Acta Sci. Pol.
Oeconomia 20 (4) 2021, 39–48
ISSN 1644-0757 eISSN 2450-047X DOI: 10.22630/ASPE.2021.20.4. 30
acta_oeconomia.sggw.pl

ORIGINAL PAPER

Received: 29.11.2021
Accepted: 30.12.2021

GLOBAL CRISES AND CYBERSECURITY ATACKS – AN ANALYSIS DURING THE COVID-19 PANDEMIC

George B. Mertoiu✉, Gabriela Mesnita

Alexandru Ioan Cuza University of Iaşi, Romania

ABSTRACT

The COVID-19 pandemic has affected all nations in various ways, both economically and especially socially. The new normality, as social behavior dictated by the restrictions imposed, sustained online interaction, a factor that allowed an increase in cyberattacks. This paper intends to analyze the cyberattacks conducted during the COVID-19 pandemic, starting from a series of international events such as the crisis in Venezuela or Ukraine. A part of this study is a quantitative analysis of the results obtained from consulting the Scopus database. In this part, in addition to the most important authors and key words used, we aimed to find if the countries that are the main targets of cyberattacks are also involved in researching cybersecurity during pandemic. Cyberattacks are analyzed in terms of motivation and targets, aiming to identify possible solutions based on the *modus operandi* of attackers and what will be the next steps in the research.

Key words: cyberattacks, crises, coronavirus, COVID-19, cybercrime, hacktivism
JEL codes: F60, I30, L86

INTRODUCTION

Over time, humanity has faced events that have led to situations of instability or danger to individuals, groups or societies, known as crises [Bundy et al. 2017]. These have been marked by unexpected negative changes, with some authors considering them "processes of transformation of outdated systems that can no longer be managed" [Venette 2003].

The crises that humanity has faced and that continue to manifest themselves, can be framed in several typologies, the best known being the economic/ /financial, humanitarian, pandemic or military crises. In a broad sense, they fall into several types, depending on the mode of manifestation, the area of spread or their effects. These events had effects depending on the type of manifestation, the most common being the social ones such as loss of jobs, decreased quality of life or impaired physical integrity. In the process of eliminating the effects of crises and returning to normal, the focus is on maintaining activities and supporting efforts to minimize impact. Thus, there has been a decrease in interest and effort for security, whatever it may be, from physical security to cybersecurity.

The paper analyzes the existence of a correlation between recent crises, focusing on the pandemic and cyberattacks from the same period, respectively, their motivation, to support further research on cybersecurity risk management.

Thus, the paper seeks to provide conclusive answers to the following questions:

1. Was the COVID-19 pandemic a factor in increasing the number of cyberattacks?

George B. Mertoiu https://orcid.org/0000-0002-4871-1413; Gabriela Mesnita https://orcid.org/0000-0003-1681-1505
✉george.mertoiu@student.uaic.ro

2. Is there a relationship between the rate of cyberattacks recorded and the ongoing crises?
3. Can the targets of future cyberattacks be predicted depending on the type of crisis?
4. What are the motivations and modus operandi of cyberattacks and how can they be countered?

To support research on cybersecurity risk management by identifying the correlation between crises and cyberattacks, the second part of the study will explain the research methodology that will allow, in the third part, a comparative analysis between recent crises and cyberattacks. And in the fourth part of the paper, a bibliometric analysis of research on studying cyberattacks during the COVID-19 pandemic will be performed. Thus, the data obtained, correlated with the analysis of the literature, will allow obtaining the answer to the three questions.

RESEARCH METHODOLOGY FOR ESTABLISHING A CORRELATION BETWEEN CRISES AND CYBERATTACKS

The methodological approach will involve the use of qualitative methods of research, which will analyze public sources of information and literature. Also, quantitative methods such as bibliometric analysis will be used.

In the qualitative approach, data will be obtained on the crises of the last decade that has affected various geographical areas, respectively, the cyberattacks conducted in times of crisis. These will be the subject of a cause-and-effect analysis on the association between the two types of events. The time frame chosen was primarily due to the low volume of data on cyberattacks that occurred before 2010. Additionally, some of these crises were echoes of the global financial crisis of 2007–2008, considered, by many economists, the most important crisis since the "Great Depression" of 1929–1930. Also, the same methodological approach will allow an analysis of the literature on cyberattacks during the pandemic, to identify whether there is a causal relationship between the context of the crisis and the motivation, respectively, their targets.

