Havas, Attila; Amann, Philipp; Letizi, Marco; Nitsch, Holger; Türkşen, Umut

Working Paper

Futures of the interpenetration of criminal and lawful economic activities in the European Union in 2035: Scenarios and policy implications

KRTK-KTI Working Papers, No. KRTK KTI WP - 2023/37

Provided in Cooperation with:
Institute of Economics, Centre for Economic and Regional Studies, Hungarian Academy of Sciences

Suggested Citation: Havas, Attila; Amann, Philipp; Letizi, Marco; Nitsch, Holger; Türkşen, Umut (2023) : Futures of the interpenetration of criminal and lawful economic activities in the European Union in 2035: Scenarios and policy implications, KRTK-KTI Working Papers, No. KRTK KTI WP - 2023/37, Hungarian Academy of Sciences, Institute of Economics, Centre for Economic and Regional Studies, Budapest

This Version is available at:
https://hdl.handle.net/10419/297038

INSTITUTE OF ECONOMICS
Centre for Economic and Regional Studies

HUN-REN
Hungarian Research Network

Közgazdaság- és Regionális Tudományi Kutatóközpont
KÖZGAZDASÁG-TUDOMÁNYI INTÉZET

KRTK-KTI WORKING PAPERS | KRTK-KTI MŰHELYTANULMÁNYOK

Futures of the interpenetration of criminal and lawful economic activities in the European Union in 2035: Scenarios and policy implications

ATTILA HAVAS – PHILIPP AMANN – MARCO LETIZI

– HOLGER NITSCH – UMUT TURKSEN

KRTK-KTI WP – 2023/37

December 2023

INSTITUTE OF ECONOMICS, CENTRE FOR ECONOMIC AND REGIONAL STUDIES
HUNGARIAN RESEARCH NETWORK (HUN-REN)
BUDAPEST

ABSTRACT
Policy-makers – working on various domains, notably regulations, home affairs, security, science, technology, and innovation (STI) policies – need to pay close attention to possible new ways and methods for the interpenetration of criminal and lawful economic activities. This paper is aimed at assisting these policy-makers by presenting four possible futures (scenarios) on the interpenetration of criminal and lawful economic activities and considering their implications.
These scenarios assume that the interpenetration of criminal and lawful economic activities – just as most other types of crime – cannot be fully eradicated. There are two competing groups of actors whose capacities, activities, and efficiency largely determine the possibilities for, and repercussions of, the interpenetration of criminal and lawful economic activities: criminal actors and law enforcement agencies (LEAs). The scenarios, therefore, are shaped by two main dimensions: i) whether LEAs are well-resourced, strong, and effective or not, and ii) whether large criminal organisations or small-scale ones are the dominant criminal actors. Hence, the four scenarios consider various types of 'push' and 'pull' factors that influence actors to commit – or not – criminal economic activities; the main types of these activities; features of regulations; research, technological development, and innovation activities by the criminal actors vs LEAs; as well as the activities, capabilities, and resources of LEAs.
By considering the nature of the criminal activities that aim at penetrating lawful economic activities, and the options to prevent, monitor, and fight these crimes, the report explores a range of policy implications, especially for STI policies and regulations. Further, it stresses the multi-level nature of policy-making in the EU, as well as the need for collaboration with the willing countries outside the EU. Criminal actors can penetrate lawful economic activities in the EU when commissioned by hostile ('rogue') states that aim to weaken and/or undermine the EU and its Member States as part of their geopolitical power games.

JEL codes: K42, M48, O17, O38, O39
Keywords: Criminal economic activities; Fighting crime; Preventing crime; Information and communication technologies; Social science research; Regulation; Prospective analyses; Scenarios

Attila Havas
Institute of Economics, Centre for Economic and Regional Studies
and AIT Austrian Institute of Technology, Center for Innovation Systems and Policy
havas.attila@krtk.hu-ren.hu

Philipp Amann
Former Head of Strategy, European Cybercrime Centre, Europol

Marco Letizi
Global Consultant of the European Commission, Council of Europe, and United Nations

Holger Nitsch
CEPOLIS, Hochschule für den öffentlichen Dienst in Bayern

Umut Turksen
Coventry University

Az illegális és törvényes gazdasági tevékenységek összefonódásának jövőbeni lehetőségei az Európai Unióban: Jövőképek és szakpolitikai következmények

HAVAS ATTILA – PHILIPP AMANN – MARCO LETIZI

– HOLGER NITSCH – UMUT TURKSEN

ÖSSZEFOGLALÓ

A szakpolitikai döntéshozóknak – akik különböző területeken, elsősorban a szabályozás, a belügyek, a biztonság, a tudomány-, technológia- és innovációpolitika területén dolgoznak – nagy figyelmet kell fordítaniuk a bűnözés és a törvényes gazdasági tevékenységek összefonódásának lehetséges új módjaira és módszereire. A tanulmány célja, hogy a szakpolitikusokat támogassa a bűnözés és a legális gazdasági tevékenységek összefonódásának négy lehetséges jövőképének bemutatásával és ezek következményeinek mérlegelésével.

A négy jövőkép alapfeltevése, hogy a bűnözés és a törvényes gazdasági tevékenységek összefonódását – a legtöbb más bűncselekménytípushoz hasonlóan – nem lehet teljesen felszámolni. Két, egymással versengő csoport képességei, tevékenységei és hatékonysága határozza meg jelentős mértékben a bűnözés és a törvényes gazdasági tevékenységek összefonódásának lehetőségeit és következményeit: a bűnözők és a bűnüldöző szervek (LEA-k). A jövőképeket ezért a következő „változók” alakulása alakítja: i) a bűnüldöző szervek jól felszereltek, erősek és hatékonyak vagy sem, illetve ii) a nagy vagy a kisebb bűnszervezetek a domináns bűnügyi szereplők. A négy jövőkép figyelembe veszi a gazdasági bűncselekmények elkövetésére ható különböző tényezőket; e tevékenységek főbb típusait; a szabályozás jellemzőit; a bűnügyi szereplők és a LEA-k kutatás-fejlesztési és innovációs tevékenységét; valamint a LEA-k tevékenységeit, képességeit és erőforrásait.

A tanulmány a törvényes gazdasági tevékenységekbe való beépülést célzó bűncselekmények jellegét, valamint az e bűncselekmények megelőzésére, nyomon követésére és leküzdésére irányuló lehetőségeket veszi számba, és szakpolitikai következményeit elemzi, különösen a tudomány-, technológia- és innovációpolitika és szabályozás területén. A szakpolitikai tervezés többszintű jellegét is hangsúlyozza, valamint az EU-n kívüli országokkal való együttműködés szükségességét.

JEL: K42, M48, O17, O38, O39

Kulcsszavak: Gazdasági bűnözés; Bűnüldözés; Bűn megelőzés; Információs és kommunikációs technológiák; Társadalomtudományi kutatások; Szabályozás; Előretekintés; Jövőképek

TABLE OF CONTENTS

1) INTRODUCTION*

The four freedoms of the EU Single Market – free movement of goods, services, people, and capital – are invaluable for EU citizens and businesses. These freedoms, however, are also abused by criminal actors, significantly undermining citizens' quality of life and the lawful businesses' competitiveness. Further, with the advancement of technologies, citizens and businesses can benefit from new opportunities but they are also confronted with a series of problems, such as insufficient consumer protection, distorted competition, lack of environmental risk assessment or abuse of technologies. The penetration of legal economic activities by criminal actors is a far-reaching, costly abuse, which exploits new technologies developed by themselves or by lawful actors. Clearly, potential victims need to be aware of threats and make their best efforts to protect themselves. Yet self-protection alone is not enough against mighty organised criminal groups. The state needs to apply its tools – especially effective regulations and well-endowed, well-organised law enforcement agencies (LEAs) – to prevent, monitor, and fight the interpenetration of criminal and lawful economic activities. The state also needs to protect itself against corruption, tax evasion, smuggling, human and migrant trafficking, counterfeit of goods and means of payment, etc.

