FORESIGHT ON DEMAND: “FORESIGHT TOWARDS THE 2ND STRATEGIC PLAN FOR HORIZON EUROPE”

The interpenetration of criminal and lawful economic activities

RAPID EXPLORATION

Authors:
Elisa Wallwaey (Fraunhofer ISI)
Kerstin Cuhls (Fraunhofer ISI)
Attila Havas (AIT Austrian Institute of Technology, Center for Innovation Systems and Policy & Institute of Economics, Centre for Economic and Regional Studies)

December 2022

CONTENT

SUMMARY

As the world economy operates more and more through computerised transactions, new possibilities for intertwining criminal and lawful economic activities open up, as well as new opportunities for law enforcement agencies to fight crime. Considering the tremendous and potentially devastating damages caused by criminal economic activities, the issue should be high on the agenda of policy-makers, including R&I policy-makers. The race between criminal actors and the state trying to protect companies and citizens will be a permanent one. The paper provides and overview of trends and drivers in these domains, highlighting potential disruptions. It also presents four scenarios with a time horizon of 2040 to explore the role of R&I activities and regulations in shaping the possibilities for the interpenetration of criminal and lawful economic activities and derive policy implications.

The complex nature of criminal economic activities, their detection, investigation, and prosecution is related to research and innovation in at least three areas. First, research in, and the development and improvement of, information and communication technologies necessary to monitor, track and analyse criminal activities. Second, regulatory techniques for preventing innovators from i) moving outside the sphere of lawful activities; ii) moving too far and entering a grey zone where regulation is missing; and iii) settling on clear-cut criminal behaviour. Third, research in, and the development and improvement of, forensic techniques of reconstructing what actually happened, and thus attributing responsibility for crime.

1 INTRODUCTION

The field of criminal economic activities[1] encompasses a huge variety of possible criminal acts ranging from capital investment and several other types of financial offences (e.g., accounting fraud or tax evasion), insolvency fraud, money laundering, and work-related offences to violations of competition law. Likewise, there are different types of (potential and actual) victims. They can be individuals, businesses or the state. Given this diversity, one should not be surprised by the fact that there is no generally accepted definition of criminal economic activities. Instead, depending on various factors (such as legal systems, criminal codes and cultural factors), the understanding of the term varies from country to country. For the aim of this paper, we define criminal economic activities as non-violent criminal and illicit activities 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.

Furthermore, it is important to consider that many criminal economic activities are so-called "control-related offences": their detection highly depends on internal control measures, applied by either individuals or organisations to defend their assets, as well as on external ones, applied by respective governmental bodies. These measures can be technical or societal control mechanisms, including legal ones. Thus, a lack of internal control measures might result in a high amount of unnoticed crime. The same holds true when agencies, such as police forces or law enforcement agencies, lack capacities and time for detecting economic crimes.

Apart from some sensational or potentially scandalous cases, criminal economic activities rarely make the headlines of newspapers or news broadcasts. Still, the potential damages stemming from these crimes are devastating and – in the worst case – ruining the economic livelihood of people and causing businesses to go bankrupt. Thus, the macroeconomic and societal implications of such incidents should not be underestimated.

When taking the case of the German police crime statistics (Polizeiliche Kriminalstatistik, PKS) as an example, the tremendous amount of possible financial damages caused by criminal economic activities becomes obvious. In 2011–2021 these crimes accounted on average for less than two percent of all registered offences that include damage assessments while nearly half of all financial damages registered are induced by these offences amounting to an average sum of €3.8 billion per year.[2] Considering the amount of cases remaining unnoticed by victims, or cases, in which victims deliberately refrain from filing a complaint despite being aware of the offence, the damages caused by criminal economic activities are estimated to be several times higher than officially recorded.

An important issue regards the relation of economic and cybercrime. With the ever-growing digitalisation of private and professional lives, an abundance of opportunities opens up for criminality – and criminals are very creative in finding loopholes. Indeed, many non-violent crimes nowadays have a digital counterpart. Activities in the field of economic cybercrime range from e.g., digital scam of sensitive information, infecting computers with viruses or ransomware, sending spam mails, constructing fake websites or profiles on social media, to digital embezzlement and taking websites hostage and only restoring them upon the payment of a ransom. According to recent evidence, “since the pandemic started, there has been an increase in such types of cybercrime as denial-of-service attacks, fraud, cyber-related harassment, hate crimes, media hacking, phishing, and online shopping fraud (Buil-Gil et al. 2021; Collier et al. 2020; Horgan et al. 2021; Kemp et al. 2021; Plachkinova 2021). For example, drawing on victimisation data, Sampson and Ojen (2021) find that phishing and hacking have been commonly experienced cybercrimes in

1 For the sake of simplicity, occasionally we also use the term “economic crime” in this paper, although it is not a precise synonym for criminal economic activities.

2 The annual PCS reports and the corresponding data can be retrieved online: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html. The calculations in this paper are based on Table 7 for each year.

Nigeria. Notably, phishing emails on COVID-related topics such as asking for donations, sending malicious links to tax relief documents or free health advice have been particularly widespread (Fontanilla 2020; see Pawlicka et al. 2021 and Regalado et al. 2022 for further examples).

Furthermore, criminal economic activities and organised crime overlap to a significant extent. This holds for example true if presumably respectable businesses are used for illegal conduct, like money laundering or selling counterfeit products. Some (legal) experts even speak of "organised economic crime" because of the extensive mingling of these criminal categories. For example, in his 2020 book on economic and organised crime, Liebl dedicates a whole chapter to the topic,[3] while Le Moglie and Sorrenti (2020) elaborate further on the topic: using Italy as an exemplary case, they show how deeply legitimate economic actors and groups of organised criminals are interwoven.[4] Already in 2000, Di Nicola and Scartezzini dealt with the decisive role of IT in this mingling.[5]

Regulation plays a decisive role in answering two fundamental questions: (i) what is a crime and (ii) what is a grey zone? Here, we consider multi-level regulation, including EU guidelines, national laws and decrees, sectoral level regulation etc. as setting the boundaries for what is allowed and what is not.

