343.9.02:{616.98:578.834]-036.21(100)

COVID-19 PANDEMIC AND NEW OPPORTUNITIES FOR ORGANIZED CRIME GROUPS

Tanja Miloshevska[48]
Ss. Cyril and Methodius University, Faculty of Philosophy, Institute for Security, Defense and Peace

Abstract: Since the beginning of 2020, the COVID-19 pandemic and the associated policies have transformed the environment in which organized crime groups operate. The COVID-19 has generated different opportunities for organized criminal groups and provoked them with different challenges. Due to the transformations induced by the pandemic, organized criminal groups had greater opportunities to further infiltrate the legal economy and to strengthen their illegal governance, possibly posing additional threats for governments. The analysis of illustrative cases shows evidence on the fact that the COVID-19 emergency has affected the behavior of some organized criminal groups by providing them with new opportunities to gain legitimacy and support in the community within which they operate, as well as to expand and diversify their investments. Study of how these groups have responded to the pandemic yields better understanding of how they work and enables the devising of more effective counter-strategies.

Key words: Covid-19 pandemic, organized crime, criminal activity, security threats.

Introduction

The fallout of the COVID-19 pandemic is having a profound impact on our societies and economic systems, which, in turn, influences and shapes organized crime and illicit markets. The socio-economic impact of the COVID-19 crisis is likely to be deep and long-lasting and may exacerbate pre-existing inequalities prevalent across societies in various areas, ranging from access to food supplies, education, health care and others.

These processes are already affecting the way criminal networks operate, and the nature of law enforcement responses to them. Most notably, organized criminal groups have been given further opportunities to exploit public funds made available by governments to help vulnerable groups. Moreover, those organized criminal groups that aspire to govern markets as well as territories have an opportunity to reinforce their control over land and deepen their bonds with communities, as the current crisis has exacerbated some States' fragility.

The COVID-19 pandemic has been a crisis of an unprecedented nature. The pandemic has proven to be more than a global public health crisis and has resulted in considerable changes in the serious and organized crime landscape in the EU and beyond. Criminals have quickly capitalized on these changes by shifting their market focus and adapting their illicit activities to the crisis context. The immediate impact of the COVID-19 crisis has been most visible in the counterfeiting and distribution of substandard goods, cybercrime, organized property crime, and various types of fraud schemes.

[48] Contact address: tanja@fzf.ukim.edu.mk

The mid to long-term consequences of the pandemic will result in further vulnerabilities. A prolonged pandemic will put a heavy strain on European and global economies, with indications that some countries are already entering an economic downturn. Learning from previous crises, it can be anticipated that a volatile economic situation with growing poverty and social inequality will serve as a breeding ground for organized and serious crime.

Organized crime groups and new business opportunities

Criminals will intensify their activities to fully exploit emerging vulnerabilities, in order to compensate for lost profit during the lockdown period. Criminals will continue to rely on the use of new technologies and further expand their technical capabilities. Criminal groups have quickly adapted to profit from the new business opportunities the pandemic economy has presented, taking advantage of the increased and widespread demand for certain products (Europol, 2020a).

The pandemic has clearly highlighted the dynamic nature of **cybercrime.** Since the outbreak of the pandemic, an increased number of COVID-19-related domains have been created to support different cybercrime activities.

The number of cyber-enabled and pandemic-related scams, COVID-19-themed malware, ransomware and phishing attacks notably increased during the pandemic, targeting individuals, businesses and the health sector alike (Europol, 2020b). With the roll out of COVID-19 vaccinationcampaigns, it is expected that the number of vaccine specific cybercrime activities will surge, including cyber-attacks on pharmaceutical research.

A global economic crisis may bring ordinary EU citizens into closer proximity to organized crime. Communities may become more tolerant of certain types of crime such asthe distribution of counterfeit goods or the cultivation of cannabis. This may also make individuals more vulnerable to recruitment by criminal groups due to a lack of alternative legal prospects. Young people with advanced technical skills who are unable to gain employment intheir chosen fields of expertise may turn to crime in order to finance themselves. This may result in a significant increase in the number of individuals engaging in cybercrime or offering cybercrime-related services.

The impact of the COVID-19 crisis on the drug markets has been relatively limited. Aside from initial and localized disruptions in the supply and distribution of drugs during the first lockdown, the trafficking of drugs has continued (Europol, 2020c). Despite fluctuations in the price and supply of drugs on the European market early in the pandemic, the drug market has largely returned to prepandemic levels.

