MEST Journal
DOI 10.12709/mest.09.09.01.17

THE NATURE OF SHADOW DIGITAL ECONOMICS

Serghei Ohrimenco
Academy of Economic Studies of Moldova, Laboratory of Information Security, Chisinau, Moldova

Grigori Borta
Academy of Economic Studies of Moldova, Laboratory of Information Security, Chisinau, Moldova

JEL Category: **D84, O17, P37**

Abstract

The purpose of this paper is to analyze, discuss, and develop a study of world universal digitalization processes as well as challenges and threats, and develop an approach to defining the shadow digital economy. Along with huge innovative achievements, digitalization processes are accompanied by the formation of a digital economy and the growth of illegal activities. Digital economy implies total globalization, creates an ultra-high competitive environment, provides a new quality of life, business, and public services. At the same time, many traditional areas of activity are being destroyed. In addition to understandable achievements, it is necessary to analyze new obvious and hidden threats that digitalization processes carry. The analysis shows the causes and factors of the emergence and functioning of the new segment in the shadow economy. The approaches to the definition of this category and its content are discussed. A classification of criminal-oriented products and services that are the basis of a highly profitable illegal business has been proposed. The problem of confrontation with Shadow Digital Economics acquires particular urgency in the face of the emergence of new overt and hidden threats to the individuals, society, and the state. The main components of the digitalization process are analyzed. Conclusions are drawn about the development of shadow digitalization processes and the formation of a shadow digital economy, which is directly related to cybersecurity.

Keywords: *digital economy; shadow digital economy; threats to the digital economy; information security; cybersecurity*

1 INTRODUCTION

The problems of the digitalization of the economy are being studied by many scientists in most countries of the world. Achievements in the manufacturing sector, in everyday life, are being noted everywhere. However, at the same time,

The address of the corresponding author:
Serghei Ohrimenco
osa@ase.md

with achievements, there has been a rapid growth in criminal activities related to the use of information and communication technologies. The analysis of scientific publications, statistical data, analytical reports of leading information security firms allows us to speak with confidence about the formation of a new sector of the shadow economy - the shadow digital economy (SDE). The accumulated experience in the analysis of the "achievements" of SDE (Ohrimenco & Borta, Informal Economics of Information Threats., 2013) (Ohrimenco & Borta, Social Aspects of Shadow Information Economics., 2014) (Ohrimenco, Borta, & Bochulia, Shadow of Digital Economics., 2019) (Okhrimenko & Borte, 2012), allows us to put forward the assumption that this type of activity is directed against the individual, society and the state and combines many manifestations - from developing software abuses to organizing attacks on crypto exchanges with fraudulent withdrawal of cryptocurrencies.

The limited scope of the article does not allow considering all the problems of confrontation with the manifestations of SDE. Therefore, the main attention of the authors was directed to the analysis of literature sources, development of definitions, and analysis of the latest developments in the field of cybersecurity.

2 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 the University of Novi Sad, Faculty of Economics in Subotica, Department of Business Informatics and Quantitative Methods (Raković, Sakal, Matković, & Marić, 2020). This publication continues the tradition of compiling literary reviews on the problems of shadow digital technologies. Another significant review of approaches to the definition of the studied category is the work of Friedrich Schneider, who has undoubted superiority in the field of research of the shadow economy in developed and developing countries in collaboration with Rita Remeikiene, and Ligita Gaspareniene. The given set of scientific works allows us to suggest that they form the basis of a new scientific field of research (Remeikiene, Gaspareniene, & Schneider, The definition of digital shadow economy., 2017) (Gaspareniene & Remeikiene, Digital Shadow Economy: a Critical Review of the Literature., 2015) (Gaspareniene L. , Remeikiene, Ginevicius, & Skuka, 2016) (Gaspareniene, Remeikiene, & Scneider) (Wu & Schneider, 2019) (Medina & Schneider, Shadow Economies Around the World: What Did We Learn Over the Last 20 Years?, 2018) (Medina & Schneider, Shadow Economies around the World: New Results for 158 Countries over 1991-2015., 2017) (Medina & Schneider, Shedding Light on the Shadow Economy: A Global Data-base and the Interaction with the Official One., 2019) (Remeikiene, Gaspareniene, & Schneider, Concept, motives and channels of digital shadow economy: consumers' attitude., 2017) (Schneider F. , Implausible Large Differences of the Size of the Underground Economies in Highly Developed European Countries?, 2017).