On an international scale, different regulations, legal, and political systems shape what is deemed as legal – and what is perceived as being illegal. There are rare cases in international law concerning criminal economic activities. When something is forbidden, then it is clear. Otherwise, whether a certain behaviour is understood as being illegal or merely as morally questionable, depends on national contexts and cultural factors. What constitutes illegal behaviour in one jurisdiction is not necessarily punishable by (criminal) law in another – and vice versa. Further, there are grey zones between lawful and criminal economic activities where boundaries are blurred. Crane (2005), for example, elaborates on the question when legal practices of strategic market observation turn into illegal practices of industrial espionage.[6] It is unclear if we will see more of these grey areas, or if clear-cut international regulation will become the norm.

In this paper we focus on issues with potential policy relevance, mainly for EU R&I policies, although the issue can be of relevance to other policy domains as well.

2 THE CURRENT SITUATION

As the world economy operates more and more through computerised transactions, new possibilities for intertwining criminal and lawful economic activities open up, as well as new opportunities for law enforcement agencies to control citizens and fight crime. One condition facilitating criminal economic activities is the recent deregulation of financial markets, opening windows of opportunity for making money in grey zones or illegally.

In the 2022 edition of its Global Crime Trend Report, the International Criminal Police Organisation (INTERPOL) identifies crime trends. The top four of the trends mentioned there are directly related to economic and partially to cyber crime: 1) money laundering, 2) ransomware, 3) phishing and online scams, and 4) financial fraud.[7]

There are opposing views discussing whether it is possible to control the interpenetration of criminal and legal markets by tracking and removing the proceeds of crime in the economy. One

3 Liebl (2020).

4 https://cepr.org/voxeu/columns/when-godfathers-become-entrepreneurs-organized-crimes-infiltration-legal-economy (last accessed on Nov 22, 2022).

5 Di Nicola & Scartezzini (2000).

6 Crane (2005).

7 https://www.interpol.int/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report (last accessed on Nov 22, 2022).

view assumes that this is feasible and would open up a possibility of differentiating and controlling criminal and legal markets. Another view claims that establishing the lawful origins of funds used in every transaction is impossible – and even undesirable. The main question here is as follows: What level of control is technically feasible and (at the same time) socially and economically desirable?

2.1 Types of criminal economic activities

As legal order evolves, criminal economic activities evolve too; and usually at a much faster pace than regulators can keep up with. This holds true especially in view of (technological) developments in digitalisation, where the rate of innovation is so high that regulation can possibly be enacted only with a considerable delay. Furthermore, as the complexity of the related issues increases, there is a lack of experts to support law enforcement and we observe a lack of a sufficient level of skills of the technical and legal personnel – as well as a lack of legal entities to fight all criminal economic activities.

Being unbound by law, legislative principles, and regulations, criminal economic activities constitute a very innovative "sector", in which innovation is driven by the incentive of (potentially) high gains as rewards for taking some risks of incurring legal consequences in case the criminal action is reported to law enforcement agencies and the perpetrator is caught and punished. Especially in the case of criminal economic activities, experts regularly refer to extraordinary low detection and prosecution rates. Besides other possible reasons, this fact results from five particularities of criminal economic activities:

1) Depending on the modus operandi used for committing the crime, the victim(s) might not even be aware of the incident.
2) In fear of e.g., losses of reputation and customers' trust that in the future may result in shrinking revenues, many companies are reluctant to report economic crimes to law enforcement agencies.
3) As a study on economic espionage in German small and medium sized enterprises (SME) has shown, incidents of economic crime that only lead to minor losses are rarely reported to official agencies. Over half of the respondents indicated that they would refrain from filing a complaint if the damages caused by the incident are only minor.8
4) Even when crimes are reported, there frequently is a mismatch between the criminal act itself and the offense reported. For example, a business might be aware of computers or data storage devices having been stolen and reports the theft to the agencies, while the actual target of the crime might not be the stolen goods themselves but the (sensitive) information stored on it.
5) In case of still unregulated terrain, such as the deep sea, outer space and cyberspace (see the Deep Dive report on Global Commons), economic crimes, like illegal exploration and extraction of resources, do not only occur in grey zones but also often remain undetected. As long as no damage occurs, this is maybe no crime at all. But what about the long-term consequences and damages?

As already mentioned above, criminal economic activities include a multitude of quite diverse offences. Thus, it is worth considering the following questions:

1) What or who is the target of the offense? (Section 2.1.1)
2) Who commits economic crime? (Section 2.1.2)
3) Who is responsible for the prevention and for the prosecution of economic crime? (Section 2.2)

8 Bollhöfer & Jäger (2018), pp. 59–60.

2.1.1 Targets and aims of economic crimes

On the one hand, the field encompasses financial crimes such as blackmailing, embezzlement, and tax evasion – the last one often being related to attempts of cutting social security costs. The aim is usually to achieve monetary gains – be it for personal use or on behalf of a third party. The target of a financial crime depends largely on the actual crime committed and can range from individuals to businesses, or the state.

As regards different types of "illegal earnings", roughly three main categories can be distinguished:

1) Obtaining a large amount of money through a single offence.
2) Digitally stealing small amounts of money from many people's bank accounts over a certain period of time, unnoticed but eventually amounting to huge gains for the criminals.
3) Financial gains by legal enterprises engaging in criminal activities; be this intentional or without even noticing the illegal nature of their own behaviour.

On the other hand, there is economic cybercrime on a level that can hardly be estimated as activities in cyberspace are hard to track with perpetrators hiding behind false IP addresses, setting up fake websites, or using the Darknet, e.g., for exchanging software or programme codes on unregulated and illegal "cyber markets".

Furthermore, the manipulation of stock exchanges, either for economic gain or for causing huge losses, and thus creating geopolitical tensions, poses a hazardous threat possibly affecting the economic wellbeing of entire nations.