Therefore, policy-makers – in various domains, notably regulations, home affairs, security, science, technology, and innovation (STI) policies – need to pay close attention to possible new ways and methods that facilitate the interpenetration of criminal and lawful economic activities. This policy brief aims at assisting these policy-makers by devising four possible futures (scenarios) in 2035 and considering their implications. The presented scenarios are not predictions, rather, they depict possible futures.[1]

This policy brief is organised as follows. Section 2 explains the logic that underpins the scenarios. Section 3 depicts four possible future states (scenarios) and derives specific policy implications. Given the nature of the criminal activities that aim at penetrating lawful economic activities, as well as the possibilities to prevent, monitor, and fight these crimes, the group of experts identified policy implications, especially for STI policies and regulations, considering the multi-level nature of policy-making in the EU, as well as the need for collaboration with willing countries outside the EU. As crime has internationalised, nation-states on their own cannot be successful in fighting crime, especially organised crime. Section 4 briefly discusses state-sponsored criminal economic activities as those are becoming of crucial importance in light of rising geopolitical tensions. In conclusion, section 5 summarises the overall policy implications, not tied to a specific scenario.

* This paper is the result of one of the eight Deep Dive Foresight Studies performed in the frame of the 'European R&I Foresight and Public Engagement for Horizon Europe' project, conducted by the 'Foresight on Demand' consortium for the European Commission. During the summer of 2023, an expert team identified factors of change and met in four workshops to build scenarios and derive policy implications. Other experts from national and EU public administration have also contributed to this policy brief in various ways, through various channels. Furthermore, the process was supported by discussions in the Commission's internal Horizon Europe Foresight Network. Finally, we are especially grateful for the guidance and editorial contributions of Nikolaos Kastrinos (DG RTD, European Commission) and Totti Könnölä (Insight Foresight Institute).

[1] Exploring multiple scenarios helps expand one's own span of observation further towards the future, to possible threats and opportunities that might not be in the immediate attention span or might be excluded for being unlikely.

2) FOUNDATIONS FOR THE SCENARIOS

The four scenarios, confined to the European Union[2], are based on the assumption that interpenetration of criminal and lawful economic activities – just as most other types of crime – cannot be fully eradicated. Crime has been around for millennia and will be part of our future as well.

In this policy brief, we refer to *criminal economic activities* as non-violent criminal and illicit activities[3] committed by an individual, a group of individuals, or a (criminal) organisation with the purpose of (i) gaining wealth or other advantage, as well as (ii) causing significant losses to the victim(s), e.g., a rival organisation, be it a firm, a government body, or an entire state. The focus is on the (possibilities for) interpenetration of criminal and lawful economic activities, and not on all economic crime. The *interpenetration of criminal and lawful economic activities* refers to illicit funds reinvested both in criminal activities and in legal activities, in which case, they are integrated into the legal economy after having been laundered.

There are two competing groups of actors whose capacities, activities, and efficiency largely determine the possibilities for, and repercussions of, the interpenetration of criminal and lawful economic activities: criminal actors and LEAs. The outcomes of their race - or 'game' – have major repercussions for society and the economy, and occasionally for the environment as well.

2.1 Criminal actors

Criminal actors include both large and small-scale organisations, as well as individuals who may commit crimes on their own and/or be recruited or 'commissioned' by criminal organisations to play different roles, and the overall landscape significantly differs depending on whether large or small-scale organisations play the dominant role. Potential and actual victims, as well as various government agencies other than LEAs are also part of 'the game'.

Lawful economic activities are conducted by law-abiding businesses (honest firms with good intentions). Seemingly law-abiding firms, set up by criminal actors (individuals or organisations), engaged in lawful economic activities provide a "channel" for the interpenetration of criminal and lawful economic activities. States with seemingly robust regulatory framework may be infiltrated by criminal actors without being detected for a long time.[4]

The types, intensity, and frequency of criminal organisations' (and individuals') activities[5] are shaped conditioned by 'push' and 'pull' factors. Push factors motivate actors to engage in criminal economic activities as they are dissatisfied with the opportunities to earn money as lawful actors. Push factors are weak when firms and individuals are satisfied with the opportunities to earn money as lawful actors. In contrast, push factors are strong when:

- taxes and social contributions are perceived as too high by firms and/or individuals;

---

[2] Our scenarios are confined to the European Union for two reasons. First, jurisdiction is a decisive issue when it comes to fighting criminal activities. Second, systematically considering other world regions would make this exercise far too complex. However, from time to time it is worth highlighting the relevance – possible impacts – of extra-EU actors or factors. For instance, when major actors – those with strong financial muscles – are dissatisfied with the opportunities to earn money as lawful actors in their own territory outside the EU, they might enter the EU, either as lawful or illicit actors.

[3] Although criminal economic activities are non-violent by their nature, they might involve violence, e.g., when these are committed by mafia-type organisations.

[4] Danske Bank fined €470m over international money laundering scandal, Euronews, 14/12/2022, https://www.euronews.com/2022/12/14/danske-bank-fined-470m-over-international-money-laundering-scandal

[5] The typical perpetrators and victims of criminal economic activities, as well as the types of harms caused are summarised in Annex 1.

- individuals face difficulties in finding employment in the legal economy, offering a decent wage (sufficient for leading a 'normal' life) because the economy is stagnating or declining, and/or because of a highly skewed income and wealth distribution (perceived as 'unjust'); and
- lack of (or insufficient) investment opportunities in the 'white' economy 'pushes' certain actors into the grey or dark zones of the economy.

Criminal actors seek investment opportunities in legitimate economic activities as well as in criminal activities to increase their wealth of lawful or unlawful origin. Organised crime groups tend to penetrate lawful economic activities to dominate the territory where they operate.

The most important 'pull' factor is the efficacy of regulations as regulatory loopholes are likely to attract criminal actors, while 'tight' regulations discourage them from entering well-protected sectors or entire economies. We consider both national and EU-level regulations.[6]

Regulations affect the interpenetration of criminal and lawful activities through another important channel. When LEAs have the necessary legal tools (empowerment) to fight crime, they are strong players in the 'game', otherwise they are weak. Thus, it is worth highlighting the main features of effective vs. ineffective regulation:

Regulation is effective when

- behaviours in society comply with its intentions and regulation is trusted as fair and morally correct;
- legal actors – the state, businesses, and civil society – play a decisive role in setting rules and regulations[7]
- people are willing to report illegal activities; and
- regulatory loopholes are minimised as lucrative opportunities for criminal economic activities are limited.

When regulation is effective, the 'pull factors' to engage in criminal economic activities are weak.

Regulation is ineffective when

- Behaviours in society do not comply with its intentions, either because they choose to suffer the consequences of non-compliance, or because of lack of consequences, e.g., through regulatory loopholes. Loopholes in regulation can manifest themselves in various ways. For example, the legal provisions do not cover new types of assets such as non-fungible tokens, or the diversity of national approaches allows for forum shopping by criminals, whereby they can choose softer legal regimes, in terms of criminalisation and punishment therein, to conduct their activities.

Sudden, disruptive – technological, economic, or societal – changes, especially when those provide opportunities for designing new business models by criminal actors may weaken even the most effective regulatory regime.

---

[6] The primary sources of EU law consist of treaties and general principles of EU law, and the secondary sources include regulations, directives, decisions, recommendations, and opinions. In this report we use the term 'regulations' to refer to these various types of legal instruments that are created by the EU to govern the thematic issues that are identified as priority areas that can be interpenetrated by criminal activities. Given the limited space available and in the interest of making the report succinct, it is not possible to analyse every single legal instrument and provisions therein.

[7] Wide societal involvement in setting regulations is an important factor in creating regulations that are trusted and seen as morally correct. Yet, some are critical of stakeholder involvement in regulation as creating the conditions for regulatory capture, regulatory bias, and loopholes.

Criminal actors can penetrate lawful economic activities in the EU commissioned by hostile ('rogue') states that aim to weaken the EU as part of their geopolitical power game. We consider that possibility separately because it falls 'outside' our scenarios. Yet we will highlight the link between this threat and specific elements of our scenarios.

2.2 Law enforcement agencies

The other major actors in 'the game' are the LEAs. Disregarding a radical option, in which the state is practically dismantled, and all potential victims are left alone to protect themselves against criminal actors, LEAs will keep this role in the future as well.

LEAs are strong when they

- have clearly set mandates and strategic objectives;
- operate in an environment characterised by effective regulations;
- are entitled to use the necessary legal and technological tools to prevent, monitor, and fight criminal economic activities;
- are governed by appropriate bylaws and internal rules;
- are intact from corruption and internal irregularities;
- have the necessary resources, skills, capacities, and capabilities to monitor and fight criminal economic activities;
- have the necessary resources to develop new technological and non-technological tools to prevent, monitor, and fight criminal economic activities (either in-house, in collaboration with other public or private entities, or to commission other public or private entities to develop these tools);
- have access to the necessary pieces of information, held by other government bodies and agencies, to prevent, monitor, and fight criminal economic activities;
- can rely on effective collaboration with the relevant public and private entities.

