DR. BALÁZS GÁTI[1]

Possible links between digitalization, cybercrime, and the COVID-19 pandemic

Abstract

The research aims to provide insight into relationship between COVID 19 pandemic, digitalization and cybercrime with special attention to their interconnection points and interactions. Currently, the COVID 19 pandemic is present in more than 200 countries around the world. This has an impact on social and economic life as well as on people's privacy. As part of the fight against the coronary virus epidemic, governments have been forced to lockdown, which has changed the socio – economic environment in which the digital revolution has already played a major role. All of these changes have obviously led to a further increase in digitalization, in which not only the working conditions have been changed, but it has also plaid a significant role in the fight against the pandemic.

The COVID-19 pandemic also caused changes in the modes of crimes, the perpetrators react very quickly, the number of acts committed in cyberspace has increased significantly. In this paper we present the main types of offenses as well. In the fight against cybercrime, the digitalization plays even more significant role, by combining Internet of Things (IoT) with Blockchain, enterprise and individual users, what can create a reliable, secure network that protects data from attackers.

Introduction

Digitalization in the 21st century interweaves all areas of society, so there is no economic and legal area that would not be affected.[2] This is often referred to as the Fourth Industrial Revolution.[3] According to Schwab "*The Third used electronics and information technology to automate production. Now a Fourth Industrial Revolution is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.*" Let's think to technologies like artificial intelligence, robotics, the Internet of Things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, materials science, energy storage, and quantum computing. Digital solutions help create jobs, advance education, boost competitiveness and innovation and can improve the lives of citizens. Among others, digital technology has a key role to play in transforming the economy and society.[4]

The last major pandemic was the Spanish flu[5] that erupted exactly a hundred years ago. Restrictions caused by the coronary virus that caused the pandemic in 2020 -scientifically known as COVID-19[6]- accelerated the digital switchover, which had to take place in a very short time in many areas, such as education, a significant part of jobs, and the entertainment industry. Digitalization is an essential component of the EU's response to the economic crisis caused by COVID-19. As such, the COVID-19 pandemic has made the need to accelerate the digital transition in Europe more pressing.[7]

"[...] estimation of these effects assumes that there was a digital transformation already underway, be-

[1] PhD Student, University of Pécs, Faculty of Law, Criminology and Penal Execution Law Department.

[2] Dávid Tóth, Digitalization trends in the Hungarian Criminal Procedure. In: Belaj, Ivan; Vajda, Halak Željka; Slobodan, Stojanović (szerk.) 10. Međunarodna Konferencija Razvoj Javne Uprave.

[3] Klaus Schwab, *The Fourth Industrial Revolution: What it Means, how to Respond.* (WEF, 2016,)www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond. Accessed 15.01.2021.

[4] Balázs Gáti ," Major legal and economic aspects of digitalization in the EU with special attention to recent developments on data protection " In*: Szilovics, Csaba; Bujtár, Zsolt; Ferencz, Barnabás; Breszkovics, Botond; Szívós, Alexander Roland (szerk.) Gazdaság és pénzügyek a 21. Században ii. – konferenciakötet = Business and economy in the 21st century II.. – Conference proceedings* Pécs, Magyarország , (Pécsi Tudományegyetem, Állam- és Jogtudományi Kar 2020) 207 p. pp. 139–154. , 16 p.

[5] "Influensa, FLU", Centeres for Deseases (CDC), https://www.cdc.gov/flu/pandemic-resources/1918-commemoration/1918-pandemic-history.htm, Accessed 15.01.2021.

[6] "Coronavirus disease (COVID-19)", WHO, pandemic, https://www.who.int/emergencies/diseases/novel-coronavirus-2019, Accessed 15.01.2021

[7] "A digital future for Europe " Council of the European Union, https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe Accessed 15.01.2021.

fore the pandemic set in, and it will take certain forms owing to the impact of the lockdowns."[8]

Criminals have quickly seized the opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities. Organized crime groups[9] are notoriously flexible and adaptable and their capacity to exploit this crisis means we need to be constantly vigilant and prepared.[10] The higher number of users has also significantly increased the number of potential victims.[11]

The aim of the article is to present the effects of COVID-19 on both digitization and cybercrime, as well as their interactions and criminological aspects, and the main types of treats committed in cyberspace.[12]

Digitalization and the Covid-19 pandemic

The WHO data stream is currently affected by the COVID-19 pandemic in 223 countries and the number of confirmed cases 107 423 526.[13]

Governments around the world restricted movement of people, using social distancing and lockdowns, to help stem the global coronavirus (COVID-19) pandemic.

The lockdowns across countries have entailed a rise in the use of information systems and networks, with massive changes in usage patterns and usage behavior. Employees are adjusting to new norms – with meetings going completely online, office work shifting to the home, with new emerging patterns of work.

These changes have come across most organizations, whether in business, society, or government.

All these changes have fundamentally changed both business and the digital economy, education, and our daily lives using digital technologies. The data below show a further rapid growth of the digital transformation, while we are already living in an era of the digital revolution.

Internet services have seen rises in usage from 40% to 100%, compared to pre-lockdown levels. Video-conferencing services like Zoom have seen a ten-times increase in usage, and content delivery services like Akamai have seen a 30% increase in content usage.[14]

Along with synchronous modes of teaching, video conferencing platforms like Zoom and Google Meet, the synchronous platforms like edX and Coursera have also seen an increase in enrolments. The use of video- and audio-conferencing tools increases significantly, organizations ramps up their technology infrastructure. This leads to increased investment in bandwidth expansion, network equipment, and software that leverages cloud services.[15]

Digital transformation technologies such as Cloud, Internet-of-Things (IoT), Blockchain (BC), Artificial Intelligence (AI), and Machine Learning (ML), constitute a bulk of the of what is being adopted by organizations as part of their transformation effort.

Blockchain (BC) technology presents an opportunity to create secure and trusted information control mechanisms.[16]

Based on a 2020 survey of OECD, since the start of the COVID-19 crisis, demand for broadband communication services has soared, with some operators experiencing as much as a 60% increase in Internet traffic compared to before the crisis, and the COVID-19 crisis also placed an unprecedented demand on communications networks.

