Estimation of the Key Segments of the Cyber Crime Economics

Serghei Ohrimenco
Laboratory of Information Security
Academy of Economic Studies of Moldova
Chisinau, Moldova
osa@ase.md

Grigori Borta
Product Management
FusionWorks
Chisinau, Moldova
grigori.borta@gmail.com

Valeriu Cernei
Partner, IT Audit & Advisory
BSD Management SRL
Chisinau, Moldova
valeriu.cernei@bsd.md

2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) | 978-1-6654-0682-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/PICST54195.2021.9772165

***Abstract*—Our everyday world is rapidly changing with the help of digital transformation and is increasingly dependent on information technology, and because of that our society needs to be prepared for new challenges and threats that come with the change. The composition of the latter is constantly shifting due to the development and improvement of computer technology, software, and methods for collecting, processing, and storing information and data. In these conditions, the relevance of scientific works on topics related to research in the field of cybercrime as an economic phenomenon increases drastically. The digital transformation of all aspects of daily activity turns the user's devices into the target of attacks aimed at taking possession of their private information (accounts, banking details, etc.) and recently even the devices' computing power. The authors see an immense necessity in studying of shadow (criminal) business models based on the development, debugging, and commercial distribution of criminal software.**

Keywords—second economics; information technology; security threats; shadow digital economics; information security

I. INTRODUCTION

In the context of rapid digitalization of all aspects of human life and society, insufficient attention is paid to the formation of latent negative trends, in which the shadow digital economy and cybercriminals play a special role. That is why, with the widespread introduction of the latest information technologies into the everyday life of the society, a new branch of knowledge has arisen - the shadow digital economy (SDE), which combines activities to promote products and services with a "shadow" focus [7]. We define the digital shadow economy as "all illegal and hidden products and services that use information technology. The most important economic elements of this area are the following: illegal economic relations, illegal activities associated with the production, distribution and use of prohibited products and services" [16].

Experts from the leading information company in the field of confronting the shadow digital economy, Digital Shadows, have identified the main categories of attackers who have a motive for abusing and using the labor of remote employees [17-19]. These include:

- organized crime: cybercrime groups have the capabilities and skills to launch targeted attacks against end-user telecommuters. The use of personal devices with fewer security and control measures makes custom applications more attractive for such operations. Access to corporate services and resources, even from the end user's own devices, makes the goal more attractive since the likelihood of unauthorized access is significantly increased.

- scammers: There has been an increase in fraudulent attempts due to the COVID-19 outbreak. They are likely to be especially effective against employees who are not used to working on personal and / or mobile devices.

- malicious insiders: those users who are not used to working remotely may face problems due to accidental disclosure of confidential data, errors in file sharing, etc.

- hacktivists: phishing attacks will continue to evolve, especially now that the end user is more vulnerable on the Internet.

The President of the European Commission U. von der Leyen, speaking in January 2021 at the World Economic Forum in Davos, underlining the existing problems, from climate change to high technologies and the impact of COVID-19, recalled that a year ago in Davos, they intensively discussed digitalization processes, but the pandemic has accelerated these processes and in order to be successful it is necessary to pay attention to the "dark side" of the digital world [21]. All the above served as the basis for this research.

II. LITERATURE OVERVIEW

Most scientific research related to SDE starts with Shadow IT. One of the latest and most comprehensive literature reviews on Shadow IT is the work of a team of authors from Serbia and Germany [1, 2]. This publication continues the tradition of compiling literary reviews on the problems of shadow digital technologies.

Research titled "Shadow IT – A Systematic Literature Review" [2] notes that "Shadow IT describes the autonomous development / procurement or management of software, hardware, or IT services (incl. SaaS, PaaS, IaaS)

978-1-6654-0682-6/21/$31.00 ©2021 IEEE

by business units (BUs), that is, individual users, business workgroups, departments, or divisions, without alignment with the IT organization. As Software-as-a-Service (SaaS) applications have become increasingly quick and easy to use, employees can now download solutions onto their workstations to help them get the job done. However, many are using these applications with little regard for security. It's not surprising then that a 2019 Forbes Insights survey titled "Perception Gaps in Cyber Resilience: Where Are Your Blind Spots?" found that more than one in five organizations experienced a cyber incident originating from an unauthorized — or "shadow" — IT resource" [3]. Among others, the following threats are: Social Engineering Attack, Cloud Crypto mining, Crypto jacking Attack, Ransomware.