The more of these preconditions are unmet, the weaker LEAs become.

2.3 Four scenarios in brief

By considering whether large or small-scale criminal organisations would be the dominant players (due to various constellations of the push and pull factors described above) on the one hand, and the strength of LEAs, on the other, we define four scenarios to contemplate about possible futures:

- Scenario 1: *Neck and neck race* between strong, resourceful, determined, well-organised large criminal organisations and strong, effectively working LEAs;
- Scenario 2: *Safe haven for legal actors*; small-scale criminal organisations try to penetrate the legal economy; lawful actors are protected by strong, effectively working LEAs;
- Scenario 3: *Protected pockets*; small-scale criminal organisations take advantage of weak LEAs; lawful economic actors need to find and to some extent create protected pockets for themselves; and
- Scenario 4: *Paradise for Criminals*; strong, resourceful, determined, well-organised large criminal organisations have the upper hand against weak, ineffectively working LEAs.

Figure 1: Four scenarios

Source of illustrations: Getty images

When describing these scenarios in more detail in the following section, we consider the main types of criminal economic activities; features of regulations; research, technological development and innovation activities to create technological opportunities to commit criminal economic activities and prevent the interpenetration of criminal and lawful economic activities; as well as the activities, capabilities, and resources of LEAs.

We present descriptions of possible futures[8] (written in the present tense, as if we were already in the year 2035).

[8] Fully-fledged scenarios – or path scenarios –, in contrast, describe both a possible future state and the path from the present leading to that future.

3) FOUR SCENARIOS ON THE INTERPENETRATION OF CRIMINAL AND LAWFUL ECONOMIC ACTIVITIES IN 2035

3.1 Scenario 1: *Neck and neck race*

Key dimensions

- Large criminal organisations
- Strong, effective LEAs

Main features

The EU's economy is flourishing, it is characterised by high growth, coupled with high taxes. Due to considerable public revenues, LEAs are strong: they have sufficient resources, skills, capabilities, and capacities to prevent, monitor, and fight the interpenetration of criminal and lawful economic activities. Lawful economic actors and other potential victims are protected by effective regulations, and they support effective actions of LEAs. Illicit actors can rarely influence regulatory processes. However, large, well-organised criminal organisations have strong incentives to engage in criminal economic activities via penetrating lawful economic activities. They have massive funds invested in the EU – in the black, grey, and white segments of the economy – taking advantage of the flourishing economy. They avoid paying high taxes and launder their sizeable illegal proceeds. Furthermore, they use their substantial resources to develop new technological tools and 'business models' to further penetrate their criminal activities into the lawful economy.

Criminal actors and criminal activities

To address former weaknesses of the legal frameworks in the EU and jurisdictions beyond the EU, improving the transnational cooperation has been crucial. The EU has claimed a leadership role at the global level in the fight against organised crime and money laundering.

However, organised crime groups and mafia-type organisations have found their ways to penetrate lawful economic activities, taking advantage of their high capacity to penetrate the political, judicial, social, and economic fabric, even at a high level.

Effective regulation, paradoxically at a first glance, incentivizes creativity to circumvent it. As competition is reduced criminal gains can be high. Criminal economic activities include sophisticated schemes of tax evasion (incl. social contributions), money laundering, and corruption to occasionally cut rifts in the bastions of effective regulations. Blockchain technology and decentralised financial products (such as non-fungible tokens) are widely used by criminal actors for money laundering, e.g., at telematic auctions of luxury goods and works of art, precious stones, and other so-called safe-haven assets (or "refugee goods"). Counterfeiting activities are flourishing as well-funded and well-managed companies specialise in producing and/or distributing illegally branded goods of high esteem. Counterfeiting takes place inside the EU to some extent, but mostly in South-East Asia.

Regulation

Private entities are allotted a significant degree of responsibility and obligation to record and report their activities to competent authorities. Due diligence and anti-money-laundering and tax compliance monitoring and reporting obligations are placed on accountants and auditors. However, accountants, auditors, and tax advisers often fail to report criminal activities. As they are dependent on their clients for income, they face a strong conflict of interest.

The interpenetration of organised criminal and lawful economic activities is facilitated by insiders, either by public servants and/or private actors imbued by crime detection and

prevention responsibilities (e.g., suspicious transaction reporting under anti money laundering [AML] regulations), or collusion between these entities by corrupt practices.

Regulatory requirements result in extensive reporting, which creates information pollution for LEAs. Analysing and screening large volumes of transactions for traces of criminal activities necessitate advanced technological tools. Large criminal groups, with ample resources, adapt and change their methods and practices frequently and rapidly to stay ahead of this technological race with LEAs. As a result, even when the regulations and policies applied to oversee financial transactions are deemed to be robust and effective, a significant part of criminal activities remains undetected.

R&D and innovation activities

Large criminal groups devote significant resources to "in-house" R&D and innovation (RTDI), especially on digital tools to penetrate lawful economic activities, e.g., money laundering via cryptocurrencies and attacks against smart contracts. They use encryption technologies as protective measures against LEAs. Potential victims are then also forced to devote considerable resources to RTDI activities to protect their digital systems (storing sensitive data and administering financial flows) against more sophisticated forms of attack. They are engaged in both in-house and extramural RTDI activities (incl. private-public partnerships).

LEAs spend sizeable amounts on RTDI activities in digital technologies, training, and education, as well as prevention and awareness. This includes addressing the criminal abuse of encryption and privacy-enhancing technologies and the abuse of cryptocurrencies. They rely on public-private partnerships and collaboration with academia.

Overall, R&D investments by criminal actors are significant and when used effectively, they pose a major challenge.

Law enforcement agencies: activities, capabilities, and resources

LEAs have a strong mandate to fight economic crime. Their needs are translated into regulations, especially concerning investigative methods and information exchange. LEAs are legally authorised to use advanced technologies and can react to challenges stemming from technological innovations, such as the criminal abuse of cryptocurrencies and other virtual assets. AI and cryptography are major investment areas.

However, acquiring and maintaining technological superiority is a challenge because a large share of the technological knowledge comes from third parties and there are always possibilities of leakage. Furthermore, as the technological state of the art in criminal organisations is hard to ascertain, it is impossible to know reliably whether LEAs are sufficiently advanced to have a technological advantage in their fight against crime.

LEAs regularly organise awareness-raising campaigns pointing to the threats of certain crimes for the citizens and other potential victims. They often conduct these activities in close collaboration with businesses. Prevention of criminal economic activities is supported by citizens who trust both regulations and LEAs.

Crimes are measured and monitored vigorously to allow LEAs to concentrate on the most significant threats. Monitoring of policing is conducted both internally and by independent external bodies. Training and education of LEAs' staff are also prioritised according to the threats.

LEAs are very effective in fighting illicit trade, trafficking of human beings and illicit waste trade. They are somewhat less successful against corruptive crimes, money laundering and in recovering proceeds of crime.

LEAs' activities are strongly interlinked with other state (regulatory) bodies, and thus they gain access to pertinent information. Whistle-blowers, as another important source of information, are protected effectively. Both prevention and fighting of crime are strongly supported by a well-organised exchange of relevant information among LEAs across the EU, as well as with a sufficiently large number of relevant countries outside the EU.

3.2 Scenario 2: *Safe haven for legal actors*

Key dimensions

- Small-scale criminal organisations
- Strong, effective LEAs

Main features

Large criminal organisations have kept a minimal presence in the EU as they found ample, more profitable opportunities in other regions, where LEAs are weaker and regulations are ineffective. Stringent and effective regulation in the EU is an important disincentive for them. Some of them operate from 'criminal safe havens' outside the EU and target victims online or commit online crime mainly outside the EU but to some extent also in the EU. Small-scale criminal organisations do not possess the skills, contacts, and resources to internationalise, and therefore largely keep operating in their country of origin in the EU, becoming the dominant type of criminal actors. They try to find ways to penetrate lawful economic activities. LEAs have the necessary resources, skills, capacities, and capabilities to be strong in the EU and they are also supported by effective regulation. Small-scale criminal organisations are unable to influence the regulatory processes. Thus, the EU provides a relatively safe haven for legal actors.