The long-term consequences of the pandemic may manifest particularly severely in the area of financial crime (Levi, Smith, 2020). Businesses operating in sectors suffering particularly negative economic pressures, such as the hospitality, catering and tourism sectors, are becoming more vulnerable to criminal infiltration (Europol, 2020d).

Money laundering poses a high risk in times of financial crises. Criminals may increasingly attempt to launder money through dormant companies, buy out financially affected cash-intensive businesses, or invest in property in the construction sector(Europol, 2020)

As a result of heightened pressures exerted on banks during an economic crisis, due diligence procedures may be weakened elevating the risk of loan fraud. Money launderers may also increasingly misuse online financial services and virtual assets to conceal their illicit proceeds. Trade based money-laundering activities are also expected to intensify.

The COVID-19 pandemic has led to a considerable increase in the output of sanitary and medical waste, posing a significant risk to the environment and public health alike (Europol, 2020d).

A reduction in the number of inspections and controls of waste shipments by supervisory authorities enabled some criminals to traffic and illegally dispose of waste. Widespread economic hardship may open up additional opportunities for illicit waste traffickers. A general decline in corporate revenues may entice companies to take advantage of such illicit services in order to reduce waste disposal costs.

Latest trends and threats from criminal groups

The European Union recently released its "Serious and Organized Crime Threat Assessment 2021 (SOCTA)," a major report on the latest trends and threats from criminal groups operating in the EU. The report provides key findings on how criminal activity is evolving based on the Covid-19 pandemic, changing technology, cryptocurrency, and other factors. Despite its focus on the EU, these serious and organized crime threats are prevalent across the globe, and by exploring the roles of criminals within such processes, this assessment seeks to outline how a better understanding of those roles allows for a more targeted operational approach in the fight against them.

The five of the key findings and their implications for government regulators, financial institutions, and law enforcement agencies are:

1. **Money laundering as a growing issue.**"The scale and complexity of money laundering activities in the EU have previously beenunderestimated. Serious and organized crime [...] fundamentally relies on the ability to launder vast amounts of criminal profits."

2. **Criminals rely on legitimate business entities to facilitate their illegal activity.** "Legal business structures such as companies or other entities are used to facilitate virtually all types of criminal activity with an impact on the EU. More than 80 % of the criminal networks active in the EU use legal business structures for their criminal activities."

3. **Criminals have seized new opportunities created by the global pandemic.** "The Covid-19 pandemic has had a significant impact on the serious and organized crime landscape in the EU. Criminals were quick to adapt [their modes of operation] to take advantage of the pandemic."

4. **Criminal groups continue to evolve and adapt.** "Criminal networks are extremely adaptable and flexible in response to new measures and changes in legislation, the market/economic situation and law enforcement action. Their fraudulent schemes

are constantly evolving and improving in order to take advantage of the weaknesses of the state and legislation."

5. **Value-added tax (VAT) fraud and excise tax fraud continues to generate billions of Euros in losses.** "VAT fraud consists of avoiding the payment of VAT or fraudulently claiming repayments of VAT from national authorities following an illicit chain of transactions. Missing Trader Intra Community (MTIC) fraud is the abuse of the VAT system rules for cross-border transactions, involving the acquisition of goods [...] from another Member State which are then sold through a chain of companies [...] with VAT added. The VAT is then not paid to the tax authorities." Losses are estimated at 50 billion euros or more each year (SOCTA, 2021).

These "governance-type" organized criminal groups operate in many countries around the world. The illegal governance role of OCGs can be observed in different contexts, both in developing and developed countries (Albanese, 2011).

Traditional Italian mafias, such as the Sicilian Cosa Nostra, the Calabrian 'Ndrangheta, the Neapolitan Camorra, as well as the Russian Mafia, the Triads in Hong Kong and Macau, and the Japanese Yakuza, are the archetypical OCGs that yearn for governance. Yet, other criminal groups in the post-Euromaidan Ukraine, OCGs in China, and certain Latin American structured trafficking groups, criminal organizations in the United Kingdom and Nigeria, street gangs in the United States, in Brazil, South Africa, and other countries, all perform—albeit to varying extents—a governance role.

In the context of the analysis presented here, 'governance-type' organized criminal groups are understood to be criminal groups that aspire to exercise security governance in the areas they control. This is done by managing ordinary criminality and providing a secure environment to protect businesses paying protection fees and seeking to win the favor of local populations (Aziani at all. 2019).

