant Smuggling Centre: 3rd Annual Activity Report – 2018'. Retrieved from: https://www.europol.europa.eu/publications-documents/emsc-3rd-annual-activity-report-%E2%80%93-2018
Europol. (2018b). 'Glass eels traffickers earned more than EUR 37 million from illegal exports to Asia'. Retrieved from: https://www.europol.europa.eu/newsroom/news/glass-eel-traffickers-earned-more-eur-37-million-illegal-exports-to-asia
Europol. (2018c). 'Internet Organised Crime Threat Assessment (IOCTA) 2018'. Retrieved from: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018
Europol. (2019a). 'Internet Organised Crime Threat Assessment (IOCTA) 2019'. Retrieved from: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
Europol. (2019b). 'Operation OPSON VII - Analysis report'. Retrieved from: https://www.europol.europa.eu/publications-documents/operation-opson-vii-analysis-report
Europol. (2019c). 'Over 5 tonnes of smuggled glass eels seized in Europe this year'. Retrieved from: https://www.europol.europa.eu/newsroom/news/over-5-tonnes-of-smuggled-glass-eels-seized-in-europe-year
Europol. (2019d). 'Trafficked By Voodoo Threats: One Of The Largest Operations In Europe Rescues 39 Nigerian Women [Press release]'. Retrieved from: https://www.europol.europa.eu/newsroom/news/trafficked-voodoo-threats-one-of-largest-operations-in-europe-rescues-39-nigerian-women
Europol. (2020a). 'Beyond the pandemic – how COVID-19 will shape the serious and organised crime landscape in the EU'. Retrieved from: https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu
Europol. (2020b). 'Environmental crime'. Retrieved from: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/environmental-crime

Europol. (2020c). 'How COVID-19-related crime infected Europe during 2020'. Retrieved from: https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020
Europol. (2020d). 'MTIC (Missing Trader Intra Community) Fraud'. Retrieved from: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/mtic-missing-trader-intra-community-fraud
Europol. (2020e). 'Organised property crime'. Retrieved from: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/organised-property-crime
Europol. (n.d.). 'Money muling'. Retrieved from: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling
Europol & EUCPN. (2019). 'Preventing Physical ATM Attacks'. Retrieved from: https://www.europol.europa.eu/publications-documents/preventing-physical-atm-attacks
Europol & Eurojust. (2019). 'Common challenges in combating cybercrime'. Retrieved from: https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime
Europol-Interpol. (2016). 'Migrant Smuggling Networks: Joint Europol-INTERPOL Report - Executive Summary'. Retrieved from: https://www.europol.europa.eu/publications-documents/europol-interpol-report-migrant-smuggling-networks
Europol & Interpol. (2018). 'Operation OPSON VI: Targeting counterfeit and substandard foodstuff and beverage'. Retrieved from: https://ec.europa.eu/food/sites/food/files/safety/docs/official-controls-food-fraud_opson-vi-report.pdf
Eurostat. (2015). 'Trafficking in human beings'. Retrieved from: https://ec.europa.eu/anti-trafficking/publications/trafficking-human-beings-eurostat-2015-edition_en
Eurostat. (2018). 'Handbook on the compilation of statistics on illegal economic activities in national accounts and balance of payments - 2018 edition'. Retrieved from: https://ec.europa.eu/eurostat/documents/3859598/8714610/KS-05-17-202-EN-N.pdf/eaf638df-17dc-47a1-9ab7-fe68476100ec
Eurostat. (2020). 'HICP (2015 = 100) - annual data (average index and rate of change)'. Retrieved from: https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=prc_hicp_aind&lang=en
EY. (2015). 'Implementing the destination principle to intra-EU B2B supplies of goods: Feasibility and economic evaluation study'. Retrieved from: https://ec.europa.eu/taxation_customs/sites/taxation/files/docs/body/ey_study_destination_principle.pdf
Fanusie, Y., & Robinson, T. (2018). 'Bitcoin laundering: an analysis of illicit flows into digital currency services'. Retrieved from: https://www.blockchainwg.eu/wp-content/uploads/2018/01/Bitcoin_Laundering.pdf
Farolfi, S., Pegg, D., & Orphanides, S. (2017). 'Cyprus "selling" EU citizenship to super rich of Russia and Ukraine'. *The Guardian*, 17 September.
FATF. (2006). 'Report on New Payment Methods'. Retrieved from: http://www.fatf-gafi.org/publications/methodsandtrends/documents/reportonnewpaymentmethods.html
FATF. (2010). 'Money laundering using new payment methods'. Retrieved from: fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf
FATF. (2011). 'Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants'. Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf
FATF. (2012). 'Illicit Tobacco Trade'. Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Illicit%20Tobacco%20Trade.pdf
FATF. (2013). 'The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing'. Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf
FATF. (2014). 'Virtual currencies: key definitions and potential AML/CFT risks'. Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
FATF. (2015). *Guidance for a risk-based approach to virtual currencies*. Retrieved from Paris, France: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

