SHADOW DIGITAL TECHNOLOGIES – THREATS TO NATIONAL SECURITY

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

Valeriu Cernei
Academy of Economic Studies of Moldova,
Laboratory of Information Security, Chisinau, Moldova
valeriu.cernei@bsd.md

ABSTRACT

Shadow Digital Economy (SDE) is a sector of economic relations covering all types of production and economic activities that, in their focus, content, nature and form, contradict the requirements of the law and are being carried out contrary to state regulation of the economy and bypassing control over it. The paper provides an interaction model between the main segments of the shadow digital economy and an analysis of statistical information characterizing these segments. The paper provides an analysis of the category "Shadow Digital Technologies" (SDT), their components such as information systems, users' activity or inactivity, basic processes and rules, as well as the formation of new challenges and threats to the security of the individual, society and the state. Particular attention is paid to the transition elements: from shadow digital technologies to a shadow digital economy - the economic component has always been the final goal of criminal activity. The authors note that SDT and SDE are socio-economic phenomena, they are a set of developed, but underground markets for information and software products and services, have an ultra-high intellectual potential, a large amount of material and financial resources, and huge economic opportunities. By their structure, these markets are heterogeneous both, in terms of volumes and prospects for causing damage to the individual, society and the state. The paper concludes that the application of new digital technologies in the economy brings new challenges and risks. It can be stated that digital services control level decreases while opportunities for the implementation of a wide range of illegal actions for information leakage increases. Completely new threats appear, and these threats are related to the explosive growth of the importance of social networks in the life of society and the introduction of new technologies, such as artificial intelligence, virtual/augmented reality, the Internet of Things (IoT) and the influence on the operation of equipment (for example, household appliances, cardiostimulators, etc.). At the end of the article, we formulated the main risks related to implementation and adoption of cryptocurrencies by financial institutions. The review of the threats confronting concepts would allow states to stimulate the introduction and development of new financial technologies in a controlled manner by once side, as well as mitigating potential risks, by the other side.

Keywords: *Shadow Digital Technologies, Shadow Digital Economics, Threats, Financial Sector, National Security*

1. INTRODUCTION

The World is rapidly changing under the influence of digital transformation. At the same time new challenges and threats, which may have an unpredictable impact, are being identified. The fourth industrial revolution led to significant changes in the information infrastructure: the introduction of robotic systems, artificial intelligence, autonomous vehicles, AR / VR, transition to remote work, etc.

The COVID-19 pandemic had and is still having its impact on the global supply chain, by generating new threats to information resources, systems and networks [1,2,3]. All this has facilitated a significant increase in the risks associated with the use of shadow digital technologies.

2. SHADOW DIGITAL TECHNOLOGIES

Combating threats to national security and illegal processing of various information forms and content is of a particular relevance in the context of digital transformation and building a digital society and digital economy. A total globalization and an extremely high competitive environment is being created within the economy digitalization process, which requires new qualifications and high-quality education. At the same time, many traditional areas of activity are disappearing or changing their structure. Therefore, along with the benefits of the digital economy, it is necessary to reanalyze known and hidden threats evolved because of the digitalization processes. The 4th Industrial Revolution brought new technologies as artificial intelligence, robotics, autonomous vehicles and other achievements into our lives, which are used not only for social progress. As a result, today's computer crimes structure and characteristics from those that were 20-30 or even 10 years ago in terms of methods, factors and motives. Criminal activities are being transformed, crime itself is moving into the digital environment. Activities of specialized criminal groups (public and private) targeting states and commercial interests in a cybernetic environment also pose a serious danger. The annual Global Risk Reports consistently highlight the risks associated with technological threats such as: cybersecurity failure; digital inequality; IT infrastructure breakdown; tech governance failure; adverse tech advances. According to the results of surveys, the risks associated with cybersecurity have consistently been among the top five most significant for 2012-2020. At the end of 2021, the top ten most significant risks included Digital power concentration (6th place) and Digital inequality (7th place) [4]. The starting point of the SDE is the concept “shadow IT” (Shadow IT, Stealth IT or Client IT). Shadow IT is a currently misunderstood and relatively unexplored phenomena. The concept is present in all types of organizations, state or commercial structures. Various definitions are used, in particular:

1) Shadow IT refers to IT devices, software and services outside the ownership or control of IT organizations [5].
2) Shadow IT represents all hardware, software, or any other solutions used by employees inside of the organizational ecosystem which have not received any formal IT department approval [6].
3) Information Technology (IT) used for business processes is not only provided by the organization´s IT department. Business departments and users autonomously implement IT solutions, which are not embedded in the organizational IT service management. This increasingly occurring phenomenon is called Shadow IT [7].
4) As many leading thinkers have pointed out, technology has brought about the merging of the work life and the personal life. This has lead to the transfer of “consumer” experience on the internet into the expectations for “employee” experience at the enterprise. Thus, we have witnessed a process at which, initially shadow IT, have entered the workspace somehow naturally [8].
5) Employees increasingly use unauthorized technologies at the workplace, referred to as Shadow Information Technology (SIT). Previous Research identifies that shadow technologies are often collaborative systems used by employees to communicate and share content with co-workers, clients, or external partners. Considering that Shadow Information Technology is often a collaborative system, and its usage has the objective of effective and productive completion of work tasks, we propose that this employee initiative, called

Shadow Information Technology, can stimulate organizational knowledge sharing (KS), which is central to knowledge management practices [9].

6) "Shadow IT" is the term sometimes used to describe the situation when business units buy, own and operate IT resources with little or no assistance from the IT group. Many IT departments consider shadow IT inefficient and a source of risk, and see part of their role as containing its spread. This approach is not only futile but a waste of valuable talent in the workforce [10].

In summary, Shadow IT deals mainly with equipment, devices and software that is installed and operated with no authorization. Shadow IT can get to the user's workplace in two ways. First, technology components are independently installed by the user without control from the relevant department and information security service. The second way is much more difficult and imply the use of technologies for unauthorized software installing. For example, a user receives an email message that has a .doc or .pdf attachment. The developer of this abuse uses social engineering elements and techniques and forces files opening. This action leads to the installation of a special program in the computer's memory, which aims at performing a set of actions, including such as launching appropriate processes in the memory, copying certain information as well as covering up traces of presence. In practice, there are various tools and techniques designed to facilitate unauthorized access to information as personal data, trade and government secrets and so on. Shadow IT itself not necessarily have an objective to damage. A “bad intention” should exit and a final objective which expand the normal lawful behavior. "Shadow Digital Technologies" (SDT) is a larger concept, which includes Shadow IT components such as equipment and mobile devices, software and information systems, etc., as well as users’ activity or inactivity, specific processes, activities and rules that govern functioning of Shadow IT components. Thus, bad intentioned humans will always follow diverse interests, for example, access to confidential information in case of in case of confrontations between governments and their intelligence services, disruption of services in case of confrontations between organizations, access to personal data and, finally, earning more money. Logically, SDT is part of the SDE, which uses economic law and principles to achieve its objectives. The Digital Economy involves the unification of classical economic lows and digital technologies. Digital economy facilitates the economic inclusion; however, it may also increase the chances of instability due to systematic risks. Taken together, SDT represents a part and a form of SDE, which can be defined as ”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” [11]. Figure 1 shows a graphical presentation of SDT as part of SDE and both, being part of the legal Economy, but using criminal tools and techniques.

Figure following on the next page

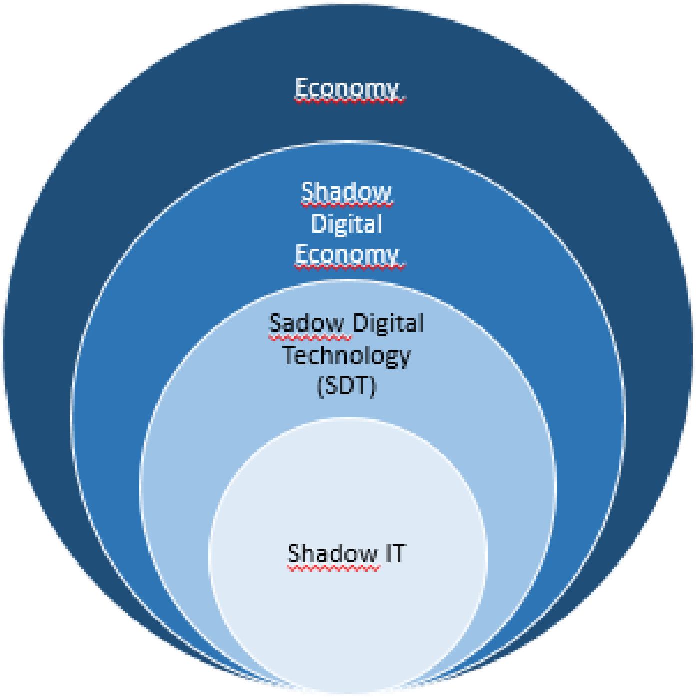

Figure 5: SDT place and correlation with SDE
(Source: Developed by the authors)

Particular attention is paid to the transition and usage of shadow digital technologies to a shadow digital economy - the economic component has always been the final goal of criminal activity. The authors conducted a study of the connection between SDT and SDE and proposed the key elements of the cybercriminal economy [12]. Thus, using SDT it is possible to cause significant damage to the enterprises and organizations information systems, as well as to information resources owned by States. The high-level interaction relationship between criminals, SDT, SDE and the impacted actors is shown in the following figure.