Besides governance ambitions, criminal organizations have also the need and the capacity to infiltrate the legal economy in different ways for the purposes of laundering the proceeds of their illegal activities, logistically supporting those activities, and expanding their sources of income (Levi and Soudijn, 2020).The COVID-19 pandemic provides organized criminal groups with new opportunities to expand their infiltration. Indeed, the crisis has exposed numerous businesses to a severe shortage of capital. In the absence of sufficient and ready-to-obtain public subsidies, these businesses may be at greater risk of criminal infiltration (Stephany et al. 2020). More fragile economies are those where we expect organized crime infiltration to be higher because less solid companies and businesses operating in the grey economy have greater difficulties in obtaining loans from legitimate financial institutions. The banking system may not be able and willing to support struggling businesses because of increased systemic risk as well as their specific risk of loan default. On the other hand, organized criminal groups can compensate for the higher risks because of the high liquidity at their disposal, often lent with usurious interest rates, and they can be more effective than legitimate financial institutions in debt recovery by trespassing the boundaries of legality (Lavezzi, 2014).

Opportunities have arisen not only in the private sector. By relying on corruption practices and political connections, organized crime may indeed infiltrate public procurement in order to illicitly obtain public funds (Pinotti, 2015). For example, this has frequently been the case of earthquakes in Southern Italy (e.g., those in Belice in 1968, Irpinia in 1980 or Abruzzo in 2009). On those occasions, Cosa Nostra, the Camorra and other OCGs took advantage of reconstruction works to obtain public procurements and subsidies, and to strengthen their grip on local businesses and markets (Riccardi et al. 2016). This is of importance because already in the first month of the pandemic, the distress caused by the spread of the virus and by the social distancing measures induced the governments of several countries to plan unprecedented injections of liquidity into their economies (Rizwan et al. 2020).

Main contributing factors

The main contributing factors to the risk of embezzlement are:

- ✓ the sheer amount of disbursements and
- ✓ the need for rapid action.

The latter, in particular, may result in relaxed scrutiny on the use of funds. Urgency, in fact, may hinder the ability of governments to devise and activate proper public procurement policies, thus increasing the risk of criminal misappropriations.The amount of information on illegal governance activities far exceeds the direct evidence of criminalinfiltration in the legal economy. Two factors may explain this.

1. First, illegal governance activities maytake place prior to episodes of infiltration in the legal economy.

2. Second, illegal governance measuresare more public and explicit than attempts to infiltrate the legal economy. A systematic analysis ofopen sources also allowed for the identification of a number of instances of OCGs' involvement in boththe provision of and trafficking in medical products generated by the COVID-19 emergency.

Nevertheless, tentative patterns are already emerging that point to the following:

- ➢ The COVID-19 crisis has offered unique opportunities to OCGs around the world;
- ➢ Organized criminal groups are targeting legitimate businesses that are struggling because of thecrisis;
- ➢ New markets in medical equipment are being exploited by OCGs;
- ➢ In some cases, governments have failed to enforce restrictions, allowing OCGs to step in;
- ➢ OCGs have increasingly sought out opportunities to commit various forms of cybercrime
- ➢ The ways in which OCGs have responded to the crisis depends on their size and internal structure (Boyle, Banuelos, 2021).

These groups are seeking to benefit from the COVID-19 response, just as they have done in the past during other humanitarian crises. OCGs, such as the Sicilian Cosa Nostra, the Calabrian 'Ndrangheta, as well as the Russian Mafia, the Triads in Hong Kong and Macau,

and the Japanese Yakuza, are again looking for opportunities to defraud legal economies and exploit funds made available by governments.

The global recession sparked by the pandemic and the national lockdowns have brought several businesses to collapse, produced massive layoffs, and placed severe stress on national institutions and public expenditure. Unable to cope with these challenges in such a short time, many states have left gaps in their emergency responses, which, in turn, have provided opportunities for OCGs to take advantage of the situation. The industries at highest risk are businesses experiencing liquidity shortage and those with actual high demand products and services.

The fact that many more business activities are now being conducted online has led to an increase in phishing, credit card fraud, pirated sites for fake donations, and cyber-attacks. There have been multiple reports of fake and cloned websites as well as suspicious email addresses. Many of these scams involve coronavirus-related topics, such as the sale of face masks and disinfectants. Moreover, OCGs have begun trafficking in both non-certified and stolen high-demand products such as face masks and disinfectants (UNODC, 2020).

A growing body of evidence shows that COVID-19-related scams are taking place on the 'surface web', (Szurdi et.al, 2020) which refers to the Internet pages indexed by search engines. The supply of counterfeit and substandard medical equipment as well as sanitary and pharmaceutical products increased significantly both on the surface and dark web (Europol, 2020a). A study of several Dark Web anonymous marketplaces conducted in April 2020 sought to address this gap and identify a range of transactions involving medicines and medical equipment related to COVID-19.