Along with the cited works, it should be noted that the first authors who used the category "shadow information economy" were the authors of the monograph "Market of Information Services and Products". In chapter 5 of the monograph (Rodionov, Gilyarevskiy, Tsvetkova, & Zalayev, 2002), paragraph 5.2.4 "Shadow information economy" is highlighted, which begins with the main premise of our study - "Consideration of the shadow sector of the information economy and information activity is required to assess its volume and the potential damage it causes." At the same time, it is pointed out that the real losses of the Russian budget due to the shadow nature of private business in the field of information services and products are not so great and this type of shadow business is one of the few that deserves to be removed from the shadows by introducing a tax-free regime to support its development. Thus, in Russia, a certain part of information activity and the market of information services and products are in the shadow. The shadow sector does not have a criminal basis and is associated with low efficiency of information activities, the level of development of which does not allow not only to finance growth but also to carry out simple reproduction subject to payment of all taxes. Attention should be paid to the allocation by the authors of a part of the market for information services and products, which is in the shadow and the absence of a criminal basis. Over the past time, the picture has changed dramatically - not only a part of the market for information products

and services has become clandestine and criminal, but also a whole shadow industry has been formed that brings high profits.

The works of the authors Ligita Gaspareniene, Rita Remeikiene, Friedrich Schneider (Gaspareniene & Remeikiene, Digital Shadow Economy: a Critical Review of the Literature., 2015) (Gaspareniene, Remeikiene, & Navickas, The concept of digital shadow economy: consumer's attitude, 2015) take a different approach, basing on the processes of global digitalization (digitization) of the economy. The authors propose the following definition of shadow digital economy: "illegal activity in cyberspace, which allows generating illegal flows of money for illegal service providers and sellers, as well as depriving the income of legal service providers and sellers" (Schneider & Haigner, 2018) (Schneider F. , Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism?).

The work of researchers from Brazil analyzed the approaches to the definition of Shadow IT (Mallmann, Macada, & Oliveira), the impact of shadow use of IT, and other aspects. Shadow IT is defined 1) as any hardware, software, or services built, introduced, and used to work without explicit approval or even knowledge of the organization: 2) shadow IT distinguishes from closely related concepts such as workaround, bring-your-own, and IT consumerization; 3) individual shadow IT usage as 'the voluntary usage of any IT resource violating injunctive IT norms at the workplace as a reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization'. Shadow IT type classification is also included here, which includes the following:

1. Cloud services (Internet-based software and software as a service, such as communication and content sharing software to communicate and share work information with coworkers, clients, and partners, among other cloud services that are not authorized or is unknown by the IT department. These systems are also called mobile shadow IT once it can be accessed outside the workplace and examples of these systems are WhatsApp, Facebook, Skype for Web, Dropbox, Google Apps, and so on).
2. Self-made solutions (Solutions developed by employees on the company's computers to perform their work tasks. For example, an excel spreadsheet or an application developed by employees).
3. Self-installed (Software installed by employees to perform their work tasks, on the company's computers. For example, downloaded a freely available software on the web).
4. Self-acquired devices (Devices such as notebooks, servers, routers, printers, or other peripherals purchased by employees. These devices are purchased directly from retail rather than being ordered through the official catalog of the IT department. It includes the use of applications in the employee's devices at the workplace. For instance, smartphones, notebooks, tablets, and so on.).

