SARA **L**aw **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N^{o}. 1 (2022), pp. 283-291

DIGITAL CRIMINALISATION AND MIGRANT SMUGGLING

I.-R. RUSU

Ioana-Raluca RUSU
Phd. Student - Police Academy "**Alexandru Ioan Cuza**", Bucharest, RO
E-mail: rusu.ioanaraluca@yahoo.co.uk
ORCID ID: https://orcid.org/0000-0003-3393-2069

Abstract

The present article focuses on deep diving into the following four main aspects: 1. Crime forms evolution versus societal developments
2. Distinctions between cybercriminals and criminals and associations related to digitalisation of crime
3. Software applications and tools enabling organized crime group members to commit various crimes, including migrant smuggling
4. Impact of technology on crime and possible developments.

Key words: *crime forms, cybercrime, cybercriminals, digitalisation, migrant smuggling.*

INTRODUCTION

This aim of this essay is to illustrate the strong interdependencies between crime forms, and in particular cybercrime and migrant smuggling, and the social implications of digitalization. While the digital evolution has given noteworthy benefits to society, it has also raised serious concerns about its bona fide use, especially by criminals.

The digital revolution (called recently as the fourth industrial revolution) *(Namli U, 2021, 1-22)*, which started around 1980 with the appearance of the Internet and after of other mobile devices, social networking, big data, and computing clouds, enabled the appearance of the so-called cybercriminals. From communication to manufacturing to how we live our lives, the digital revolution has changed everything. Some opinators consider that we're still in the early stage of the digital era, that has been ongoing for a few decades. As an increasing number of technological devices become interconnected, the full impact of the digital revolution will likely be felt in ways we can't even imagine.

Overall, it can be assumed that organised crime groups (OCGs) are continuously evolving and looking for adapted techniques which may facilitate criminal activities, eluding the vigilance of relevant law enforcement authorities.

1. CRIME FORMS EVOLUTION VERSUS SOCIETAL DEVELOPMENTS

This section deals with the review of the existing sources related to crime types and their evolution, providing a strong foundation for the subsequent analyses and interpretation of the results.

Since the middle of the 20th century, the advent of digital images and audio files led to the development of the digitization process, and the emergence and rapid spread of digital systems resulted in the development of social media, starting with the most well-known[2] that in a very short period of time have managed to connect hundreds of millions of people into billions of real and fake digital identities around the globe. The outcome is that people all over the world, be they students, office workers or business people, can now communicate online and at the same time write, take photos, read, broadcast and get information in real time, on the basis of which they take decisions.

This huge amount of data, the millions of interactions (texts, images, likes, comments, videos, etc.) hangs and is processed every second in the virtual space. All these human relationships, all these connections are made possible by the interaction of billions of terabits of digital information exchanged between digital systems. All these interactions, through the use of the digital network, lead to new ways of approaching human relations, to new ways of buying and transferring services, material or intellectual goods, of conducting various activities or businesses, of protecting an asset or a banking account, of possibly expressing the political opinion, etc.

Aside positive factors that influence social and political life, the development of a digital social environment also has a negative role through the impact created in the development of the underworld. The typology and main modi operandi of offences are continuously changing and the distinctive features of the criminal phenomenon will aim to adapt according to the social interactions of potential victims. It is rather obvious that in line with the new social developments, new ways in which people interact in the online environment, the establishment of new routines in the social life within a community, new crimes and new ways to counter crime will emerge, following the way in which the virtual environment is used to make various payments, the way the human community uses digital information. This tends to be more accurate for organized crime, involving groups with a hierarchical or organizational structure that will try to take advantage of legislative loopholes, by analyzing how they can minimize risks and always looking for new opportunities to maximize their illegal profits.

Various national and international entities with competences in the fight against serious and organized crime categorize crime forms slightly different.