Further in-depth analysis of vendor behaviouron Dark Web marketplaces may offer insightsinto the ways in which the COVID-19 pandemicis influencing illicit online sales of goods such asmedical devices and equipment and licit pharmaceuticalmedicines. Studying the long-term impactof COVID-19 on online narcotics sales will be ofequal importance, as buyers may face obstacles inmeeting dealers face-to-face and as a result mayturn increasingly to online sources to purchaseillicit drugs. Furthermore, confinement measuresand the closure of borders introduced in manycountries to contain the spread of the pandemicpose significant challenges to online vendorsseeking to ensure the shipping of their productsis not disrupted. Disruptions or alterations to traditionalprocurement and shipping flows may beable to be identified through studying the longtermimpact of the COVID-19 pandemic on onlinesales of illicit drugs (UNODC, 2020).

Changes in the modus operandi of organized criminal groups

Evidence shows that organized criminal groups are using the COVID-19 pandemic to infiltrate the legal economy and strengthen governance activities in response to emergencies triggered by the ongoing crisis (UNODC, 2020).

The involvement of organized criminal groups in the provision of medicines ostensibly related toCOVID-19, such as chloroquine, both in terms of infiltrating the legal supply chain and managing their illicit trade, is supported by evidence from seized shipments of illegal medical products in several countries (FEMHP, 2020).

Such groups are reconsidering their strategies and increasingly switching to other types of crime involving falsified goods such as PPE and medicines (Sinn, 2018).

Various types of cybercrime involving fraudulent medical products have been linked to new modus operandi of organized criminal groups resulting from the COVID-19 pandemic, as illustrated by the following examples:

-The UK's National Cyber Security Centre (NCSC) said it took down more than 2,000 on-line coronavirus scams in March 2020 which included 471 fake online shops selling fraudulent COVID-19-related items (BBC, 2018).

-Police in France removed 70 fraudulent websites claiming to sell chloroquine in April 2020 (Bleu, 2020).

-COVID-19-related scams in the USA amounted to approximately US$13.4 million from the beginning of January to mid-April 2020 and have affected more than 18,000 citizens (Iacurci, 2020).

-In the first four months of 2020, 1,541 cyber-attacks related to COVID-19 were detected in the United Arab Emirates including 775 malware threats, 621 email spam attacks and 145 URL attacks (Nasir, 2020). A considerable number of cyber-attacks and scams related to the COVID-19 pandemic was recorded worldwide during the first four months of 2020. Such scams include social media advertisements and websites for the purchase of PPE, test kits, sanitizer and falsified medicines.

-Qualitative assessments of the situation in Macedonia indicate that organized criminal groups are moving away from drug trafficking to other types of crime involving falsified medical products such as protective equipment and pharmaceutical products (UNODC, 2020). Cybercrime using various malware and ransomware packages themed around COVID-19 are also predicted to be part of the new modus operandi.

- In Mexico, it has been reported that organised criminal groups, such as drug cartels, are likely to switch to cybercrime. It is expected that online fraud, including through phishing attacks, will rise during the period of emergency measures put in place to curb the spread of the pandemic (UNODC, 2020). Due to the growing demand for protective equipment, there are increased shipments of medical equipment circulating worldwide, which organized criminal groups may take advantage of transport illicit drugs from one country to another. A case involving 14 kg of cocaine smuggled into the UK in a consignment of face masks was reported in April 2020 (Reuters, 2020).

Large-scale transnational fraud involving the purchase of protective equipment has also been identified as part of the new modus operandi of organized criminal groups emerging as a result of the COVID-19 pandemic.

Conclusion

The pandemic has both reduced certain organized crime activities, while, simultaneously, providing opportunities for new ones. Organized criminal groups are trying to increase their profits not only by infiltrating private companies but also by misusing public funds.

However organized criminal groups will carry on to develop and find new ways to exploit events like the global pandemic and changing technology. Both government and private sector organizations have more options than ever before for using data and advanced analytic tools to identify criminal activity quickly, prevent many losses before they occur and become more efficient than ever, in spite of limited resources.