The quantitative methodological approach consists of a bibliometric analysis on the most relevant bibliographic sources that dealt with the cyberattacks during the COVID-19 pandemic. The search results, performed on the Scopus platform, included only scientific articles from journals and papers published in the volumes of specialized conferences. The analysis was performed using the VOSviewer software tool (version 1.16.16).

For comprehensive research on cyberattacks during the coronavirus pandemic, the Scopus database was queried in the title and summary of studies published in journals or conference volumes, using the following terms of reference: ("cyber attacks or "cyber-attacks" or "cyberattacks") and ("covid-19 or coronavirus"). One hundred twenty-three (123) results were obtained, containing research conducted between 2020 and 2021. The choice of key words aimed to obtain an overview of cybersecurity research from the perspective of identifying the motivation and targets of cyberattacks during the pandemic of COVID-19.

A REVIEW OF MOST KNOWN CRISES FROM THE LAST 10 YEARS

From economic crises to armed attacks on the population or the spread of pathogens, the world has always faced degenerative situations, capable of affecting one or more nations. In many cases, the manifestation of a crisis at the level of a nation has had effects outside it as well. The effects and the causes involved adjacent factors, some of which were cyberattacks conducted to or from the affected country.

Table 1 gives a brief overview of the main crises of the last decade. The crises listed are important for the following reasons:

– Although they have manifested themselves on the territory of a nation, their effects have spread beyond borders, having an extensive impact.
– Some of the governmental measures that favored the emergence of crises were generated by the global financial crisis from 2007–2008.

Table 2 shows a series of cyberattacks identified between 2013 and 2018 and which occurred because of the crises mentioned in Table 1. In addition to the factors that triggered and maintained these crises, nations have had to deal with numerous cyberattacks with major negative effects on electronic systems and

Table 1. The most publicly known crises from the last 10 years

Period	Naming	Observations
2010–2014	Portuguese financial crisis	– a financial crisis from 2001, exacerbated by the global crisis of 2007–2008; – many street protests; – a great damage to the socio-economic level.
2012–present	The socio-economic and political crisis in Venezuela	– the crisis began during the presidency of Hugo Chávez (2012); – very high inflation with great impact on purchasing power, health and law systems; – a massive emigration of population.
2013–2014	The Ukrainian crisis	– crisis during 2013–2014 on the several levels, known as Orange Revolution; – a lot of social protests related to EU or pro-Russian orientation.
2014– 2015	The financial crisis in the Russian Federation	– crisis was the result of the sharp devaluation of the Russian national currency [Viktorov and Abramov 2020]; – was caused by two major factors: the drop in oil prices by almost 50% in 2014 and the result of international economic sanctions imposed on Russia [Kitroeff 2014].
2015– 2016	The financial crisis in the People's Republic of China	– crisis was caused by the Chinese stock market turmoil that began on June 12, 2015, with the appearance of the stock market bubble and ended in early February 2016 [Riley and Yan 2015].
2018– present	The financial and economic crisis in Turkey	– crisis was due to the decline in the value of the Turkish lira, high inflation and rising borrowing costs; – was caused by the excessive current account deficit of the Turkish economy and the large amounts of private debt denominated in foreign currency [Borzou 2018, O'Brien 2018].

Source: The authors.

data. The attacks were mainly aimed to affect the systems of government institutions, their assignment being a difficult task due to the complexity, but also the misleading techniques used by attackers (e.g. the use of IP addresses from other geographical areas or the creation of variables in the source code, in a language other than the attackers' source language).

The analysis of the types of attacks exposed in Table 2 highlights the year 2014 as one of transition from ideologically motivated attacks to those motivated financially or supported by the state.

In order to verify the hypothesis regarding the trend of cyberattacks, all these events, made public in the period 2012–2020, were analyzed from the point of view of motivation. According to the data showed in the public environment (Fig. 1), for the period 2012–2014, the trends of cyberattacks were marked by the actions of ideologically motivated groups (Hacktivism) and those with financial motivation (Cyber Crime) [Passeri 2015].

Based on the comparison, it can be seen that the attacks with ideological motivation, between 2013 and 2014, decreased from 44% (2013) to 24.9% (2014), while the financially motivated ones registered a significant increase, from 47% (2013) to 62.3% (2014).