Ransomware is analyzed as a foundation for modern cybercrime in "Ransomware, Inc: the Rise of Targeted Ransomware Crime Syndicates" [4]. The research notes that Ransomware, which rakes in a cool $1 Billion per year for its operators, claims a new victim every 11 seconds. It is also important to note the top 3 attack vectors used in the deployment of Ransomware are two predominant tactics, phishing emails and remote desktop protocol (RDP) services opened to the internet. With the COVID-19 pandemic, RDP has increasingly been opened more so now than ever to employees needing to work from home who still need to access intranet resources for companies.

The research titled "The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War" [5] notes that the second economy is at risk. It is evident that the magnitude and prevalence of cybersecurity threats in our lives is increasing. In 2006, McAfee Labs counted an average of 25 threats a day; by 2016, the number was more than 400,000, or more than 300 threats per minute. New malware alone is up 60 percent, there has been a 30 percent increase in targeted attacks, and a billion personal records are stolen every year. As it has been for more than 30 years, cybersecurity is the very definition of dynamic. The authors of this paper find it important to underline the following statement from the research: "Today, the second economy refers to the vast and interconnected set of digital systems that move alongside or serve as underpinnings for our first economy. Billions of IP (Internet Protocol)-enabled sensors are like oxygen in the always on, always connected world. Through the proliferation of smart devices in this new second economy, transactions occur instantaneously and globally, often with no direct human involvement."

We would also like to separate the research on applied information security into its own category: Artificial Intelligence and Blockchain for Cybersecurity Applications [24], New Cooperation Portfolio for Defense [25], Blockchain for Cybersecurity and Privacy [26], Business Models for Innovation, Digital Transformation, and Analytics [27], Countering Cyber Threats to Financial Institutions [28], Political and Economic Implications for Cyber Terrorism [29], Threats and Responses for Government and Business [30] and others.

III. Research Methodology

Effective cybersecurity is very difficult. Several organizations, based on wide professional input, have developed best practice types of documents as well as standards for implementing and evaluating cybersecurity. There are persistent reports of cyberspace operations in the media. The confrontation is carried out at several levels: the state against the state, commercial structures against commercial structures, single users against higher levels. The state-on-state cyber operations revealed in the media include those by the United States and Iran against each other; Israel and Iran against each other; Russia against Estonia, Georgia and Ukraine; and Chinese attempts to steal intellectual property on an industrial scale. A Russian cyber operation against the US in late 2020, the 'SolarWinds hack', has also been prominent. There have been operations by Iran against Saudi Arabia, by North Korea against Sony Pictures and the global banking system, and by the US, the UK, and Australia against the Islamic State (also known as ISIS or ISIL). Some operations have been conducted in an unrestrained manner, resulting in many unintended victims [31].

In short, cyberspace has become, perhaps inevitably, a key and risky new environment for statecraft and competition between states in the twenty-first century. It has also become a major, and arguably the largest domain of organized crime. There are no reliable estimates of the costs of cyber-crime at a national level:

- It is possible to document lower-end estimates of certain types of cyber-crime, such as credit-card fraud.
- but such sub-categories cannot capture the full range of economic costs from the many types of cyber-crime that extend beyond direct losses, for example by causing reputational damage or degradation of share value.

Since 2017 there has been a surge in reported losses from ransomware (malware that prevents access to critical data until the required ransom amount is paid), which have totaled tens of billions of dollars. The damage done by the various types of cyber-crime has inevitably led to a new world of litigation, regulatory fines, and insurance claims.

Thus, from the point of view of the research methodology, the focus was on developing a common approach to identifying the main segments of SDE and their contribution to the formation of the cost of losses from cybercrime.

States and firms are therefore trying to mitigate the risks that cyber threats pose to their digital economies, critical national infrastructure, and citizens by making considerable investment in protective cyber-security capabilities. More fundamentally, states have realized the degree to which their economic prosperity, as well as their national security and geostrategic influence, is dependent on their management of cyber risks. The huge surge in the number of people working digitally from home because of COVID-19 has had obvious implications for cyber security, with a spike in malign cyber activity.

Available statistical data published by leading manufacturers of computer and communication equipment, software, companies working in the field of information security, as well as the media were used in the implementation of this study.