The authors completely agree with the opinion expressed in the work (Levene, 2019) that the risk of malware is underestimated in terms of possible losses. The ability of criminal structures to create, modernize, and use malware to undermine a business has been sufficiently studied in terms of effectiveness, scale, and cost. In most cases, business owners prefer to keep silent about the attacks against them, losses and recovery costs (if this was possible).

3 OBTAINED RESULTS

This section goes into the results obtained in the process of the research: definitions of shadow information technologies are offered.

The starting point of our study is "shadow IT" (Shadow IT, Stealth IT, or Client IT). Various definitions are used, in particular, "Shadow IT are all the third-party IT solutions, including cloud applications and services that are not controlled by the corporate IT department." Cloud solutions, which represent a large part of Shadow IT, can replace an employee function or an entire department, and become part of the enterprise services. Statistics of the actual use of cloud solutions in the corporate sector are amazing: there are hundreds of solutions, and not dozens, like many IT and information security experts believed.

However, from a security point of view, cloud applications and services are a "blind spot" (Oreshkina, 2017).

1. Shadow IT refers to IT devices, software, and services outside the ownership or control of IT organizations (Gartner).
2. Shadow IT represents all the hardware, software, or any other solutions used by employees within the organizational ecosystem that have not received official approval from the IT department (Silic & Back, 2014).
3. Business units and users autonomously implement IT solutions that are not embedded in the organizational management of IT services. This increasingly growing phenomenon is called Shadow IT (Zimmermann & Rentrop, 2014).
4. Shadow IT is defined as a set of IT tools used to perform IT functions, but not part of the main IT organization.
5. The authors define Shadow IT as an IT solution used by employees to perform their work tasks without the approval and official support of the IT department (Mallmann, Macada, & Oliveira, 2016).
6. For example, the so-called Shadow IT is third-party IT solutions that are not controlled by corporate governance. And these are not always clouds, it can be any information systems that are out of sight or control. Shadow IT infrastructure is not always evil, it often arises from "good" motives to optimize legitimate business processes.

Therefore, it must be identified and analyzed, and only if necessary, an alternative is offered. This will help to make the cloud environment controlled, convenient, and secure (Akinin, 2018).

1. Shadow IT is a term used to describe the situation when business units acquire, own, and manage IT without the help of an IT department. IT departments consider shadow IT as inefficient as resources well as a source of risk and see part of their task as constraining its spread (Meier, 2015).
2. Shadow IT is becoming increasingly important as digital methods of work simplify the work of business units creating their own IT solutions.

Previous research on shadow IT systems often used fixed reports of good or evil: they were noted as powerful driving forces for innovation or demonized as missing central management. We present a method for IT managers and architects to enable a more subtle understanding of shadow IT systems concerning their architectural embeddability (Fiirstenau & Hannes, 2014).

1. The term "shadow systems" refers to stand-alone software solutions or extensions of existing solutions that are not developed or controlled by the central IT department (Fiirstenau, Sandner, & Anapliotis, 2016).
2. Shadow IT refers to IT devices, software, and services that are present in the organization but are not serviced by the IT department. They are not registered with the IT department, their state and work are not monitored, moreover, the IT department may not know anything about them.

Accordingly, security policies and regulations also do not apply to them. And this is a serious threat to corporate security. According to the forecast of Gartner, by 2020 a third of successful attacks on information resources of organizations will be performed through Shadow IT (Lesnova, 2019).

Shadow IT is used to describe IT solutions and systems created and applied inside companies and organizations without their authorization. This is considered a vital foundation for technological advancement and innovation because these efforts can become potential prototypes for IT solutions that are approved in the future. Even though these solutions can help in the advancement of IT innovations, they may not conform to the company's requirements in terms of reliability, documentation, control, security, and more (Technopedia, 2020).