Even if in practice a multitude of crimes can be encountered, based on criminal practice it has been possible to divide illegal acts into five large fundamental categories: „*crimes against a person, crimes against property, inchoate crimes, statutory crimes, and financial crimes*" *(Basit A, 2020, 263- 275).*

However, in this article we choose to elaborate more in detail two (see the highlighted words below) of the main ones described to fall under Eurojust's mandate: CBRN-E (chemical, biological, radiological and nuclear substances), core international crimes, crimes against children, cybercrime, drug trafficking, economic crimes, migrant smuggling, PIF crimes (crimes against the financial interests of the European Union), terrorism and trafficking in human beings *(Kemp Steven, Buil-Gil David, Moneva A, Miró-Llinares F, Díaz-Castańo N, 2021, 480-501).*

2. DISTINCTIONS BETWEEN CYBERCRIMINALS AND CRIMINALS AND ASSOCIATIONS RELATED TO DIGITALISATION OF CRIME

2.1 What is cybercrime?

Some internet security companies define cybercrime as the criminal activity that either targets or uses a computer, a computer network or a networked device.[5] Other noteworthy sources define it „*as the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy*"[6]**.** Europol recent reports *(Adhoob M, 2021, 273-275),* indicate that cybercrime is becoming more aggressive and confrontational. This can be seen across the various forms of cybercrime, including high-tech crimes, data breaches and sexual extortion.

2.2 Cybercriminals versus traditional criminals

If, normally, the criminal can be any person who has committed a criminal act or has been convicted for committing an illegal act, the cybercriminal is that person who, with the help of a digital tool, usually a computer, with the support of an information system, attacks the digital environment.

For increased efficiency, cybercriminals organize themselves in groups, having well-established roles such as: leaders who form the link with criminal organizations, cybercriminals who have specific technical knowledge (of software development, web development, hardware development), to maintain their own IT structures and which by using specialized algorithms create interfaces, spams and phishing schemes that help any person without advanced digital knowledge to easily access the software of an application, people with banking knowledge, haulers, etc. [8]

Obviously, the roles overlap, but the emergence of new challenges and the desire not to be caught, to be the best, transformed specialization within the criminal group an asset. When we talk about new challenges we refer to crackers, known to the general public as hackers. If initially the hacker (grey hat) did not intend for the activity carried out by him to have bad effects, nowadays the illegal hacker (black hat) has appeared, using his digital skills to identify weak points and infect IT network security systems with viruses.

The illegal hacker aims to gain various advantages by selling his services.

2.3 Does technology make criminal activities easier to commit and more difficult to detect?

While some experts suggest that criminals are generally backward in their choices of techniques and that the real pioneers in using things like communication technology are the police and other agencies of the state, others consider that many types of technological change can facilitate crimes by making detection more difficult and enabling multiple iterations in a shorter period of time. [9]

As it is well known, cybercriminals can carry out an illicit activity both offline (without using the computer) when we refer to leaders, transporters or other persons who practically facilitate or ensure the logistics of the criminal group or online when the crime is committed by connecting to the IT network or social media. In the latter case, the person who commits the crime, using the digital environment, is part of the group of black hat hackers because these people have the ability and are trained to adapt the illegal to daily habits, to the routine that is established within the social group being targeted. We can say that the digital environment influences the community by transforming economic, political, artistic, cultural, financial relations, etc. towards the emergence and support of a digital society. These transformations and connections between the relationships that appear in society also influence the field of crime, creating an interrelationship between the behaviors of social actors, and the connections that appear will influence, according to the principle of action and reaction, the activity within the society.

3. SOFTWARE APPLICATIONS AND TOOLS ENABLING ORGANIZED CRIME GROUP MEMBERS TO COMMIT VARIOUS CRIMES, INCLUDING MIGRANT SMUGGLING

Digital services and tools are more and more used in our daily lives and for a variety of criminal activities, including migrant smuggling. Migrant smugglers and document fraudsters use the benefits of anonymity, availability, and the variety of clients accessible through technology-enabled communication channels, allowing them to hide their real identities and to protect illegal activities from law enforcement eyes.

Particularly interesting for the current period is that the „*global health crisis seems to have triggered a pandemic digital crime, organized and unorganized*”[10].

Human society, as a whole, faced a new situation generated by the organized crime resulting from the lockdown and the restrictions, imposed by state governments, related to the socialization and movement of people in order to prevent and combat the Covid-19 pandemic. Thus, the organized crime networks moved into the virtual environment.

The Covid-19 pandemic has "affected every aspect of our lives"[11] and decisively influenced the life of human society, the way society uses and will use digitalisation. If the ban on the movement of people was initially a brake for organized crime organizations, the criminal impulse was generated by the virtual environment, by society's need to progress through the use of the Internet. European Union states face "ransomware attacks, known as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, but also online fraud related to digital identity"[12].