2.1.2 Perpetrators of economic crimes

Next to organised crime groups using criminal proceeds in the lawful segment of the economy (e.g. money laundering, corrupting politicians and government officials), there are also lawful businesses facilitating unlawful economic activities; be it on purpose or due to negligence. This applies, amongst others, to accountants or lawyers who might not be aware of the crimes committed by their – apparently honest and law-abiding – clients.

Furthermore, there are novel economic activities that enter new terrain where no clear-cut legal rules exist yet. Criminals are usually faster in finding loopholes than regulations can be devised and enacted. One example of this is obvious when looking at the early days of crypto currencies. We should expect more of this type of economic crimes in the future.

2.2 The rabbit and the hedgehog: the dilemma of prevention and prosecution

Considering the tremendous and potentially devastating damages caused by economic crimes, the issue should be high on the agenda of policy-makers in general; and this holds especially true for R&I policy-makers. The results of the 2022 edition of the "Global Economic Crime and Fraud Survey" by PricewaterhouseCoopers (PwC) provide indications pointing in this direction. Businesses in the so-called technology sector, that are usually more involved in R&D activities than others, are particularly prone to becoming victims of economic crime.[9]

One problem for policy-makers and law enforcement are the (compared to other types of crime) exceptionally low detection and prosecution rates of economic crimes referred to in section 2.1. The reluctance of the victims to report incidents of economic crime to official agencies is only one reason for this. As most of the times many people or organisations have been victimised, criminal investigations are complex and require expertise, time, and endurance by the investigators. This issue is already challenging at the national level, but in case of crimes on an international scale, it certainly intensifies due to e.g., differing legal systems, varying legislation and regulations being

9 PwC (2022), p. 3.

applicable, difficulties related to (joint) international investigations or the absence of extradition agreements between the states involved.

But there is another important issue explaining the low reporting rates: the nature of the perpetrator(s). Here the question of relevance is if they are external or internal to the victimised company or organisation as this might have implications for 1) the willingness to officially report the crime (when externals commit the crime, the likelihood to file a complaint is presumably higher), and 2) the responsibility for the prevention of it (e.g., law enforcement agencies, private security agencies, the potential victims themselves via internal measures, …).

3 NOVEL DEVELOPMENTS, EMERGING TECHNOLOGICAL AND OTHER OPPORTUNITIES

3.1 Some trends and drivers

Major drivers for crime are linked to motivation, but others to technological possibilities. A strong motivation can, for example, be found in the luring of high gains combined with the low perceived risk of detection. Thus, given the "right" preconditions, a cost-benefit calculation suggests that committing a certain crime will be more profitable than obeying the law. Apart from this fundamental motivating factor, we can distinguish several types of motives especially pertinent to criminal economic activities:

1) Criminals exploiting the intrinsic motivation of engineers to conduct research and innovate for their own, illegal purposes. This phenomenon already exists but may expand until 2040.
2) The politically motivated wish to spy on or threaten other countries; the prime motivations being greed and/ or the desire to gain power or at least some influence over those countries. As geopolitical tensions intensify, this is definitely to increase with the technological means available. It is assumed that it is supported by new satellite systems that are and will be installed all around the world in the coming years.
3) Perceived economic needs of the individual or of groups in case of economic crises may rise as some countries are heading towards a recession (view from the year 2022). This was always a motivation for crime, but in times of multiple crises – exploding price of energy, recession and inflation – groups or individuals may be in a precarious situation and see illegal activities as the only way out of crisis.

Other trends, drivers and single developments can already be seen today and may expand in the future if not addressed. They all increase the possibilities for committing crimes or acting in a grey zone:

1) Technological possibilities that come up now or are still unknown today will unfold in a way that they open up new pathways for criminal economic activities. In some cases, unregulated or deregulated market segments may also be exploited.
2) The further development and use of distributed ledger technologies, such as blockchain or other crypto currencies as well as their use for “safe” documentation will lead to new possibilities in money laundering via crypto currencies as these cannot be traced back at a certain point in time or when handed over through many stations. This kind of misuse is clearly on the rise.
3) The Darknet allows for a completely different infrastructure with cryptofiles, which the state or police cannot access. This offers new possibilities for illegal products and their trade (from drugs to whatever is imaginable). With new technological means and the knowledge to handle them, the potential to commit crime will further increase.
4) The new possibilities in internet and “metaverse” take place in unregulated areas (at least for a certain time). They may be intentionally and unintentionally exploited and the borders of “crime” are already and will even become more blurred as nobody is able to follow, for example the flow of money, anymore.

5) If Artificial Intelligence develops further as real machine learning systems, this opens up new possibilities for acquiring money.[10] Currently, we see financial markets using AI in a way that is so fast that bankers and brokers cannot follow anymore. This may lead to another stock market crash (Dodson 2008; Dabholcar 2018) or the digital version of a "run on the bank", called a "flash crash."[11] Who is to blame and responsible in case it happens?
6) Identification with face recognition (Sarabdeen 2022), fingerprint or iris scan is well known, but will be newly combined to prove the identity for several services (see, e.g., project IMPULSE). They make it more difficult to steal identities, but as in these cases, many identities can be created, people do not only get confused or lazy with their updating and taking care of their identities, creative people will find their way to copy fingerprints (or steal the finger), use digital face twins or other copies of the identification devices. This remains a race between criminals and legal authorities.
7) Identity theft is still on the rise. Phishing is already used by many in sophisticated ways, but the more technology offers to imitate real persons, real letters, logos or webpages, the more easy it becomes to convince people to click on a link, and thus open the door for the next crime. With ever more advanced equipment and more creativity, much more identity theft can be expected.
8) In a study about law abiding behaviour, Dong and Zeb describe the role of education in "nurturing" lawful citizens. Especially the high school and university periods are important, because „an integral part of the educational process is the imparting of moral values and law-abiding behaviours in students" (Dong and Zeb 2022:1). Where is it taught in the future and what is law abiding behaviour? Values will likely play a more prominent role here in the future.
9) Crypto communication within criminal organisations or between single individuals is becoming easier with new tools. Crypto video tools exist and may expand.