Even though these definitions touch upon very important points, in the authors' opinion, some of them lack the depth required to describe the phenomenon of SDE. The analysis of the abovementioned definitions of SDE allows us to identify five main approaches: legal, mathematical, sociopsychological, organizational and managerial, economic, and financial.

1. The legal approach describes this category from the perspective of legal science, focusing on illegal activities.
2. The mathematical approach considers Shadow IT as a model of management of the shadow activity of participants in the information sector with the release of the life cycle of individual products and services, as well as monetization processes.

3. The organizational and managerial approach is to determine SDE from the point of view of the organizational and legal form of interaction between participants in the shadow markets for products and services.
4. The socio-psychological approach analyzes the activities of the participants in terms of irrational economic behavior, attracting a large number of specialists in information and communication technology.
5. The economic and financial approach considers SDE as financial structures that launder money through the use of various frauds based on information and communication technologies in the legal market for goods and services.

Let us formulate the definition of the shadow digital economy, based on its specificity in terms of the production of goods and services, the life cycle of products and services, etc. Thus, SDE is a sector of economic relations that encompasses all types of production and business activities that, by their focus, content, nature, and form, are contrary to the requirements of legislation and are carried out contrary to state regulation of the economy and bypassing control over it.

The basis of the SDE is the shadow business activity, the general features of which are as follows:

1. hidden, latent (secret) character, meaning, the activity that is not registered by the state authorities and is not reflected in the official reporting;
2. coverage of all phases of the process of social reproduction (production, distribution, exchange, and consumption);
3. the parasitic nature of all processes, ranging from the disclosure of the source code of a software product to the monetization of botnets by renting.

A slightly different approach is used in the works of L. Gaspareniene, R. Remeikiene, F. Schneider (Schneider & Haigner, 2018), based on the processes of universal digitalization (digitization) of the economy. In particular, the following definition of the shadow digital economy is proposed: “illegal activity in cyberspace, which allows generating illegal money flows for illegal service providers and vendors, as well as depriving incomes of legal service providers and vendors” (Mallmann, Macada, & Oliveira, 2016). In our opinion, we should agree with the thesis proposed by F. Schneider in a joint article with A. Buen (Schneider, Buehn, & Montenegro, Shadow Economies All over the World, 2010) - researchers trying to measure the volume of the shadow economy face a basic and complex issue - to define this phenomenon. A general definition is used (the authors of the article call this definition a work in progress) - these are all types of unregistered activity that contributed to the gross national product. The proposed narrower definition of the shadow economy includes the following: The shadow economy includes all legally produced goods and services that are deliberately hidden from public authorities for the following reasons:

1. Avoiding taxes (for example, income or value-added tax).
2. Avoiding social security contributions payments.
3. Avoid using certain labor market standards, such as minimum wages, maximum working hours, safety standards, etc.
4. Avoid adherence to certain administrative procedures. Thus, summing up the analysis of existing approaches to the definition of SDE, the authors of this study propose the following definitions:
   a. SDE is a specific domain of economic activity with its inherent structure and system of economic relations. Specificity is defined by illegality, informality, as well as the criminal nature of the economic activity and the concealment of income.
   b. From an economic point of view - a sector of economic relations, covering all types of production and economic activity, which, by their nature, content, nature, and form, contradict the requirements of existing legislation and are carried out contrary to state regulation of the economy and bypassing control over it.
   c. From a technological point of view, SDE is an individual and collective activity that is illegal, associated with the design, development, distribution, support, and use of information and communication technology components, which is hidden from society. Thus, SDE is all illegal and hidden goods and services that use and are

based on information technology. The most important economic elements of this sphere are the following: illegal economic relations, illegal activities related to the production, distribution, and use of prohibited products and services.

Thus, SDE is all illegal and hidden goods and services that use and are based on information technology. The most important economic elements of this sphere are the following: illegal economic relations, illegal activities related to the production, distribution, and use of prohibited products and services. The concept model of SDE is represented in Figure 1.