Criminal actors and criminal activities

Large criminal groups concentrate their resources outside the EU, and thus small-scale criminal groups are the main players inside the EU, taking higher risks for lower rewards. They have carved out for themselves certain criminal sectors where they can operate, especially online scams, counterfeiting of means of payment, theft, and illegal betting. They pursue criminal displacement strategies, that is, focus on areas with less effective regulation in place.

Some tax evasion (incl. social contributions) and money laundering subsist. Corruption still creates sporadic tailored regulatory loopholes mainly at the regional and local levels.

Regulation

The overall high efficacy of regulations prevents small-scale criminal groups from turning the interpenetration of criminal and lawful economic activities into a "big business" that would poison large chunks of the economy. Still, there are some weak spots. Crime as a service, such as the carding business or cyber-extortion services on the dark Web, is not addressed effectively by regulations. Investment and donations by criminal actors in strategic fields and sectors (e.g., political parties, banking, energy, telecom, transport) are still present.

The European Public Prosecutor's Office's competence is still limited to acting only in restricted domains.

R&D and innovation activities

Small-scale criminal groups do not have the financial muscle to fund the development of radical new technologies and 'business models' that could create new opportunities for crime as a big business. Nonetheless, they have resources to hire individuals – poorly paid and retired digital experts, as well as students – to develop and use technological tools for small-scale online scams, counterfeiting of means of payment, and illegal betting.

Large criminal groups operate mainly outside EU. Their 'in-house' RTDI activities, as well as the 'extramural' ones they commission, constitute continuously a potential threat for EU jurisdictions. Whilst criminal actors are not spending significant sums on R&D and innovation in the EU, potential victims still must devote resources to RTDI activities to protect their digital systems (hosting sensitive data and administering financial flows), both as in-house and extramural projects (incl. private-public partnerships).

Law enforcement agencies: activities, capabilities, and resources

Regulation reflects the operational needs of LEAs and LEAs are fit for addressing the interpenetration of criminal and lawful economic activities. All other relevant tools and regulations are also in place for LEAs to work effectively.

LEAs have sufficient resources to fund RTDI projects supporting them in fighting the main types of crimes: online scams, counterfeiting of means of payment, and illegal betting. More generally, their RTDI activities are aimed at strengthening their encryption capabilities and their ability break into ICT systems used by criminals. Co-operation with external RTDI partners does not play a decisive role but it is not negligible either.

International co-operation works well both within the EU and outside it, helping to reduce the number of international criminal havens. The financial incentives to commit economic crimes are curtailed by the risk of failing and/or getting caught. Money laundering and tax crimes are charged in a way that the rate of asset recovery is high, and the likelihood of ultimately accruing profit when caught is low.

Public-private partnerships in the financial sector, e.g., with private investigative units, are also in place and working effectively. Nevertheless, there is still a certain percentage of economic crime. Training, tailored to specific crimes – e.g., by state-owned businesses, monopolistic structures, or diplomatic actors – is provided to counter these threats.

3.3 Scenario 3: *Protected pockets of legal actors*

Key dimensions

- Small-scale criminal organisations
- Weak, ineffective LEAs

Main features

Large criminal groups focus their activities outside the EU where they can exploit more profitable opportunities. Small-scale criminal organisations take advantage of the low intensity of the large criminal organisations' activities, as well as the lucrative opportunities for criminal economic activities offered by regulatory loopholes. Hence, they are the dominant criminal actors in an EU with a fast-evolving crime-scene. They exploit new technologies and disruptive business models taking advantage of the absence of effective regulations ensuring robust cybersecurity, safety, and health standards. Lawful economic actors try to find protected pockets for their businesses, especially in those domains where regulation still works. It is an 'unstable' scenario as lawful

economic actors push for more effective protection, and thus stronger LEAs, supported by effective regulation.

Main types of criminal actors and criminal activities

Large criminal groups have limited presence in the EU, for the activities in which they can invest their resources are more lucrative in other territories. Yet, ineffective regulation in the EU keeps them interested. They constantly search for emerging opportunities.

Within the EU small-scale criminal groups are important players. They take greater risks for relatively low rewards, but they have carved out for themselves certain criminal sectors where they enjoy exclusivity and impunity (online scams, brand counterfeiting, counterfeiting of means of payment, theft, illegal betting, etc.).

Tax evasion (incl. social contributions), money laundering, corruption (to create specific, tailored regulatory loopholes for criminal economic activities) are pervasive.

Regulation

The ineffective regulatory regime has led to disastrous consequences. Both private and public entities are unwilling to assume roles and responsibilities in protecting citizens' rights. Providing basic public services has become very expensive.

The effectiveness of the regulations is not seen as an important social concern. It is neither investigated nor assessed, and accountability for regulatory failures is limited. There is complacency in relation to desired outcomes by policy-makers and regulators and this also hides the true nature of the problems that society faces.

New technologies, as well as disruptive business models, are exploited by criminals as there are no effective regulations ensuring robust cybersecurity, safety, and health standards. Once a new technology-driven service emerges in a given sector, it quickly finds its use in different sectors, posing requirements for new sectoral regulations.

Those sectors, where immediate, direct economic incentives to engage in criminal economic activities are – seemingly – weak, become petri dishes for undue influence and manipulation of public opinion and political choices, or an avenue for activities with strong incentives. Weakly regulated sectors with little strategic importance are targeted by criminal organisations to hide and traffic more valuable goods.

R&D and innovation activities

Small-scale criminal groups hire experts, especially poorly paid and retired digital experts, as well as students, to develop and use technological tools for online scams, counterfeiting of means of payment, and illegal betting, as well as target vulnerable communities, e.g., pensioners for instance as money mules.

In a complex and highly dynamic but also highly fragmented digital underground, criminal groups rely on the "Crime as a Service" (CaaS) model.[9] Each actor, from sophisticated criminal groups to

[9] There is no legal or official definition of CaaS. It can be described as a criminal activity where an experienced criminal develops advanced tools or services which are put up either for sale or rent to other, often less experienced criminals. This enables criminals with limited knowledge and expertise to carry out effective or complex activities with relative ease. (Ajay Unni, What You Need To Know About Crime As A Service (CaaS), StickmanCyber, 11 January 2022, https://www.stickmancyber.com/cybersecurity-blog/what-you-need-to-know-about-crime-as-a-service-csaas#:~:text=What%20is%20CaaS%3F,out%20attacks%20with%20relative%20e)

the fledgling cybercriminals specialises in particular skill-sets and areas of expertise. This creates a division of labour and the adoption of a wide range of niche functionalities. The availability of tools and services to commit crimes has lowered the entry barrier for criminals as they no longer need to have the technical skills and expertise to commit crimes.

Large criminal groups operate mainly outside EU. Their 'in-house' RTDI activities, as well as the 'extramural' ones commissioned by them serve those activities. Yet they also invest in modifying and further developing emerging technologies, as well as new business models that – given ineffective regulations – offer them new opportunities inside the EU. Hence, they also devote resources to develop and use encryption technologies as protective measures against investigations by LEAs in the EU. Overall, criminal actors are spending noteworthy sums on RTDI, posing major challenges.

Potential victims, therefore, devote an increasing amount on RTDI activities to protect their digital systems (hosting sensitive data and administering financial flows). They fund both in-house and extramural RTDI projects (incl. private-public partnerships).

LEAs' RTDI expenditures are increasing, focussing on fighting online scams, counterfeiting of means of payment, and illegal betting, as well as new types of crimes, facilitated by emerging technologies and new business models. They also aim to strengthen their encryption capabilities and break into ICT systems used by criminals. Co-operation with external RTDI partners plays an increasingly important role, as the main sources of high-tech criminal capacities are external to the EU.

Law enforcement agencies: activities, capabilities, and resources

Ineffective regulations prevent LEAs from fighting the penetration of criminal actors into lawful economic activities to a satisfactory extent. LEAs' surveillance and investigative tools are weak – some advanced technological tools are even missing – and thus fall short of effectively fighting these crimes. Further, training for LEAs' officers is not specific enough, not tailored to tackle the most harmful crimes.

Corruption is at a damaging level in various government bodies and offices, including LEAs, as organised crime has infiltrated those organisations. The high-level and pervasive corruption severely weakens the sporadic, half-hearted attempts to tighten regulations.

