ASEJ
Scientific Journal
Bielsko-Biala School of Finance and Law

Volume 26 | Number 4 | December 2022

ISSN2543-9103
eISSN2543-411X
www.asej.eu

Bielsko-Biała

Bielsko-Biala School of Finance and Law
Wyższa Szkoła Finansów i Prawa w Bielsku-Białej

Scientific Journal

Zeszyty Naukowe

Academic Quarterly Publication
Vol 26, No 4 (2022)

Bielsko-Biala 2022

Scientific Journal of Bielsko-Biala School of Finance and Law
The Journal is published by Bielsko-Biala School of Finance and Law; ISSN 2543-9103, eISSN 2543-411X.

The Journal is a quarterly publication with the scoring of 70 assigned by the Polish Ministry of Education and Science, prompting quality scientific work with local and global impacts, conducting a peer-review evaluation process and providing immediate open access to its content. The publication features original research papers as well as review articles in all areas of science, with particular emphasis on social sciences (including Finance, Economics, Business, Law, Internal Security) and technical sciences (especially IT).

The Scientific Journal Office
Bielsko-Biala School of Finance and Law University Press
ul. Tańskiego 5, 43-382 Bielsko-Biała;
tel. +48 33 829 72 42, fax. +48 33 829 72 21; http://www.wsfip.edu.pl; http://asej.eu

ISSN 2543 – 9103 eISSN 2543-411X

December – 2022

Contents

Editorial Words

Dear esteemed readers,

It is my great pleasure to welcome you to the latest edition of ASEJ, the academic journal that brings you the latest research in the fields of law, economics, logistics, finance, psychology, criminology, computer science, and security. This issue features a diverse range of articles from leading experts in these fields, showcasing their latest research and insights into current trends and challenges.

As we continue to face unprecedented challenges and rapidly evolving technological advancements, it is more important than ever to stay up-to-date with the latest research and trends in these fields. This issue of ASEJ offers valuable insights and perspectives that are essential for anyone seeking to stay at the forefront of their respective disciplines.

We would like to take this opportunity to express our sincere gratitude to the authors for their hard work and contributions to the advancement of knowledge. We would also like to acknowledge the invaluable support of the Bielsko-Biala School of Finance and Law for their continued commitment to publishing this journal, which serves as a platform for the exchange of the latest knowledge and insights.

Virtual reality (VR) technology has been advancing at a rapid pace, and with its growth come a range of challenges in various fields, including economics, law, security, and computer science. In the realm of economics, one challenge is determining how to integrate VR technology into existing business models. VR has the potential to revolutionize the way companies conduct business, but it also requires significant investment and infrastructure to do so. Additionally, there are concerns about how VR will impact the job market, as it could potentially eliminate the need for certain types of jobs while creating new ones in the VR industry.

In this issue, we also explore the growing significance of virtual reality in law, economics, finance, and security. As VR technology continues to evolve, it presents both opportunities and challenges in these fields. For example, in economics, VR has the potential to revolutionize the way businesses operate, but it also requires significant investment and infrastructure. In law, the use of VR raises important questions around data protection, privacy, and intellectual property rights. In finance, VR can be used to enhance customer experiences and provide new insights into investment opportunities. In security, VR presents new risks and challenges, such as ensuring the safety of users and protecting sensitive data from cyber threats.

We hope that this issue of ASEJ will prove insightful and informative for our readers, and we look forward to your feedback and contributions in future editions.