FATF & MENAFATF. (2015). 'Money laundering through the physical transportation of cash'. Retrieved from: https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf
FATF/Moneyval. (2010). 'Money Laundering through Money Remittance and Currency Exchange Providers'.
Fazekas, M., Kazmina, Y., and Nikulina, O. (2020). 'Investments by organised crime groups in the legal economy'. Technical Paper, Government Transparency Institute, Budapest.
Fazekas, M., & Kocsis, G. (2015). Uncovering high-level corruption: cross-national corruption proxies using government contracting data. *European Research Centre for Anti-Corruption and State-Building Working Paper* (46).
Fazekas, M., & Tóth, I. J. (2017). Corruption in EU Funds? Europe-wide evidence of the corruption effect of EU-funded public contracting.
Ferentzy, P., & Turner, N. (2009). 'Gambling and organized crime - A review of the literature'. *Journal of Gambling Issues*(23), 111–155.
Ferrante, L., Fontana, S., & Reito, F. (2019). 'Mafia and bricks: unfair competition in local markets and policy interventions'. *Small Business Economics*, 1–24.
Ferwerda, J., & Kleemans, E. R. (2019). 'Estimating money laundering risks: An application to business sectors in the Netherlands'. *European Journal on Criminal Policy and Research, 25*(1), 45–62.
Florêncio, D., & Herley, C. (2010). 'Phishing and money mules'. Paper presented at the 2010 IEEE International Workshop on Information Forensics and Security.
Focus on Labour Exploitation (FLEX) Shaky Foundations. (2018). 'Labour Exploitation in London's Construction Sector'. Retrieved from: https://www.labourexploitation.org/publications/shaky-foundations-labour-exploitation-londons-construction-sector
Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). 'Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?'. *The Review of Financial Studies, 32*(5), 1798–1853.
Food Fraud Advisors. (2017). 'Trends and developments in food fraud 2017'. Retrieved from: https://www.foodfraudadvisors.com/trends-and-developments-in-food-fraud-2017/
FRA. (2015). 'Severe labour exploitation: workers moving within or into the European Union - States' obligations and victims' rights'. Retrieved from: https://fra.europa.eu/sites/default/files/fra-2015-severe-labour-exploitation_en.pdf
FRA. (2019). 'Protecting migrant workers from exploitation in the EU: workers' perspectives'.
Franklin, J. (2007). 'An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants'. Paper presented at the ACM Conference on Computer and Communications Security.
FRONTEX. (2020). 'Risk analysis for 2020'. Retrieved from: https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Annual_Risk_Analysis_2020.pdf
Frunza, M.-C. (2019). *Value Added Tax Fraud*: *Routledge Research in Finance and Banking Law*. Abingdon: Routledge.
FWI SCIC. (2016). 'Putting a Price Tag on Underreported Cargo Theft in Europe'. Retrieved from: http://www.sensitech.com/en/media/UnderreportedCargoTheftweb_tcm35-10477.pdf
Gallus, S., Lugo, A., La Vecchia, C., Boffetta, P., Chaloupka, F. J., Colombo, P., . . . Gilmore, A. (2014). 'Pricing Policies And Control of Tobacco in Europe (PPACTE) project: cross-national comparison of smoking prevalence in 18 European countries'. *European journal of cancer prevention, 23*(3), 177–185.
Gee, J., & Button, M. (2019). 'The Financial Cost of Fraud 2019'. Retrieved from: https://www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/The-Financial-Cost-of-Fraud-2019.pdf
Geeraerts, K., Illes, A., & Schweizer, J. (2015). 'Illegal shipment of e-waste from the EU: A case study on illegal e-waste export from the EU to China'. London: Institute for European Environmental Policy. Retrieved from: https://www.researchgate.net/publication/311233314_Illegal_shipment_of_e-waste_from_the_EU_A_case_study_on_illegal_e-waste_export_from_the_EU_to_China
Gilmour, N., & Ridley, N. (2015). 'Everyday vulnerabilities – money laundering through cash intensive businesses'. *Journal of Money Laundering Control*, 18(3), 293–303. doi:https://doi.org/10.1108/JMLC-06-2014-0019
Global initiative against transnational organised crime. (2020). 'Smuggling in the time of COVID-19: The impact of the pandemic on human-smuggling dynamics and migrant-protection risks'. Retrieved from: https://globalinitiative.net/smuggling-covid-19/

Godart, B. (2010). 'IP crime: The new face of organized crime: From IP theft to IP crime'. *Journal of Intellectual Property Law & Practice*, 5(5), 378–385.
Golden, M.A, and Picci, L. (2005). 'Proposal for a new measure of corruption, illustrated with Italian data', *Economics & Politics*, 17: 37-75.
Goldman, E., Rocholl, J., & So, J. (2013). Politically connected boards of directors and the allocation of procurement contracts. *Review of Finance*, 17(5), 1617-1648.
Gottschalk, P. (2010). Criminal entrepreneurial behaviour. *Journal for International Business and Entrepreneurship Development*, 5(1), 63–76.
Grabosky, P. (2007). 'The internet, technology, and organized crime'. *Asian journal of criminology*, 2(2), 145–161.
Grimes, J. (2019). 'Fighting financial crime post Brexit: what next?'. Retrieved from: https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/fighting-financial-crime-post-brexit-what-next
Gruber, S. (2019). 'Cultural Heritage Offences: A View from Asia'. In S. Hufnagel & D. Chappell (Eds.), *The Palgrave Handbook on Art Crime*. London: Palgrave Macmillan.
Gunn, L. (2020). 'European Payment Terminal Crime Report 2019. Period: January to December'.
Gurciullo, S. (2014). 'Organised crime infiltration in the legitimate private economy - An empirical network analysis approach'. Retrieved from: https://arxiv.org/abs/1403.5071
Hall, A., Koenraadt, R., & Antonopoulos, G. A. (2017). 'Illicit pharmaceutical networks in Europe: organising the illicit medicine market in the United Kingdom and the Netherlands'. *Trends in Organized Crime, 20*(3–4), 296–315.
Hassan, M., & Schneider, F. (2016). 'Size and development of the shadow economies of 157 countries worldwide: Updated and new measures from 1999 to 2013'. *IZA Discussion Paper Series* (10281).
Hayes, A. (2020). 'Transportation sector'. Investopedia, 17 April. Retrieved from: https://www.investopedia.com/terms/t/transportation_sector.asp
Healy, C. (2017). 'Exploitation through begging as a form of trafficking in human beings – over-estimated or under-reported?'. In Piotrowicz, R., Rijken, C, & Uhl, B.H. (Eds), *Routledge Handbook of Human Trafficking* (157–167). Abingdon: Routledge.
Henley and Partners. (2020). 'Henley Passport Index and Global Mobility Report'.
Herwartz, H., Tafenau, E., & Schneider, F. (2015). 'One share fits all? Regional variations in the extent of the shadow economy in Europe'. *Regional Studies, 49*(9), 1575–1587.
HM Government. (2018). 'Serious Violence Strategy'. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/698009/serious-violence-strategy.pdf
HM Government. (2020a). 'Freeports Consultation. Boosting Trade, Jobs and Investment Across the UK'.
HM Government. (2020b). 'The Future Relationship with the EU. The UK's Approach to Negotiations'.
Home Office. (2018a). 'Eighth Annual Report to Parliament on the Application of Protocols 19 and 21 to the Treaty on European Union (TEU) and the Treaty on the Functioning of the Union (TFEU) in Relation to EU Justice and Home Affairs (JHA) Matters (1 December 2016 – 30 November 2017)'. Retrieved from: https://www.gov.uk/government/publications/eighth-annual-report-to-parliament-on-eu-justice-and-home-affairs-matters
Home Office. (2018b). 'Serious and Organised Crime Strategy'. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf
HM Treasury and Home Office. (2017). *National risk assessment of money laundering and terrorist financing 2017*.
Hoorens, S., Hunt, P., Malchiodi, A., Pacula, R. L., Kadiyala, S., Rabinovich, L., & Irving, B. (2012). 'Measuring IPR infringements in the internal market: Development of a new approach to estimating the impact of infringements on sales'. Santa Monica, CA: RAND Europe.
Huang, K., Siegel, M., & Madnick, S. (2018). 'Systematically understanding the cyber attack business: A survey'. *ACM Computing Surveys (CSUR), 51*(4), 1–36.
Huisman, W., & Kleemans, E.R. (2014). The challenges of fighting sex trafficking in the legalised prostitution market of the Netherlands. *Crime Law and Social Change,* 61(2): 215-228.
Hunter, M. (2019). 'African illicit financial flows: designing and prioritising responses'. Retrieved from: https://enactafrica.org/research/research-papers/african-illicit-financial-flows-designing-and-prioritising-responses
Hyytinen, A., Lundberg, S. & Toivanen, O. (2018). 'Design of public procurement auctions: Evidence from cleaning contracts', *The RAND Journal of Economics*, 49: 398-426.