Since 2014, the phenomenon of hacktivism has been constantly declining, with significant percentages registering attacks with financial motivation. According to Fig. 1, from 2015 to 2016, the attacks conducted by cybercrime groups increased by 5%, and it is interesting that the attacks with an impact on the social environment (Cyber Warfare) increased from 2.4 to 4.3%.

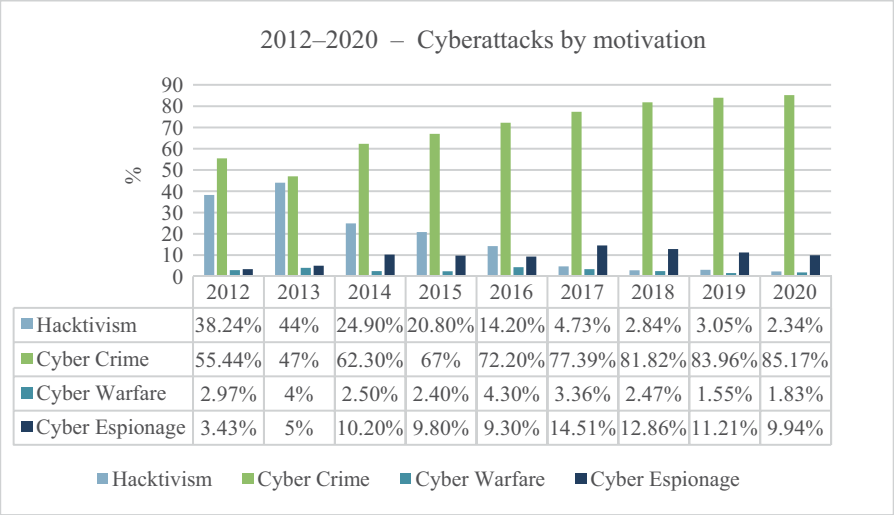
Between 2017 and 2020, the percentage of ideologically and financially motivated attacks continued on the same trend since 2014. Simultaneously, there is an increase in the volume and complexity of cyberattacks, given that organized crime groups have developed business models. profitable around phishing and ransomware attacks, the techniques and tools are marketed on the cybercrime-as-a-service platforms of DarkWeb. There is also an increase in state-sponsored attacks (Cyber Espionage), around 10%, which indicates an intensification in the race to obtain information.

Table 2. Cyberattacks during crises

Period	Cyberattacks	Cyberattacks targets
2013–2014	The hacktivism group „Anonymous" initiated the #OpPortugal operation which was intended to disrupt online government operations due to the violation of human rights [Pastebin 2014].	online government systems of the Portuguese government
2013	The group of hackers known as „r00ts3curity" or „# r00ts3c" carried out cyberattacks on sites in Ukraine, gaining access to data that was later made public. The attacks targeted web platforms of the Kharkiv Regional Scientific Library (www.library.kharkov.ua), Dentistry Of Sevastopol (www.vityaz.in. Ua) and the Center for the Receipt and Processing of Information and Specific Control (dzz.gov.ua) [Lee 2013].	online computer systems of Ukrainian government institutions
2014	Anonymous and Lulzsec groups launched the #OpVenezuela campaign, launching cyberattacks on government websites in Venezuela [Boone 2014]. During the operation, the members of Anonymous obtained and published a series of data on the governmental and presidential steps, which allowed the existence of this crisis [Support Anon Candanga 2019].	online computer systems of the Venezuelan government and presidency
May 2014	An unidentified group of hackers gained access to the Central Electoral Commission of Ukraine and deactivated parts of the network using advanced cyberespionage malware.	online computer systems of Ukrainian government institutions
May 2015	The German Bundestag computer network. BfV, Germany's internal intelligence service, was accessed unauthorized, with German investigators making public that the attacks were supported by the Russian Federation, and their goal was to obtain information about the functioning of the Bundestag, the German government and NATO [Winderm 2016].	online information systems of the German internal intelligence service
December 2015	Cyberattacks have taken place in the Russian Federation, compromising the IT infrastructure of three Ukrainian energy distribution companies and temporarily disrupting consumers' electricity supply [Zetter 2016].	industrial computer systems of Ukrainian energy suppliers
2015	The data of more than 21 million people has been compromised as a result of unauthorized access to the „US Office of Personnel Management" systems by a hacking group in China.	online computer systems of US government agencies
2015–2016	Cyberattacks by Chinese entities targeted Philippine government institutions, along with a medical center and smaller local government units, simultaneous with periods of heightened geopolitical tensions [Piiparinen 2016].	government computer systems in the Philippines
2016	Hackers in China have unauthorized access to workstations and servers of the Federal Deposit Insurance Corp., the US bank deposit insurance agency.	online computer systems of US government agencies
2018	Hackers of Turkish origin attacked at least 30 organizations, including government ministries, embassies and security services. According to British and American officials, the activity bears the marks of a state-backed cyberespionage operation carried out to promote Turkish interests [Stubbs 2020].	government information systems in Greece, Cyprus and Iraq