All the above motives and developments may remain relevant in the future. Motivating factor 3 is especially expected to be more relevant in the near future, leading to more crime just because of need. But only a few individuals possess enough "criminal energy" and knowledge to be successful in committing these crimes – without being caught. Opportunities 1 to 7 exist everywhere and possibilities increase: innovation in digitalisation is an essential precondition for the development of new, and further "improvement" of already existing, crime potential in digital environments, from payment systems to crypto circumvention. During the first wave of the pandemic, the Internet became the default mode of communication as strict lockdown measures were implemented. It remains a major platform for work, classes, consultations, shopping, and socialising. As such, we have already observed a so-called "switch" from the physical world to the digital one (Miró-Llinares & Moneva 2019; Monteith et al. 2021; Plachkinova 2021). That is likely to continue, possibly intensify. This greater activity in the digital space has provided new opportunities for motivated offenders to exploit vulnerable groups and systems including infiltration of individual computers, health care systems, and video conferencing tools (Chawki 2021; Collier 2020; Collier et al. 2020; Monteith et al. 2021; Pawlicka et al. 2021). Thus, especially technological developments in this area might open up new avenues for criminal activities related to digital economies and markets.

To sum up, the area at hand seems to be shaped by a competition, a race or mutual pushing and pulling between law-makers, law enforcement agencies, and criminals of who find a new niche to occupy and exploit. On the side of law enforcement agencies, skills, resources and motivation for time-consuming investigations or detecting crime in cyberspace are often missing. It is a matter of available resources and the time needed to detect and fight this kind of crime.

But there are different innovations that may open new avenues for criminal economic activities. Digitalisation of economic activities is a visible first step, but other technologies offer further possibilities. For instance, human enhancement technologies open up possibilities for biohacking and the ambition to better monitor supply chains may open doors to new forms of misusing this

10 https://unicri.it/sites/default/files/2020-11/Abuse_ai.pdf

11 https://medium.datadriveninvestor.com/the-good-the-bad-ai-automation-in-the-us-financial-services-industry-7bcd32daade2

kind information. Fake profiles, stolen identities, digital twins and "deep fake" technologies can also be misused to commit digital economic crimes while staying anonymous on the internet. Hacking the human being's surrounding (computers, smartphones, digital aura, infrastructure of the home...) or internal spare parts (artificial organs, exoskeletons ...) combined with blackmailing are conceivable crimes of the future. A huge amount of creativity is expected here, also in combination with artificial intelligence applications and new genetic engineering. Stealing the identity of persons for economic and other crimes is already on the rise and it is highly likely to further increase. People are more and more vulnerable to digital fraud and other kinds of crime in the virtual world as new possibilities for criminality are constantly emerging and diversifying.

However, if people refuse to use digital technologies (as a protective measure), they are excluded from certain economic activities and social life fora. Still, too much security (e.g., two or more factor authentication) erect rather high technical hurdles for lots of users and requires patience from them. There are still many people who just refuse authentication, are careless about passwords (still many people use 123456) or other identifyers, and use no double checks at all. This makes it easy for criminals to be "successful".

3.2 Potential future issues and disruptions

Thinking with a longer term view, there are many potential issues that may occur and several questions need to be considered:

- What if criminals in their R&I activities remain ahead of lawful companies, regulatory bodies, law enforcement agencies, and other decision-makers, especially in digital innovations?
- What if criminals offer significantly higher "salaries", qualitatively better education and training and other incentives to experts, e.g., researchers or skilled personnel of law enforcement agencies; personnel who are rare and highly specialised? (It means a much higher incentive than in 2022.)
- What if criminals become major R&D funders (e.g., for money laundering)? What if they invest their funds, obtained from illegal activities, directly in R&I and researchers depend on these projects?
- What if national banks are no longer the masters of currencies but the many crypto and other currencies are in the hands of everyone to be used, certified, borrowed or distributed? What is the role of states, the national banks, and their currencies, then?
- What if the Darknet is such a sophisticated place that it is much ahead of any state offer?
- What if citizens can make use of the Darknet in an easy way and, thus more an more of their activities from shopping to obtaining and sharing information take place there?
- How does the role of the state change, if it constantly does not have the resources (money, capacities, and capabilities) to fight criminal economic activities? What are the signals citizens notice in such a state and how will they react to these signals?
- What if new internet spaces and "metaverse" places are hosted in unregulated areas or offer unregulated worlds intentionally (not only for gaming)?
- What if Artificial Intelligence causes the next big financial market crash? Or shall we ask "when" (not "if") it occurs?
- What if people cannot identify themselves, anymore, without any account or identity that has one or two additional identifiers?
- What if we have to live with our digital twins plus a number of other digital identities? Can we keep pace in knowing them?
- What if there is no value education? Churches are losing their power and mandate for this.
- What if the full traceability of financial flows becomes possible? What if this poses a risk to creativity and innovation in and for lawful economic activities?

- What if money does not exist, anymore, and is replaced by “virtual money” or a new kind of technology, that is based on trust? Many countries already replaced physical money, but the systems behind are vulnerable (see Wirecard scandal).
- What if complicated regulation and law procedures keep criminals ahead of law-making and offer unregulated or “grey” zones to exploit the vulnerability of various types of victims?
- Which level of regulation is necessary to secure a safe environment for R&I? Which level is desirable to keep innovation and creativity vibrant for lawful economic activities?
- What if the reliance on self-regulation facilitates economic misdemeanour?
- What if the criminals control a large part of the economy?
- What if rogue states actively facilitate illegal activities, e.g., via crypto currencies, so that they directly undermine state functions of other states?
- What if a large number of companies under financial pressure decide to resort to criminal "service providers" in specific fields, as is already observed in some cases (e.g., waste disposal)?
- What if legally operating businesses are unconsciously used by criminals, e.g., for money laundering, on a large scale and this is undermining their business?

3.3 Four scenarios

It is intrinsically difficult to draw scenarios for the different possible futures, in which crime might develop. Concerning R&I activities, as well and R&I policies and regulation, different scenarios are instructive. We need to consider various types of actors in these scenarios: criminals, potential victims to be defended, legislators and regulators, and law enforcement agencies.