ICMPD. (2020). 'ICMPD Migration Outlook 2020: 10 thing to look out for in 2020 - Origins, key events and priorities for Europe'. Retrieved from: https://www.euneighbours.eu/sites/default/files/publications/2020-02/ICMPD%20publication.pdf

IFAW. (2018). 'Disrupt: Wildlife Cybercrime - Uncovering the scale of the online wildlife trade'. Retrieved from: https://d1jyxxz9imt9yb.cloudfront.net/resource/210/attachment/original/IFAW_-_Disrupt_Wildlife_Cybercrime_-_FINAL_English_-_new_logo.pdf

ILO. (2012). 'Global Estimate of Forced Labour Regional Factsheet European Union'.

Interpol. (2013). 'Guide to Carbon Trading Crime'. Retrieved from: https://www.interpol.int/en/content/download/5172/file/Guide%20to%20Carbon%20Trading%20Crime.pdf

Interpol. (2017). 'Research identified illegal wildlife trade on the Darknet [Press release]'. Retrieved from: https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2017/Research-identifies-illegal-wildlife-trade-on-the-Darknet

Interpol. (2018). 'Global Wildlife Enforcement: Strengthening Law Enforcement Cooperation Against Wildlife Crime'. Retrieved from: https://www.interpol.int/en/content/download/5179/file/WEB_Wildlife%20ProspectusMarch2019.pdf

Interpol. (2020). 'INTERPOL Strategic Analysis Report: Emerging criminal trends in the global plastic waste market since January 2018'. Retrieved from: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-alerts-to-sharp-rise-in-plastic-waste-crime

Interpol Office of Legal Affairs. (2014). 'COUNTERING ILLICIT TRADE IN TOBACCO PRODUCTS: A guide for policy-makers'. Retrieved from: www.scoop.it/doc/download/7I4OaIFV7TA7Jx_2bnpwWfA

Investopedia. (2019). 'Financial technology - Fintech'. Retrieved from: https://www.investopedia.com/terms/f/fintech.asp

IP Crime Group. (2019). 'IP Crime and Enforcement: Report 2018–19'. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/842351/IP-Crime-Report-2019.pdf

Joossens, L., Lugo, A., La Vecchia, C., Gilmore, A. B., Clancy, L., & Gallus, S. (2014). 'Illicit cigarettes and hand-rolled tobacco in 18 European countries: a cross-sectional survey'. *Tobacco control, 23*(e1), e17–e23.

Keatinge, T. (2016). 'Heading for the Brexit? Tackling Financial Crime Needs More, Not Less Partnership'. Retrieved from: https://rusi.org/commentary/heading-brexit-tackling-financial-crime-needs-more-not-less-partnership

Kenny, C. (2007). 'Construction, corruption, and developing countries'. Retrieved from: https://openknowledge.worldbank.org/handle/10986/7451

Khan, M. (2020). 'EU explores green bonds as part of €750bn borrowing spree'. *Financial Times* Retrieved from: https://www.ft.com/content/7a893f6d-08c9-426c-8f19-aa19d434b018

Kilmer, B. & Pacula, R. (2009). 'Estimating the size of the global drug market: A demand-side approach'. Santa Monica, Calif.: RAND Corporation. Retrieved from: https://www.rand.org/pubs/technical_reports/TR711.html

Kilvington, J., Day, S., & Ward, H. (2001). 'Prostitution policy in Europe: A time of change?'. *Feminist Review, 67*(1), 78–93.

Klima, N. (2011). 'The goods transport network's vulnerability to crime: opportunities and control weaknesses'. *European Journal on Criminal Policy and Research, 17*(3), 203–219.

Klašnja, M. (2016). 'Increasing rents and incumbency disadvantage', *Journal of Theoretical Politics*, 28: 225-65.

KPMG. (2016). 'Brexit: Potential Fraud Risks in a Time of Change'. Retrieved from: https://assets.kpmg/content/dam/kpmg/uk/pdf/2016/10/brexit-potential-fraud-risks.pdf

KPMG. (2017). 'Project SUN: A study of the illicit cigarette market in the European Union, Norway and Switzerland - 2016 Results'. Retrieved from: https://assets.kpmg/content/dam/kpmg/uk/pdf/2017/07/project-sun-2017-report.pdf

KPMG. (2019). 'Project Stella: A study of the illicit cigarette market in the European Union, Norway and Switzerland'. Retrieved from: https://www.stopillegal.com/docs/default-source/external-docs/kpmg-project-stella/project-stella-methodology.pdf?sfvrsn=aea077d7_2

Kruisbergen, E. W., Kleemans, E. R., & Kouwenberg, R. F. (2015). 'Profitability, power, or proximity? Organized crime offenders investing their money in legal economy'. *European Journal on Criminal Policy and Research, 21*(2), 237–256.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). 'Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands'. Santa Monica, Calif.: RAND Corporation. Retrieved from: https://www.rand.org/pubs/research_reports/RR1607.html

Kshetri, N., & Voas, J. (2017). 'Do crypto-currencies fuel ransomware?'. *IT professional, 19*(5), 11–15.