"*The underlying Internet infrastructure is also facing unprecedented demands. One critical element of this infrastructure are IXPs, which are bulk traffic exchange crossroads where multiple networks connect (to exchange traffic). IXPs report record net increases of up to 60% in total bandwidth handled per country from December to March 2020.*[17]

According to measurements by the Deutscher Commercial Internet Exchange in Frankfurt, the world's total Internet traffic peaked at 9.1 terabits per second in the spring (the previous record was 8.3 terabits).[18]

The Cable.co.uk analyzed data from the Oxford Coronavirus Government Response Tracker (Ox-

[8] De' R, Pandey N, Pal A., "Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice" *Int J Inf Manage.*(2020 Dec) 55 .

[9] Dávid Tóth, István László Gál, László Kőhalmi, Organized Crime in Hungary JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW 2 : 1 pp. 23-25. , 6 p. (2015).

[10] László Kőhalmi, "Some issues of criminal liability by reason of economic decisions" *Journal of Eastern-European Criminal Law* (6 : 1 , 2019) ,pp. 44-52. , 9 p.

[11] "Catching the Virus Cybercrime, Disinformation and the COVID-19 Pandemic". Europol, www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic, Accessed 15.01.2021.

[12] László Kőhalmi, Jogállam és büntetőjog – avagy kételyeim az ezredforduló kriminálpolitikája körül. In Krisztina Karsai (szerk.): Keresztmetszet: tanulmányok fiatal büntetőjogászok tollából. Pólay Elemér Alapítvány, Szeged. pp. 128–129. 17p. (2005).

[13] "Coronavirus disease (COVID-19) pandemic" WHO,https://www.who.int/emergencies/diseases/novel-coronavirus-2019, Accessed: 11.02.2021.

[14] Mary Branscombe, *The New Stack; 2020. The network impact of the global COVID-19 pandemic.*https://thenewstack.io/the-network-impact-of-the-global-covid-19-pandemic/ Accessed: 05.01.2021.

[15] Shah D. Class Central's MOOC Report; 2020. MOOC Watch 23: *Pandemic brings MOOCs back in the spotlight – Class central.* https://www.classcentral.com/report/moocwatch-23-moocs-back-in-the-spotlight/ Accessed: 05.01.2021.

[16] Nitin Upadhyay, "Demystifying blockchain: A critical analysis of challenges, applications and opportunities. "*International Journal of Information Management.*(2020) 54, Accessed: 06.01.2021.

[17] "OECD Policy Responses to Coronavirus (COVID-19), Keeping the Internet up and running in times of crisis". OECD, https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/ Accessed: 05.01.2021.

[18] Johannes Wiggen, *The Impact of COVID-19 on Cyber Crime and State-Sponsored Cyber Activities*, (Berlin, Konrad Adenauer Stiftung, 2019) 2.

CGRT), and over 364 million broadband speed tests courtesy of M-Lab to compare average internet speeds in 114 countries during and outside of their most stringent COVID-19 lockdown periods. According to his research, the average speed of the Internet fell by 6.31% worldwide, but with an uneven distribution: while in China the decline was 50%. The Cable annual global broadband speed tracker has demonstrated global increases of around 20% year-on-year since 2017.[19]

This study also supports the association with increased data traffic caused by the COVID-19 epidemic.

Digital Marketing Trends in Ecommerce – the new face of digital marketing

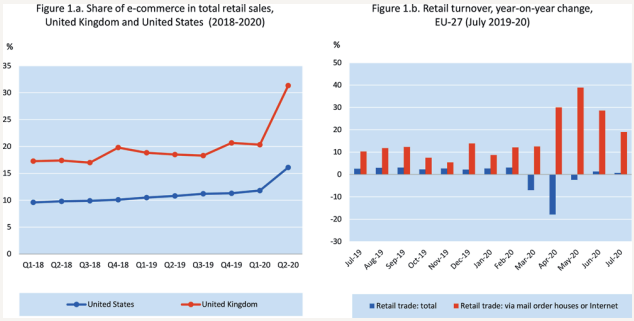
The COVID-19 pandemic has undoubtedly had a significant effect on digital marketing trends this year. Its full impact is yet to be seen, but businesses have been forced to adapt to the changing circumstances on a weekly or even daily basis.

The SEMrush study has collected and analyzed recent data from over 2,000 of the world's most visited ecommerce websites across multiple categories, including Fashion, Consumer Electronics and Health and Beauty, to determine what the new face of digital marketing looks like. The analysis revealed that shifts in the ecommerce landscape and consumer shopping patterns had already arrived: Monthly "buy online" searches almost doubled in the first month of the pandemic: there were 27,500+ searches in March 2020 vs. 14,800+ in February 2020 across all categories. Looking at the overall year-on-year (YoY) trend for June (2019 vs. 2020), these searches rose globally by 50%. Worldwide searches for food delivery services increased by an average of 180%. The average YoY traffic growth for ecommerce sites in the first half of 2020 was around 30%. Ecommerce sales have already been growing at unprecedented rates. In 2020, e-Marketer forecasts a collective $3.914 trillion in ecommerce sales.[20]

OECD studies include the following key messages. The COVID-19 crisis accelerated an expansion of e-commerce towards new firms, customers, and types of products. Despite persistent cross-country differences, the COVID-19 crisis has enhanced dynamism in the e-commerce landscape across countries and has expanded the scope of e-commerce, including through new firms, consumer segments (e.g. elderly) and products (e.g. groceries).[21]

In the EU-27, retail sales via mail order houses or the Internet in April 2020 increased by 30% compared to April 2019, while total retail sales diminished by 17.9% .The resulting shifts from brick-and-mortar retail to e-commerce are likely significant across countries.

Figure 1. The COVID-19 crisis has increased the share of e-commerce in total retail



Source: OECD's elaboration based on data from the US Census Bureau, the Office for National Statistics in the United Kingdom and Eurostat.

While official statistics are not available for most other countries, estimates suggest that online orders were up across several regions during the first half of 2020, including Europe, North America, and Asia-Pacific (OECD, 2020). For Asian-Pacific countries, e-commerce had already increased significantly during the first quarter of 2020, while the increase occurred later in Europe and North America, namely after several OECD countries followed Italy's example and introduced confinement measures within a short period of time of each other.[22]

According to the McKinsey study the shift to digital persists across countries and categories as consumers in most parts of the world keep low out-of-home engagement. Food and household categories have seen an average of over 30 percent growth in online customer base across countries. Online growth for China seems more moderate, as the country had a high level of online penetration prior to the pandemic.[23]

Studies draw attention to the fact that, although individual e-commerce changes do not affect individual countries and certain sectors of the commer-

[19] "How global broadband speeds changed during COVID-19 lockdown periods" Cable.co.uk. https://www.cable.co.uk/broadband/speed/broadband-speeds-covid-19-lockdown/ Accessed: 05.01.2020

[20] "Digital Marketing Trends in Ecommerce https://www.semrush.com/blog/2020-digital-marketing-trends-in-ecommerce " SEMRUSH, 2020 Accessed: 05.01.2021

[21] "E-commerce in the time of COVID-19," 7 October 2020, OECD, http://www.oecd.org/coronavirus/policy-responses/e-commerce-in-the-time-of-covid-19-3a2b78e8/#endnotea0z2 Accessed: 05.01.2021.