The level of recorded crime is lower than the actual level as citizens have lost their faith in the state, and thus do not report all crimes.

The level of harmonisation of regulations on co-operation among the LEAs across the EU and beyond the EU is low. Small-scale criminal actors perceive and use EU countries as safe havens.

For example, a malware developed by a criminal organisation for encrypting data and controlling operational systems can be sold for cyberattack and cyberextortion. For other examples, see EUROPOL (2023): Cyber-attacks: The Apex of Crime-as-a-Service (IOCTA 2023) https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf.

3.4 Scenario 4: *Paradise for criminals*

Key dimensions

- Large criminal organisations
- Weak, ineffective LEAs

Main features

The EU economy is flourishing and provides ample opportunities for large, well-organised criminal organisations to conduct profitable business activities in the white, grey, and black segments of the economy. These illicit actors are successfully influencing the regulatory processes to advance their interests. They can also afford to fund the development of new technological tools and 'business models' to penetrate the lawful economy even more deeply through their criminal ventures. Although LEAs are also well-funded thanks to public revenues, they are substantially weakened by ineffective regulations. As lawful economic actors and other potential victims are not protected by effective regulations, LEAs are faced with even more demanding tasks, reducing their efficacy in fighting economic crimes.

Main types of criminal actors and criminal activities

The largest, best-organised transnational criminal groups with massive financial resources are the dominant actors. They counterfeit products, smuggle drugs and human beings, including migrants and organise their integration in the black market via illegal employment, prostitution, and child or forced labour. They are active in illegal waste management and waste smuggling, tax evasion, financial fraud, money laundering, and corruption, especially aimed at weakening regulations. Outside the EU, they invest in different legal and illegal activities (including tourism, construction, mining, waste smuggling, illegal fishing, forestry, and mining). They then launder their illegal proceeds in the legal economy of the EU. They also exploit tax asymmetries by locating the various stages of their illicit activities in jurisdictions that offer the greatest tax advantages, the strongest guarantees of impunity, and the best opportunities for concealing and moving assets.

The criminal underground has achieved a high maturity characterised by a distribution of tasks and groups specialising in certain aspects of the criminal value chain and the Crime-as-a-Service model is widely in use. Criminal organisations are active in controlling their territory for mafia-type organisations, including local corruption. Besides, they have their 'own-account' activities, e.g., online scams, brand counterfeiting, counterfeiting of means of payment, theft, and illegal betting. This 'paradise for criminals' is also used by large criminal organisations to target victims outside the EU.

Regulation

Numerous criminal organisations operate similarly to law-abiding businesses. On the surface, criminal networks, companies, and businesses have legitimate and well-established structures that include supply chains, service and/or product delivery, customer base, etc. As incentives to engage in criminal economic activities are strong and regulation is weak, the combination of legal and illegal activities and the collaboration between lawful and illicit entities thrives.

Regulatory frameworks do not obviously contradict citizens' values, but they leave enough room for favouritism and vested interests to flourish. Information and data are limited and often unreliable, and monitoring the state of regulatory compliance by citizens and businesses is difficult. There is limited investment in capacity and capability building for compliance by lawful

economic actors and government bodies. Corruption is at a damaging level in various government bodies and offices, and organised crime has infiltrated those organisations.

A particularly challenging sector is the decentralised finance sector, including the non-fungible token (NFT) trading sector. It suffers from ineffective regulations: there is no obligation to report suspicious activities. No technological means to spot those activities are in place either. Due to the lack of regulatory oversight, the sector offers strong incentives for criminal organisations to achieve sizeable financial gains along with ample opportunities for laundering proceeds of crime and engaging in illicit transactions.

R&D and innovation activities

It is highly profitable for large criminal groups to invest a noteworthy chunk of their massive financial resources in 'in-house' RTDI activities and commission other actors to create technological opportunities, especially digital tools to penetrate lawful economic activities via technological tools, e.g., money laundering via cryptocurrencies. These criminal groups also devote significant resources to purchasing tools and services in the digital underground.

Small-scale criminal groups also get their share and can afford to invest in 'extramural' technological development activities.

Due to the lack of effective LEAs, criminal actors use a relatively small share of their R&D expenditures to develop and use encryption technologies as protective measures against the investigations conducted LEAs.

Potential victims are forced to devote significant resources to RTDI activities to protect their digital systems (hosting sensitive data and administering financial flows), both as in-house and 'extramural' projects (incl. private-public partnerships).

LEAs spend significant resources on RTDI activities in digital technologies, mainly to strengthen their encryption technologies and capabilities to break into ICT systems used by criminals. They rely on public-private partnerships.

Law enforcement agencies: activities, capabilities, and resources

LEAs are not able to counter the criminal actors' penetration into lawful economic activities to a satisfactory extent. Organised crime groups have created this 'playground' for themselves by influencing the regulatory processes. LEAs' surveillance and investigative tools are also insufficient, given the weaknesses of regulations. This leads to a frustration inside LEAs and hence a rise in corruption in LEAs, too.

Disinformation spread by organised crime makes it difficult to identify illegal activities and corruption in the financial and other sectors of the economy, as well as in government bodies, including LEAs.

There is little harmonisation of regulations on co-operation among the LEAs across the EU and beyond, and the public is mostly unaware of the risks, threats, and the likelihood of unknowingly supporting mafia-type organisations.

4) THE FOUR SCENARIOS AND STATE-SPONSORED CRIMINAL ECONOMIC ACTIVITIES

Major geopolitical tensions are not specific to any of the above scenarios and their emergence cannot be explained by factors internal to the EU. These tensions stem neither from the dominant types of criminal actors' strategies and operations in the EU, nor from the strength and efficacy of LEAs in fighting the interpenetration of criminal and lawful economic activities. Yet geopolitical tensions may prompt harmful economic crimes. Thus, they are related to, but not necessarily a characteristic of, any of the above four scenarios.

When geopolitical tensions lead to sanctions against certain states outside the EU, sanctions-busting is a major form of criminal economic activity. These tensions might also lead to mass migration, and thus human trafficking. Further, 'rogue' states might sponsor certain actors to penetrate lawful economic sectors (activities) of the enemy's economy, to weaken the enemy as much as possible, e.g., by undermining trust in its financial system, including the stock exchange, banks, and insurance companies; weakening major firms in decisive sectors by stealing their sensitive data and funds; blocking critical infrastructure; weakening citizens' trust in the state in various ways; counterfeiting goods and means of payment; intensifying human trafficking; smuggling migrants, etc.

While the root cause cannot be explained by the 'game' between criminal organisations vs LEAs in the EU, the strategies, capacities, capabilities, and day-to-day operations of these two types of players do influence the ease and ways, in which state-sponsored economic crimes are planned, organised, and committed.

When large criminal organisations are resourceful and well-organised, rogue states can more easily find strong, efficient inside-(domestic)-actors to cause significant harm and/or undermine the fundamental values of the EU. Besides the 'domestic' large criminal organisations, rogue states can also mobilise their own assets and services and/or commission third countries' criminal organisations. To reduce harm, effective, well-equipped, well-trained LEAs (including border forces) and other counter-intelligence agencies are needed in the EU.

Counter-intelligence agencies need to be equipped with all the necessary human and financial resources and technological capabilities and tools to protect the EU economy. They need an appropriate mandate to fight the types of crimes committed in this situation. Regulators also should consider how to tighten, amend, and extend regulations to make LEAs' and the other relevant agencies' activities more efficient when fighting these types of economic crimes.

Rogue states can commission 'domestic' large criminal organisations to commit significantly harmful crime in the EU. While we would not expect rogue states to engage with small scale criminal organisations, regulatory instability and weakness may allow small-scale criminal organisations to grow fast into actors that could attract the interest of rogue states.

Criminal organisations committing economic crimes commissioned by rogue states can cause more harm when LEAs are weak. For example, when regulatory regimes are ineffective and LEAs are weak, sanctions busting becomes a relatively simple and low-risk form of criminal economic activity, and thus will be prevalent and highly profitable. That is a win-win for the large criminal organisations and rogue states. It can easily result in a devastatingly huge political and economic loss for the EU.

In sum, besides applying the necessary diplomatic, political, security, and military tools, strengthening LEAs – and all the other relevant state organisations and services –, developing technological tools and tightening the regulatory system are a must to prevent, monitor, and fight state-sponsored economic crimes.