Lamensch, M., & Ceci, E. (2018). 'VAT fraud: Economic impact, challenges and policy issues'. Retrieved from: http://hdl.handle.net/2078.1/222731

Lavorgna, A. (2014). 'The online trade in counterfeit pharmaceuticals: New criminal opportunities, trends and challenges'. *European Journal of Criminology, 12*(2), 226–241.

Luechinger, S., & Moser, C. (2014). The value of the revolving door: Political appointees and the stock market. Journal of Public Economics, 119, 93-107.

Leukfeldt, E. R., Kruisbergen, E. W., Kleemans, E. R., & Roks, R. R. (2019). Organized Financial Cybercrime: Criminal Cooperation, Logistic Bottlenecks, and Money Flows. In T. Holt & A. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1-20): Palgrave.

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). 'Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime'. *European Journal on Criminal Policy and Research, 23*(3), 287–300.

Levi, M. (2015). 'Money for crime and money from crime: Financing crime and laundering crime proceeds'. *European Journal on Criminal Policy and Research, 21*(2), 275–297.

Levi, M. (2016). 'The impacts of organised crime in the EU: some preliminary thoughts on measurement difficulties'. *Contemporary Social Science, 11*(4), 392–402.

Levi, M., Innes, M., Reuter, P., & Gundur, R. V. (2013). 'The Economic, Financial & Social Impacts of Organised Crime in the European Union'. Brussels: Publications Office.

Levi, M., & Maguire, M. (2004). 'Reducing and preventing organised crime: An evidence-based critique'. *Crime, Law and Social Change, 41*(5), 397–469.

Levi, M., & Soudijn, M. (2020). 'Understanding the laundering of organized crime money'. *Crime and Justice, 49*(1), 579–631.

Lewis, J. (2018). 'Economic Impact of Cybercrime — No Slowing Down'. Retrieved from: https://www.csis.org/analysis/economic-impact-cybercrime

L'Hoiry, X.D. (2012). 'Tobacco smuggling: A review of the literature', *European Journal of Crime, Criminal Law and Criminal Justice*, 20: 415.

Liao, K., Zhao, Z., Doupé, A., & Ahn, G.-J. (2016). 'Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin'. *2016 APWG Symposium on Electronic Crime Research (eCrime)*, 1–13.

Lord, N., Flores Elizondo, C. J., & Spencer, J. (2017). 'The dynamics of food fraud: The interactions between criminal opportunity and market (dys) functionality in legitimate business'. *Criminology & Criminal Justice, 17*(5), 605–623.

Maftei, L. (2012). 'An Overview of the Tobacco Black Market in Europe'. *CES Working Papers, Vol. 4*(Iss. 3a), 541–553.

Maillette, M. N. (2015). 'Case study: Financial indicators of the Mafia in the Montreal municipality infrastructure. In: C. Huang, A. Lyhyaoui, Z. Guofang, & N. Benhayoun (Eds.), *Emerging Economies, Risk and Development, and Intelligent Technology: Proceedings of the 5th International Conference on Risk Analysis and Crisis Response*. London: Taylor and Francis.

Markovska, A., & Zabyelina, Y. (2016). 'Enforcing prohibitions in weak states: Gambling in Ukraine'. In P. van Duyne, Scheinost, M., Antonopoulos, G.A., Harvey J., and von Lampe, K. (Eds.), *Narratives on Organised Crime in Europe: Criminals, Corrupters & Policy*. Wolf Legal Publishers.

Marvin, H. J., Bouzembrak, Y., Janssen, E. M., Van der Fels-Klerx, H., van Asselt, E. D., & Kleter, G. A. (2016). 'A holistic approach to food safety risks: Food fraud as an example'. *Food research international, 89*, 463–470.

Masini, S. (2018). 'Mafia makes billions from the Italian food industry'. Interviewer: Eurobsit.

Massari, M., & Monzini, P. (2004). 'Dirty businesses in Italy: a case-study of illegal trafficking in hazardous waste'. *Global Crime, 6*(3–4), 285–304.

Mawby, R. I. (2012). *Burglary*. New York: Routledge.

McGuire, M. (2018). 'Into the web of profit: An in-depth study of cybercrime, criminals and money'. Retrieved from: https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

Medina, L., & Schneider, F. (2019). 'Shedding Light on the Shadow Economy: A Global Database and the Interaction with the Official One'. Retrieved from: https://www.ifo.de/DocDL/cesifo1_wp7981.pdf