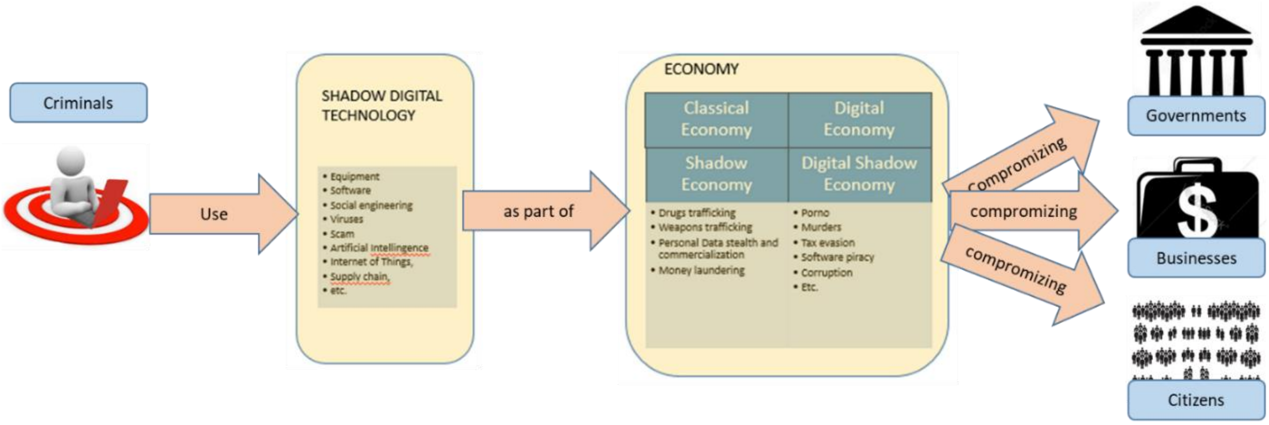

Figure 6: The high-level interaction relationship between criminals, SDT, SDE and the impacted actors
(Source: Developed by the authors)

As we see in the Figure 2, bad intentioned persons/criminals make use of shadow technology to compromise Governments, Organizations and citizens as part of and by using principle of the economy. They ”go shadow” by breaking the rules and applying unaccepted, criminal behavior.

3. MODERN FINANCIAL THREATS

The analysis of the latest achievements in the field of information and communication technologies and the practice of combating computer crimes allows us to distinguish two main directions [13, 14, 15]:

1) Technology oriented threats. Most experts and observers predict new threats coming from new technologies (e.g., 5G, the cloud, APIs, IoT/AI-IoT, *aaS providers, blockchain, AI, digital assistants, and smartphones). Additionally, we are less concerned about the nature of the threat (e.g., malware, phishing, denial of service, and password attacks) and more troubled that new technologies bring new vulnerabilities and new methods of cybercrime.
2) Entity oriented threats. These are directed to any: humans, organizations, strategic industries and critical infrastructure, government or alliances. Entities are increasingly being targeted by adopting more new technologies with potentially more vulnerabilities. The attack surface is also increasing due to the pervasiveness of IoT/AI-IoT devices, ever-broadening global hyperconnectivity, and a pivot to remote work. Cyberattacks are more sophisticated with attempts to control computer systems to immobilize, disturb, or control the technology. For example, we may see more weak-link data exfiltration attacks along organizations' supply chains. Unfortunately, the speed and scale of cyberattacks are growing exponentially, resulting in alert fatigue among frontline cyber-defenders.