IV. Analysis

The processes of digital transformation of the economy (for example, the implementation of the Industry 4.0 concept) have generated new threats: - attacks are becoming more sophisticated due to automation and the use of artificial intelligence and machine learning methods; - connection of a huge number of new unprotected devices (the industrial Internet or the Internet of things, as a data transfer network between physical objects that are equipped with built-in means and technologies for interacting with each other or with the external environment). Hackers use devices such as video cameras, coffee machines, etc. to breach the network; - as a result, the number of targets for attacks increases sharply. In the process of researching the main products and services of criminal orientation related to SDE, the following main and relevant segments were identified: cyber weapons, as the concentration of all the achievements of information and communication technologies at the level of counteraction between states; targeted attacks and APT groups; attacks on crypto exchanges, and identity theft. But one should not ignore the well-known attack tools on the resources of information and communication systems: web attacks, crypto jacking, email attacks, malware, ransomware, mobile malware, etc.

Cyberweapons. Cyber weapons are malicious software used for military or intelligence purposes. Recently, more and more cases of such software use have surfaced. One of the main characteristics of such attacks is a narrow focus, in contrast to cybercriminals who seek to infect as many victims as possible. Most often, such developments are sponsored or carried out by government agencies. The most prominent examples of such software are Stuxnet, Flame, Duqu, Gauss. Zero-day vulnerabilities are almost always exploited in such malware. Among the countries that have officially announced the presence of special units, whose activities are related not only to cyber defense, but also to cyber-attacks, are the following: USA, UK, Russian Federation, France, Germany, Estonia, Iran, Israel, South and North Korea, China, Australia, and some others. With the qualitative and quantitative growth of cyber threats, cybersecurity spending is constantly increasing (including spending on firewalls and threat analysis) by governments and the private sector, and it is estimated [32] that the cost is approaching 0.1% of global GDP. Some researchers argue that the current risks and costs associated with cloud technology and 5G outweigh the benefits of digitalization. Cybersecurity costs are on the rise. For example, according to the Center for Strategic and International Studies (CSIS, https://www.csis.org), in 2014, global spending on cybersecurity amounted to $575 billion. (or 0.8% of world GDP). For the European Union, the cost is estimated at 0.41% of GDP or $55 billion. per year [33,35]. In our opinion, cyber espionage is an integral part of cyber weapons. Cyber espionage is very costly for the European Union - as a result of such actions - 55 billion euros are lost annually; 289,000 jobs are at risk. Such significant losses will increase with the expansion of digitalization processes (5G generation, Industry 4.0), according to forecasts, 26 million new devices are expected to appear on the network. Naturally, it can be assumed that attacks on information systems and resources will increase, and their composition and number will change.

Targeted attacks. Let's analyze the meaning of this term. Information security professionals have different interpretations of the term advanced persistent threat (APT). Options include: “extended persistent threats”; “Advanced”, “developed”, “complex”, and “targeted” threats. Positive Technologies experts define APT as a well-organized, carefully planned cyberattack aimed at a specific company or an entire industry. During the event, an attacker gains unauthorized access to the network, becomes entrenched in the infrastructure, and remains unnoticed for a long time. These attacks, as a rule, are behind APT groups with significant financial resources and technical capabilities [34]. Consider the data characterizing the composition and activities of APT groups available on the MITER ATT @ CK (attack.mitre.org) and Thailand Computer Emergency Response Team (apt.thaicert.or.th) websites. The ATT & CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. The first database provides extensive information on the techniques and resources used that can be used by software developers and information security professionals. The second database is for reference and provides information on APT groups. As of June 16, 2021, 370 groups were recorded in total (of which 286 ART, 45 others and 39 unknown), with the following data being highlighted: total group aliases - 961, total operations 1647, total counter operations 104, unique source countries 28, unique victim countries 168, unique victim sectors 42, unique tools 1540, total tool aliases 2278, unique external references 6037. The statistics on the countries of origin of these groups are interesting: China - 115, Russia - 46, Iran - 34, North Korea - 10, USA - 8, India - 6, Turkey - 4, etc. Top 28 victim countries include USA - 146, UK - 98, Russia - 86, Germany - 79. The breakdown for victim sectors is represented in TABLE I.