Moreover, „*online technologies and social interactions have played a key role in activities such as migrant smuggling, drug trafficking, and terrorism*”**[**13],[14].

In general, criminals tried to take advantage of the situation generated by the restrictions imposed during the Covid-19 pandemic in particular to „*raise prices (justifying this with the greater risks due to the pandemic), and increasingly did so by advertising their online services*”**[**15].

As regards drug trafficking, since meeting and travel bans have been an obstacle to the identification of new drug customers or distributors during the health crisis generated by the Covid-19 pandemic, we state without fail that online communication was the one primarly used between criminal groups [16].

Regarding migrant smuggling, a plethora of advertisements for facilitation services posted on social media confirm that criminal networks use applications like Instagram, Telegram, Facebook, WhatsApp, Viber, etc. to recruit people willing to take huge risks in order to reach their desired countries of destination.

JHA Agencies (Europol) and European Member states have taken steps to block encrypted communications of criminal networks, and more specifically Sky ECC communication service since March 2021[17].

Criminals from the Balkans obviously really trusted the application to be safe, so they exchanged messages on it as if they were ordinary phone messages. They allegedly paid several thousand euros to the Canadian company Sky Global for the coding of their application. However, the US Federal Bureau of Investigation (FBI) seized the site and arrested the company's management early 2021. The company's devices were *specially designed to prevent the police from actively monitoring the communication between members of transnational criminal organizations* according to the US indictment against the company's CEO.

The actions resulted in a large number of arrests, as well as numerous house searches and seizures in Belgium and the Netherlands. American and European services managed to crack the encrypted application Sky, after which, evidence of a series of crimes began to unfold. It is an application similar to Viber or WhatsApp, only users believed that it was protected. That is why they openly discussed almost all criminal acts via the application.

During 2021, another similar operation resulted with 800 criminals arrested in the biggest ever law enforcement operation against encrypted communication. The US Federal Bureau of Investigation (FBI), the Dutch National Police (Politie), and the Swedish Police Authority (Polisen), in cooperation with the US Drug Enforcement Administration (DEA) and 16 other countries have carried out with the support of Europol one of the most extensiv and sophisticated actions to combat criminal activity. With the help of a company that used devices to encrypt information, criminal organizations in more than 100 countries were targeted.[18].

4. IMPACT OF TECHNOLOGY ON CRIME AND POSSIBLE DEVELOPMENTS

Technological progress changes mindsets, improves technology, production processes and creates the conditions for human development, but at the same time it can create disruptions to social life by using new technological discoveries for illegal purposes. It is clear that the digital environment, cybernetics, the interaction between man and machine, has created the possibility for criminal organizations to lay the foundations for new criminal approaches, much more sophisticated and more difficult to prevent and combat by most law enforcement officers who do not have specialised training in this domain.

The offences of crime organizations cannot be contained in a single pattern, because even a simple crime of theft can hide the interest of the organized crime organization in committing illegal activities in the cyber field. Thus, the theft of a card, identity data or bank accounts can turn into a cybercrime and because of this the frontier between the psychic, physical and virtual dimensions of cybercrime is increasingly difficult to establish.

However, these revolutionary developments do not seem to trigger also the necessary criminological theoretical interpretive framework and to generate modern research hypotheses.

The research on how cyber as a whole influences the activity of the human community and especially criminal activities must focus on the interaction between the online environment and the offline environment because the impact on the criminal world is major.

In addition, studying the impact on the underworld networks could shed more light on the constantly changing modi operandi and help law enforcement authorities to take proportional measures.

Albeit outside the purpose of this paper, hybrid cybercrime and subsequently the hybrid warfare and its various connections, represent some of the topics that are expected to be recurrently addressed in the near future. This is mainly due to the Russian aggression in Ukraine and the instrumentalization of migrant smuggling, as seen at the European-Belarussian land borders.