Source: The authors.

Starting from these data that reveal correlations between crises and cyberattacks, it is found that in the case of the events in Table 1, governmental systems were targeted, for ideological reasons, to subsequently target data and information that bring financial benefits to the attacker, by capitalizing on them in decisions with macroeconomic impact (cyber espionage campaigns). Given that the pandemic crisis has affected all nations, the next chapter will analyze whether the target and motivations of cyberattacks have experienced the same trend as in the case of the analyzed crises or have particularities.



	2012	2013	2014	2015	2016	2017	2018	2019	2020
Hacktivism	38.24%	44%	24.90%	20.80%	14.20%	4.73%	2.84%	3.05%	2.34%
Cyber Crime	55.44%	47%	62.30%	67%	72.20%	77.39%	81.82%	83.96%	85.17%
Cyber Warfare	2.97%	4%	2.50%	2.40%	4.30%	3.36%	2.47%	1.55%	1.83%
Cyber Espionage	3.43%	5%	10.20%	9.80%	9.30%	14.51%	12.86%	11.21%	9.94%

Fig. 1. Cyberattacks by motivation, from 2012 to 2020

Source: The authors calculations using statistical data from [https://www.hackmageddon.com].

CYBERATTACKS DURING THE CORONAVIRUS PANDEMIC

Although the above-mentioned crises have affected several nations, the coronavirus pandemic (COVID--19) has had a considerable impact on the international economic and social life. In the second half of 2020, emerging markets were already in recession, followed by those of developed countries [Zumbrun 2020]. The recession has seen unusually large and rapid increases in unemployment in many countries. To all these effects, a major contribution was made by the consequences of the crises that nations such as Turkey or Venezuela have gone through or are still going through.

The variety of cyberattacks that occurred around the aforementioned events reveals that it is not surprising that they intensified during the COVID-19 pandemic. The crises have caused an international disruption, people having to adapt their daily routines to a new reality: work from home, lack of social interactions, physical activity and fear of not being prepared. [Lindseyh 2020]. Also, the sudden change of work contexts led companies to improvise new ways of doing business, which led to the vulnerability of IT infrastructures in the process of ensuring interoperability. Since the beginning of the pandemic crisis, there has been an intensification of attacks through malware or scams, those conducted through phishing campaigns increasing by about 600% [Fleming 2020].

In April 2020, Google blocked 18 million phishing emails daily using Machine Learning techniques [Kumaran 2020]. Such attacks are conducted for financial reasons, and are intended to exploit the recipient by creating a seemingly legitimate framework of the message source. Given this international framework, a bibliometric analysis of the most relevant bibliographic sources that dealt with the subject of cyberattacks during the COVID-19 pandemic would facilitate the finding of answers to our research questions.

Bibliometric analysis of results

The bibliometric analysis created an overview of the research of cyberattacks conducted during the pandemic and the application of the results to ensure cybersecurity. In this sense, it was considered to identify the key words of the studies in the field, respectively, of the main authors with a significant contribution. The level of involvement of the main countries that are the target of attacks in the process of supporting studies on improving the defense techniques of their own systems was also monitored.

Table 3. The most significant key words

Key word	Occurrences
Network security	55
Cyberattacks	38
Cyber security	32
COVID-19	25
Computer crime	23
Security of data	21
Crime	18
Cybersecurity	18
Internet of things	18
Malware	15

Source: Self representation using Scopus exported data.

Table 4. The most significant authors

Author	Documents	Citations
Bellekens X.	2	13
Gupta R.	2	9
Tanwar S.	2	9
Gupta D.	2	3
Khan R.A.	2	3
Konstantinou C.	2	3
Kumar S.	2	3
Renaud K.	2	2
Agrawal A.	2	1

Source: Self representation using Scopus exported data.