Melzer, S., & Martin, C. (2016). 'A brief overview of illicit trade in tobacco products.' in, Illicit Trade: Converging Criminal Networks (OECD).
Meneghini, C., Favarin, S., Andreatta, D., & Savona, E. (2017). 'An exploratory estimate of the extent of illicit waste trafficking in the EU'. Retrieved from: http://www.blockwaste.eu/
Mikhaylov, A., & Frank, R. (2016). 'Cards, money and two hacking forums: An analysis of online money laundering schemes'. Paper presented at the 2016 European Intelligence and Security Informatics Conference (EISIC).
Mills, H., Skodbo, S., & Blyth, P. (2013). 'Understanding organised crime: estimating the scale and the social and economic costs'. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246390/horr73.pdf
MONEYVAL. (2012). 'Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction'. Retrieved from: https://rm.coe.int/research-report-criminal-money-flows-on-the-internet-methods-trends-an/168071509a
Moore, T., Clayton, R., & Anderson, R. (2009). 'The economics of online crime'. *Journal of Economic Perspectives, 23*(3), 3–20.
Morselli, C., Laferrière, D., & Reeves-Latour, M. (2012). 'International experiences in collusion and corruption in the construction industry'. *Commission d'enquête sur l'octroi et la gestion des contrats publics dans l'industrie de la construction*.
Nagy, H. Z. A., & Mezei, K. (2016). 'The Organised Criminal Phenomenon on the Internet'. *JE-Eur. Crim. L.*, 137.
National Audit Office. (2019). 'The UK border: preparedness for EU exit October 2019, HC 98, session 2019–2020'.
National Research Council. (2015). 'Understanding the U.S. illicit tobacco market: characteristics, policy context, and lessons from international experiences'. Retrieved from: https://www.nap.edu/catalog/19016/understanding-the-us-illicit-tobacco-market-characteristics-policy-context-and
Naylor, R. T. (2004). *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*: Cornell University Press.
Nelen, H. (2008). 'Real estate and serious forms of crime'. *International Journal of Social Economics, 35*(10), 751–762.
Nets. (2019). 'European Fraud Report – Payments Industry Challenges'. Retrieved from: https://www.paymentscardsandmobile.com/research/european-fraud-report-payments-industry-challenges/
NFCU. (2016). 'Food Crime: Annual Strategic Assessment – A 2016 Baseline'. Retrieved from: https://www.food.gov.uk/sites/default/files/media/document/fsa-food-crime-assessment-2016.pdf
Noel, L. (2018). 'Independent review into serious and organised crime in the waste sector'. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/915937/waste-crime-review-2018-final-report.pdf
Norwegian Initiative on Small Arms Transfers. (N.d.). Homepage. Retrieved from: http://nisat.prio.org/
OECD. (2002). 'Measuring the Non-Observed Economy: A Handbook'. Retrieved from: https://ec.europa.eu/eurostat/ramon/statmanuals/files/oecd_measuring_non_observed_economy_2002_EN.pdf
OECD. (2007). 'Preventing Corruption in Public Procurement.' In. Paris: OECD Publishing.Retrieved from: http://www.oecd.org/gov/ethics/Corruption-Public-Procurement-Brochure.pdf
OECD/EUIPO. (2019). 'Trends in Trade in Counterfeit and Pirated Goods'. Paris: OECD Publishing.
OECD-EUIPO. (2020). 'Trade in Counterfeit Pharmaceutical Products'. Retrieved from: http://www.oecd.org/gov/trade-in-counterfeit-pharmaceutical-products-a7c7e054-en.htm
Olken, B.A. (2007). 'Monitoring corruption: evidence from a field experiment in Indonesia', *Journal of Political Economy*, 115: 200-49.
Operti, E. (2018). 'Tough on criminal wealth? Exploring the link between organized crime's asset confiscation and regional entrepreneurship'. *Small Business Economics, 51*(2), 321–335.
Optimity Advisors. (2015). 'A study on smuggling of migrants: Characteristics, responses and cooperation with third countries'. Retrieved from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/emn-studies/study_on_smuggling_of_migrants_final_report_master_091115_final_pdf.pdf

Oyoo, G. O. (2020). 'Impact of Mobile Money on Financial Crime, Money Laundering, and Terrorism Financing.' *Impact of Mobile Payment Applications and Transfers on Business* (213–230). IGI Global.

Paesano, F. (2019). Working paper 28: Regulating cryptocurrencies – Challenges and considerations. *Basel Institute on Governance.* Retrieved from: https://baselgovernance.org/publications/working-paper-28-regulating-cryptocurrencies-challenges-and-considerations

Paoli, L. (2014). 'How to tackle (organized) crime in Europe? The EU policy cycle on serious and organized crime and the new emphasis on harm'. *European Journal of Crime, Criminal Law and Criminal Justice, 22*(1), 1–12.

Paoli, L., Adriaenssen, A., Greenfield, V. A., & Conickx, M. (2017). 'Exploring definitions of serious crime in EU policy documents and academic publications: A content analysis and policy implications'. *European Journal on Criminal Policy and Research, 23*(3), 269–285.

Papadouka, M. E., & Haenlein, C. (2017). *Organised Crime and Illicit Trade in Europe*. Retrieved from: https://rusi.org/sites/default/files/201705_rusi_organised_crime_and_illicit_trade_in_europe_olaf_papadouka_haenlein.pdf

Partingdon, R. (2019). 'What is a free port? All you need to know about the free-trade zones'. *The Guardian*.

Pegg, D. (2017). 'Corrupt Brazilian tycoon among applicants for Portugal's golden visas'. *The Guardian*.

Persi Paoli, G., Aldridge, J., Ryan, N., & Warnes, R. (2017). 'Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web'. Santa Monica, Calif.: RAND Corporation. Retrieved from: https://www.rand.org/pubs/research_reports/RR2091.html

Petrunov, G. (2011). 'Managing money acquired from human trafficking: case study of sex trafficking from Bulgaria to Western Europe'. *Trends in Organized Crime, 14*(2–3), 165–183.

Phelps, J., Biggs, D., & Webb, E. L. (2016). 'Tools and terms for understanding illegal wildlife trade'. *Frontiers in Ecology and the Environment, 14*(9), 479–489. doi:10.1002/fee.1325

Pinotti, P. (2015). 'The causes and consequences of organised crime: Preliminary evidence across countries'. *The Economic Journal, 125*(586).

Plachta, M. (2020). 'Disparate Visions of the EU-UK Police and Judicial Cooperation After Brexit'. *International Enforcement Law Reporter, 36*(3), 114–116.

Poniatowski, G., Bonch-Osmolovskiy, M., María, J., Durán-Cabré, Esteller-Moré, A., & Śmietanka, A. (2019). 'Study and Reports on the VAT Gap in the EU-28 Member States: 2019 Final Report'. Retrieved from: https://ec.europa.eu/taxation_customs/sites/taxation/files/vat-gap-full-report-2019_en.pdf

Ponsaers, P., Shapland, J., Williams, C., & Williams, C. C. (2008). 'Does the informal economy link to organised crime?'. *International Journal of Social Economics, 35(9)*:7, 644–650.

Prieger, J., & Kulick, J. (2018). 'Cigarette Taxes and Illicit Trade in Europe'. *Economic Inquiry, 56*(3), 1706–1723.

Pro Wildlife, et al. (2017). 'EU IVORY TRADE: THE NEED FOR STRICTER MEASURES: Paper submitted to the European Commission'. Retrieved from: https://www.prowildlife.de/wp-content/uploads/2017/08/EU_IvoryTradeBrief.pdf

Profiling, M. S. (2015). 'Enhancing Physical Security: The Impact of Internet and Social Media Exposure'. *Concierge Security Report, 1*(3).