5) POLICY IMPLICATIONS

Exploring multiple futures provides insights into the challenges and opportunities faced by governments and society in the intersection of criminal and lawful activities. Competition between LEAs and criminal organisations within a jurisdiction is important, but it is not the only factor in shaping the interpenetration of criminal and lawful economic activities.

Differences with the legal orders of other jurisdictions affect opportunities for crime, as do interventions from the outside, be they state-sponsored or simply the result of internationally organised criminal networks. Depending on the effectiveness of regulation and law enforcement, criminal activities can be loosely organised networks of individuals and small organisations, more densely organised activities resembling large firms and syndicates, or even as an important sector with economic and political reach involving mixtures of criminal and lawful businesses and significant crime-as-a service markets.

As economic crime is often difficult to detect, its extent is difficult to assess accurately, and thus it is very difficult for governments and LEAs to estimate whether it is prevailing in the competition against crime or whether it is staying behind. It is thus important to:

1) Enhance monitoring and foresight capabilities of LEAs in the EU and its Member States in cooperation with third countries

- Sudden changes might make an effective regulatory system ineffective. Policy-makers should continuously inform themselves with the most up-to-date and trustworthy statistics related to the policy and regulatory aims and targets and anticipate disruptive forces that may arise. These include disasters, pandemics, war, sudden influx of forced migrants, and new technology (e.g., decentralised financial products such as NFTs).
- Monitor and assess the emergence of new technologies and business models focusing on their potential use by criminal actors to penetrate lawful economic activities.
- Monitor and assess the potential of sectors with seemingly weak incentives to conduct criminal economic activities to be used as 'launch pads' of harmful criminal activities.
- Use systematic horizon-scanning to understand potential, risks and threats before they materialise, to improve the authorities' ability to meet regulatory objectives.

Wide private sector dominance in technology development risks leading to over-reliance on their services and co-opting their interests in regulation and policy. Closer collaboration between EU entities, the private sector and academia is needed to assess and avoid such risks as the criminal uses of innovations in various domains (e.g., taxation, social insurance, financial sector, NFTs and other virtual assets, gaming, mining, fishing as well as mobility of people, goods, and capital).

2) Develop technological tools by the EU and its Member States in cooperation with third countries for anticipating, preventing, monitoring, and fighting harmful criminal economic activities

- Continue supporting the development of analytical tools that can detect patterns indicative of criminal activities in financial transactions, e.g., exploiting big data. Such a system, characterised by learning capabilities, should train itself with the evidence obtained from the cases investigated, that is, using reliable training data. This learning process needs to be supervised by human experts.
- Support the development of AI-driven technological solutions that help in dealing with the volume challenge, that is, the significant volumes of data collected in the context of criminal investigations, as well as the information created by regulatory requirements. Then AI can play a key role in automating steps of the analysis process, supporting the human analyst, and in detecting patterns of criminal behaviour that may be hard to spot for humans.

- Support the development of technologies, potentially using blockchain infrastructure, to solve the two fundamental problems of traceability and transparency of information flows. Effective traceability of financial flows (using "Follow the money" solutions) concerns the fragmentation and spatial distribution of information resulting in information asymmetry between controller and controlled. Transparency concerns the centralisation of trust and the possibility of corruption of information by the possible malicious third-party guarantor.
- Support the development of technological tools to monitor if incentives and business models to penetrate lawful economic activities change.

3) Fund joint social science research projects in the EU and its member states in cooperation with third countries for understanding economic and behavioural incentives for crime and developing regulation against it

- Fund regulatory science projects aimed at supporting the development of effective regulatory tools and regimes, as well as the monitoring and evaluation of regulations.
- Fund economic and behavioural science projects to
  - develop more reliable methods to identify assets and wealth stemming from lawful economic activities vs disproportioned and unexplained wealth; and
  - have a better understanding of the
    - incentives to commit criminal economic activities under various regulatory regimes;
    - organisation, management, and operation of large and small-scale criminal organisations;
    - patterns of their criminal behaviour;
    - incentives to co-operate as 'insiders' with criminal actors;
    - economic impacts of loose vs tight regulations.
- Fund research on ethical issues in technological development and regulations.
- Devise governance and funding mechanisms that do not undermine the independence of the regulator, e.g., when it is funded by its stakeholders or members, and do not create a conflict of interest.
- Research ethical aspects in the employment of artificial intelligence or machine learning tools for risk identification and analysis in the financial sector.

Going beyond the implications for R&I policies, from the perspective of our future scenarios, the following more general policy interventions are important to restrict and prevent the interpenetration of criminal and lawful economic activities:

4) Develop framework conditions for effective governance and law enforcement in the EU and its member states in cooperation with third countries

- Tighten cooperation among the EU member states to harmonise their regulations relevant for preventing and fighting the interpenetration of criminal and lawful economic activities.
- Strike a balance between data protection requirements and the needs for data and information collection, exchange, and analysis to fight criminal economic activities.
- Develop regulatory coverage and practices to protect whistle-blowers.
- Strengthen the role and resources of the European Public Prosecutor's Office.
- Develop appropriate internal ethical and operational practices for the government offices (funding agencies, especially those that manage public procurement projects, regulators, tax and customs offices).

- Consider what formal mechanisms, such as regulatory sandboxes, help work with innovators to test new products, services or approaches that support regulatory objectives of mitigating illicit activities and protecting citizens.
- Ensure a regulatory framework for the effective use and development of analytical tools deployed to fight criminal economic activities by LEAs.
- Put in place rules and procedures across the EU member states to identify assets and wealth stemming from lawful economic activities vs disproportioned and unexplained wealth in reliable ways.
- Consider if and how regulations in the EU member states can be exploited by entities that are not driven (purely) by commercial incentives and revise regulations accordingly.
- Equip LEAs in the EU member states with the means to deal with high profile individuals, diplomatic personnel with immunity, state-owned businesses, and other influential actors.
- Facilitate co-operation among regulatory bodies in the EU member states and align regulations with the willing non-EU countries.

5) Enhance the cooperation in the EU and with third countries for more effective monitoring and assessment of criminal and lawful activities and law enforcement

- Harmonise how and what information is collected by LEAs to have a sound understanding of the interpenetration of criminal and lawful economic activities in the EU. Harmonise formats for reporting information across the different levels from local to international law enforcement.
- Put in place rules and procedures for effective exchange of information among LEAs and other relevant government offices (in particular, tax and border/ customs authorities) across the EU member states.
- Assess the efficacy of regulations regularly by independent bodies.
- Put in place rules and procedures for effective exchange of information with LEAs in co-operative non-EU countries to facilitate criminal investigations and prosecution as well to recover illicit assets.

ANNEX 1: MAIN TYPES OF CRIMINAL ECONOMIC ACTIVITIES RELEVANT FROM THE ANGLE OF THE INTERPENETRATION OF CRIMINAL AND LAWFUL ECONOMIC ACTIVITIES

Activity	Offenders	Victims	Economic, social, and environmental impacts (direct and indirect damage and harms)	Policy relevance
Virtual assets and blockchain tech - Wash-trading of NFTs and NTTs (including in-game money laundering)	Individuals and organised crime groups	Citizens Companies The state	Distrust in government and law enforcement agencies (LEAs) Dent in the integrity of the financial services	Financial regulation Anti-money-laundering directives Taxation
Abuse of modern encryption technology and privacy enhancing technologies	Organised crime groups, state actors	Citizens Companies	Direct harm for persons (financial loss) Indirect harm for losing trust in the economic (esp. financial) system	Tech regulations, data protection Technology development (e.g., quantum key distribution, post-quantum cryptography)
Use of innovative forms of decentralised financial products (e.g., NFTs, smart contracts, liquidity mining)	Individuals and organised crime groups	Citizens Companies	Financial damage Loss of trust in technology	Trade and financial regulations Taxation
Criminal use and abuse of AI (deepfakes, synthetic identities, large-scale fraud)	Organised crime groups, state actors, individuals	Citizens Companies The state	Distrust in government and democracy in general Threats to national security Direct harm for all actors (financial loss), Indirect harm for losing trust in the economic (esp. financial) system	Regulation on AI