Table 3 contains the most used key words in the research and highlights, as we found earlier, that in the pandemic period, cyberattacks were financially motivated, being conducted through malware applications. They also targeted equipment in the Internet of things category, with research focused on ensuring network and data security. To identify the authors with the most important contributions, it was taken consider the number of citations. Thus, the most important authors are included in Table 4.

The analysis shows that their interest is focused on identifying new opportunities and technologies, such as artificial intelligence, to ensure cybersecurity, given the types of cyberattacks that occurred during the pandemic and their targets.

The results of the analysis showed that the main countries, according to the authors' affiliation, in which pandemic cyberattacks were studied and ways to counter them, are the United Kingdom, India, the United States, Saudi Arabia and China. Notably the list of countries includes countries such as Portugal, Turkey, Ukraine and the Russian Federation, which were involved in this research, possibly because of the events during the crises they faced. The data obtained show that the pandemic had and has an important impact on cybersecurity worldwide, being marked according to research, by financially motivated cyberattacks.

Literature review on cyberattacks during COVID-19 crisis

As COVID-19 has spread worldwide, it has also led to a significant threat to a technology-based society, manifested by campaigns of cyberattacks on both organizations/institutions and home users. Since the onset of the pandemic, numerous reports have highlighted the fraudulent use of the name of public authorities (e.g., WHO) and medical or pharmaceutical organizations [Bryan 2020, MalwareBytes 2020] in attacks targeting platforms involved [Krebs on Security 2020, Smithers 2020] in creating personal protective equipment [Europol 2020] and providing solutions against COVID-19 [Norton 2020, Paul 2020]. These attacks, also known as scams, targeted in particular the public, especially people who performed their professional activities at home. The changes that have taken place in the way of performed the professional activity, respectively at home, have caused a high level of cybersecurity problems and challenges that could not be previously estimated by the industry. Cybercriminals have used this opportunity to expand their attacks through traditional methods of fraud [Nurse 2019] using increased stress, anxiety and worries facing society. These negative aspects were complemented by the low level of training of software vendors, especially about the security of their products.

Cyberattacks related to the pandemic crisis have used, as a way of propagation, social engineering (SE), one of the main methods have produced negative effects, especially by targeting critical infrastructure, such as hospitals and medical services. In the current

situation, social engineering is one of the most significant security threats faced by various organizations in both the public and private sector [Abraham 2010]. Although data on the number of cyberattacks that used SE as the initial method of obtaining unauthorized access are not yet known, statistics for 2020 show that approximately 2,332 events have been reported to the Internet Crime Complaint Center (IC3), of which, approximately 39.9% were infecting computers with malware, and 15.4% of gaining unauthorized access to user accounts [Johnson 2021].

To further increase the success of cyberattacks, hacking entities have registered numerous of web domains containing words such as "covid" and "corona" [Check Point 2020]. Such domains are seemingly credible and therefore accessible, especially if they are associated with terms such as "WHO", "Centers for Disease Control and Prevention (CDC)" or key words (e.g. Corona-virusapps.com, anticovid19-pharmacy.com, etc.) [Brewster 2019, 2020]. The names of communication platforms have also been used to increase the credibility, such as Zoom, Microsoft or Google, both in emails and in domain names (e.g. http://log.microsoftonline.com- common-oauth2-eezylnrb.medyacam.com/common/oauth2/) [Check Point 2020]. This is all the more important as they are the main technologies used by millions of users around the world for educational, professional or social activities. The proportion of new malware used in COVID-19 attacks has increased by 15% [Nabe 2020]. The main malware applications identified in the attacks were updated versions of the already known ones, such as Metaljack, REMCOS, Emotet, LOKIBOT, SpyMax (disguised in the Corona live 1.1 application) FORMBOOK, Trickbot and Ginp. Some attacks even used a form of machine learning that allowed them to integrate into the environment and remain undetected [Lallie 2021].

Another form of attack related to the pandemic situation was the one carried out through ransomware applications, hackers managing to combine data exfiltration with their encryption, to have an advantage in determining the victims to make redemption payments. At the organizational level, ransomware attacks targeted in particular the institutions involved in combating the effects of the pandemic, this being a modus operandi specific to entities focused only on financial gains. Regarding ransomware applications, a notable threat was COVIDLock, an Android application (COVID-19 Tracker) that should provide an updated map of Covid cases, but which, encrypts the mobile device and asks the user for a payment for unlocking [Anderson 2020].