PwC. (2016). 'Food fraud vulnerability assessment and mitigation: Are you doing enough to prevent food fraud?'.

PWC & Strategy. (2020). 'Where next for banking? COVID-19: UK industry focus'.

Raets, S., Janssens, J., & Vander Beken, T. (2019). 'Financing of Trafficking in Human Beings in Belgium'. In Shentov, O. & Rusev, O. (Eds), *Financing of Organised Crime: Human Trafficking In Focus*, 129–160. Center for the Study of Democracy.

Ravenda, D., Valencia-Silva, M. M., Argiles-Bosch, J. M., & García-Blandón, J. (2019). 'Money laundering through the strategic management of accounting transactions'. *Critical Perspectives on Accounting, 60*, 65–85.

Reuter, P. (1997). 'The mismeasurement of illegal drug markets: the implications of its irrelevance'. Santa Monica, CA.: Rand Corporation. Retrieved from: https://www.rand.org/pubs/reprints/RP613.html

Reuter, P. (2013). 'Are estimates of the volume of money laundering either feasible or useful?'. In Unger, B. & van der Linde, D. (Eds), *Research handbook on money laundering*. Edward Elgar Publishing.

Reuter, P. & Tonry, M. (2020). Organised crime: Less than meets the eye. *Crime and Justice*. (49).
Ribeiro, J., Reino, L., Schindler, S., Strubbe, D., Vall-llosera, M., Araújo, M. B., . . . Monteiro, M. (2019). 'Trends in legal and illegal trade of wild birds: a global assessment based on expert knowledge'. *Biodiversity and Conservation, 28*(12), 3343–3369.
Riccardi, M. (2014). 'When criminals invest in businesses: Are we looking in the right direction? An exploratory analysis of companies controlled by mafias'. In Caneppele, S. & Calderoni, F. (Eds), *Organized crime, corruption and crime prevention,* 197–206. Springer.
Richards, G. (2018). 'How to Tackle Organised Crime in Construction'.
Richet, J.-L. (2013). 'Laundering Money Online: a review of cybercriminals methods'. Retrieved from: https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf
Ritzen, L. (2011). 'Mapping "infected" real estate property'. *Journal of Money Laundering Control*.
Roberts, D. L., & Hernandez-Castro, J. (2017). 'Bycatch and illegal wildlife trade on the dark web'. *Oryx, 51*(3), 393–394.
Rucevska, I., Nelleman, C., Isarin, N., Yang, W., Liu, N., Yu, K., . . . Devia, L. (2015). 'Waste crime – waste risks: gaps in meeting the global waste challenge'.
RUSI. (2020). 'Free Ports, Not Safe Havens. Preventing Crime in the UK's Future Freeports'.
Saggers, T. (2019). 'An assessment of the extent of Albanian speaking organised crime groups involved in drug supply in the European Union: Characteristics, role and the level of influence'. Lisbon: European Monitoring Centre for Drugs and Drug Addiction.
Sanchez, G. (2018). 'Five misconceptions about migrant smuggling (9290846070)'. Retrieved from: https://globalinitiative.net/wp-content/uploads/2018/05/Five-Misconceptions-About-Migrant-Smuggling-European-University-Institute-2018.pdf
Sanders, T. (2008). 'Selling sex in the shadow economy'. *International Journal of Social Economics, 35*(10), 704–716.
Sanders, T. (2013). *Sex Work*. Abingdon: Routledge.
Sat, D. M., Kasatkin, A., Kornev, I., Krylov, G., & Evgenyevich, K. (2016). 'Investigation of money laundering methods through cryptocurrency'. *Journal of theoretical and applied information technology, 83*(2), 244–254.
Savona, E. (2014). 'Organised crime numbers'. *Global Crime, 15*(1–2), 1–9.
Savona, E., & Berlusconi, G. (2015). 'Organized Crime Infiltration of Legitimate Businesses in Europe: A Pilot Project in Five European Countries. Final Report of Project ARIEL – Assessing the Risk of the Infiltration of Organized Crime in EU MSs Legitimate Economies: a Pilot Project in 5 EU Countries'.
Savona, E., & Riccardi, M. (2015). 'From illegal markets to legitimate businesses: The portfolio of organised crime in Europe'.
Savona, E., & Riccardi, M. (Eds.). (2018). 'Mapping the Risk of Serious and Organised Crime Infiltration in Europe – Final Report of the MORE Project'. Milan, Italy.
Savona, E., Riccardi, M., & Berlusconi, G. (2016). *Organised crime in European businesses*. New York, USA: Routledge.
Schneider, F. (2017). 'The Dark Side: Crime Has Gone Global'*.* In *A Closer Look at Globalization – The Positive Facets and the Dark Faces of a Complex Notion*. Paper presented at the 16th Trilogue, Salzburg.
Shea, A. (2018). 'Shooting Fish in A Bliss Bucket: Targeting Money Launderers in the Art Market'. *Columbia Journal Of Law & The Arts, 41*, 665–687.
Shentov, O., Rusev, A., & Antonopoulos, G. A. (2019). 'Financing of Organised Crime: Human Trafficking in Focus'. Retrieved from: https://research.tees.ac.uk/en/publications/financing-of-organised-crime-human-trafficking-in-focus
Scherrer, A. & Thirion, E. (2018). 'Citizenship by Investment (CBI) and Residency by Investment (RBI) Schemes in the EU: State of Play, Issues and Impacts', *Study of the European Parliamentary Research Service*, PE, 627: 128.
Shimazono, Y. (2007). 'The state of the international organ trade: a provisional picture based on integration of available information'. *Bulletin of the World Health Organization, 85*, 955–962.
Siegel, D. (2019). 'Human smuggling reconsidered: the case of Lesbos'. Paper presented at the The 19th cross-border Crime Colloquium.
Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J., & Salas, A. (2020). Exploring the use of Zcas h cryptocurrency for illicit or criminal purposes.
Simmons, M. (2018). 'Theorizing Prostitution: The Question of Agency'. In Dank, B. M. (Ed.), *Sex Work and Sex Workers.* Routledge: New York.

Sina, S., Gerstetter, C., Porsch, L., Roberts, E., Smith, L., Klaas, K., & de Castillo, T. F. (2016). 'Wildlife Crime'. *Policy Department A: Economic and Scientific Policy. Directorate General for Internal Policies*.