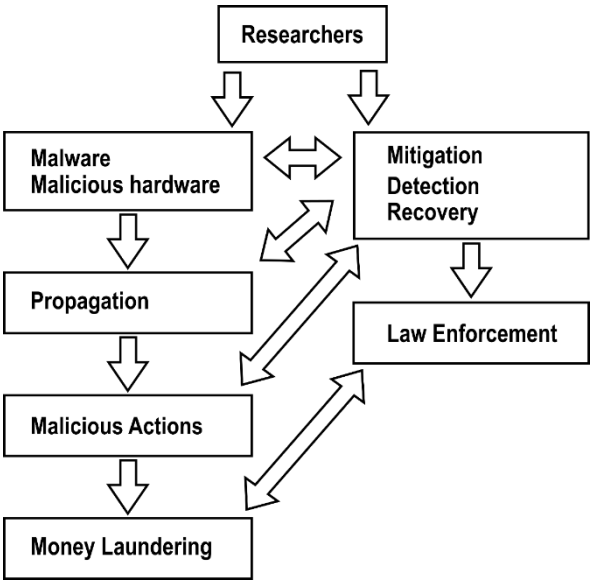

Figure 1. Concept model of SDE.

As a result of the research, it was concluded that the shadow digital economy is forming against the backdrop of the development of global digitalization processes. Let us formulate the definition of the shadow digital economy based on its specificity in terms of the production of products and services, the life cycle of products and services, etc. The following definition of SDE is proposed:

1. the shadow digital economy (SDE) is a sector of economic relations covering all types of industrial and economic activities, which in their direction, content, nature, and form contradict the requirements of the law and are implemented contrary to state regulation of the economy and bypassing control over it. All individual and collective activities that are illegal, associated with the design, development, dissemination, support, and use of components of information and communication technologies, hidden from society are encompassed by the shadow information economy. That is, the shadow information economy is all the illegal and hidden products and services that use and are based on information technology. The following are the most important economic elements of this sphere: illegal economic relations, illegal activities related to the production, distribution, and use of prohibited products and services.
2. Shadow information economy - an activity related to the research, design, production, distribution, support, and use of components of information and communication technologies, hidden from society and the state, outside state control and accounting, and also, most often, illegal. Thus, the reason for the existence of a shadow information economy is the presence of conditions under which it is beneficial to hide their activities or own individual elements.
3. The shadow information economy is all the collective or individual activity that parasitizes in all areas of society, based on the use of information and communication technology components. This type of illegal activity should be considered as a special segment, which is characterized by the following systemic properties: universality, integrity, communication with the external environment, structure, ability to self-organization and continuous development, the presence of a constructive (productive sector) and a destructive (criminal sector) element.

The main conclusion is that the SDE represents a technical, technological, economic basis for cybercrime and combines a set of actions directed against the individual, society, and the state.

Another 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 activity of the SDE. Cybercrime was estimated at $ 1.5 trillion in 2018, according to a study by Bromium. 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 with 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 (Williams, 2019).

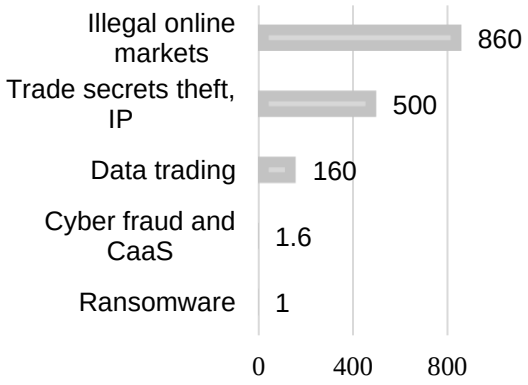

Figure 2. Yearly income from cybercrime in 2018 in billion USD.
Authors based on (Williams 2019).

This article makes an interesting suggestion 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 - actions in illegal online markets;
- $ 500 billion - trade secrets theft, IP;
- $ 160 billion - data trading;
- $ 1.6 billion - cyber fraud and cybercrime as a service;
- $ 1 billion - ransomware.