Tax evasion	Individuals, legal entities	The state Honest taxpayers	The principle of free competition in the market is undermined Loss of financial resources for the state, and thus fewer and/ lower quality services to citizens	Trade, financial regulations, taxation, wealth distribution
Illegal waste trade	Waste disposal companies Organised crime groups	Honest companies The community The environment	The principle of free competition in the market is undermined Loss of financial resources for the state, and thus fewer and/ lower quality services to citizens	Trade, financial and environmental regulations Investment policies Concessions and permits
Corruption, including misappropriation of EU and national (public) funds	Anyone (active corruption) Public officers (passive corruption)	Proper functioning and reputation of the public administration	Income inequality/ distribution, distrust in governments	Taxation Social security regulation Technological innovation (e.g., AI for detection)
Money laundering	Anyone	Honest competitors The state Citizens	The principle of free competition in the market is undermined Loss of financial resources for the state, and thus fewer and/ lower quality services to citizens	Taxation Social security regulation Technological innovation (e.g., AI for detection)
Illegal mining	Unauthorised, small and large-scale miners	Honest competitors The environment The international community Citizens	The principle of free competition in the market is undermined Access to technology (cf. rare earth and metal) Environmental degradation	Trade, financial and environmental regulations, Investment policies, Concessions and permits
Sanctions busting (e.g., illegal oil and timber trade)	Organised crime groups, state actors	Honest competitors The environment The international community Citizens	The principle of free competition in the market is undermined International co-operation is harmed The regulatory framework at a global level is damaged Environmental degradation	Trade, financial and environmental regulations, Investment policies, Concessions and permits
Human trafficking	Individuals, organised crime groups	Persons Communities	Human rights, well-being of individuals and communities, distorted labour market	Social security regulation, Citizenship and immigration policies, Foreign policy
Counterfeiting	Individuals, organised crime groups	Honest firms, esp. brand-owner companies Consumers The state	The principle of free competition in the market is undermined Financial losses for companies and individuals	Trade and financial regulations Taxation Technological solutions to detect counterfeit products

Illegal, unreported, and unregulated fishing	Individuals, organised crime groups	Communities relying on the biodiversity Marine ecosystems	Biodiversity is reduced Financial losses for companies and individuals	Trade, and financial regulations Technological tools to detect illicit fishing

Source: Experts' assessment

ANNEX 2: TRENDS AND DRIVERS

Applying the STEEPV classification method, the experts have identified the following trends and drivers:

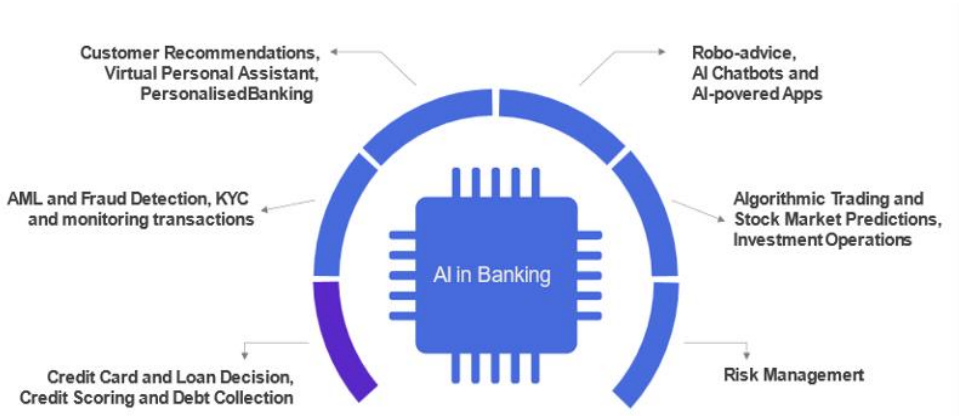
- **Social**
  - Spreading of conspiracy theories (mis- and disinformation)
  - Access to technology
  - Social tensions
  - Income and wealth distribution (equity/ inequality) [it is also an economic and political issue]
  - Societal trust
  - Willingness to co-operate (among state and private sector actors and citizens)
- **Technological**
  - AI development
  - Digitalisation of criminal economic activities
  - Borderless nature of the internet and availability of (pseudo) anonymous technologies and services
  - Crime as a service: digital underground economy providing the tools and services needed to commit crime
  - Technological literacy and skill gap of law enforcement agencies' officers
- **Economic**
  - Taxation, social security regulation
  - Investment policy, investment opportunities
  - Ease of doing business (registration, legal fees, etc.)
  - Lack of, or fragmented, legislation and regulation
- **Environmental**
  - Climate change, loss in biodiversity
  - Waste trade
- **Political**
  - Political interests of foreign actors
  - Geopolitical tensions
  - Citizenship & immigration policy
- **Value-related**
  - Whistle-blower protection
  - Asymmetric risk (disproportionate impact, low risk - high profit)

ANNEX 3: CHALLENGES IN FIGHTING THE PENETRATION OF CRIMINAL ACTORS TO LAWFUL ACTIVITIES

AI increasing the need for automated surveillance and tools

Given the increased volume and number of transactions, often involving several jurisdictions, it can go beyond human capacity to assess and process them. This necessitates employing technological tools to analyse risks 'hidden' in these transactions. For example, banks use automated suspicious transaction monitoring tools which operate against a finite number of risk parameters.

Fig. 1. Applications of Artificial Intelligence in the Banking Sector



Source: Analysis of models by Owczarek, D. (2022) AI in Banking. Applications and Benefits of Artificial Intelligence in Financial Services. *Nexocode*, 29 March, https://nexocode.com/blog/posts/ai-in-banking.applications-and-benefits-of-artificial-intelligence-in-financial-services/

Limited agency of the EU and EU bodies

The EU possesses supranational powers to enact legal instruments and make decisions pertaining to the functioning of the EU Single Market and effective implementation of an EU policy in an area that has been subjected to harmonisation measures. However, it has limited competence for substantive criminal law. It is argued that more thought must go into drafting regulations and directives that seemingly focus on legitimate economic activities yet offer ample opportunities for criminal activities to interpenetrate this realm.

According to the Treaty on the Functioning of the European Union (TFEU), the EU can harmonise criminal procedural law in three distinct areas, namely: admissibility of evidence, rights of individuals in criminal procedure, and rights of victims of crime. These specific areas are underpinned by the human rights treaties and jurisprudence (which have become primary law since the Lisbon Treaty).[10] Such measures can only take place "to the extent necessary to facilitate mutual recognition of judgments and police and judicial cooperation having a cross-border dimension" whereby the EU can establish "minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension". An exhaustive list of these is provided in Art. 83(1) TFEU which includes: terrorism, trafficking in human beings, sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime.

[10] Note that Art. 82(2)(d) TFEU also provides that harmonisation can also concern "any other specific aspects of criminal procedure" that have been identified by unanimous Council decision with consent of the European Parliament.

In 2011, the EU Commission published a communication for a "vision for a coherent and consistent EU Criminal Policy by 2020" whereby it identified harmonised policy areas as well as areas (e.g., the financial sector (market abuse), the fight against fraud affecting the financial interests of the Union, and the protection of the euro against counterfeiting) where criminal law measures at the EU level would be required.

To ensure effective enforcement, the Commission also identified other policy areas for harmonisation, such as

- Road transport, concerning, for instance, serious infringements of EU social, technical, safety, and market rules for professional transports;
- Data protection, in cases of serious breaches of existing EU rules;
- Customs rules on the approximation of customs offences and penalties;
- Fisheries policy, to counter illegal, unreported, and unregulated fishing; and
- Internal market policies to fight serious illegal practices, such as counterfeiting and corruption or undeclared conflicts of interest in the context of public procurement.

In various areas of policy and law, the EU does not have the competence to make decisions and/or have a limited role. For example, EUROPOL relies on the work of national LEAs to investigate and prosecute financial crimes. OLAF, on the other hand, only concerns itself with crimes against the financial interests of the EU. Moreover, OLAF's role has been greatly reduced with the establishment of EPPO, which has taken over some important competences that previously fell within OLAF's operational perimeter (combating fraud against the EU budget).

Subsequently, certain criminal activities which do not fall in the remit of the EU law and its institutions, are subject to national criminal justice mechanisms. Thus, it is not possible to create fully harmonised responses for existing and emerging areas of risk and criminal threats. In addition, despite the areas which are subject to competences and legal instruments of the EU, there are diverse approaches, interpretations, lack of or insufficient capacities and resources, and occasionally unclear competences.