[22] "Connecting businesses and consumers during COVID-19: trade in parcels", OECD Policy Responses to Coronavirus (COVID-19), OECD (2020), http://www.oecd.org/coronavirus/policy-responses/connecting-businesses-and-consumers-during-covid-19-trade-in-parcels-d18de131/. Accessed: 06.01.2021.

[23] "Consumer sentiment and behavior continue to reflect the uncertainty of the COVID-19 crisis" October 26, 2020 | Mckinsey Company, Article https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/a-global-view-of-how-consumer-behavior-is-changing-amid-covid-19# Accessed: 06.01.2020.

cial sector in the same way,[24] but the changes will be long-term. Accordingly, decision makers need to ensure that e-commerce is accessible to all, and better than ever. This will continue to drive digitalization and the growth of the digital economy, affecting not only large companies but also small businesses.[25,26].

Digitalization in the fight the pandemic

Digitalization has a significant role to play, even in the fight against pandemics, even in the areas already mentioned, which are the survival of economic life, education, and everyday life.

However, it plays a significant role in both direct protection[27] and health services[28].

The European Commission has been working to coordinate, complement and initiate measures to deal with every aspect of the coronavirus pandemic, and digital, media and telecoms play a vital role. The further improvements proposed by the EU [29] are:

- *Data, artificial intelligence and supercomputers*: Data, artificial intelligence (AI) and supercomputers are a major asset in detecting patterns in the spread of the virus, developing potential treatments and devising strategies for reconstruction.
- *Telecommunications, networks and connectivity*: Telecommunications, networks and connectivity are more vital than ever, with so much of our society confined to their homes and economy dependent on them.
- *Online platforms and disinformation*: Online platforms are important sources of information and activity. But above all, in times of crisis, they are a vital information channel.
- *Skills, collaborative working and creativity*: Digital networks provide platforms offering a wealth of information and learning, from skill sharing and collaborative working to accessing culture and creativity online
- *Cybersecurity, trust and safety online*: The networks are secure from attacks and we need to be sure that we as individuals are safe when online.

Blockchain for COVID-19

The sudden development of theCOVID-19 pandemic has exposed the limitations in modern healthcare systems to handle public health emergencies. It is evident that adopting innovative technologies such as blockchain can help in effective planning operations and resource deployments.

Blockchain technology can play an important role in the healthcare sector, such as improved clinical trial data management by reducing delays in regulatory approvals, and streamline the communication between diverse stakeholders of the supply chain, etc. Moreover, the spread of misinformation has intensely increased during the outbreak, and existing platforms lack the ability to validate the authenticity of data, leading to public panic and irrational behavior. Thus, developing a blockchain-based tracking system is important to ensure that the information received by the public and government agencies is reliable and trustworthy.[30, 31, 32]

Blockchain technology has several potential use cases that can help tackle the current pandemic crisis. It can be used to simplify the clinical trial processes for vaccines and drugs, raise public aware-

[24] "Covid 19 and e-commerce" UNCTAD, https://unctad.org/system/files/officialdocument/dtlstictinf2020d1_en.pdf, Accessed: 06.01.2021.

[25] " COVID-19 will permanently change e-commerce in Denmark" Deloite, https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/strategy/e-commerce-covid-19-onepage.pdf, Accessed: 06.01.2020.

[26] NEWS Europe, „The impact of Covid-19 on ecommerce" , E-commerce https://ecommercenews.eu/the-impact-of-covid-19-on-ecommerce/ Accessed: 06.01.2021.

[27] „ In the wake of the coronavirus crisis, the European Commission's Digital Strategy gains renewed importance as digital tools are used to: monitor the spread of the coronavirus, research and develop diagnostics, treatments and vaccines ensure that Europeans can stay connected and safe online. National contact tracing and warning apps can be voluntarily installed and used to warn users, even across borders, if they have been in the proximity of a person who is reported to have been tested positive for coronavirus. In the case of an alert, the app may provide relevant information from health authorities, such as advice to get tested or to self-isolate, and who to contact." European Commission, Digital solutions during the pandemic, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/digital-solutions-during-pandemic_en, Accessed: 06.01.2021.

[28] „Three powerful European supercomputing centres are engaged in studying and developing vaccines, treatments and diagnoses for the coronavirus. By comparing digital models of the coronavirus' proteins and matching them against a database of thousands of existing drugs, the aim is to discover which combinations of active molecules react to the virus. The supercomputers complement the classic trial and error clinical approach. A pharmaceutical company and several large biological and biochemical institutes participate by providing access to their databases of drugs. The Exscalate-4CoV project, supported by €3 million in EU funding, is conducting research using an EU-backed supercomputing platform to check the potential impact of known molecules against the structure of the coronavirus." "Using European supercomputing to treat the coronavirus" European Commission,https://ec.europa.eu/digital-single-market/en/news/using-european-supercomputing-treat-coronavirus, Accessed: 06.01.2021.

[29] "Digital technologies - actions in response to coronavirus pandemic" European Commission, https://ec.europa.eu/digital-single-market/en/content/digital-technologies-actions-response-coronavirus-pandemic, Accessed: 06.01.2021.

[30] Dounia Marbouh ,Tayaba Abbasi, Fatema Maasmi, at al.,"Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System" *Arab J Sci Eng* , (2020) 45, 9895–9911.

[31] "tracking valid data is vital to monitor the progress of the pandemic. Tech giants, researchers, and healthcare officials started using contact-tracing mobile apps that use Bluetooth-based proximity tracing or geolocation tracking functionality to help track COVID-19 cases". Paul Bischoff, "COVID-19 App Tracker: Is privacy being sacrificed in a bid to combat the virus?" CompariTech, 20 April 2020, https://www.comparitech.com/blog/vpn-privacy/coronavirus-apps/

[32] Kelsey Warner , Shireena Al Nowais, "Coronavirus: Doctors urge public to help track COVID-19 cases with tracing app. The National" 28 April 2020. https://www.thenational.ae/uae/health/coronavirus-doctors-urge-public-to-help-track-covid-19-cases-with-tracing-app-1.1012267.

ness, transparently track donations and fundraising activities, and act as a reliable data tracker.[33,34]

The COVID-19 pandemic and crime

The impact of a coronavirus epidemic on crime has special characteristics. Traditional forms of crime have been pushed into the background, and most of the acts have been transferred to the online space. However, the potential for organized crime has increased.[35]

Most governments around the world restricted the movement of people through some combination of social distancing and lockdown, as part of efforts to tackle the coronavirus pandemic. This produced a range of unintended consequences, including upon crime.