If we focus on two decisive factors, namely “who leads in R&D” and “the type of regulation” as the two axes of our matrix, we arrive at four possibilities presented in Figure 1. Strict and loose regulations also mean more or less freedom of individuals, closely related to the dichotomy between autonomy and freedom.

Figure 1: Four scenarios defined by “the type of regulation” and “who leads in R&I”

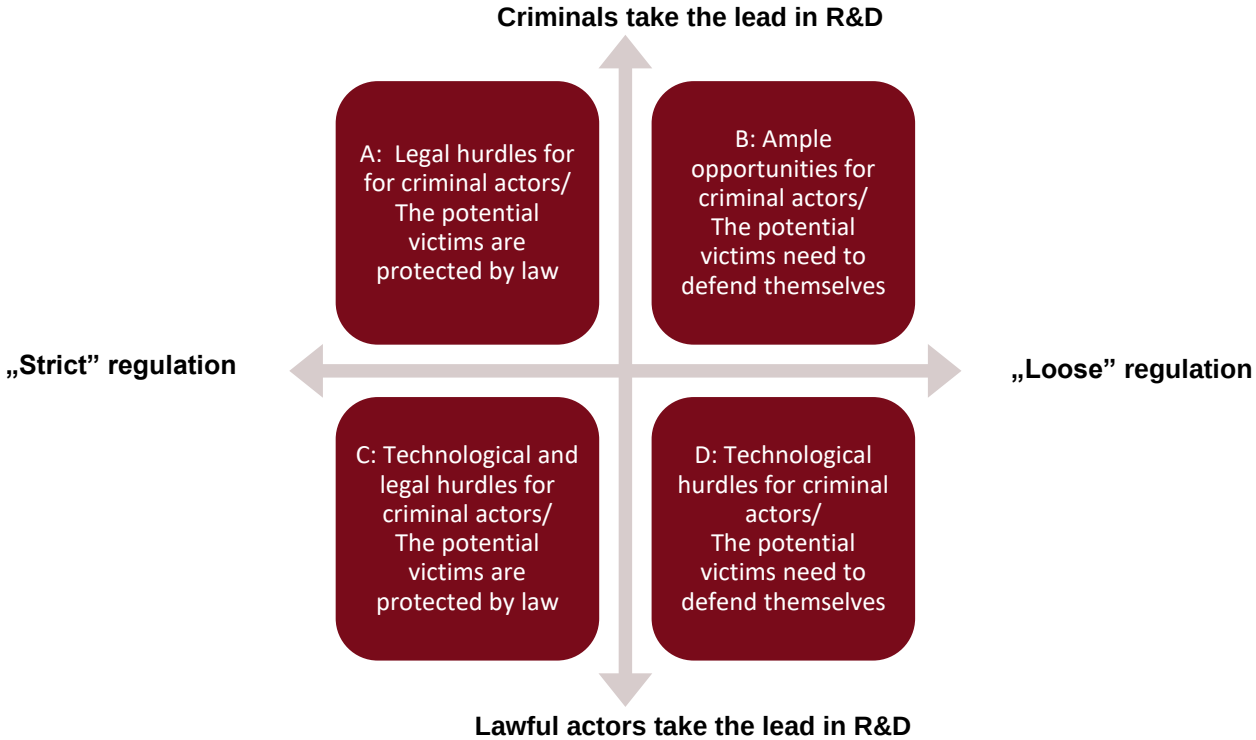

Table 1: Main features of the four scenarios

	Scenario A	Scenario B	Scenario C	Scenario D
Who leads in R&I activities	Criminals take the lead, making it harder to fight criminal economic activities Proceeds from their criminal activities, as well as the need to "clean" these proceeds, lead to significant spending on R&I by them, securing their leading position in these activities Strict regulation can restrict money laundering to some extent	Criminals take the lead, making it harder to fight criminal economic activities Proceeds from their criminal activities, as well as the need to "clean" these proceeds, lead to significant spending on R&I by them, securing their leading position in these activities Loose regulation makes money laundering relatively easy	Lawful actors take the lead, increasing the chances to fight criminal economic activities Proceeds from criminal activities are not sufficient to give the "edge" to criminal actors in R&I Strict regulation restricts money laundering, making it more difficult to close the gap in R&I with the lawful actors	Lawful actors take the lead, increasing the chances to fight criminal economic activities Proceeds from criminal activities are not sufficient to give the "edge" to criminal actors in R&I, although loose regulation makes money laundering relatively easy and R&I can be a candidate for money laundering
Regulation of economic activities (complexity, creativity, grey zones)	Strict regulations erect legal hurdles for criminal actors A few grey zones still offer some opportunities for criminal actors as the complexity of the economy precludes "watertight" regulations Strict regulations are likely to hamper creativity in lawful economic activities, as well as in R&I for lawful purposes Strict regulations constrain self-regulation by economic actors, and thus lessen opportunities for economic misdemeanour That might be counterbalanced to some extent by	Loose regulations, coupled with the lead in R&I by criminal actors, create ample opportunities for them Loose regulations foster (do not restrict) creativity in both criminal and lawful economic activities, as well as in R&I for both purposes Loose regulations give more prominence to self-regulation by economic actors, and thus create opportunities for economic misdemeanour These opportunities are further strengthened by the criminal actors' lead position in R&I	Strict regulations erect hurdles for criminal actors A few grey zones still might offer opportunities for criminal actors as the complexity of the economy precludes "watertight" regulations These opportunities are fewer than in Scenario A, as criminal actors lag behind in R&I activities Strict regulations are likely to hamper creativity in lawful economic activities, as well as in R&I for lawful purposes Strict regulations constrain self-regulation by economic actors, and thus lessen opportunities for economic misdemeanour	Loose regulations create opportunities for criminal actors, but fewer than in Scenario B as they lag behind in R&I activities Loose regulations foster (do not restrict) creativity in both criminal and lawful economic activities, as well as in R&I for both purposes Lawful actors are more successful in profiting from these opportunities Loose regulations give more prominence to self-regulation by economic actors, and thus create opportunities for economic misdemeanour That might be counterbalanced

