THE IMPACT OF COVID-19 ON TRANSPORT CRIME

Andrei Borisov,
*Associate Professor,
Law Institute of the Russian University of Transport,
Moscow, Russia*

Jonathan Lewis,
*Associate Professor, Hitotsubashi University,
Tokyo, Japan*

Abstract

The COVID pandemic has intensified crime activity around the world. The article is devoted to the analysis of the impact of the pandemic on international crime. Particular attention is paid to strengthening the activities of cybercriminals, including in the transport industry.

Key words: COVID-19, fraud, cybercrime, organized crime, transport, transport crime.

JEL codes: K-10, K-14.

1. Introduction

The COVID-19 epidemic has a profound impact on all social processes in society, including criminal manifestations, especially organized crime and illegal markets.

The most important provisions on changes in criminal activity during the pandemic are contained in the Europol report ‘Pandemic Speculator: How Criminals Exploit the COVID-19 Crisis’ [2]. Europol analysts note that criminals quickly took advantage of the opportunities to exploit the crisis by adapting their ways of acting or engaging in new criminal activities. Factors that cause changes in crime and terrorism include:

- a high demand for certain goods, protective equipment and pharmaceutical products;
- the reduced mobility and the flow of people through and into the EU;
- the citizens stay at home and increasingly work from home, relying on digital solutions;
- the restrictions in public life will make some criminal activities less noticeable and transfer them to home or online settings;
- an increased anxiety and fear that can create vulnerability to exploitation;
- reducing the supply of certain illegal goods to the EU.

2. Main part

Based on the information provided by the EU member States and its own expertise, Europol identifies three main crime areas of the COVID-19 period:

The first is cybercrime [8]. The number of cyberattacks against organizations and individuals is already significant and is expected to grow. Criminals used the COVID-19 crisis to carry out social engineering attacks dedicated to the pandemic, to distribute various malware packages.

Cybercriminals are likely to seek to use an increasing number of attack vectors, as an increasing number of employers introduce online work ('remote') and allow them to connect to the systems of their organizations.

Let's consider an example: the Czech Republic reported a cyberattack at the Brno University Hospital, which forced the hospital to close the entire IT network, postpone urgent surgical interventions and redirect new patients with acute illnesses to the nearest hospital.

The second is fraud. Fraudsters very quickly adapted well-known fraud schemes to the new situation in order to benefit from the fears and fears of victims during the crisis. These include various types of adapted versions of telephone fraud, supply fraud, and decontamination schemes. It can be expected that even

more new or adapted fraud schemes will appear in the near future, when scammers will try to capitalize on the concerns of people all over Europe.

Here is another example: an investigation supported by Europol focuses on the transfer of 6.6 million euros by a company in Singapore to a company for the purchase of alcohol-containing gels and FFP3 masks/2 [4]. The product hadn't been received.

The third is counterfeit goods. The sale of counterfeit medical and sanitary products, as well as personal protective equipment and counterfeit pharmaceutical products has increased significantly since the beginning of the crisis. There is a risk that counterfeiters will use the shortage in the supply of some goods to increasingly provide counterfeit alternatives offline.

The report 'Crime and the virus. The impact of the COVID-19 pandemic on organized crime', prepared by the international research organization "Global Initiative Against Transnational Organized Crime", is the result of generalization and comprehension of information received from state police authorities, international communities of retired police officers, as well as from our partners from government organizations, research centers and civil communities regarding the impact of coronavirus on organized crime and illegal markets.

The report notes that the pandemic is changing the face not only of the economy and finance, but also the volume, structure and principles of functioning of criminal markets and related organized crime.

At the first stage of the pandemic, there is almost everywhere a slight decrease in the crime rate and a decrease in the activity of organized crime. However, with the continuation of the pandemic and especially its deployment under the most unfavorable scenario associated with high mortality and reduced manageability in certain regions, countries and cities, a surge in organized crime activity and a significant increase in demand for illegal goods and services is quite likely.

Another context of interaction between organized crime and the pandemic is associated with the intertwining of state power with organized crime through

corruption and direct representation of crime in power. In such states, organized criminal groups (organized criminal groups) were deeply integrated into the financial sector, healthcare, and logistics even before the pandemic. In such States, the consequences of a pandemic can be especially terrible, since organized criminal groups will try to increase their power, increase the scale of controlled resources by parasitizing the medical care of the population and using resources to combat the pandemic.

Restrictions on travel and movement within cities and towns, as well as a dramatic reduction in economic activity and international trade during the first stage of the pandemic, inhibits and restricts criminal activity. However, such restrictions will only be of a short-term nature. Unfortunately, in some countries and regions, the OP is more flexible and operational than law-abiding structures. Accordingly, at the stage of the development of the pandemic, it will try to put under its control new, fast-growing areas of economic activity, including delivery services, remote trading, online financial and credit services and the provision of illegal medical services [3].

The pandemic puts government agencies under unprecedented pressure. COVID-19 forces governments to strive to achieve two incompatible goals: minimizing the sick and dead from coronavirus and saving the economy and finances from complete, irreversible destruction. Although institutional overstrain has many consequences, in relation to law enforcement agencies, the following is almost the main thing.