TABLE I. Top 10 Victim sectors

Nr.	Victim	Incidents
1	Government	152
2	Defense	93
3	Financial	84
4	Energy	66
5	Media	59
6	Telecommunications	59
7	Education	52
8	Healthcare	46
9	Manufacturing	39
10	High-Tech	32

Source: https://bit.ly/3nacrvA

Attacks on crypto exchanges. A relatively new area of cybercriminal activity is the attack on cryptocurrency exchanges, theft of cryptocurrencies and money laundering with their help. The high market capitalization of certain cryptocurrencies attracts cyber fraudsters. An additional area of activity is the attacks on crypto exchanges. Specialists analyzed attacks on cryptocurrency exchanges over the past two years and identified total losses of $882

million [34, 36] The report indicates that in 2019 cryptocurrency exchanges became a new target for aggressive hacker groups and their efforts shifted from attacks to commercial banks. Not only crypto exchanges, but also cryptocurrency companies that organize the launch of the ICO, raise funds and provide tokens for sale to private investors are targeted by attacks. Experts note that cybercriminals employ the same tools used in attacks on commercial banks, orienting them towards hacking crypto exchanges, electronic wallets and gaining access to personal user data. Another important feature of cryptocurrencies should be highlighted - taking bribes with cryptocurrencies has been very popular among officials and lawyers for several years. Such transactions can be tracked, but neither in fact nor legally can they be tied to a person. That is, it is impossible to obtain formal evidence for the investigation and the court a priori. Moreover, cryptocurrency immediately turns out to be outside the state, and it is almost impossible to confiscate it. But in the presence of the Internet, they always remain at the disposal of the owner. This is a kind of airbag for detainees.

Personal data theft. Identity theft includes activities such as intercepting identities, credit cards, usernames, and passwords. The GDPR - General Data Protection Regulation), which has direct effect in all 28 EU countries, is intended to replace the framework Directive on the protection of personal data 95/46 / EC of October 24, 1995. The new regulation gives EU residents full control over their personal data. In particular, the liability for violation of the rules for the processing of personal data is being tightened: according to the GDPR, fines reach 20 million euros, or 4% of the company's annual global income. There is no doubt that hackers are scrutinizing the new regulations for bottlenecks and preparing surprises for the information security service. The “Reverse extortion” scheme is based on the use of a data encryption mechanism from the user (encryption program) and extortion of funds (in various cryptocurrencies, mainly in bitcoins) to recover data. Such actions are described in detail in the specialized literature [37]. But the sequence of actions is somewhat different from the extortion technology. The sequence of this kind of attack is as follows:

- a hacker penetrates the network by any available means to obtain and collect personal user data, which is protected by the GDPR;
- the acquired data is threatened to be published, which will lead to a violation of the GDPR regulation and make the organization responsible for the violation of this regulation. Consequently, the organization faces a huge fine, which significantly exceeds the requested ransom.

V. Discussion

Over the past few years, cybercrime has stepped over many technical and software barriers and moved from a highly specialized niche into one of the most significant strategic risks facing the world today. The development of digital forms of fraud (cryptocurrencies and ICOs, infection with ransomware viruses, installing applications on a smartphone, phishing, etc.) largely contributes to the development of technical progress.

A separate very important problem is the study of the economic foundations of cybercrime. In this regard, the data on the economy of cybercrime looks staggering against the background of the collected statistics on the activities of the SDE. According to a study by Bromium, cybercrime was estimated at $1.5 trillion in 2018 [39]. This was the first study of its kind to examine the "dynamics of cybercrime" in the context of revenue stream and profit distribution. The study identified new criminal platforms and a thriving cybercrime economy that is self-sufficient and blurs the boundaries of legality. Gregory Webb, CEO of Bromium, commented on the study's findings as follows: “It's shocking how widespread and profitable cybercrime has become. The model of crime is to create malware and deliver it to cybercriminals as easily as shopping online. Not only is it very easy to gain access to the tools, services, and expertise of cybercriminals, this means that businesses and governments will face more sophisticated, costly, and destructive attacks as the network is profit-driven and gains traction. We cannot solve this problem using old thinking or outdated technology. The time has come for new approaches.” The report is accompanied by a summary table that provides data on the annual income generated from the implementation of selected cybercrimes, as represented in TABLE II.