	Scenario A	Scenario B	Scenario C	Scenario D
	the criminal actors' lead position in R&I		These opportunities are further reduced by lawful actors' lead position in R&I	to some extent by the lawful actors' lead position in R&I
Currencies, the role of national banks, traceability of financial flows	National banks control the issue of national currencies, but criminal actors profit from deals in crypto currencies, given their lead in R&I Financial flows are more easily traceable than in Scenarios B and D, but criminals can find or even create loopholes, given their lead in R&I	Crypto currencies gain importance at the expense of national currencies, and thus national banks play a weakening role Criminal actors profit from deals in crypto currencies, given their lead in R&I, coupled with loose regulation Financial flows are less traceable than in Scenarios A and C Criminals can profit significantly from this loose control, coupled with their lead in R&I	National banks control the issue of national currencies Crypto currencies play a minor role Criminal actors have limited opportunities for profiting from these deals, given their weak(er) performance in R&I and strict regulations Financial flows are more easily traceable than in Scenarios B and D Criminals are restricted in finding or creating loopholes, given their weak(er) performance in R&I and strict regulations	Crypto currencies gain importance at the expense of national currencies, and thus national banks play a weakening role Criminal actors profit from deals in crypto currencies, but to a significantly lesser extent than in Scenario B, given their weak(er) performance in R&I Financial flows are less traceable than in Scenarios A and C Criminals can profit from this loose control, but less so than in Scenario B
Law enforcement (capacities, resources)	Law enforcement agencies (LEA) are weakened by lack of highly skilled personnel as criminal actors offer significantly higher salaries Strict regulations give strong "teeth" to LEA and it should also mean adequate funding but that is not always the case in all EU member states	LEA suffer and are weakened by highly skilled personnel as criminal actors offer significantly higher salaries Loose regulations further weaken LEA The level of funding is lower than in scenarios A and C as loose regulation does not necessitate strong LEA with abundant resources	LEA have highly skilled personnel as criminal actors cannot offer more attractive salaries Strict regulations give strong "teeth" to LEA and it should also mean adequate funding but that is not always the case in all EU member states	LEA have highly skilled personnel as criminal actors cannot offer more attractive salaries Yet, loose regulations weaken LEA The level of funding is lower than in scenarios A and C as loose regulation does not necessitate strong LEA with abundant resources
Regulation of the net (Darknet, metaverse)	Strict regulations are in place to reduce possibilities for criminal actors	Loose regulations, coupled with criminal actors' lead in R&I create	Strict regulations are in place to reduce possibilities for criminal actors	Loose regulations create ample opportunities for criminal actors on

	Scenario A	Scenario B	Scenario C	Scenario D
	on the Darknet and in the metaverse, but given their leading position in R&I they can still create and seize opportunities	ample opportunities for them on the Darknet and in the metaverse	on the Darknet and in the metaverse Their weak(er) position in R&I further reduces their opportunities	the Darknet and in the metaverse Their weak(er) position in R&I reduces these opportunities to some extent
Artificial intelligence	Criminal actors exploit their lead in R&I to develop AI to create new opportunities to increase their proceeds from crime at the expense of individuals, companies, banks, other financial organisations (private and public), and state bodies Strict, well-targeted, and effective regulations can limit these opportunities to some extent	Criminal actors exploit their lead in R&I to develop AI to create new opportunities to increase their proceeds from crime at the expense of individuals, companies, banks, other financial organisations (private and public), and state bodies Loose regulations make it much easier to create and seize these opportunities	Lawful actors, both firms and LEA, can exploit their lead in R&I to develop AI to protect themselves against criminal actors and fight crime Strict, well-targeted, and effective regulations can further limit the opportunities for criminal actors	Lawful actors, both firms and LEA, can exploit their lead in R&I to develop AI to protect themselves against criminal actors and fight crime Loose regulations, however, make it still possible for criminal actors to create and seize some opportunities for themselves
Protection of potential victims	Strict regulations make criminal actors' life harder, and thus offer legal protection for potential victims Grey zones for crime are also constrained Self-protective measures by the potential victims are still crucial as criminal actors take the lead in R&I, and thus they can circumvent strict (state) regulations to some extent	Given loose regulations, potential victims are poorly protected by legal means Potential victims need to commit significant resources to defend themselves This need is rather strong as criminal actors are further "armed" given their lead in R&I activities	Strict regulations make criminal actors' life harder, and thus offer legal protection for potential victims Grey zones for crime are also constrained State bodies and lawful business actors are further strengthened by their lead in R&I: they can better protect themselves against criminal economic activities relying on these strengths	Given loose regulations, potential victims are poorly protected by legal means Potential victims need to commit significant resources to defend themselves State bodies and lawful business actors can rely on their lead in R&I: they can better protect themselves against criminal economic activities relying on these strengths
Value system	Strict regulations reduce grey zones, and thus offer guidance to adhere to a	Loose regulations "expand" grey zones, and thus make it more difficult to adhere to a sound value	Strict regulations reduce grey zones, and thus offer guidance to adhere to a	Loose regulations "expand" grey zones, and thus make it more difficult to adhere to a sound value