Sincerely,

Dr Muhammad Jammal
Editor of the ASEJ, Issue 4, Volume 26, 2022

Cybercriminals and criminal structures in the world of organized crime

Wojciech Jakubiec[1]

[1] Bielsko-Biala School of Finance and Law
Poland

Abstract— **In the era of galloping globalization and the world of new information technologies, the vast majority of social life has developed. Unfortunately, along with the global progress of digitization, cybercrime has also developed. Traditional criminal organizations have taken a liking to cyberspace as a place not only to commit crimes, but also to exchange information or ordinary communication, which is more difficult to recognize by law enforcement than that conducted in the real world. The crime of the virtual world has also created a different type of crime, more individual, functioning in a specific network without special personal and hierarchical dependencies. The main determinants of this type of crime that create criminal networks seem to be, for example, illegal Internet markets where goods are exchanged or payments are made for legally prohibited services, or Internet forms where illegal correspondence is conducted. The aim of the article is to present the phenomenon of cybercrime and the structures in which cybercriminals operate and find themselves.**

Keywords— cybercrime, criminal structures, criminal networks, individual criminal, organized crime.

I. INTRODUCTION

Cyberspace is an evolving, dynamic complex system, regardless of the assumed technical, information or social values (Worona, WKP 2020). Cybercrime is a concept fully sanctioned in the Council of Europe Convention on Cybercrime (Council of Europe Convention on Cybercrime drawn up in Budapest on November 23, 2001, Journal of Laws 2015.728), which proves the extent of this type of crime and the threats it poses to the citizens of the signatory countries. It also confirms the supranational, cross-border dimension of this phenomenon and indicates the need to use international procedures to combat it (see Golonka, 2016). Thus, the administrative borders of countries are no obstacle for cybercriminals because they operate in the virtual world. When presenting the issue, it is impossible to omit the concept of cyber security. This is another term that has been included in a legal act of the rank of an act in the Polish legal system. According to this definition, it is the resistance of information systems to actions that violate the confidentiality, integrity, availability and authenticity of the processed data or related services offered by these systems (Act of July 5, 2018 on the national cybersecurity system, Journal of Laws of 2018, item 1560). Nevertheless, there is a view in the literature that cybercrime is a term that is as vague and questionable as the concept of organized crime. It refers to criminal activity related to IT infrastructure, namely the Internet (Finklea & Theohara, 2013). Cybercrime covers different types of criminal behaviour, namely attacks on the integrity and availability of information technology, which in turn can be used for various predatory crimes such as fraud, forgery, theft and extortion. Masiukiewicz draws attention to the online operation of the mafia, which is an example of organized crime to a very advanced degree. As a very accurate example, he points to sport - as a new crime sector. The presented procedure concerns totalizator sports bets carried out all over the world, which are controlled by criminal circles. It describes the criminal scheme in the way presented by Kurowski, which presents a model of criminal business. There are licensors of the idea and coordinators, there is a network of legal and criminal institutions, there is a relocation of various activities, there is a certain openness of the system - access via a boarding school, it is difficult to detect the procedure (and there is no reaction from international institutions) and a high leverage of value growth is created (Masiukiewicz, 2015). Cyberspace is also a market for all kinds of illegal goods, such as drugs or pirated movies (Finklea & Theohara, 2013) or child pornography. A distinction is commonly made between information technology-enabled crimes and information technology-enhanced crimes (Choo, 2008). It is worth noting that cyberspace is not only a virtual world limited to the Internet, but one can actually perceive the essence of cyberspace creating the concept of creating a kind of parallel environment, which is a new dimension for human activities (Wasilewski, 2013) as, for example, the dark side of the Internet referred to as called Darknet.

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 26, No 4 (2022), pages 4
https://doi.org/10.19192/wsfip.sj4.2022.6
Received: March 2022 Accepted: June 2022
Published: December 2022