The report points out that cybercrime operates at multiple levels, with some large “corporate”-style trading operations bringing in over $ 1 billion and “small and medium-sized business” 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 incomes on an unprecedented scale.

Crimeware is a serious business. Developers model their activities following corporate standards to maximize profits. As an example, the emergence of "crimeware-as-a-service" (criminal software as a service) can be considered as a demonstration of its capabilities. For a short period, cybercriminals radically change their toolkits to achieve new results. An additional example is Cryptomining as an operation. The cryptocurrency market peaked at the end of 2017 and began to decline by February 2018. The downward trend in the Bitcoin index directly affected the activity of Cryptomining as an operation, which fell by more than 50% during the year. The statistical correlation between the jumps in the Bitcoin index and the popularity of “Cryptomining as an operation” can be considered as a highly profitable tool for influencing the business.

One more important feature of cryptocurrencies should be highlighted - receiving bribes by cryptocurrencies has been very popular among officials and lawyers for several years. Such transactions can be tracked, but neither actually nor legally can they be tied to a person. That is, formal evidence for the investigation and trial cannot be obtained a priori. Moreover, cryptocurrency immediately appears outside the state, and it is almost impossible to confiscate it. However, with the Internet, they always remain at the disposal of the owner. This is a kind of airbag for detainees.

We consider it possible to refer to the research by RAND Corp., titled Economic Competition in the 21st Century (Shatz, 2020). This report examines various forms of economic competition, including the concept of national competitiveness, competition for markets and investment, the use of economic instruments in areas of international competition, and competition for the nature of the global economic system. The main idea is the

thesis that geopolitical competition using economic instruments can be effective, but the use of such instruments can be very expensive. In any case, the costs of implementing them should be weighed against the benefits obtained. Among other economic instruments for geopolitical competition in the United States, the following stand out: trade policy; investment policy; sanctions; cyber tools; financial help; financial and monetary policy; production and export of energy and goods.

Cyber tools are of particular interest since they can be used to inflict damage (for example, a reference is made to the alleged shutdown of the Ukrainian power grid in 2015), as well as steal intellectual property, technology, and trade secrets.

4 CONCLUSIONS

Cybercrime and SDE are everywhere. Effects of a single criminal attack (for example, DDOS or MIM and others) affect supply chains beyond the realm of cyberspace.

A review of the content (qualitative and quantitative) is required using the following cybersecurity assessment metrics (Daultrey, 2017): Legal (cybercrime laws, regulations, training); Organizational (collection on metrics on cybersecurity, national strategy); Technical (industry standards); Capacity building (training for cybersecurity professionals, public awareness); Cooperation (international, interagency and public-private sector).

5G communication networks, which are just starting to be launched in several countries, by 2028 will hardly cope with the growing volume of data transfer. According to analysts of Bank of America Merrill Lynch, we should expect by this time the next generation networks - 6G. 6G mobile communication technologies may become one of 15 breakthrough technologies that will have a key impact on the global industry in the coming years among other similar breakthrough technologies (quantum computers, Hyperloop, nanosatellites, geoengineering, etc. Analysts believe that 6th generation networks will be able to increase speed up to 400 times higher than 5G, also, the advantages of AI will be used. Based on this, we can assume the expansion of capabilities for implementing various attacks.

A program to improve the warning system about new software abuse and countermeasures is needed. This work should be implemented with state and private institutions, primarily financial and banking activities.

The risk of using malware is underestimated, making protection efforts difficult. This leads to the fact that losses from the impact of criminal software are growing, and countermeasures are taken to reduce the effectiveness of the confrontation. The impact of criminal software is enormous, and if the resistance efforts are not significantly increased, more serious and widespread consequences in terms of coverage and cost may arise.