	Scenario A	Scenario B	Scenario C	Scenario D
	sound value system, labelling crime clearly as crime, i.e. illegitimate and socially unacceptable Some targeted research projects, funded by criminal actors, who take the lead in R&I, might undermine that value system, e.g. by relativising certain values	system, labelling crime clearly as crime, i.e. illegitimate and socially unacceptable Targeted research projects, funded by criminal actors, who take the lead in R&I, can further undermine a "shaky" value system by relativising certain values	sound value system, labelling crime clearly as crime, i.e. illegitimate and socially unacceptable Research projects, funded by lawful actors, who take the lead in R&I, can reinforce a value system against criminal activities	system, labelling crime clearly as crime, i.e. illegitimate and socially unacceptable Research projects, funded by lawful actors, who take the lead in R&I, can counterbalance these negative repercussions by underpinning a value system against criminal activities
Geopolitical conflicts	Rogue states can join forces with criminal actors, who have the lead in R&I, to cause financial turmoils, e.g. with AI tools and/or facilitate illegal activities, e.g., via crypto currencies to undermine other states Strict regulations can offer partial protection against these criminal activities	Rogue states can join forces with criminal actors, who have the lead in R&I, to cause financial turmoils, e.g. with AI tools and/or facilitate illegal activities, e.g., via crypto currencies to undermine other states Loose regulations further aggravate this dire state	Rogue states can join forces with criminal actors to cause financial turmoils, e.g. with AI tools and/or facilitate illegal activities, e.g., via crypto currencies to undermine other states The combination of strict regulations and the lawful actors' lead in R&I offer stronger protection against these criminal activities than in Scenario A	Exploiting loose regulations, rogue states can join forces with criminal actors to cause financial turmoils, e.g. with AI tools and/or facilitate illegal activities, e.g., via crypto currencies to undermine other states The lawful actors' lead in R&I offer partial protection against these criminal activities, a stronger protection than in Scenario B

4 POLICY AND FURTHER PRACTICAL IMPLICATIONS OF THE SCENARIOS

Scenario-specific implications

Scenario A: Strict regulation to some extent can constrain technological opportunities for committing crimes, but criminal actors still take the lead in R&I activities. The potential victims are protected by law, but they should not be complacent. They need to make efforts to defend themselves. Being right does not mean to be in the situation of "getting" right. There are significantly weaker opportunities for R&I for lawful economic activities for two reasons: criminals take the lead in these activities and regulations are likely to further hamper innovation by lawful actors given its "strict" nature. Yet, these researchers and innovative firms know what is allowed and what the boundaries of their research and innovation activities are. R&I policies need to focus on closing the gap between criminal and lawful actors in R&I activities and promote research on those types of regulations that are "strict" on criminal activities but do not hinder creativity and innovation for and in lawful economic activities. It might be forbidden to use AI for certain purposes

in such a scenario. Punishment when being caught is severe but – as seen in a study about the number of crimes during pandemic times and the punishment of crime Sarel (2021) – it is important to see punishment as a signal for others. Yet, drastic punishments have other types of repercussions, too, which need to be consisdered. For example, what has more disadvantages, a higher punishment by the state or that by the criminal organisation one belongs to when committing a crime. What is more harmful: leaving the criminal organisation, which might be dangerous, or being punished by the state when confessing a crime? (example from Sarel 2021 and the literature cited therein).

Scenario B offers ample opportunities for criminal actors in a world of limited regulation, significantly more than Scenario A. This may boost both crime in general and innovation to develop new types of economic crimes as well as new technologies to support the unlawful activities (e.g. new software, video tools, communication tools). Potential victims are not protected by strict and effective regulations, and thus they cannot expect much help from law enforcement agencies. It is even difficult to prove that there was a crime at all. An increasing number of various types of victims are vulnerable. They need to redouble their efforts (tools, techniques and knowledge) to defend themselves. R&I policies need to focus even more strongly in this scenario – compared to Scenario A – on closing the gap between criminal and lawful actors in R&I activities and promote research on how to tighten regulations that are likely to restrict the opportunities for criminals without "arresting" creativity and innovation for and in lawful economic activities.

In *Scenario C* criminal actors face both legal and technological hurdles, as researchers and innovative companies involved in lawful activities take the lead. Technologies to prevent and prosecute illegal economic activities are likely to evolve at a sufficiently fast pace, and effective policies are in place to foster lawful R&I activities. The potential victims are protected by legislation and have higher chances to defend themselves, thanks to advances in relevant technologies and other types of necessary knowledge. Specific education for personal economic security is offered by state organisations. R&I policies i) assist lawful actors in their efforts to keep their lead in R&I activities; and ii) play an important role in raising awareness of the potential victims and disseminate relevant knowledge to the various stakeholder groups (law-makers, law enforcement agencies, businesses, relevant NGOs, etc.) who can contribute in keeping criminal activities at bay.

In *Scenario D* criminal actors are lagging behind lawful R&I actors, while "loose" regulations do not constrain taking advantage of the creativity of both criminal and lawful actors. Here, R&I policies support the leading role of lawful R&I actors and winning the competition against criminal actors, as well as the race between criminals and the law enforcement agencies. The potential victims – be they individuals, specific social groups, businesses, or other types of organisations – need to devote considerable attention, time, and efforts to defend themselves, given the "loose" nature of regulations. They are supported by specific technology and security education provided by private and public organisations. Additional research is demanded in such a scenario on issues like "law abiding behaviour or cross-cultural studies to compare the significance of law abiding behaviour across different countries." (Dong and Zeb 2022:9). This, of course, does not only include economic crime but also academic dishonesty and plagiarism. R&I policies can also promote research on how to strengthen these "defence" capabilities of potential victims in a legal environment characterised by "loose" regulation.

Relations to research and innovation – all scenarios

The complex nature of criminal economic activities, their detection, investigation, and prosecution demonstrated so far, is related to research and innovation in at least three areas:

1) Research in, and the development and improvement of, information and communication technologies (ICT) necessary to monitor, track and analyse criminal activities. An interesting issue in this regard is whether technological solutions to full traceability (e.g., similar to those applied to products using chemicals) can be applied to money.

2) Regulatory techniques for preventing innovators from i) moving outside the sphere of lawful activities; ii) moving too far and entering a grey zone where regulation is missing; and iii) settling on clear-cut criminal behaviour.
3) Research in, and the development and improvement of, forensic techniques of reconstructing what actually happened, and thus attributing responsibility for crime.

The different scenarios have fundamentally different implications for R&I policy-making with an important exception: awareness raising is crucial in all the four scenarios. R&I policy-makers, together with their colleagues working on other policy domains, should be active in drawing potential victims' attention to economic crime, especially digital economic crime, as well as in promoting efforts aimed at developing self-defence capabilities of the potential victims, be they citizens, specific social groups, various types of businesses, other organisations, as well as state organisations. Different types of victims face different threats in all scenarios and have different level of self-defence capabilities and capacities. Policy-makers need to be aware and understand these differences and tailor their tools and efforts accordingly.