II. CYBERCRIME IS A FORM OF INTERNATIONAL ORGANIZED CRIME

Addressing the issue of international organized crime will be incomplete without discussing cybercrime. Global computerization and increasingly easier access to IT workstations and other mobile devices have led to the emergence of new ways of conducting cross-border crime and created new criminal structures. Cybercrime, cyberterrorism, illegal use of information technologies are new areas of activity of organized crime (Wódka, 2015), which generate profits or legalize the obtained funds. It is impossible to share the position that cybercrime is exclusively a supranational phenomenon. Some crimes committed in cyberspace are limited to the national or even local level. With the development of the virtual network, new forms of crime appeared, and yes, in the literature you can find the well-known term cyberterrorism or stalking, although the latter term differs from organized crime. The term cyberterrorism can be understood as behaviors such as: those that undermine the foundations of the functioning of democratic states and societies, the security of international relations, the freedom of political choices in various countries, dismantling communication or energy transmission systems based on computer systems (Sobczak, 2019). It is impossible to omit a feature that requires special attention, namely the free crossing of the borders of this type of crime. One can go a step further and ask the question, does cybercrime have a limit? Certainly, the administrative border is not the border of the virtual world. More frontiers of cybercrime should be sought in less modern areas. The phenomenon of cybercrime should also be considered as organized crime appearing in specific structures and operating patterns. Is there a direction in today's world where organized crime is heading towards cyberspace, an area that seems to be a mirror of galloping globalization and computerization? This question can be answered by citing the example of the operation of the CarderPlanet internet forum in 2001-2004, whose basic function was an illegal marketplace for stolen data, and it was also a place where professional criminals met (see Woźnica, 2014). At the same time, it was a fully organized enterprise that gathered around itself the criminal environment. So, more than twenty years ago, there was a case where organized crime was beginning to emerge in cyberspace. Referring to cybercrime as an international organized crime, it is worth noting that cyberspace is considered attractive to criminals due to the perceived anonymity and virtually limitless nature of the Internet, enabling them to exploit the opportunities of crime in large geographical differences in relative safety before the intervention of law enforcement agencies (Finklea & Theohara, 2013). The virtual world has become an area of activity for individual criminals as well as organized criminal groups, extremist circles and terrorist organizations. The Internet is used to organize and carry out criminal activities, serving as a communication tool, marketplace, place of recruitment and provision of financial services (Safjański, 2016). In principle, it is easy to see the activities of international organized crime, which, however, does not contradict the activities of individual criminals in virtual reality. Organized crime, which is an internal dilemma for many countries, over time has become a painful side of globalization, because the globalization of economic systems and technological development in the field of transport and communication have not only created great opportunities for global economic development and mutual communication, but also contributed to the creation of new favorable circumstances for the development of international crime (Wątorek, 2017). Crimes committed by members of international criminal groups mainly include: corruption, money laundering, counterfeiting, property crimes, human trafficking, environmental crimes, drug crimes, and cybercrime (Wódka, 2015), it is worth noting that yes, it's a closed directory. In the past, cybercrime was considered to be the domain of technically highly skilled criminals, but the "deskilling process" (McGuire, 2012) has been observed, where any person, even with not very high knowledge, can commit a crime, and knowledge in the field of computer science has become generally available.

III. STRUCTURES OF ORGANIZED CRIME IN CYBERSPACE

Cybercrime is not necessarily organized in the sense that it involves the cooperation of several criminals. Among the members of criminal organizations there may be various forms of cooperation or mutual dependence, e.g., loose contacts or knots. Some criminal structures use information technology to support criminal enterprises, others use information technology, namely digital encryption, for internal communication. Finally, an important distinction must be made between criminal structures that arise in real life and those criminal structures that emerge in cyberspace involving people who may never have met face to face in the real world. There has been debate about what existing criminal organizations have moved to in cybercrime and to what extent criminal structures in cyberspace resemble criminal structures in the real world. Much of this debate is highly speculative and suffers from conceptual confusion (McCusker, 2006). Entrepreneurial criminal structures can exist in the form of markets, networks or organizations (illegal companies). Illegal companies operating in cyberspace, as far as is known, usually exist in the form of individual entrepreneurs, partnerships and small groups, with a low degree of vertical and horizontal integration (Holt, 2013), which is not the same as the statutory concept of a criminal group. Perhaps there are no major differences between the real and virtual world in this regard. Zirpinis presented an interesting view on crime involving entrepreneurs, which can be compared to the structures found in cyberspace. The broadly understood corporate crime includes many of its manifestations, corresponding to various juridical forms. Within its transitional scope, there are mainly those that consist in violating the rules (prohibitions and orders) in force in the operation of enterprises. It also covers various types of crimes for which the company is only a cover or a means to commit them. While the former belongs to understood economic crime, the latter derive from traditional crime, most often economic (e.g., fraud) or other forms of it (e.g., espionage, drug trafficking, etc.). Relatively widespread manifestations of crime of enterprises of the second category in Western European