The police, together with the National Guard and, if necessary, the army, mainly, at least in the first stage of the pandemic, solve the tasks of blocking, isolating and maintaining logistics chains in working condition. They often do not have enough time to fight organized crime. Most of the criminals, as well as the whole society, were forced into isolation and minimized their activity. At the same time, young and high-tech criminals, taking advantage of increased impunity, are stepping up activities primarily related to the production and trafficking of drugs, as well as the sale of counterfeit coronavirus testing devices, artificial respiration

devices. In addition, it is known that in Italy, Spain, Portugal, Brazil and even in some states of America, high-tech organized criminal groups have placed online and DarkNet stores where you can buy the above products. Almost all of it is counterfeit.

These processes are typical not only for developed countries. For example, in Guinea-Bissau, after the disputed elections in December 2019, competing political parties consider their candidates as president and prime Minister. Accordingly, the country plunged into chaos and anarchy at the beginning of 2020. Since Guinea-Bissau became a key point for the transportation of cocaine from South America to the EU back in the mid-2000s, both opposing political forces are now informing contractors about their capabilities to perform these functions. In the current situation, Guinea-Bissau is called a drug State.

In Albania, the police forces are currently overloaded with solving logistical and blocking tasks. At the same time, March and April are the season for cannabis producers [4]. Since the police are dealing with priority tasks, criminal networks left unattended and counteracted have significantly increased the volume of supplies to EU countries.

The illegal trade in flora and fauna associated with the coronavirus has increased. Merchants promote rhino horn products as a unique cure for coronavirus. In Italy and in the United States, original counterfeit testing systems, medical beds and various kinds of ventilators can be purchased on DarkNet at speculative prices. These shops were opened by criminals from the Balkan countries and from Eastern Europe.

The information received from various countries of the world — from China and the USA, from Norway and India, from Italy and Japan - indicates that the cybercriminal, unlike traditional types of organized crime, reacted rapidly to the pandemic and uses the opportunities that have opened up.

A series of phishing attacks related to the coronavirus have begun and are multiplying. The number of fake websites [1] disguised as reliable sources is growing rapidly, including the World Health Organization, national medical

platforms, etc. Counterfeit medicines and medical equipment are advertised on these fake websites, as well as allegedly reliable wholesalers and retailers who can sell products on preferential grounds are indicated. Such a complex chain, which includes not only cybercrime, but also social engineering, exploits a combination of a shortage of protective equipment, medicines and medical equipment with panic moods characteristic of people.

In 2018, the US Government Accountability Office reported that 43% of medicines sold in legal pharmacies in the country are either counterfeit, counterfeit, or illegally imported into the country. It is safe to say that at present, in the context of a pandemic, this indicator is much higher.

3. Conclusion

The COVID-19 pandemic will be a turning point in a turbulently changing world. What is even more likely, the epidemic will attract attention for the first time and morally legitimize the so-called gray economy and gray markets.

The world is moving into an uncertain future. However, already today it is possible to identify some risks that will inevitably affect global, regional and country dynamics.

Almost all over the world, the risks of criminal penetration into the healthcare system are increasing, where huge financial and material resources are directed.

There are a number of political initiatives in the fight against OP and its intersection with the fight against the pandemic:

- to closely monitor the impact of the 'second-order' virus on security, especially where criminal organizations seek to make a profit, and to anticipate the possibility of using the pandemic to strengthen the positions and generate additional income of organized criminal groups;

- relying on active monitoring, if possible, move from a reactive to a proactive fight against crime: act as quickly as possible when operational units have received and recognized weak signals about the attempts of organized criminal groups to take control of vulnerable groups of the population, including drug users. Maximize the use of blocking in order to break the criminal markets of various directions. Do not forget about the desire of the organized criminal group to transfer activity from offline to online and make the most of such areas as extortion, fraud and introduction into law-abiding business;

- pay special attention to organized criminal groups [5; 6; 7] operating or seeking to operate in the field of healthcare, as well as trade in medicines and medical equipment. Publicly oppose attempts by criminal groups to create new markets related to the pandemic, such as the sale of counterfeit medicines, product advertising and many others.

References

1. Ulyanov M.V. (2021) Counteraction to crime in the field of information and communication technologies in the conditions of application of quarantine measures // National security. 2020. No. 2. p.54.
2. Larina E., Ovchinsky V.S. (2021) Crime and COVID-19 // Izborsky club. Moscow: 2020. 448 p.
3. Brief description of the state of crime in the Russian Federation for January-August 2020/ Official website of the Ministry of Internal Affairs of the Russian Federation.
4. Speculation on pandemics: how criminals use the Covid-19 crisis. European Union Agency for Law Enforcement Cooperation, 2020.
5. Shyla Divan, Vanessa Wells and Neil Vigdor (2020). Police act frivolously as pandemic spreads, New York Times, January 22, 2020. URL: <https://www.nytimes.com/2020/03/22/us/coronavirus-police.html>
6. Ricardo Moraes, Deborah Moreira and Rodrigo Veiga Guyer (2020). Gangs announce curfew as coronavirus hits Rio Favelas, Reuters, March 24, 2020, <https://www.reuters.com/article/us-health-coronavirus-brazilfavelas-fea/gangs-call-curfews-as-coronavirus-infects-Rio-favelas-IDUSKBN21B3EV>.
7. Stephen Dudley (2013). Gang Truce in El Salvador: Positives and Negatives, InSight Crime. URL: https://www.insightcrime.org/images/PDFs/2016/El_Salvador_Gang_Truce_Positives_and_Negatives.pdf.
8. James Cockayne (2016) Hidden Power: the Strategic Logic of Organized Crime / Hearst. URL: <https://www.hurstpublishers.com/book/hidden-power/>