According to the data's from Statista platform, from 2011 to 2020, the amount of damage caused by reported cybercrime increased significantly, to USD 4.2 billion, from around USD 500 million in 2011.Thus, a correlation between statistical data on cyberattacks by motivation and their financial impact reveals a strong upward trend in financially motivated actions.

Basically, in times of crisis, institutions, companies and citizens need to pay more attention, even requiring additional training, information or warning about the risks they may be exposed to in terms of cybersecurity.

RESULTS AND CONCLUSIONS

The pandemic situation has had and has a major impact on the human condition, whether we are talking about health, economics or technology. In a period dominated by communication dependence and the need to ensure physical and mental integrity, cybercrime groups have identified the main target of cyberattacks: the individual. Its exploitation through various techniques related to fake-news campaigns, allowed groups, access to critical infrastructure and obtaining financial or image benefits, during the disruption of the functioning of information systems. Each crisis had a correspondent in the targets and motivations of the cyberattacks conducted, regardless of the geographical area. And the percentage of those known has been constantly growing, following the technological trend, this being one of the limits of research, respectively the insufficient sample size for statistical measurements of the amount of data on cyberattacks carried out during the mentioned crisis periods.

In response to the first question in the research, the COVID-19 pandemic and its impact on the individual were factors favoring not only cyberattacks but especially their success rate. In support of the answer are data published by organizations in the field of cybersecurity and highlighting features such as the emergence of false domains containing key words about

the pandemic or communication technologies. And the analysis of the attacks during other crises reveals that the rate of these events will not depend on the type of crisis, but on the level of use of technology in that period. As a result, the number of cyberattacks during the COVID-19 pandemic was significantly higher than in other periods, due in particular to the needs of the transition of some activities performed in the physical environment to the online one. This has caused a high level of cybersecurity issues and challenges that could not be previously estimated by the industry.

The analysis of the attacks identified during the crisis revealed that the main targets were the systems belonging to governmental and/or non-governmental organizations, involved in combating the state of crisis or considered responsible for its effects. In addition to the financial motivation, as highlighted by the statistical situation of cyberattacks, the attacks aimed to obtain data and information that support decisions with macroeconomic and geopolitical impact of countries of origin (cyberespionage campaigns). Thus, these data make it possible to estimate with a high degree of probability the targets targeted during a crisis.

In response to the motivations and modus operandi, in all situations related to periods of crisis, the human factor was the main lever for gaining access to platforms or applications that subsequently facilitated the operation of internal information systems. The attacks were identified as using social engineering as a way of propagation, domain names containing key words about the crisis, respectively, updated variants of some families of malware or ransomware. The highest percentage of attacks was recorded by those motivated financial, an aspect that supports the need for research identified in the bibliometric analysis. Counteracting them will be possible by ensuring the security of data and communication networks, with the support of new technologies such as artificial intelligence, an aspect highlighted by the work of researchers such as Bellekens or Tanwar.

The novelty of this study is to highlight the different manifestations of threats depending on the type of crisis and the nation affected. The factors that influence this dependence are: the existing political structures at the level of those nations, the degree of development of those states, respectively the digitalization of the nations. Also, the research showed that during the pandemic another important factor intervened: social distance and work from home, which led to an even greater exposure to cyberthreats, because it is more difficult to be sure that the information you have access to is real. The increase in fake news information, the impossibility of validating information from several sources, the exponential increase in the use of social media generates as many vulnerabilities in terms of cybersecurity. And the fact that people are vulnerable to social engineering, highlights the need to find new forms and means to protect and raise awareness in this regard. And in this sense, future research should focus on techniques in the field of Artificial Intelligence, by combining the models of Machine Learning for Domain Generation Algorithms, Botnet and Spam Detection, with those for User Behavior.

In conclusion, although the trend of cyberattacks is increasing, the involvement of the academic community will play a major role in creating an environment favorable to the development of techniques and methods necessary to ensure cybersecurity.

ACKNOWLEDGEMENT

This paper is partially supported by the Competitiveness Operational Programme Romania under project number SMIS 124759 – RaaS-IS (Research as a Service Iasi), POC/398/1/1, SMIS 124759, ctr. nr. 236/21.04.2020.