BIBLIOGRAPHY

Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust);

Europol Regulation (Regulation (EU) 2016/794);

Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation;

References

Kemp Steven, Buil-Gil David, Moneva A, Miró-Llinares F, Díaz-Castańo N (2021) Empty Streets, busy Internet: a time-series analysis of cybercrime and fraud trends during COVID-19. Journal of Contemporary Criminal Justice; 37(4):480-501;

Sanchez G, Achilli L (2020) Stranded: the impacts of COVID-19 on irregular migration and migrant smuggling, Policy Briefs. Migration Policy Centre;

Basit A (2020) COVID-19: a challenge or opportunity for terrorist groups? Journal of Policing, Intelligence and Counter Terrorism; 15(3):263- 275;

Adhoob M (2021) Trafficking in persons. International Enforcement Law Reporter; 37(7):273-275;

Namli U (2021) Behavioural changes among street level drug trafficking organizations and the fluctuation in drug prices before and during the covid-19 pandemic. American Journal of Qualitative Research; 5(1):1-22;

Bibliographic sources on the internet

The Digital Revolution: A Historical Perspective - site https://tecroxy.com/digital-revolution, accessed on 29.10.2022;

Types of Criminal Offenses - site https://www.justia.com/criminal/offenses/, accessed on 29.10.2022;

Eurojust - Crime types - site https://www.eurojust.europa.eu/crime-types-and-cases/crime-types, accessed on 30.10.2022;

Kasperski - What is cybercrime? How to protect yourself from cybercrime - site https://www.kaspersky.com/resource-center/threats/what-iscybercrime, accessed on 30.10.2022;

Britannica - Cybercrime definition - site https://www.britannica.com/topic/cybercrime#ref235698, accessed on 30.10.2022;

Europol - Crime areas - Cybercrime - site https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime, accessed on 30.10.2022;

Expert Panel on Emerging Crimes: Hosted by the Department of Justice, Canada. In Ottawa, Ontario, Canada - How is crime changing in the 21st Century? - site https://www.justice.gc.ca/eng/rp-pr/csj-sjc/crime/rr03_20/p1.html (Date modified: 2022-08-17), accessed on 29.10.2022;

Cybercriminal - What Does Cybercriminal Mean? - site https://www.techopedia.com/definition/27435/cybercriminal, accessed on 31.10.2022;

Europol (2020) - How COVID-19-related crime infected Europe during 2020 - site https://www.europol.europa.eu/publicationsevents/publications/how-covid-19-related-crime-infected-europe-during-2020, accessed on 31.10.2022;

Europol (2021) - New major interventions to block encrypted communications of criminal networks - site https://www.europol.europa.eu/media-press/newsroom /news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks, accessed on 31.10.2022;

Europol (2021) - 800 criminals arrested in biggest ever law enforcement operation against encrypted communication - site https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-againstencrypted-communication, accessed on 01.11.2022;

https://link.springer.com/article/10.1007/s12117-022-09457-y, accessed on 01.11.2022.

Footnotes

The Digital Revolution: A Historical Perspective

Skype, YouTube, Facebook, Twitter, Instagram and other similar social media

Justitia - Types of Criminal Offenses

Eurojust - Crime types

Kaspersky - What is cybercrime? How to protect yourself from cybercrime

Britannica - Cybercrime definition

Europol - Crime areas - Cybercrime

Techopedia - Cybercriminal

Expert Panel on Emerging Crimes: Hosted by the Department of Justice, Canada. In Ottawa, Ontario, Canada

Andrea Di Nicola, Towards digital organized crime and digital sociology of organized crime, p. 14, published: 30 may 2022, Springer;

Kemp Steven, Buil-Gil David, Moneva A, Miró-Llinares F, Díaz-Castańo N (2021) Empty Streets, busy Internet: a time-series analysis of cybercrime and fraud trends during COVID-19. Journal of Contemporary Criminal Justice; 37(4):480-501;

Europol (2020) - How COVID-19-related crime infected Europe during 2020. European Union Agency for Law Enforcement Cooperation, The Hague;

Sanchez G, Achilli L (2020) Stranded: the impacts of COVID-19 on irregular migration and migrant smuggling, Policy Briefs. Migration Policy Centre;

Basit A (2020) COVID-19: a challenge or opportunity for terrorist groups? Journal of Policing, Intelligence and Counter Terrorism; 15(3):263- 275;

Adhoob M (2021) Trafficking in persons. International Enforcement Law Reporter; 37(7):273-275;

Namli U (2021) Behavioural changes among street level drug trafficking organizations and the fluctuation in drug prices before and during the covid-19 pandemic. American Journal of Qualitative Research; 5(1):1-22;

Europol (2021) - New major interventions to block encrypted communications of criminal networks;
Europol (2021) - 800 criminals arrested in biggest ever law enforcement operation against encrypted communication;