countries are the so-called fraud companies (Schwindelfirmen) and so-called masking companies (Tarnfirmen), whose traces we come across in our reality. The name of a fraud company, in a broad sense, refers to all undertakings consisting of in systematically offering little or completely worthless services under the pretext that they will bring significant benefits at moderate prices, while using dishonest means to lead the contractor to an unfavorable his economic decision. More narrowly understood, it means such companies whose existence, and usually the very creation, is based on fraudulent machinations. Their activities are so saturated with criminal economic machinations that switching to a legitimate business would spell their downfall. Masking companies hide their ultimate goal - illegal activity under the guise of a legitimate business enterprise of any industry. For their owners or shareholders, the economic effects of legal activity do not matter and they try to fulfill all obligations arising from it scrupulously. This feigned existence of the company is financed from illegal and lavish sources, such as drug, arms, human beings or espionage (Zirpinis, 1959). The main differences between cyberspace and the real world in relation to criminal organizations are the way in which these individual criminals and criminal groups are related to each other and what interdependencies exist between them. In the real world, individuals and smaller organizational units are usually embedded in larger criminal networks that use ties, in which the cooperating criminals are related to each other by various types of more or less loose ties (Kędzierski, 2014). In cyberspace, markets seem to be the dominant coordinating mechanism. This is particularly the case in the core area of cybercrime where vulnerabilities in IT infrastructure are exploited for profit (Holt, 2013; Holt & Lampke, 2010).

IV. The involvement of cybercriminals in international organized crime

Cybercriminals do not have to cooperate with trusted accomplices in committing crimes, they do not have to know each other at all, and they do not even need to know their geographical location. Criminals specialized in a specific field offer their products or services to virtually anyone who decides to pay the requested amount. A common payment method is peer-to-peer, and it is not uncommon for payments to be made using virtual currencies. Such a payment system makes it much more difficult to track the funds transferred. Internet forums and portals perform not only economic functions but also act as platforms for the exchange of illegal goods and services. They also perform important non-economic, social functions, such as communication and exchange of views. Internet portals are a key mechanism through which criminal associations develop in cyberspace. Association criminal structures facilitate contacts between criminals; they confer status, reinforce deviant values, and are an arena for the exchange of information relevant to criminal law. In online discussions, feedback posts or forum-based rating systems, users of online forums collectively establish and reinforce subcultural norms and values that determine how cybercriminals in general or in specific areas of crime should behave (Holt et al., 2010), including also in case of contact with law enforcement authorities. For example, forums for exchanging stolen bank details emphasize things like timely delivery and quick response to customer complaints (Holt & Lampke, 2010). An indispensable advantage that accompanies online forums is anonymity, which is much more difficult in the real world. More and more often there is a position that the entry of traditional organized crime groups into cyberspace, in accordance with the often put forward claim, there is a tendency for more and more frequent use of cyberspace by conventional criminal groups. An appropriate example here will be, for example, the money laundering procedure, where you can perform financial operations practically anywhere in the world, having only an IT workstation with access to the Internet.

V. Conclusion

The degree of organization of cybercriminals seems to be rather low, the development of criminal networking can be observed much more (Kędzierski, 2014). Today's IT solutions make it possible for individuals to cooperate with each other to an extent that has never been possible before in history (Sztokfisz, 2018). Individual criminals and minimalist criminal groups, specialized in providing a specific good, tool or service, respectively, contribute to complex criminal patterns without belonging to overarching criminal organizations. There is no personal hierarchy among them. Instead, participants interact as partners in market transactions with online forums serving as virtual marketplaces for illicit ventures, sometimes referred to as the "black market" (see Brol, 2018). Virtual marketplaces created outside the law enable a wide range of criminals to commit crimes, even if they do not have sophisticated technical skills, increasingly less computer skills are enough. This is a potential gateway for conventional criminals, who may not be technically skilled and may be against the use of technology, which may prove too difficult a tool for them. However, the virtual world offers crime education, you just need to get to the right places. Illegal Internet forms offer a number of instructions not only on how to commit crimes but also on how to avoid criminal liability and remain anonymous.