Several researchers have made initial examinations into how crime rates have fluctuated in the advent of COVID-19.

One of the earliest studies was by Shayegh and Malpede[36] which identified an overall drop in crime in San Francisco of 43% and Oakland of about 50% following city issuance of some of the most restrictive and early stay-at-home orders in the US, beginning March 16th, 2020 and the two weeks after.

Gerell, Kardell, and Kindgren [37] examined crime during the five weeks after government restrictions on activities began, observing an 8.8% total drop in reported crime despite the country's somewhat lax response – when compared to other countries' policies on restricting the public's movement. Specifically, the researchers found residential burglary fell by 23%, commercial burglary declined 12.7%, and instances of pickpocketing were reduced by a staggering 61% – however, there was little change in robberies or narcotics crime.

Halford[38] et al. examine crime eects for one UK police force area in comparison to 5-year averages. There is variation in the onset of change by crime type, some declining from the WHO 'global pandemic' announcement of 11 March, others later. By 1 week after the 23 March lockdown, all recorded crime has declined by 41%, with the following variations: shoplifting (↓62%), theft (↓52%), domestic abuse (↓45%), theft from vehicle (↓43%), assault (↓36%), burglary dwelling (↓25%) and burglary non-dwelling (↓25%).

István László Gál[39,40] reaches a similar conclusion regarding COVID-19 and crime rates in Hungary.

Stickle and Fergus argue that the single most salient aspect of the steep fall in crime rates during the COVID-19 pandemic are the legal stay-at-home orders (i.e., lock-down, shelter-in-place) implemented to slow the spread of the virus by promoting social distancing.[41]

Cause of decrease: Lockdowns have changed everyday life, which caused the absence of the three offender conditions: a motivated perpetrator, a lack of the right target, and the right protection.[42]

A special area of crime is organized crime, the analysis of which goes beyond the scope of this article.[43] However, it should be mentioned that during the COVID-19 pandemic, certain conditions were met that facilitated this.

„While the COVID-19 pandemic is first and foremost a global public health crisis, it has also proven to have a significant and potentially long-lasting impact on the serious and organized crime and terrorism landscape.. [...]"[44]

The short-term impact of the COVID-19 pandemic and the consequent lockdown measures imposed across the EU manifested over the course of 2020. The mid- to long term impact of the situation on society, economy and political discourse is becoming apparent and points to significant economic strain on a European and global level during and in the aftermath of a prolonged pandemic. Some countries

[33] Mehdi Benchoufi ,Philippe Ravaud ,"Blockchain technology for improving clinical research quality *"BioMed Central* , (2017) 18, 1–5.

[34] Chang, M.C,Park, " How can blockchain help people in the event of pandemics such as the COVID-19? "*J. Med. Syst.* (2020) 44 ,102.

[35] Dornfeld László, "A koronavírus-járvány hatása a kiberbűnözésre" *In medias res: Folyóirat a sajtószabadságról* és *a médiaszabályozásról,* (2020) ,v9 : 4 p. 193.

[36] Soheil Shayegh ,Maurizio Malpede, "Staying home saves lives, really! 2020. Staying Home Saves Lives, Really!" scholar.google.com/scholar_lookup?title=Staying+home+saves+lives,+really!&author=S+Shayegh&author=M+Malpede&publication_year=2020&, Accessed: 06.01.2021.

[37] Manne Gerell , Johan Kardell , Johanna Kindgren, " Minor COVID-19 association with crime in Sweden, a five week follow up." (2020)Malmo University https://osf.io/preprints/socarxiv/w7gka/

[38] Eric Halford et al.," Crime and Coronavirus: Social Distancing, Lockdown, and the Mobility Elasticity of Crime" *Crime Science* 1 (2020) 11.

[39] István László Gál, "The Possible Impact of the COVID-19 On Crime Rates in Hungary". *Journal of Eastern-European Criminal Law* . (2020) ,7: 1 pp. 165-177. 13 p.

[40] István László Gál, A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre" *Magyar Jog* , (2020) 67. évf.: 5 pp. 257–265. , 9 p. (2020)

[41] „Stay-at-home orders were issued by most states and legally required residence to stay within their homes except for authorized activities. Commonly, these activities included seeking health care, purchasing food and other necessary supplies, banking, and similar activities. The orders either outright closed or by de-facto closed broad swaths of the economy and impacted schools, private social gatherings, religious activities, travel, and more. In short, these orders disrupted the daily activities of entire populations and was the only variable that changed abruptly, just days before double-digit drops in crime around the world. As such, we believe, the Environmental Criminology suite of perspectives including; Rational Choice (Clarke & Felson, 1993) and Routine Activity (Cohen & Felson, 1979) will emerge as frontrunners in understanding the crime changes during COVID-19 and will provide insight how to influence crime in the future." Ben Stickle, Marcus Felson "Crime Rates in a Pandemic: The Largest Criminological Experiment in History" *American Journal of Criminal Justice* 4 (2020) 526–527.

[42] Lawrence E. Cohen, Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review*, (1979), vol. 44, no. 4, pp. 588–608.

[43] See: László Kőhalmi,"Szervezett bűnözés „In: *Barabás, A. Tünde (szerk.) Alkalmazott kriminológia* (Budapest, Magyarország, Ludovika Egyetemi Kiadó 2020) 654 p. pp. 461-474., 14 p.

[44] "How Covid-19-Related Crime infected Europe during 2020, 11 November 2020, Europol Report" Europol,https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020 Accessed: 07.01.2021.

have already entered into recession and others are expected to do so imminently. As witnessed in the past, economic crises are fertile ground for the growth of organized crime in terms of its scope of activities and its influence.

Economic hardship and rising unemployment may also drive the recruitment of individuals for organized crime groups (OCGs2).[45]

Digitalization and cybercrime

Before examining the connections and causes of the COVID-19 pandemic and cybercrime, it can be concluded that the growth of digitalization itself is also a factor among many that leads to the growth of cybercrime.