REFERENCES

Abraham, S., Chengalur-Smith, I.N. (2010). An overview of social engineering malware: trends, tactics, and implications. Technol. Soc., 32, 3, 183–196.

Anderson, C. (2020). CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware. Dmaintools. Retrieved from https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware [accessed 04.09.2021].

Boone, J. (2014). Global hackers hit Venezuelan government, servers 'falling like dominoes'. The World. Retrieved from https://www.pri.org/stories/2014-02-17/global-hackers-hit-venezuelan-government-servers-falling-dominoes [accessed 03.09.2021].

Borzou, D., (2018). Erdogan Is Failing Economics 101. Foreign Policy, May.

Brewster, T., (2019). Chinese Hacker Crew Stole NSA Cyber Weapons In 2016 – A Year Before They Were Leaked Online. Forbes, 7 May. Retrieved from https://www.forbes.com/sites/thomasbrewster/2019/05/07/chinese-hacker-crew-stole-nsa-cyber-weapons-in-2016--a-year-before-they-were-leaked-online/?sh=3b89b182237b [accessed 03.09.2021].

Brewster, T., (2020). There Are Now More Than 40,000 'High-Risk' COVID-19 Threats On The Web. Forbes, 22 April. Retrieved from https://www.forbes.com/sites/thomasbrewster/2020/04/22/there-are-now-more-than-40000-high-risk-covid-19--threats-on-the-web/ [accessed 03.09.2021].

Bryan, K., (2020). Fraudsters impersonate airlines and Tesco in coronavirus scams. The Times, 25 April. Retrieved from https://www.thetimes.co.uk/article/fraudsters-impersonate-airlines-and-tesco-in-coronavirus-scams-5wdwhxq7p [accessed 04.09.2021].

Bundy, J., Pfarrer, M.D., Short, C.E., Coombs, W.T. (2017). Crises and crisis management: Integration, interpretation, and research development. J Manage., 43, 1661–1692.

Check Point (2020). Coronavirus cyber-attacks update: beware of the phish. Retrieved from https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/ [accessed 03.09.2021].

Europol, (2020). Pandemic Profiteering: How Criminals Exploit COVID-19 Crisis. Retrieved from https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis [accessed 04.09.2021].

Fleming, S. (2020). Threat Spotlight: Coronavirus-related phishing. Retrieved from https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ [accessed 01.09.2021].

Johnson, J., (2021). Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2020. Retrieved from https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/#statisticContainer [accessed 23.08.2021].

Kitroeff, N., Weisenthal, J., (2014). Here's Why the Russian Ruble Is Collapsing. Businessweek. Bloomberg, December. Retrieved from https://www.bloomberg.com/news/articles/2014-12-16/no-caviar-is-not-getting-cheaper-everything-you-need-to-know-about-the-russian-ruble-collapse [accessed 03.09.2021].

Krebs on Security (2020). Live Coronavirus Map Used to Spread Malware. Retrieved from https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/\ [accessed 05.09.2021].

Krombholz, K., Hobel, H., Huber, M., Weippl, E. (2015). Advanced social engineering attacks. Inf. Secur. Appl., 22, 113–122.

Kumaran, N., Lugani, S. (2020). Protecting businesses against cyber threats during COVID-19 and beyond. Retireved from https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond [accessed 01.09.2021].

Lallie, H.S., Shephred, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. Computers & Security, 105, 102248.

Lee, J., (2013). OpUkraine kicked off by r00tsecurity. Retrieved from https://www.databreaches.net/opukraine-kicked-off-by-r00tsecurity/ [accessed 03.09.2021].

Lindseyh (2020). 10 Tips to help if you are worried about Coronavirus. Retrived from https://www.dudleyccg.nhs.uk/10-tips-to-help-if-you-are-worried-about-coronavirus/ [accessed 01.09.2021].

MalwareBytes (2020). Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book. Retrieved from https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/ [accessed 04.09.2021].

Nabe, C. (2020). Impact of COVID-19 on Cybersecurity. Deloitte. Retrieved from https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html [accessed 02.09. 2021].

Norton (2020). Coronavirus Phishing Emails: How to Protect Against COVID-19 Scams. Retrieved from https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html [accessed 03.09.2021].

Nurse, J.R.C. (2019). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. [In:] A. Attrill-Smith, Ch. Fullwood, M. Keep, D.J. Kuss (Eds). The Oxford Handbook of Cyberpsychology. Oxford University Press, Oxford, 663–690.