TABLE II. Approximate yearly income from cybercrime in 2018 (USD, billion)

Nr.	Crime category	Yearly income
1	Illegal online markets	860
2	IP theft, commercial espionage	500
3	Personal data trade	160
4	Cyber fraud, CaaS (Cybercrime-as-a-Service)	1,6
5	Extortionist malware	1,0

Source: Jason Williams. (2019). Cybercrime as an Economy. https://bit.ly/38MlSc2

This article makes an interesting assumption that if cybercrime, from an economic point of view, were a sovereign country, it would rank 13th in the world in terms of GDP. The total income, according to approximate data, is equal to $ 1.5 trillion and includes: $860 billion in actions in illegal, criminal online markets; $500 billion in theft of trade secrets, IP; $160 billion in data trading; $1.6 billion in cyber fraud and cyber-crime-as-a-service; $1 billion in ransomware. The report points out that cybercrime operates at multiple levels, with some large “corporate”-style trades bringing in more than 1 billion and “small and medium-sized”-type orders ranging from $30,000 to $50,000. A wide range of economic agents with their deep specialization (from the development of specific malicious software mechanisms to the rental of ready-made bot systems, etc.), economic relations, and other economic factors contribute to the generation, support, and confirmation of high income on an unprecedented scale.

VI. Conclusion

The widespread prevalence of SDE elements is likely to seriously slow down the economic recovery of both leading and developing countries after the COVID-19 pandemic. What are the forecasts of leading research and consulting companies [39] in the field of shadow IT? According to forecasts of a research and consulting company, Gartner by 2020, 30% of violations in the information sphere will be caused by shadow IT. A report from consulting firm Frost

& Sullivan says that more than 80% of respondents admit to using unapproved (shadow) applications in their work. Research conducted by IDG shows that the spread of shadow IT is growing by 5% annually and accounts for about 30% of enterprise IT budgets. Gartner researchers have shown that Shadow IT accounts for 30 to 40% of total IT spending. Everest Group studies have recorded that the share of shadow IT is 50% or more in IT spending in general. It should be noted that any technology that is at the stage of development and the beginning of implementation carries new security threats. They should be grouped into three groups: technical, social, and threats to national security. This work was devoted to considering only the threats of the first group. The other two groups, as well as the associated risks, remain to be explored based on the work done.

REFERENCES

[1] A. Kopper, S. Klotz, M. Westner, S. Strahringer (2019). Practitioner Perceptions on Shadow-IT and Business-Managed IT. *Journal of Information Technology Management*, Vol. XXX, Number 4, 2019.

[2] L. Raković, M. Sakal, P. Matković, M. Marić (2020). Shadow IT – A Systematic Literature Review. *Information Technology and Control,* 49(1), 144-160.

[3] Top 50 Security Threats (2020), https://splk.it/3BN70qd

[4] Alissa Valentina Knight (2020). Ransomware, Inc: the Rise of Targeted Ransomware Crime Syndicates. https://bit.ly/3BRURR5

[5] S. Grobman, A. Cerra (2016). The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War, https://doi.org/10.1007/978-1-4842-2229-4

[6] K.-Ch. Li, X. Chen, W. Susilo (2019). Advances in Cyber Security: Principles, Techniques, and Applications. Springer, https://doi.org/10.1007/978-981-13-1483-4

[7] S. Ohrimenco, G. Borta (2020). Chapter 8. Challenges for Digital Transformation in the Manufacturing Industry. Socio-Economic Development. Interdisciplinary Ecosystems Perspective. The Jubilee Book Dedicated to Professor Kazimierz Zielinski. Cracow University of Economics, 2020, Poland, Cracow. 330 p.

[8] I. Winkler, Araceli Treu Gomes (2017). Advanced Persistent Security. A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies. Elsevier Inc. p. 236.

[9] Cyber-Security Threats, Actors, and Dynamic Mitigation (2021). Edited by Nicholas Kolokotronis and Stavros Shiaeles. Taylor & Francis Group, LLC. P.392.

[10] T. Steffens (2020). Attribution of Advanced Persistent Threats. How to Identify the Actors Behind Cyber-Espionage. Springer-Verlag. p. 207, https://doi.org/10.1007/978-3-662-61313-9

[11] M. Ryan (2021). Ransomware Revolution: The Rise of a Prodigious Cyber Threat. Springer. P. 164, https://doi.org/10.1007/978-3-030-66583-8

[12] Marie de Fréminville (2020). Cybersecurity and Decision Makers. Data Security and Digital Trust. ISTE Ltd. P. 211.

[13] Dominique Augey, Marina Alcaraz (2019). Digital Information Ecosystems. Smart Press. P. 238.