Cause of the increase in criminal interest: speed, relative anonymity, and the number of users of modern information technology is growing.[46] Wall asks the questions – how has the internet transformed social behavior and how has the internet transformed criminal behavior? – and he says that the two behaviors have a similar appearance.[47]

The Center for Strategic and International Studies (CSIS), in partnership with McAfee, present Economic Impact of Cybercrime – No Slowing Down, a global report that focuses on the significant impact that cybercrime has on economies worldwide. The report concludes that close to $600 billion, nearly one percent of global GDP[48] is lost to cybercrime each year, which is up from a 2014 study that put global losses at about $445 billion. The report attributes the growth over three years to cybercriminals quickly adopting new technologies and the ease of cybercrime growing as actors leverage black markets and digital currencies.

The COVID-19 pandemic and cybercrime

Cybercrime has come to the fore and is showing significant growth.

As early as March 2020, the Council of Europe drew attention to the dangers of cybercrime in connection with the epidemic.[49] The COVID-19 pandemic renders individuals and society extremely vulnerable in all respects. During this crisis, we all rely more than ever on computer systems, mobile devices and the Internet to work, communicate, shop, share and receive information and otherwise mitigate the impact of social distancing.

The unprecedented coronavirus pandemic is profoundly affecting the global cyber threat landscape.

According to Catherine de Bolle Executive Director of Europol, „looking back at the last eight months, we can trace how criminals have used uncertainty and change to identify and exploit opportunities targeting individual citizens, businesses and the public sector... The fallout from the COVID-19 pandemic has weakened our economy and created new vulnerabilities from which crime can emerge... Economic and financial crime, such as various types of fraud, money laundering, intellectual property crime, and currency counterfeiting, is particularly threatening during times of economic crisis."[50]

In its reports, Europol focuses on the various elements of crimes since the beginning of the Covid-19 pandemic.

It not only analyzes each criminal conduct, but also studies on economic crime[51], organized crime, terrorism[52], and, of course cybercrime.

It deals with drug trafficking, migrant smuggling, and deception, which cause significant damage mainly in the health environment.

[45] See" How Covid-19-Related Crime infected Europe During 2020" Europol, 11 November 2020.

[46] David S. Wall, *Cybercrime*, (Cambridge, Polity, 2007) 3.

[47] „How has the internet transformed social behavior? ¬ Informational exchanges ¬ the internet is based upon intangible informational exchanges ¬ everything leaves a data trail (disappearance of disappearance!) ¬ Globalization and Glocalism ¬ globalization shapes the relationship between the global and the local (hence the term glocalisation) ¬ Networks ¬ Distributed networks and grid technologies create new forms of commercial and emotional relationships between individuals. [Ideas such as Tipping Point, Wisdom of Crowds, Wikinomics] ¬ Asymmetric not symmetric relationships-empowered single agent ¬ Has both a Panoptic and Synoptic effect CYBERCRIMES exhibit similar characteristics". „How has the internet transformed criminal behavior? ¬ Information – Values online are linked to ideas, not physical property ¬ Why bank robbery? Virtual theft (e.g. of intellectual property)? ¬ Global – Changes in the scope of criminal opportunity ¬ There are generational differences cybercrime in terms of levels of mediation by technology ¬ Substantive changes in types of criminal behavior ¬ Network – Changes in the organization of crime and division of criminal labour – reaching victims through networks ¬ Gives one person control over the whole criminal process ¬ Makes the organization of criminal activity more efficient. ¬ Broadens the span of criminal activity to give offenders a global reach – creates single empowered agent – 50m X £1 robberies?? Cybercrime Motivations – distance from victim – self-satisfaction – peer respect – revenge – protest/terror – criminal /financial gain". David S Wall, „CYBERCRIME: What is it and what do we do about it? – Mapping out and policing cybercrimes" https://core.ac.uk/download/pdf/9582049.pdf, Accessed: 07.01.2021.

[48] James Lewis, *Economic Impact of Cybercrime – No Slowing Down.* (*CSIS* 2018), www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf Accessed: 07.01.2021.

[49] "Cybercrime and COVID-19" Council of Europe https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19,Accessed: 07.01.2021.

[50] "Financial and Economic Crime Targeted by New Europol Center" Europol, https://www.bankinfosecurity.com/financial-services-crime-targeted-by-dedicated-europol-center-a-14411. Accessed: 07.01.2021.

[51] Dávid Tóth, Kockázatelemzés egyes gazdasági bűncselekmények kapcsán BÜNTETŐJOGI SZEMLE 8 : 1 pp. 108-114. , 7 p. (2019).

[52] Dávid Tóth, Melánia Nagy, „The types of terrorism – with special attention to cyber and religious terrorism". *JURA* (2019) 25 : 1 pp. 413-422. , 10 p.

The main types of cybercrime based on EUROPOL Report[53]

In the following, based on Europol's reports, we highlight the most common types of offenses and acts.

Counterfeit and sub-standard goods:

The distribution of counterfeit and substandard goods has been one of the key criminal activities during the pandemic. With the onset of the pandemic, the demand for healthcare and sanitary products (masks, gloves, cleaning products, hand sanitizers), as well as personal protective equipment increased significantly.[54]

Some additional developments, such as the sales of fake 'corona home test kits' and fraudulent pharmaceutical products, advertised as allegedly treating or preventing COVID-19, have been particularly worrying from a public health perspective. Scammers have already offered fake vaccines.[55]

While some product offers for counterfeit goods related to the COVID-19 pandemic have appeared on the dark web, the product offerings available there remain limited compared to the surface web, which continues to host the primary distribution platforms for counterfeit goods. Dedicated websites have been set up for the purposes of selling counterfeit sanitary and pharmaceutical products. These often disappeared shortly after receiving negative reviews by defrauded customers. Targeted ads on social media platforms, web shops and in some cases messaging apps have been also reported to have been used to drive up the sales of counterfeit or non-existent goods.[56, 57, 58]

Cybercrime- Phishing

Phishing emails through spam campaigns with a specific reference to COVID-19 and with the primary purpose of harvesting credentials and other sensitive data, as well as infecting users, Phishing emails have been also reported to come from organizations which, for example, focus on disease prevention and health. SMS phishing[59] and phishing attacks occurring against crowdfunding campaigns have been also noted.[60]

Malware, ransomware and malicious apps

The trend of ransomware-targeted attacks against public health organizations appeared to have decreased towards the second quarter of 2020. Cybercriminals have exploited new attack surfaces; malware has appeared on typo-domains relating to commonly used video conferencing software, exploiting the attack vector of increased teleworking practices.[61]

Child sexual exploitation

With children spending more time online due to the various restrictions introduced in response to the COVID-19 pandemic, the potential increase in demand for CSAM and attempt to engage in child sexual exploitation has been a considerable threat. Though it has remained a priority for law enforcement, it has been difficult to quantify the seriousness of the threat posed.[62] Offenders are likely to attempt to take advantage of emotionally vulnerable, isolated children through grooming and sexual coercion and extortion. Children allowed greater unsupervised internet access will be increasingly vulnerable to exposure to offenders through online activity such as online gaming, the use of chat groups in apps, phishing attempts via email, unsolicited contact in social media and other means.