VI. References

Brol,(2018) "Black Market Exchange in the Digital Age", "Economics of the 21st Century",

Chao (2008) "Organized crime groups in cyberspace: A typology: Trends in Organized Crime", 11(3),

Golonka (2016) "Cybercrime - international standards of combating the phenomenon and Polish criminal regulations", "Legal studies: dissertations and materials",

Kędzierski, (2014)"The network nature of contemporary criminal organizations operating in the area of organized crime and terrorism", "Review of Internal Security 10/14".

The Council of Europe Convention on Cybercrime, drawn up in Budapest on November 23, 2001, Journal U.2015.728.

Holt (2013) “Exploring the social organization and structure of stolen data markets. Global Crime”, 14 (2-3),

Holt, Blevins, & Burkert. (2010)“Considering the pedophile subculture online. Sexual Abuse”, 22(1)

Finkle & Theohara (2013). “Cybercrime: Conceptual issues for Congress and US law enforcement. Washington, DC: Congressional Research Service,

McCusker (2006). “Transnational organized cyber crime: Distinguishing threat from reality. Crime”, “Law and Social Change”, 46 (4)

McGuire (2012). “Organized crime in the digital age. London, England: John Grieve Center for Policing and Security

Safjański, (2016) "Tactical and forensic aspects of the operation of the European Center for Combating Cybercrime", "Police Review"

Sobczak, (2019) "Crime in cyberspace between Polish and international regulations", "Cybersecurity and Law"

Sztokfisz (2018) , "Peer to peer markets as a contemporary manifestation of economic freedom", "Scientific Journals of the University of Economics in Katowice

Act of July 5, 2018 on the national cybersecurity system, Journal Laws of 2018, item 1560.

Wasilewski, (2013) "Definition Outline of Cyberspace", "Homeland Security Review

Wątorek, (2017) "Selected areas of the asymmetric threat of cross-border organized crime", "Yearbook of International Security"

Woźnica,(2014) "CarderPlanet - pioneers of organized cybercrime", "Kultura i Polityka"

Wódka,(2015) "International organized crime - typology, characteristics and combating", "On security and defence".

Zirpinis,(1994) “Scwindelfirmen und anderen (unlauteren) kriminallen Unternehmen des Wirtschaftslebens, Wiesbaden 1959, p. 28, op. O. Górniok, "Economic Crime and Combating it", Warsaw

WSFiP conducts research and educates students in the following fields:

Finance and Accounting
- Treasure Administration
- Banking
- Corporate Finance
- Accountancy
- Accounting and Finance in Public Sector Institutions
- Corporate Accounting and Controlling
- Audit
- Management and Finance in Real Estate

Law
- this program gives strong legal foundations to undertake further professional training for judges, prosecutors, atorneys, notaries, bailiffs.

Administration
- Fiscal Administration
- Local Government Administration

Logistics
- this program gives good preparation for work in logistics companies as well as in other economic and administrative units.

Cyberspace and Social Communication
- Communication and Image Creations
- Safety in the Cyberspace

Internal Security
- Administration and Management in Security
- Security and Public Order
- Security and Development in Euro-region
- Security of Information and Information Systems
- Security in Business
- Criminology and Investigative Studies
- Criminology and Forensics
- Protection of People and Property
- Public Order Agencies

Information Technology
- Databases and Net Systems
- Computer Graphics and Multimedia Techniques
- Design of Applications for Mobile Devices
- IT Services in Public Administration Units

Postgraduate courses
- Administrative studies
- Fiscal Administration
- Law and management in health service