The growth of criminal software is steady; the frequency of distribution of new species is growing from year to year. Moreover, as a result, criminal software represents a more serious threat to business than targeted attacks on information systems.

The introduction of criminal software is not expensive and does not require much effort on the part of motivated participants, which ensures the optimization of ongoing attacks to achieve profitable goals. The ability to increase responsiveness and change strategies has led to the emergence of increasingly sophisticated and targeted attacks on business programs.

WORKS CITED

Akinin, A. (2018). *Shadow IT. Everyone out of the shadow!* Retrieved from https://bit.ly/3c3eGYS

Daultrey, S. (2017). *Cybercrime. Invisible problems, imperfect solution.* Retrieved from https://bit.ly/2QWks6f

Fiirstenau, D., & Hannes, R. (2014). *Shadow IT Systems: Discerning the Good and the Evil.* Retrieved from https://bit.ly/30tNNaq

Fiirstenau, D., Sandner, M., & Anapliotis, D. (2016). *Why do Shadow Systems Fail? An Expert Study on Determinants of Discontinuation.*

Gartner. (n.d.). *Gartner IT Glossary.* Retrieved from Gartner: https://gtnr.it/2LnuJHl

Gaspareniene, L., & Remeikiene, R. (2015). Digital Shadow Economy: a Critical Review of the Literature. *Mediterranean Journal of Social Sciences. Vol 6, No 6 S5*.

Gaspareniene, L., Remeikiene, R., & Navickas, V. (2015). The concept of digital shadow economy: consumer's attitude. *3rd Global Conference On Business, Economics, Management, And Tourism*.

Gaspareniene, L., Remeikiene, R., & Schneider, F. (n.d.). *The factors of digital shadow consumption.*

Gaspareniene, L., Remeikiene, R., Ginevicius, R., & Skuka, A. (2016). Critical Attitude Towards The Theory Of Digital Shadoweconomy: Literature Review And New Foundations. *Terra Economicus, Vol. 14, No 4.* Retrieved May 3, 2020, from https://bit.ly/2L9wMNn

Lesnova, L. (2019). *Shadow IT: a threat from the shadow.* Retrieved from https://bit.ly/2YqYeOm

Levene, B. (2019). *Crimeware in the Modern Era: A Cost We Cannot Ignore.* Retrieved from https://bit.ly/2WrDSlt

Mallmann, G. L., Macada, A. C., & Oliveira, M. (n.d.). The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users. *Business Information Review 2018, Vol. 35(1) 17–28.* Retrieved May 3, 2020, from https://bit.ly/2SxH5ic

Mallmann, G., Macada, A., & Oliveira, M. (2016). *Can Shadow IT Facilitate Knowledge Sharing in Organizations? An Exploratory Study.*

Medina, L., & Schneider, F. (2017). Shadow Economies around the World: New Results for 158 Countries over 1991-2015. *CESifo Working Paper Series 6430, CESifo Group Munich*.

Medina, L., & Schneider, F. (2018). Shadow Economies Around the World: What Did We Learn Over the Last 20 Years? *IMF Working Papers 18/17, International Monetary Fund*.

Medina, L., & Schneider, F. (2019). Shedding Light on the Shadow Economy: A Global Data-base and the Interaction with the Official One. *CESifo Working Paper Series 7981, CESifo Group Munich.*

Meier, J. (2015). *Every Employee Is a Digital Employee.* Retrieved from https://bit.ly/2Y7N9Sv

Ohrimenco, S., & Borta, G. (2013). Informal Economics of Information Threats. *International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE-2013)*.

Ohrimenco, S., & Borta, G. (2014). Social Aspects of Shadow Information Economics. *4th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE-2014)*.

Ohrimenco, S., Borta, G., & Bochulia, T. (2019). Shadow of Digital Economics. *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T).*

Okhrimenko, S., & Borte, G. (2012). Tenevaya informatsionnaya ekonomika. *Formirovaniye sovremennogo informatsionnogo obshchestva – problemy, perspektivy, innovatsionnyye podkhody*.