Dark web

The numbers of overall criminal listings on dark markets have fluctuated over time as a result of vendors' decreased ability to source and/or deliver goods. Nonetheless, the number of listings offering COVID-19-related products such as masks, fake test kits and pharmaceuticals on dark web platforms has been increasing. The dark web has been extensively used to carry out fraud as well, by taking money and never delivering the illicit products purchased.[63]

[53] See in Europol, "How Covid-19-Related Crime infected Europe During 2020, 11 November 2020, Europol Report".

[54] „Viral marketing – counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic" Europol 2020, https://www.europol.europa.eu/newsroom/news/viral-marketing-counterfeits-in-time-of-pandemic, Accessed: 07.01.2021.

[55] „Beyond the pandemic – how COVID-19 will shape the serious and organized crime landscape in the EU" Europol 2020, https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu, Accessed: 07.01.2021.

[56] See,"Viral marketing – counterfeits, sub-standard goods and intellectual property crime in the COVID-19 pandemic" Europol 2020.

[57] István L.Gál, Zoran Pavlović, „Corruption In Healthcare and New Regulations: One step forward, two back". In: *Jelena, Kostić; Aleksandar, Stevanović (szerk.) Uloga društva u borbi protiv korupcije Belgrád, Szerbia* (Institut za uporedno pravo, Instituta za kriminološkai sociološka istraživanja 2020) pp. 303-316. , 14 p.

[58] Dávid Tóth, „The new Directive related to counterfeiting "*In: Czeferner, Dóra; Mikó, Alexandra (szerk.) XIII. Országos Grastyán Konferencia előadásai,* Pécs, Magyarország ,(PTE Grastyán Endre Szakkollégium 2015) 344 p. pp. 324-332. , 9 p.

[59] Andrea Kraut, László Kőhalmi, Dávid Tóth, „Digital Dangers of Smartphones" *Journal of Eastern-European Criminal Law* (2020) 7 : 1 pp. 36-49., 14 p.

[60] „COVID 19: Phising and smishing scams" Europol 2020, https://www.europol.europa.eu/covid-19/covid-19-phishing-and-smishing-scams, Accessed: 07.01.2021.

[61] „Catching the virus – cybercrime, disinformation and the COVID-19 pandemic", Europol 2020," https://www.europol.europa.eu/newsroom/news/catching-virus, Accessed: 07.01.2021.

[62] " Exploiting isolation – Offenders and victims of online child sexual abuse during the COVID-19 pandemic" Europol 2020, https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic, Accessed: 07.01.2021.

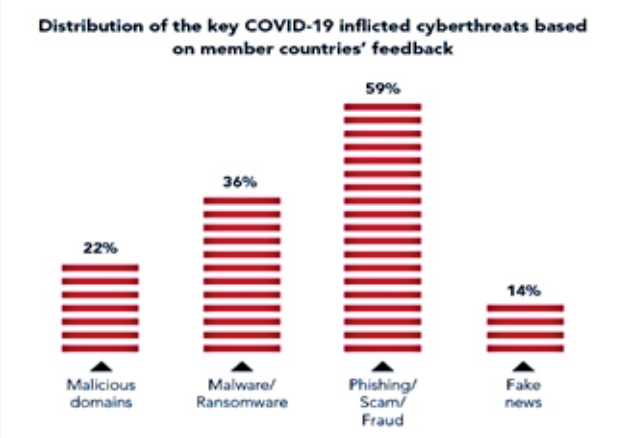
[63] „Catching the virus – cybercrime, disinformation and the COVID-19

Interpol, UNODC and other research, such as the Benchmark study, are also in line with Europol's data. Based on these studies, we intend to use statistical data to demonstrate the effects of COVID-19 on crime and cybercrime.

Cybercrime main types based on INTERPOL Report[64]

Key findings highlighted by the INTERPOL assessment of the cybercrime landscape in relation to the COVID-19 pandemic include: Online Scams and Phishing, Disruptive Malware (Ransomware and DDoS), Data Harvesting Malware, Malicious Domains, Misinformation.

Figure 2: shows the distribution of cyber threats and their main types.



Source: INTERPOL report shows alarming rate of cyberattacks during COVID-19S

COVID 19 Cyber Threat Analysis by UNODC[65]

What are the main threats by UODC survey? Malicious Campaigns – like phishing e-mail: the biggest threat vector for individuals and organizations. This includes the impersonating an official website, spreading malware, and the fake campaigns. Increased use of disinformation and social media is typical based on the data from the study.

New websites are being registered to disseminate information related to the pandemic. Of the end of March 2020, *more than 9,000 domains* were registered with the Corona Virus theme. There are websites that are trying to investigate misinformation related to COVID-19.7 In a little over a month, *more than 50 articles have been* debunked and proven *false.* It has become exceedingly difficult to keep up with the amount of misinformation related to the current situation.

In the field of Social Media Enhanced Usage the below statistics have been gathered from a survey of more than 25,000 consumers in 30 markets and it was conducted from March 14th to March 24th, 2020.

The application *WhatsApp has seen a 40% increase in usage overall.* Initially it jumped 27% in usage at the very beginning of the crisis. During the mid-phase of the pandemic, that number reached 41% and finally for countries already in the later phase of the pandemic, WhatsApp usage has jumped by 51%. In specific countries, the usage can even represent a much higher value. For example, WhatsApp usage in Spain was up to 76%. However, this application is not alone in its enhanced usage; the study found that Facebook, Instagram, *WeChat and Weibo also witnessed a 40% increase* in their interaction time.[66]

COVID-19 Benchmarking Report December 2020[67]

This report provides the results of our third in a series of studies exploring the ways that the fight against fraud has changed in the wake of COVID-19.[68]

The questions first of the report: How COVID -19 is affecting the overall level of fraud

A growing number of survey participants have observed an increase in fraud in the wake of COVID-19. As of November 2020, *79% of respondents said they have seen an increase in the overall level of fraud* (compared to 77% in August and 68% in May), *with 38% noting that this increase has been*

pandemic" Europol 2020, https://www.europol.europa.eu/newsroom/news/catching-virus, Accessed: 07.01.2021.