[14] S. Sedkaoui, M. Khelfaoui (2020). Sharing Economy and Big Data Analytics. ISTE Ltd. P. 259.

[15] Dietmar P. F. Möller (2020). Cybersecurity in Digital Transformation. Scope and Applications. Springer, https://doi.org/10.1007/978-3-030-60570-4.

[16] Divya Gupta Chowdhry, R. Verma, M. Mathur (ed.) (2020). The Evolution of Business in the Cyber Age. Digital Transformation, Threats, and Security. Apple Academic Press Inc.

[17] M. Fuentes (2020). Trading in the Dark: An Investigation into the Current Condition of Underground Markets and Cyber-Criminal Forums, https://bit.ly/3DTIWUA

[18] V. Kropotov, R. McArdle, F. Yarochkin. (2020). Commodified Cybercrime Infra-structure: Exploring the Underground Services Market for Cybercriminals, https://bit.ly/38Su4Hz

[19] V. Kropotov, R. McArdle, F. Yarochkin. (2020). The Hacker Infrastructure and Underground Hosting: Services Used by Criminals, https://bit.ly/3n6IFYj.

[20] 2020 Internet Crime Report. (2020), https://bit.ly/3jNV8Ow.

[21] von der Leyen U., Ursula von der Leyen's message to Davos Agenda: Full transcript. (2021), https://bit.ly/3h9CtLw.

[22] B. Middleton (2017). A History of Cyber Security Attacks. 1980 to Present. Taylor & Francis Group.

[23] T. Z. Ahram, D. Nicholson. (2019). 9th International Conference on Applied Human Factors and Ergonomics and the Affiliated Conferences. Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, held on July 21–25, 2018, in Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA.

[24] Y. Maleh, Y. Baddi, M. Alazab, L. Tawalbeh, I. Romdhani (2021). Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Springer, https://doi.org/10.1007/978-3-030-74575-2.

[25] BETTER TOGETHER. Towards a new cooperation portfolio for defense (2016). The Hague Centre for Strategic Studies.

[26] Y. Maleh, M. Shojafar, M. Alazab, I. Romdhani. (2020). Blockchain for Cybersecurity and Privacy. Taylor & Francis Group, LLC.

[27] I. Otola, M. Grabowska. (2021). Business Models. Innovation, Digital Transformation, and Analytics.

[28] P.-L. Pomerleau, D. L. Lowery (2020). Countering Cyber Threats to Financial Institutions. A Private and Public Partnership Approach to Critical Infrastructure Protection. Springer, https://doi.org/10.1007/978-3-030-54054-8.

[29] N. Kolokotronis, S. Shiaeles. (Ed). (2021). Cyber-Security Threats, Actors, and Dynamic Mitigation. Taylor & Francis Group, LLC.

[30] J. Caravelli, N. Jones (2019). Threats and Responses for Government and Business. ABC-CLIO, LLC.

[31] Cyber Capabilities and National Power: A Net Assessment (2021). The International Institute for Strategic Studies, https://bit.ly/3zSzrCv.

[32] Lee-Makiyama H. Stealing Thunder. ECIPE, No. 2/18. (2018), https://bit.ly/38FuJvs.

[33] A Lloyd's emerging risk report (2017), https://bit.ly/3rtjizK.

[34] Report: Cryptocurrency Exchanges Lost $882 Million to Hackers. (2018), https://bit.ly/37QWoKV.

[35] Leslie F. Sikos, Kim-Kwang, Raymond Choo (2020). Data Science in Cybersecurity and Cyberthreat Intelligence. Springer Nature Switzerland AG.

[36] Crypto Crime Report. Decoding increasingly sophisticated hacks, darknet markets, and scams. (2019), https://bit.ly/34LqPQL.

[37] Stephen Willis (2019). Is GDPR the new hacker scare tactic? https://bit.ly/38KCa50.

[38] Jason Williams. (2019). Cybercrime as an Economy, https://bit.ly/3jRfciY.

[39] Short Guide on Shadow it Digital Footprinting, Continuous Monitoring &digital risk protection. (2019), https://bit.ly/2WXbpHW.

[40] S. Ohrimenco, G. Borta, T. Bochulia (2019). Shadow of Digital Economics. 2019 International Scientific-Practical Conference "Problems of Infocommunications. Science and Technology". PIC S&T'2019 October 8-11, 2019 Kyiv, Ukraine (2019).