Oreshkina, D. (2017). *Shadow IT in your network.* Retrieved from https://bit.ly/2XKntw2

Raković, L., Sakal, M., Matković, P., & Marić, M. (2020). Shadow IT – A Systematic Literature Review. *Information Technology and Control*. Retrieved from https://bit.ly/3bZA5SQ

Remeikiene, R., Gaspareniene, L., & Schneider, F. (2017). Concept, motives, and channels of digital shadow economy: consumers' attitude. *Journal of Business Economics and Management. Volume 18, 2017 - Issue 2.* Retrieved May 3, 2020, from https://bit.ly/3deQtPK

Remeikiene, R., Gaspareniene, L., & Schneider, F. (2017). The definition of digital shadow economy. *In: Technological and Economic Development of Economy*. Retrieved May 3, 2020, from https://bit.ly/3bZAzbC

Rodionov, I., Gilyarevskiy, R., Tsvetkova, V., & Zalayev, G. (2002). *Rynok informatsionnykh uslug i produktov.* Moscow: MK-Periodika.

Schneider, F. (2017). *Implausible Large Differences in the Size of the Underground Economies in Highly Developed European Countries?* Linz: Johannes Kepler Universitet.

Schneider, F. (n.d.). *Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime, and Terrorism?*

Schneider, F., & Haigner, S. (2018). *Implausible Large Differences in the Size of the Under-ground Economies in Highly Developed European Countries? A Comparison of Different Estimation Methods.* Retrieved from https://bit.ly/2NXLKKu

Schneider, F., Buehn, A., & Montenegro, C. E. (2010, 07). *Shadow Economies All over the World.* Retrieved 10 06, 2015, from worldbank.org: https://openknowledge.worldbank.org/bitstream/handle/10986/3928/WPS5356.pdf?sequence=1

Shatz, H. (2020). *Economic Competition in the 21st Century.* Retrieved from https://bit.ly/3lmlVQQ

Silic, M., & Back, A. (2014). *Shadow IT - a view from behind the curtain.*

Technopedia. (2020). *Techopedia explains Shadow IT.* Retrieved from https://bit.ly/30xJhYv

Williams, J. (2019). *Cybercrime as an Economy.* Retrieved from https://bit.ly/3lrJQhT

Wu, D., & Schneider, F. (2019). Nonlinearity Between the Shadow Economy and Level of Development. *IMF Working Papers 19/48, International Monetary Fund*.

Zimmermann, S., & Rentrop, C. (2014). *On the Emergence of Shadow IT - a Transaction Cost-based Approach.*

Received for publication: 05.09.2020
Revision received: 23.09.2020
Accepted for publication: 30.12.2020

How to cite this article?

Style – **APA** *Sixth Edition:*

Ohrimenco, S., & Borta, G. (2021, January 15). The nature of shadow digital economics. (Z. Cekerevac, Ed.) *MEST Journal, 9*(1), 146-156. doi:10.12709/mest.09.09.01.17

Style – **Chicago** *Sixteenth Edition:*

Ohrimenco, Serghei, and Grigori Borta. 2021. "The nature of shadow digital economics." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 9 (1): 146-156. doi:10.12709/mest.09.09.01.17.

Style – **GOST** *Name Sort:*

Ohrimenco Serghei and Borta Grigori The nature of shadow digital economics [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, January 15, 2021. - 1 : Vol. 9. - pp. 146-156.

Style – **Harvard** *Anglia:*

Ohrimenco, S. & Borta, G., 2021. The nature of shadow digital economics. *MEST Journal,* 15 January, 9(1), pp. 146-156.

Style – **ISO 690** *Numerical Reference:*

The nature of shadow digital economics. **Ohrimenco, Serghei and Borta, Grigori.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, January 15, 2021, MEST Journal, Vol. 9, pp. 146-156