The threats of criminal activities are rising with the expansion of new technologies, especially in the IT sector. Cyberware, crypto currency misuse, fraud and small daily-life betrayals are ever more easily gaining ground. If this trend continues, and the public organisations are not well-equipped with the required technologies, time resources, capacities, and know-how of their personnel, the honest man is the fool and will pay the bill.

The race between criminal actors and the state trying to protect companies and citizens will be a permanent one – at least until 2040.

REFERENCES

Bollhöfer, E. & Jäger, A. (2018): Wirtschaftsspionage und Konkurrenzausspähung: Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Reihe A: Arbeitsberichte, Band A 8 09/2018.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S. & Díaz-Castaño, N. (2021): Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. European Societies, 23(1), 47–59. https://doi.org/10.1080/14616696. 2020.1804973.

Bullinger, L. R., Carr, J. B. & Packham, A. (2021): COVID-19 and Crime. Effects of Stay-at-Home Orders on Domestic Violence. American Journal of Health Economics, 7(3), 249–280. https://doi.org/10.1086/713787.

Chawki, M. (2021): Cybercrime in the context of COVID-19. in: K. Arai (Ed.), Intelligent computing. Lecture notes in networks and systems (Vol. 285, pp. 986–1002). Springer. https://doi.org/10.1007/978-3-030-80129-8_65.

Collier, B. (2020): Boredom, routine activities, and cybercrime during the pandemic (Briefing Paper). University of Cambridge. https://www.cambridgecybercrime.uk/COVID/COVIDbriefing-4.pdf.

Collier, B., Horgan, S., Jones, R. & Shepherd, L. (2020): Issue No 1 the implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations. The Scottish Institute for Policing Research.

Crane, A. (2005): In the company of spies: When competitive intelligence gathering becomes industrial espionage. Business Horizons, 48, 233–240.

Curnow, D. (2021): The Psychology of Embezzlement, The Art of Control and Intervention. https://doi.org/10.1007/978-3-030-74439-7.

Dabholkar, S. (2018): AI Will Cause a Global Financial Crisis. World Economic Forum. https://itmunch.com/ai-will-cause-global-financial-system-collapse-world-economic-forum/

Di Nicola, A. & Scartezzini, A. (2000): When economic crime becomes organised – the role of information technologies. Current Issues in Criminal Justice, 11(3), 343–348.

Dodson, S. (2008): Was software responsible for the financial crisis? The Guardian. https://www.theguardian.com/technology/2008/oct/16/computing-software-financial-crisis.

Fontanilla, M. V. (2020): Cybercrime pandemic. Eubios Journal of Asian and International Bioethics, 30(4), 161–165.

Horgan, S., Collier, B., Jones, R. & Shepherd, L. (2021): Re-territorialising the policing of cybercrime in the post-COVID-19 era: Towards a new vision of local democratic cyber policing. Journal of Criminal Psychology, 11(3), 222–239. https://doi. org/10.1108/JCP-08-2020-0034.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F. & Díaz-Castaño, N. (2021): Empty streets, busy Internet: A time-series analysis of cybercrime and fraud trends during COVID-19. Journal of Contemporary Criminal Justice, 37, 480–501. https://doi.org/10.1177/10439862211027986.

Liebl, K. (2020): Wirtschafts- und Organisierte Kriminalität, 3rd edition. Wiesbaden: VS Verlag für Sozialwissenschaften.

Le Moglie, M. & Sorrenti, G. (2020): When godfathers become entrepreneurs: On the organized crime's infiltration in the legal economy. https://cepr.org/voxeu/columns/when-godfathers-become-entrepreneurs-organized-crimes-infiltration-legal-economy (last accessed on Dec 1, 2022).

Miró-Llinares, F. & Moneva, A. (2019): What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks “Did cybercrime cause the crime drop?”. Crime Science, 8(1), 12. https://doi.org/10.1186/s40163-019-0107-y.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C. & Glenn, T. (2021): Increasing cybercrime since the pandemic: Concerns for psychiatry. Current Psychiatry Reports, 23(4), 18. https://doi.org/10.1007/s11920-021-01228-w.

Pawlicka, A., Choraś, M., Pawlicki, M. & Kozik, R. (2021): A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic. Business Horizons, 64, 729–734. https://doi.org/10.1016/j.bushor.2021.07.010.

Plachkinova, M. (2021): Exploring the shift from physical to cybercrime at the onset of the COVID-19 pandemic. International Journal of Cyber Forensics and Advanced Threat Investigations, 2(1), 50–62. https://doi.org/10.46386/ijcfati.v2i1.29.

PwC (2022): Protecting the perimeter: The rise of external fraud. Global Economic Crime and Fraud Survey 2022. https://pages.pwc.de/content-form?qs=dc7fcb176550eb1a6d1e950e3a1ac396b5c08c8064100f9d7340ba2417c51ff729ead2ec6a819a82828b04991d53e0fd37125fc7f2606f57313c16749b57295e2566ca86d6c4f8b6af906f69f70cb247 (last accessed on Oct 11, 2022).

Regalado, J., Timmer, A. & Jawaid, A. (2022): Crime and deviance during the COVID-19 pandemic, Sociology Compass, 16, e12974. https://doi.org/10.1111/soc4.12974. https://doi.org/10.1111/soc4.12974.

Sampson, A. S. & Ojen, I. M. (2021): Perception analysis of COVID-19 pandemic, cybercrime and well-being of online fraud victims in Calabar, Nigeria. International Journal of Public Administration and Management Research, 6(4), 29–35.

Sarabdeen, J. (2022): Protection of the rights of the individual when using facial recognition technology. Heliyon, 8(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086.

Sarel, R. (2021): Crime and punishment in times of pandemics. European Journal of Law and Economics, 54(2), 155-186. https://doi.org/10.1007/s10657-021-09720-7.

Velasco, C. (2022): Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum, 23(1), 109–126. https://doi.org/10.1007/s12027-022-00702-z.