[64] „INTERPOL report shows alarming rate of cyberattacks during COVID-19" Interpol, https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, Accessed: 07.01.2021.

[65] „ Several dark web malicious websites are advertising COVID-19 Phishing Email Kits using an infected email attachment disguised as a map of the virus's outbreak for various prices that can range from 150$ up to 1000$. Cybercriminals purchasing these "kits" can then use them to start their email campaigns targeting anyone from individuals to large scale organizations. These infections are made possible by unpatched operating systems and the infected attachment will exploit the weaknesses of the computer it is visualized on." „United Nations Office on Drugs & Crime, COVID-19: Cyber Threat Analysis" https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf, Accessed: 08.01.2021.

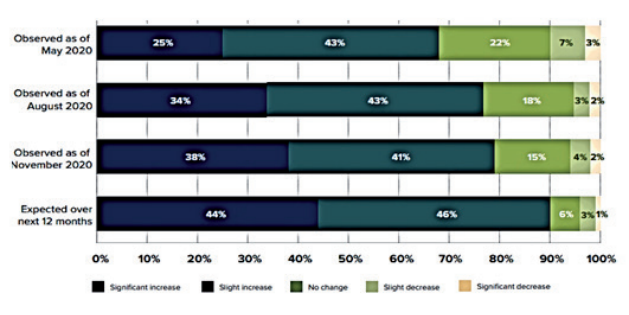
[66] Sarah Perez, „Report: WhatsApp has seen a 40% increase in usage due to COVID-19 pandemic" https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19-pandemic/. Accessed: 08.01.2021.

[67] „FRAUD IN THE WAKE OF COVID-19: Benchmarking Report" ACFE, December 2020 Edition, Covid-19%20Benchmarking%20Report%20December%20Edition%20(1).pdf, Accessed: 08.01.2021.

[68] Approximately half (49%) of the survey respondents are located in the United States or Canada, and 17% live in Sub-Saharan Africa. Smaller proportions of participants live in Western Europe (8%), Southern Asia (7%), the Asia-Pacific region (7%), the Middle East and North Africa (5%), Latin America and the Caribbean (4%), and Eastern Europe and Western/Central Asia (3%).

significant (compared to 34% in August and 25% in May). As we look toward 2021, our members expect this trend to persist; *90% anticipate a further increase* in the overall level of fraud over the next 12 months, with 44% saying this change will likely be significant.

Figure 3: Change in the overall level of fraud



Source: Covid-19 Benchmarking Report December 2020

The second: How COVID 19 is affecting specific fraud risks

The way specific fraud risks are affecting organizations also continues to evolve in the wake of COVID-19. Among the categories of the 12 fraud risks, several of these risks are affecting organizations more significantly than others. Specifically, cyber fraud (e.g., business email compromise, hacking, ransomware, and malware) continues to be the most heightened area of risk, with *85% of respondents already seeing an increase in these schemes*, and 88%expecting a further increase over the next year. Other significant fraud risks in terms of both observed and expected increases include payment fraud (e.g., credit card fraud and fraudulent mobile payments), identity theft, and unemployment fraud.

Fig.4. Top 5 fraud schemes – predicted increase over 12 months due to the coronavirus

Source: Covid-19 Benchmarking Report December 2020

The third: How COVID-19 is affecting organizations' anti-fraud programs

The survey asked participants about the expected changes in the budgets and resources for their anti-fraud programs. *41% of organizations are planning to increase their overall anti-fraud budget*, while only 13% anticipate a reduced budget for next year. Similarly, anti-fraud staffing is largely expected to either increase (one-third of organizations) or remain flat (53% of organizations), with just 14%expecting cutbacks or layoffs within their anti-fraud teams.

Nearly *half (48%) of organizations anticipate increased investments in anti-fraud technology*, and 38% plan to increase the use of fraud-related consultants or other external resources.

The fourth: How COVID-19 is affecting the ability to fight fraud

The majority of our survey respondents noted that preventing, detecting, and investigating fraud have all become more difficult in the wake of COVID-19. More than three-quarters (77%) indicated that fraud prevention and fraud investigation are more challenging now than they were previously—with 26% and 31%, respectively, saying that these activities are significantly more difficult. Similarly, 71% of survey participants see fraud detection as more challenging (20% significantly so) than it was before the pandemic.

Digitalization against cybercrime

Digitalization increases the risk of cyberattack, and this is exacerbated by theCOVID-19 pandemic. Cyberattacks have become progressively more complex due to the increasing use of sophisticated malware and threat from professional cyber organizations. Users or organizations with malicious intent attempt to steal valuable data such as financial data, personal identifiable information, intellectual property, and health records. Several strategies, such as monetizing data access through the use of advanced ransomware techniques or disrupting business operations through DDoS attacks, have been attempted.

The peer-to-peer and decentralization structure of blockchain technology helps in improving its cyber defense since the platform can prevent malicious activities through robust consensus algorithms and detect data tampering due to its inherent features such as transparency, immutability, data encryption, auditability, and operational resilience

due to no single point of failure.[69,70] Blockchain opens up new ways to combat the rampant threat of cybercrime in a variety of ways.[71,72,73,74]

Future plans

The COVID-19 pandemic renders individuals and society extremely vulnerable in all respects. During this crisis, it is necessary to rely more than ever on computer systems, mobile devices and the Internet to work, communicate, shop, share and receive information and otherwise mitigate the impact of social distancing. The COVID-19 Pandemic – Guidelines for Law Enforcement,[75] issued by INTERPOL will be useful for criminal justice practitioners.

Criminal justice authorities need to engage in full cooperation to detect, investigate, attribute and prosecute the above offences and bring to justice those that exploit theCOVID-19 pandemic for their own criminal purposes.

With the Budapest Convention[76] a framework for effective cooperation with the necessary rule of law safeguards is available to 65 States. As a result of capacity building programs, many States should now be able to act. It is also clear that additional solutions are required to address future crises. Capacity building for criminal justice authorities must be further enhanced. And the 2nd Additional Protocol to the Budapest Convention that is currently under negotiations will be crucial to permit instant cooperation in urgent and emergency situations.