EUROPOL as the EU's law enforcement agency cannot start its own investigations, nor does the Agency have executive powers. However, it is very effective in co-ordinating, supporting, and de-conflicting international operational action against serious and organised crime as well as terrorism within its mandate. In a way, EUROPOL provides "law enforcement as a service" by officering intelligence-related and analytical expertise, tools, and technical/ investigative support as well as top-level expertise, skills, and tooling (cryptocurrency analysis, access to encrypted data in the context of an investigation, etc.) to Member States. Unique operational law enforcement platforms such as J-CAT combined with industry advisory groups and academic networks create the 'network of networks' that are needed in the successful fight against (financial) crime.

Latest EU regulations and directives such as MiCA (Markets in Crypto-Assets Regulation), DORA[11] (Digital Operational Resilience for the Financial Sector and Amending Regulations), AMLD (Anti-Money Laundering Directive) or NIS 2 (The Directive on measures for a high common level of cybersecurity across the Union)[12] as well as the ongoing negotiations at the UN level for an international cybercrime convention will help streamline and harmonise legislation and judicial mechanisms in the fight against (financial) crime. However, it remains to be seen how effective these frameworks will be considering the important and strong focus on privacy and data protection at the EU level, which may impact upon the tools and data LEAs

[11] https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[12] https://eur-lex.europa.eu/eli/dir/2022/2555

and EUROPOL can use e.g., when it comes to tracing cryptocurrencies and other virtual assets. While a fully harmonised response to (financial) crimes at the EU level, let alone at the global level, will be difficult to achieve, it should be possible to establish universal definitions and principles, as well as taxonomies and standards.

Mafia-type organisations

Infiltration methods of the mafia-type organisations

The infiltration method carried out by mafia-type organizations

The Management of a legal company is a way for:

- ❑ **create new job opportunities strengthening the social consensus**
- ❑ **Extending the mafia-type organization power within the community**
- ❑ **Establish relationships with entrepreneurs and politicians to "pull the strings" when needed (set up a temporary association of companies to win a public contract, support elections campaigns to put the right persons in key functions to obtain favors when needed, etc.)**
- ❑ **Launder and reinvest part of their huge illicit profits into the legal market**

The foremost mafia-type organizations' "protected" sectors are the public construction industry and the waste disposal industry which are capital-intensive sectors so at high-risk of money laundering. In these sects, the public administration regulates participation by requiring license, permission, and specific prerequisites so to significantly reduce free competition.

Reduction of free competition ➡ Infiltration of public administration ➡ Corruption cases

Money laundering

Organised crime (OC) and mafia-type organisations have at their disposal enormous amounts of funds earned through criminal activities that have already undergone several money laundering (ML) phases – placement and layering – and need to complete the integration phase into the legal economy. To do this, OC and mafia-type organisations look for market sectors that involve heavy investments and are characterised by high profit margins. The most lucrative economic sectors are waste management, public construction, mining (especially 3TG mining, that is, gold, tin, tungsten, tantalum, and other rare earth elements (REEs) mining), and installation of renewable energy systems. In the search for the most lucrative economic sectors, OC and mafia-type organisations have invested heavily in certain economic sectors, e.g., 3TG mining in Africa and South-East Asia; management of the waste collection and disposal system in some municipalities of several countries in Africa, West Balkans, and South-East Asia; construction of tourist villages in several African countries.

Climate change

A new market sector is related to climate-change effects. The companies infiltrated by mafia-type organisations can make substantial investments in strategic sectors such as water desalination or purification, the contextual irrigation of ever larger areas afflicted by desertification, or the activities of precision agriculture (PA), relying on advanced S&T solutions to improve crop yields and high-tech sensor and analysis tools to assist management decisions. PA is adopted throughout the world to increase production, reduce labour time, and ensure the effective management of fertilisers and irrigation processes.

Trafficking in human beings

Trafficking in human beings (THB) and migrant smuggling are correlated with the effects of climate change (along with armed conflicts, political instability, and persecution), as the migration of many people, or even entire populations from regions that can no longer be cultivated due to desertification or repeated flooding stimulates these criminal activities.

Green Deal objectives

The EU Green Deal stipulates that member states shall be carbon neutral by 2050 and to do so they shall promote renewable energy generation. Hence, they shall invest in building windmills and photovoltaic solar farms. That requires a significant use of REEs of which the EU is in short supply. Apart from the European Union's current dependency on other countries such as China for the supply of REEs, the investments by mafia-type organisations in several developing countries (South America, Africa, and South-East Asia) for the extraction of REEs will create a dependency of EU (and other) states on these mafia-type organisations (suppliers).

Financial might

Mafia-type organisations, due to their turnovers, can be considered as states. For example, the 'Ndrangheta (Italian mafia-type organisation from Calabria), today considered the most powerful mafia in the world, with an annual turnover of approximately EUR 150 billion (National Anti-Mafia Directorate Report), putting to the 56th place in the world GDP ranking. (From a different angle, the annual turnover of the 'Ndrangheta is comparable to that of Hungary and is higher than that of Kazakhstan.) The market economy at a global level needs to be reconsidered: criminal and mafia organisations act as parallel states and can also play a decisive role in highly sensitive sectors such as energy or REEs. This imbalance in the availability of financial resources in the market between 'infiltrated' and honest companies will create an increasing competitive advantage of the former over the latter. This could lead, in the medium- long term to progressive contamination of honest companies: many will go bankrupt while others will be incorporated into 'infiltrated' companies. Hence, the challenge of interpenetration between the legal and illegal economy is pervasive at all levels of the global economic system.

Penetration of the political, and socio-economic fabric by mafia-type organisations

Mafia-type organisations, as opposed to other types of OC, have objectives beyond making profits. Their primary objectives are to penetrate the

- economic fabric through the infiltration of legal companies operating in the market. These economic activities, in addition to representing real investments in the legal economy, are instruments for achieving social consensus because they distribute wealth over the territory, provide jobs, and thus create social consensus;
- social fabric: economic activities that can be traced back to criminal or mafia-type organisations compensate for the lack of social protection mechanisms, which should be the prerogative of the State, and become real social shock absorbers that combat unemployment, and thus create social consensus. Mobsters and criminals are no longer seen as people to be avoided but as those to be referred to and respected. There is thus a real public recognition of the honour and respectability of organised crime and mafia members as they are recognised as having a role in protecting the labour market and the economic system in general.

- political fabric: social consensus is translated into political consensus. Mafia-type organisations promote their political candidates in local and national elections. Once elected, mafia-type organisations have direct control of politics both at a local and national level, which will be directed towards legislation that favours and protects their economic interests.

Economic cycles, investment needs and opportunities

The post-lockdown recovery phase as well as the cyclical financial crisis, represent further opportunities for the expansion of the criminal economy. Mafias inject significant financial resources, the proceeds of their multiple illegal activities, into legal circuits, infiltrating them to a considerable extent. For example, the health emergency has impacted the national economic systems already in difficulty, reducing the availability of financial liquidity and creating new pockets of poverty and social hardship. In this situation, mafia-type organisations can consolidate their social consensus in the territory, especially in the poorest regions, posing as an alternative welfare, but also exacerbating tempers. Moreover, economic paralysis can open prospects of expansion and enrichment for the mafias comparable to the growth rates that only a post-war context can offer. The global market is increasingly in need of large amounts of liquidity and will therefore tend to be more and more dependent on capital injections of illicit origin. This will tend to increasingly legitimate criminal activities that are integrated into the legal economy. Ultimately, the global market may become a hostage to the massive capital injections by mafia-type organisations. A major threat is an implicit acceptance by governments of the integration of financial flows of illicit origin into the global economy.

There are capital-intensive economic sectors that are very attractive to criminal groups because, as they require significant funding, they make it possible to invest significant financial flows (and, therefore, to recycle substantial funds of illicit origin) and earn sizeable profits.

Some of these capital-intensive sectors are generally the direct responsibility of public administrations, which outsource the management of these activities to private third parties through public tenders. The calling of public tenders has a twofold significance: i) they are the legal instrument through which the public administration entrusts to private third parties to conduct certain economic activities that are the direct responsibility of the public administration; and ii) they represent an instrument for the selection and control of the entities entrusted with such services. Although the regulations for these types of activities are generally very strict, mafia-type organisations – by definition – can penetrate the public administration and, through corrupt practices, orient the decision-making activities of public officials to their advantage. The risk is that economic subjects awarded important public tenders are linked, even indirectly, to mafia organisations.