References

1. Albanese, J.S. ed., *Transnational Crime and the 21st Century: Criminal Enterprise, Corruption, and Opportunity*, 1 edition, New York: Oxford University Press, 2011.
2. Aziani, A., Favarin, S., and Campedelli, G.M., 'Security Governance" Mafia Control Over Ordinary Crimes", *Journal of Research in Crime and Delinquency*, vol. 57, No. 4, pp. 444-492, 2019.
3. BBC News, "Coronavirus: UK forces hundreds of scam Covid-19 shops offline", 21 April 2020, online https://www.bbc.com/news/technology-52361618
4. *Europol* 2020a. Viral marketing, 2020, online https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-substandard-goods-and-intellectual-property-crime-in-covid-19-pandemic.
5. *Europol* 2020b. How COVID-19 related crime infected Europe in 2020, online https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020
6. *Europol,* Pandemic profiteering – How criminals exploit the COVID-19 crisis, online https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis
7. *Europol* 2020c, Enterprising criminals: Europe's fight against the global networks of financial and economic crime, 2020, online https://www.europol.europa.eu/publications-documents/enterprising-criminals-%E2 %80 %93-europe %E2 %80 %99s-fight-against-global-networks-of-financialand-economic-crime.
8. *Europol* 2020d, Beyond the pandemic – how COVID-19 will shape the serious and organized crime landscape in the EU, 2020, online https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscapein-eu.
9. European Union Serious and Organized Crime Threat Assessment, SOCTA, *A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organized Crime*, EUROPOL, online https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment, 2021.
10. Federal Agency for Medicines and Health Products, "*Coronavirus: the FAMHP seizes postal packages containing counterfeit and other illegal medicinal products against COVID-19*", 31 March 2020, onlinehttps://www.famhp.be/en/news/coronavirus_the_famhp_seizes_postal_packages_containing_counterfeit_and_other_illegal_medicinal.
11. France Bleu, *"Coronavirus: les gendarmes de Strasbourg luttent contre les escrocs du web"*, 18 April 2020, online https://www.francebleu.fr/infos/faits-divers-justice/coronavirus-les-gendarmes-de-strasbourg-luttentcontre-les-escrocs-du-web-1587201320.

12. Iacurci, G., "Americans have lost $ 13.4 million to fraud linked to Covid-19", *CNBC,* 15 April 2020, online https://www.cnbc.com/2020/04/15/americans-have-lost-13point4-million-to-fraud-linked-to-covid-19.html.

13. Joe Boyle, Tania Banuelos*, The Impact of COVID-19 on organized crime*. UNODC (United Nations Office on Drugs and Crime), Vienna, 2021.

14. Lavezzi AM. Organised crime and the economy: a framework for policy prescriptions. *Global Crime* 15(1–2):164–190, 2014, online https://doi.org/10.1080/17440572.2013.868626.

15. Levi and Smith. *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19,* Australian Institute of Criminology Research Report, 2020.

16. Levi M, Soudijn M. Understanding the Laundering of Organized Crime Money. *Crime Justice* 49:579–631, 2020, online https://doi.org/10.1086/708047.

17. Nasir, S., "Coronavirus : cyber experts warn of 'sharp spike' in criminal activity", *The National,* 21 April 2020, onlinehttps://www.thenational.ae/uae/coronavirus-cyber-experts-warn-of-sharp-spike-in-criminal-activity-1.1008945.

18. Pinotti P. The Economic Costs of Organized Crime: Evidence from Southern Italy. *Economic Journal* 125(586):F203–F232, 2015.

19. Reuters, "Drug smugglers hide $1.3 million worth of cocaine in UK face mask consignment", 16 April 2020, online https://www.reuters.com/article/us-britain-crime-cocaine/drug-smugglers-hide-1-3-million-worth-of-cocaine-in-uk-face-mask-consignment-idUSKCN21Y1V0.

20. Riccardi M, Soriani C, Giampietri V. *Mafia Infiltration in Legitimate Companies in Italy. Organized Crime in European Businesses.* Routledge, Abingdon, 2016.

21. Rizwan MS, Ahmad G, Ashraf D. Systemic risk: The impact of COVID-19. *Finance Research Letters,* 36(101682):1–7, 2020, online https://doi.org/10.1016/j.frl.2020.101682.

22. Sinn, A. *The link between illicit tobacco trade and organised crime*, 2018, onlinehttps://www.eesc.europa.eu/sites/default/files/files/mr_arndt_sinn_speech.pdf.

23. Stephany F, Stoehr N, Darius P, Neuhäuser L, Teutloff O, Braesemann F. The CoRisk-Index: A Data-Mining Approach to Identify Industry-Specific Risk Assessments Related to COVID-19 in Real-Time. ArXiv: 2003.12432 [Econ, q-Fin], 1–2, 2020.

24. Szurdi et.al. "*Studying How Cybercriminals Prey on the COVID-19 Pandemic*", Palo Alto Networks Blog, 2020.

25. UNODC field office assessment, May 2020.

26. United Nations Office on Drugs and Crime, *COVID-19-related Trafficking of MedicalProducts as a Threat to Public Health*, Vienna, 2020.