O'Brien, M. (2018). Turkey's economy looks like it's headed for a big crash. Washington Post, 13 July. Retrieved from https://www.washingtonpost.com/business/2018/07/13/turkeys-economy-looks-like-its-headed-big-crash/ [accessed: 03.09.2021].

Passeri, P. (2015). 2014 Cyber Attacks Statistics. Retrieved from https://www.hackmageddon.com/2015/01/13/2014-cyber-attacks-statistics-aggregated/ [accessed 03.09.2021].

Pastebin (2014). #OpPortugal. Retrieved from https://pastebin.com/VsEGgfRw [accessed 03.09.2021].

Paul, K. (2020). US Authorities Battle Surge in Coronavirus Scams, From Phishing to Fake Treatments. The Guardian, 19 March. Retrieved from https://www.theguardian.com/world/2020/mar/19/coronavirus-scams-phishing-fake-treatments [accessed 01.09.2021].

Piiparinen, A. (2016). China's Secret Weapon in the South China Sea: Cyber Attacks. Retrieved from https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/ [accessed 03.09.2021].

Riley, Ch., Yan, S. (2015). China's stock market crash... in 2 minutes. CNNMoney, July. Retrieved from https://money.cnn.com/2015/07/09/investing/china-crash-in-two-minutes/index.html [accessed 03.09.2021].

Smithers, R. (2020). Fraudsters use bogus NHS contact-tracing app in phishing scam. The Guardian, 13 May. Retrived from https://www.theguardian.com/world/2020/may/13/fraudsters-use-bogus-nhs-contact-tracing-app-in-phishing-scam [accessed 01.09.2021].

Stubbs, J., Bing, Ch., Menn, J. (2020). Exclusive: Hackers acting in Turkey's interests believed to be behind recent cyberattacks – sources. Reuters, 27 Jannuary. Retrieved from https://www.reuters.com/article/us-cyber-attack-hijack-exclusive-idUSKBN1ZQ10X [accessed 01.09.2021].

Support Anon Candanga (2019). Op Venezuela. Retrieved from https://anoncandanga.com/tag/op-venezuela/ [accessed 03.09.2021].

Venette, S.J. (2003). Risk communication in a High Reliability Organization: APHIS PPQ's inclusion of risk in decision making. Faculty of the of Agriculture and Applied Science, North Dakota State University, Fargo [PhD thesis].

Viktorov, I., Abramov, A. (2020). The 2014–15 Financial Crisis in Russia and the Foundations of Weak Monetary Power Autonomy in the International Political Economy. New Political Economy, 25, 4, 487–510.

Zetter, K. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. Wired, March.

Zumbrun, J. (2020). Coronavirus Slump Is Worst Since Great Depression. Will It Be as Painful?. The Wall Street Journal, 10 May. Retrieved from https://www.wsj.com/articles/coronavirus-slump-is-worst-since-great-depression-will-it-be-as-painful-11589115601 [accessed 03.09.2021].

GLOBALNE KRYZYSY I ATAKI NA CYBERBEZPIECZEŃSTWO – ANALIZA PODCZAS PANDEMII COVID-19

STRESZCZENIE

Pandemia COVID-19 dotknęła wszystkie narody w różnych wymiarach – zarówno gospodarczym, jak i społecznym. Nowa normalność jako zachowania społeczne podyktowane nałożonymi ograniczeniami podtrzymała interakcje online, co umożliwiło zwiększenie zakresu cyberataków. Artykuł ma na celu analizę cyberataków przeprowadzanych podczas pandemii COVID-19, począwszy od serii wydarzeń międzynarodowych, takich jak kryzys w Wenezueli czy na Ukrainie. Częścią tego badania jest ilościowa analiza wyników uzyskanych z przeglądu zasobów bazy Scopus. W tej części, oprócz najważniejszych autorów i użytych słów kluczowych, starano się ustalić, czy kraje będące głównymi celami cyberataków są również zaangażowane w badanie cyberbezpieczeństwa podczas pandemii. Cyberataki są analizowane pod kątem motywacji i celów atakujących. Wskazano również kolejne kierunki badań w tym zakresie.

Słowa kluczowe: cyberataki, kryzysy, koronawirus, COVID-19, cyberprzestępczość, haktywizm