Slack, B., & Rodrigue, J. P. (2020). 'Transport safety and security'. In J. P. Rodrigue (Ed.), *The geography of transport systems* (Vol. 5). New York: Routledge.

Sosnowski, M. C., Knowles, T. G., Takahashi, T., & Rooney, N. J. (2019). 'Global ivory market prices since the 1989 CITES ban'. *Biological Conservation, 237*, 392–399. doi:10.1016/j.biocon.2019.07.020

Soudjin, M. (2015). 'Hawala and money laundering: potential use of Red flags for persons offering hawala services'. *European Journal on Criminal Policy and Research, 21*(2), 257–274.

Spink, J., & Moyer, D. C. (2011). 'Defining the public health threat of food fraud'. *Journal of food science, 76*(9), R157–R163.

Spink, J., Moyer, D. C., Park, H., & Heinonen, J. A. (2013). 'Defining the types of counterfeiters, counterfeiting, and offender organizations'. *Crime Science, 2*(1), 1.

Stambøl, E. M. (2019). 'The EU's fight against transnational crime in the Sahel'. *Institute for European Studies Policy Brief, 4*.

Stein, F. M., Wong, J. C., Sheng, V., Law, C. S., Schröder, B., & Baker, D. M. (2016). 'First genetic evidence of illegal trade in endangered European eel (Anguilla anguilla) from Europe to Asia'. *Conservation Genetics Resources, 8*(4), 533–537.

Straub, S. (2014). Political firms, public procurement, and the democratization process.

Sullivan, B. A., Chan, F., Fenoff, R., & Wilson, J. M. (2017). 'Assessing the developing knowledge-base of product counterfeiting: a content analysis of four decades of research'. *Trends in Organized Crime, 20*(3–4), 338–369.

Sustainable Eel Group. (2018a). 'Again, Germany has been used as transit country for glass eel trafficking! [Press release]'. Retrieved from: https://www.sustainableeelgroup.org/germany-is-transit-country-for-one-of-planets-greatest-wildlife-crime-2/

Sustainable Eel Group. (2018b). 'Quantifying the illegal trade in European glass eels (Anguilla anguilla): Evidences and Indicators'. Retrieved from: https://www.sustainableeelgroup.org/wp-content/uploads/2018/02/SEG-Report-2018-1-V1-1.pdf

Suvantola, L., Favarin, S., Mehlbaum, S., Sahramäki, I., Savona, E., Spapens, T., & Kankaanranta, T. (2017). 'Blocking the loopholes for illicit waste trafficking (blockwaste) - Final Consolidated Report'. Retrieved from: https://drive.google.com/file/d/1ItSzdolm0Gt4D7iw9XdlohxqvRa81h5I/view

't Sas-Rolfes, M., Challender, D. W. S., Hinsley, A., Veríssimo, D., & Milner-Gulland, E. J. (2019). 'Illegal wildlife trade: Scale, processes, and governance'. *Annual Review of Environment and Resources, 44*(1), 201–228. doi:10.1146/annurev-environ-101718-033253

Tax Justice Network. (2020). 'Financial Secrecy Index '. Retrieved from: https://fsi.taxjustice.net/en/.

Tenti, V. (2012). 'Framing Mafia Infiltration in the Public Construction Industry in Italy'. Report prepared for the Canadian Commission d'enquête sur l'octroi et la gestion des contrats publics dans l'industrie de la construction. Retrieved from: https://www.lapresse.ca/html/1554/7P-119.pdf

Terziev, V., Petkov, M., & Dragomir, K. (2018). 'Eurojust casework on mafia-type criminal organisations'. *Proceedings of SOCIOINT 2018.*

The Anti-Counterfeiting Group. (2020). 'Online fraudsters exploit COVID-19 fears'.

Tiniti, P., & Reitano, T. (2016). *Migrant, Refugee, Smuggler, Saviour*. London: Hurst & Co Publishers.

Tops, P., van Valkenhoef, J., van der Torre, E., & van Spijk, L. (2018). 'The Netherlands and synthetic drugs: an inconvenient truth'. The Hague: Eleven International Publishing.

Tracit. (2019). 'Mapping the Impact of Illicit Trade on the Sustainable Development Goals'. Retrieved from: https://www.tracit.org/uploads/1/0/2/2/102238034/standalone_traffickingpersons.pdf

TRAFFIC. (2020). 'An overview of seizures of CITES-listed wildlife in the European Union: January to December 2018'. Retrieved from: https://www.traffic.org/site/assets/files/12745/eu-seizures-report-2020-final-web.pdf

Transcrime. (2015a). 'An European outlook on the illicit trade in tobacco products'. *Trends in Organized Crime, 19*(3/4), 300–328. doi: 10.1007/s12117-015-9260-1.

Transcrime. (2015b). 'From Illegal Markets to Legitimate Businesses: The Portfolio of Organised Crime in Europe'. Retrieved from: http://www.transcrime.it/pubblicazioni/the-portfolio-of-organised-crime-in-europe/