Based on their investigations, UNODC[77] made the following recommendations.

Cybercrime MENA Program[78] has different activities and procurement planned for the following months that will strengthen countries' capacities to respond more efficiently to the COVID-19 crisis from a Digital World's perspective.

Enhanced Cybersecurity for the Critical Infrastructures at the country level.

– Development of Standard Operating Procedures to ensure a proper digital response.

– Procurement of internationally recognized training for first responders and government officials.

– Procurement of digital forensics equipment to ensure proper investigation of various cyberattacks in the current context.

– Assessment of needs and regional coordinated assistance response.

– Cybercrime investigations specialized interventions to prevent further attacks.

– Digital Forensics response to various crime scenes or data tracking.

– Legislative review and counsel.

– International Cooperation assistance.

– Social Media Awareness campaign on specific pandemic issues.

In the current time, there is an immediate need for these activities to assist countries in ensuring the response is leveled across the world.

Summary

The Covid-19 pandemic is a social, economic, health crisis, with all its challenges. It is also a challenge for all fields of science in terms of developing both research and coping strategies. In this paper we ex-

[69] Eric Piscini, David Dalton, Lory Kehoe, " Blockchain & Cybersecurity Point of View. Deloitte, 2017" https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf, Accessed: 08.01.2021.

[70] Fenyvesi Csaba, „A kriminalisztikai világtendenciák – Különös tekintettel a digitális felderítésre" In: *Mezei, Kitti (szerk.) A* bűnügyi tudományok és az informatika ,Pécs, Magyarország, Budapest, Magyarország (Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont 2019) 204 p. pp. 64-82., 19 p.

[71] Ralph Tkatchuk, "Is Blockchain the ultimate weapon against cybercrime?" http://dataconomy.com/2017/10/blockchain-ultimate-weapon-cybercrime-2/, Accessed: 08.01.2021.

[72] Catherine Luff, "Cybersecurity and the future of blockchain technology", http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm, Accessed: 08.01.2021.

[73] Lester Coleman, "$81 Million Cyberheist Underscores Need for Blockchain Security", https://www.ccn.com/81-million-cyberheist-need-for-blockchain-security/, Accessed: 08.01.2021.

[74] „ Originally developed for the digital currency called Bitcoin, blockchain technology created a platform for a new segment of Internet, influenced the decentralization of the network by the principle of a distributed registry, and began to be used in all kinds of combinations and combinations for various purposes, including cybersecurity. The use of blockchain technology for ensuring cybersecurity and its leading potential in that is unlimited, thanks to such unique properties as reliability, accessibility, high adaptability, economic efficiency, and profitability. Our results show that the use of blockchain technologies in combating cybercrime, including cyber terrorism, can extend to the control of financial services, transport, or any other industry. However, the growth of criminal activity using blockchain technologies will also intensify if law enforcement agencies cannot technologically competently, at a faster pace, detect these developing centres, determine their actions, and destroy illegal plans." Olga Vorobyova, Julia Polyakova, Olga Borzenkova, "Leading Opportunities for Fighting Cyberterrorism Using Blockchain Technology " In: *6th International Conference on Social, economic, and academic leadership*, (Atlantis Press,) 523,528, 2352-5398, https://doi.org/10.2991/assehr.k.200526.076, Accessed: 08.01.2021.

[75] "COVID-19 Pandemic – Guidelines for Law Enforcement" https://www.interpol.int/content/download/15014/file/COVID19_LE_Guidelines_PUBLIC_26mar2020.pdf, Accessed: 08.01.2021.

[76] "Council of Europe, Budapest Convention and related standards" https://www.coe.int/en/web/cybercrime/the-budapest-convention, Accessed: 08.01.2021.

[77] „As evidently indicated by UNODC's Cybercrime Global Program initiative, "Now is not the time to de-invest in specialist cybercrime law enforcement. The capability and capacity to counter cybercrime are vital components for protecting Critical National Infrastructure, keeping children safe online, empowering industry, securing hospitals and supporting economic recovery from COVID-19." UNODC "Global Programm on Cybercrime, CYBERCRIME AND COVID19: Risks and Responses" (14 April 2020),www.unodc.org/documents/Advocacy Section/UNODC_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf , Accessed: 08.01.2021.

[78] UNODC "MENA Regional Programme, COVID-19: How to stay safe from cybercriminals exploiting the pandemic"(March 2020), https://www.unodc.org/middleeastandnorthafrica/en/web-stories/covid-19_-how-to-stay-safe-from-cybercriminals-exploiting-the-pandemic.html, Accessed: 08.01.2021.

amined the relationships between digitization and crime/cybercrime in connection to coronavirus epidemic, and their influences to each other.

Considering the effects of COVID-19 epidemic, one might suppose several connections between these scientific areas independently of each other. These connections are cited in this work from previous publication.

It can be clearly seen that digitalization, which has undergone tremendous development, necessarily requires further growth and development as a result of the epidemic – as it is a consequence of the COVID-19 pandemic itself – lockdown needed to protect against it, restrictions and changes in certain economic sectors (e.g. e-commerce) – make this necessary.

At the same time, from a health point of view, epidemic surveillance, control tools, clinical trials, vaccine research, and application similarly require it.

The increase in digitalization processes is also a unique way to increase the opportunities for the rapidly adaptable criminal layer in this area – especially in cyberspace.

Statistics show that "traditional" crime patterns have declined as a result of the epidemic, while the number of online crimes has increased significantly, even in the first few months of the epidemic.

The changes in the digitalization and the criminology affect governments, economic actors, those involved in education, and the masses of people locked up their homes. Protecting against cyber-attacks has become more important now than ever, requiring further improvements in many areas of digitalization, enhancing cybersecurity, all the more so because criminals themselves use these methods. Several technologies are awaiting further development, such as Blokchain, IoT, and AI.

However, the protection needs to be applied more widely than ever before, as it affects users of supercomputers as well as simple users of telephones.

According to et al Ben Stickle and Marcus Felson the COVID-19 pandemic might be declared a huge social experiment.

Examining the changes in the digitization and cybercrime, I wanted to draw the attention to the actual tendencies in their connections, the risk of further growth of cybercrime, and encourage researchers to study these modern criminological challenges.

The populations of several continents live in the era of significant changes in the economic, technologic and social life, and this Covid-19 epidemic even highlights the significance of these changes which might serve a special aspect of the criminology in this quite "inverse situation".