Transparency International. (2006). Curbing Corruption in Public Procurement. Retrieved from: https://www.transparency.org/en/publications/curbing-corruption-in-public-procurement-a-practical-guide
Transparency International. (2017). 'Tainted Treasures: Money Laundering Risks in Luxury Markets'.
Transparency International. (2018). 'European gateway: Inside the murky world of Golden Visas'.
Transcrime. (2019). ITTP NEXUS in Europe and Beyond (Transcrime – Università Cattolica del Sacro Cuore: Milano).
Treadwell, J. (2012). 'From the car boot to booting it up? eBay, online counterfeit crime and the transformation of the criminal marketplace'. *Criminology & Criminal Justice, 12*(2), 175–191.
Trend Micro. (2011). 'Cybercriminals Selling PayPal Accounts for Personal Gain'.
UK Parliament. (2018). 'VAT fraud: cooperation between tax administrations'.
UNEP, CITES, IUCN, & TRAFFIC. (2013). 'Elephants in the dust : the African elephant crisis - a rapid response assessment'. Retrieved from: https://portals.iucn.org/library/sites/library/files/documents/2013-002.pdf
Unger, B., Siegel, M., Ferwerda, J., de Kruijf, W., Busuioic, M., Wokke, K., & Rawlings, G. (2006). 'The amounts and the effects of money laundering'. Report prepared for the Dutch Ministry of Finance. Retrieved from: https://www.maurizioturco.it/bddb/2006_02_16_the_amounts_and_.pdf
UNODC. (2010). 'The Globalization of Crime: A Transnational Organized Crime Threat Assessment'. Retrieved from: https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf
UNODC. (2011a). 'Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes - Research Report (final draft)'. Retrieved from: https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf
UNODC. (2011b). 'Smuggling of Migrants: A global review and annotated bibliography of recent publications'. Retrieved from: https://www.unodc.org/documents/human-trafficking/Migrant-Smuggling/Smuggling_of_Migrants_A_Global_Review.pdf
UNODC. (2014). 'Global report on trafficking in persons'. Retrieved from: https://www.unodc.org/documents/data-and-analysis/glotip/GLOTIP_2014_full_report.pdf
UNODC. (2015). 'Drug Money: The Illicit Proceeds of Opiates Trafficked on the Balkan Route'. Retrieved from: https://www.unodc.org/documents/data-and-analysis/Studies/IFF_report_2015_final_web.pdf
UNODC. (2018). 'Global study on Smuggling of Migrants'. Retrieved from: https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2018_web_small.pdf
UNODC. (2020). 'World Wildlife Crime Report'. Retrieved from: https://www.unodc.org/documents/data-and-analysis/wildlife/2020/World_Wildlife_Report_2020_9July.pdf
US National Cancer Institute & WHO. (2016). 'The economics of tobacco and tobacco control'. Retrieved from: https://cancercontrol.cancer.gov/brp/tcrb/monographs/21/docs/m21_complete.pdf
US Payments Forum. (2018). 'Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions'. Retrieved from: https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf
Van Daele, S., & Vander Beken, T. (2010). 'Exploring itinerant crime groups'. *European Journal on Criminal Policy and Research, 16*(1), 1–13.
Van de Bunt, H. (2008). 'A case study on the misuse of hawala banking'. *International Journal of Social Economics, 35*(9), 691–702.
van Dijk, J., Van der Knaap, L. M., Aebi, M. F., & Campistol, C. (2014). 'Counting what counts: tools for the validation and utilization of EU statistics on human trafficking'.
Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C. H., Klievink, B., . . . Van Eeten, M. (2018). 'Plug and prey? measuring the commoditization of cybercrime via online anonymous markets'. *Proceedings of the 27th USENIX Security Symposium*, 1009–1026.
Victorian Law Reform Commission. (2020). 'The infiltration of organised crime groups into lawful occupations and industries'. Retrieved from: https://www.lawreform.vic.gov.au/content/3-infiltration-organised-crime-groups-lawful-occupations-and-industries

Vincent, M. (2020). 'Brexit risks making London's dirty money fight harder, say lawyers'. *Financial Times*.
Walle, G. V. (2008). 'A matrix approach to informal markets: towards a dynamic conceptualisation'. *International Journal of Social Economics, 35*(9), 651–665.
Western Union. (2020). 'Notice of 2020 Annual Meeting of Stockholders'. Retrieved from: https://www.wuannualmeeting.com/pages/notice-of-annual-meeting-of-stockholders/
WHO. (2015). 'Illegal trade of tobacco products: What you should know to stop it'. Retrieved from: https://apps.who.int/iris/bitstream/handle/10665/170994/WHO_NMH_PND_15.3_eng.pdf;jsessionid=23A27DFD93CC37063C9B372C08E92E6E?sequence=1
WHO FCTC. (2014). 'Combating the illicit trade in tobacco products from a European perspective'. *Regional Studies Series, Paper R/3*.
Williams, C. (2015). 'The informal economy as a path to expanding opportunities'. Retrieved from: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2804172_code2015439.pdf?abstractid=2804172&mirid=1
Williams, P. (2001). 'Organized crime and cybercrime: Synergies, trends, and responses'. *Global Issues, 6*(2), 22–26.
Wollinger, G. R., Querbach, M., Röhrig, A., König, A., & Isenhardt, A. (2018). 'Offender organization and criminal investigations with regard to organised residential burglary'. Retrieved from: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_147%20en.pdf
World Bank. (2019). 'Worldwide governance indicators'. Retrieved from: http://info.worldbank.org/governance/wgi/
World Bank. (2009). Annual integrity report, fiscal year 2008: protecting development's potential. Retrieved from https://documentos.bancomundial.org/en/publication/documents-reports/documentdetail/305111468339613097/undefined
WWF. (2018). 'Second-biggest direct threat to species after habitat destruction'. Retrieved from: https://wwf.panda.org/our_work/our_focus/wildlife_practice/problems/illegal_trade/#:~:text=Wildlife%20trade%20can%20also%20cause,by%20humans%20of%20some%20species
WWF. (2019). 'Two years after China bans elephant ivory trade, demand for elephant ivory is down'. Retrieved from: https://www.worldwildlife.org/stories/two-years-after-china-bans-elephant-ivory-trade-demand-for-elephant-ivory-is-down
WWF. (n.d.). 'Coalition to End Wildlife Trafficking Online'. Retrieved from: https://www.worldwildlife.org/pages/coalition-to-end-wildlife-trafficking-online
Yin, S. (2006). 'A new framework for maritime security inspection under U.S. security protocols'.
Yin Sun, H., & Vatrapu, R. (2017). 'A First Estimation of the Proportion of Cybercriminal Entities in the Bitcoin Ecosystem using Supervised Machine Learning'. Paper presented at the Proceedings of 2017 IEEE International Conference on Big Data.
Young, M. A. (2016). 'Financial transparency in Britain's secrecy jurisdictions has just got a whole lot murkier following the UK's decision to leave the EU'. *Journal of International Banking Law and Regulation, 31*(11).

GETTING IN TOUCH WITH THE EU

In person
All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email
Europe Direct is a service that answers your questions about the European Union. You can contact this service:
–by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
–at the following standard number: +32 22999696, or
–by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online
Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en
EU publications
You can download or order free and priced EU publications from: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).
EU law and related documents
For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu
Open data from the EU
The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

doi:10.2837/64101