Strategic developing industries is a specific domain of interest and include areas as integrated circuits (ICs) and software, new-generation networks (internet, digital TV and mobile networks), advanced computing (grid-based and peta/teraflop computer systems), biomedicine, genome research and traditional medicine, spatial applications combining 5G and satellite application (such as meteorological, environmental and geolocations), civil aircraft and advanced engines, AI, 5G and mobile devices, new materials needed in IT, biotechnology and aerospace industries, electric and hybrid vehicles, others. This domain is impacted by both, technological and entity oriented threats. The financial sector as a component of governments' critical infrastructure has been an exclusive domain of advanced technologies and for decades. According to Cybersecurity & Infrastructure Security Agency, the Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities. Realizing the value of the data it is entrusted with, like banking records and personal identifiable information (PII), and the detrimental impact of cyber breaches, this critical sector is seen as a figure in risk. Power outages, natural disasters, pandemic, sabotage, and an increased number of cyberattacks demonstrate the wide range of potential risks facing the financial sector. A major failure of the financial sector represents a huge impact on national security. Being the center of digital transformation, the financial sector has formed a new segment of modern financial markets - fintech. Fintech uses all modern digital technologies: artificial intelligence, big data technologies, distributed registry tools, biotechnologies. At the same time, the most well-known objects of FinTech are cryptocurrency and tokens. Cryptocurrencies, regardless of the attitude of regulatory authorities to them, have become a virtual reality of the financial sector and are actively used to pay for goods and services. Cryptocurrencies create opportunities — from the development of innovative technologies to the creation of new jobs and replenishment of the national budget. Anyone with Internet access and an account can use cryptocurrencies, there is no restriction and can be traded 24/7 all over the world.

The peculiarity of cryptocurrencies is its anonymity and unaccountability of the state that defines a range of risks to society and the state. The growing popularity and especially secrecy aspects attract attention of Criminals. The operation of cryptocurrencies facilitates money laundering; tax evasion, etc. In addition, cybercriminals can hide their identities when trading illegal software, confidential data, and services in digital currencies. Cryptocurrency is the most preferred form of exchange in cases of ransomware and other types of attacks. Moreover, Cybercriminals can hack the cryptocurrency trading platforms itself and steal funds, compromising cryptocurrency accounts, use of crypto-malware, and so on.

4. CONCLUSION

Digital transformation brings new challenges and risks, which are directly related to the expansion of technologies in the economy and private life. Due to complexity of the new technologies options and possibilities to control digital services decrease, the possibilities for the realization of a wide range of illegal actions and the risk of information leaks increases increase. Completely new threats, that are associated with the explosive growth of the technological landscape, appear. More, the high and very high adoption of social networks by the individuals and society facilitates the related risks exploitation. The current concepts, aimed to deal with modern threats, including those related to SDT and, consequently SDE, should be reviewed and rebuilt. The reviewed concepts should include a cardinal amendment of the legislative base and the creation of conditions under which the realization and concealment of all types of illegal activity become not only criminally punishable, but also economically unprofitable. In the absence of any Internet ”borders”, cooperation at the state, regional and international levels in order to resist cybercrime and cyberterrorism is a mandatory condition. Governments should run programs that can reduce the size of the SDE by running reforms of the financial sector and adapt it to the new reality.

LITERATURE:

1. Adrian T.H. Kuah, Roberto Dillon (2021). Digital Transformation in a Post-COVID World. Sustainable Innovation, Disruption, and Change. CRC Press. ISBN: 978-1-003-14871-5 DOI: 10.1201/9781003148715
2. Levi West (2020). The Coronavirus Cybersecurity Survival Guide. Top Tips to Protect You from a Cyber Attack.
3. Robert Slade (2021). Cybersecurity Lessons from CoVID-19. CRC Press. ISBN: 978-1-003-13667-5
4. The Global Risks Report 2021, 16th Edition. ISBN: 978-2-940631-24-7 http://wef.ch/risks2021
5. Information Technology Gartner Glossary, Retrieved September 2, 2022, from https://www.gartner.com/en/information-technology/glossary/shadow
6. Silic, Mario and Back, Andrea, Shadow it – A View from Behind the Curtain (2014). Computers & Security, Vol. 45, p. 274-283, 2014, Available at SSRN: https://ssrn.com/abstract=2933014
7. S. Zimmermann, Christopher Rentrop (2014). On the Emergence of Shadow IT - a Transaction Cost-Based Approach. https://www.semanticscholar.org/paper/On-the-Emergence-of-Shadow-IT-a-Transaction-Zimmermann-Rentrop/2d6fad07a2695cc0a86c1523aa8b48af467d5652
8. Elitsa Shumarova, Paul A. Swatman (2008). Informal eCollaboration Channels: Shedding Light on “Shadow CIT”. 21st Bled eConference eCollaboration: Overcoming Boundaries Through Multi-Channel Interaction. June 15 - 18, 2008; Bled, Slovenia. https://www.researchgate.net/publication/271195453_Informal_eCollaboration_Channels_Shedding_Light_on_Shadow_CIT

9. Gabriela Labres Mallmann, Antônio Carlos Gastaud Maçada, and Mírian Oliveira (2016). Can Shadow IT Facilitate Knowledge Sharing in Organizations? An Exploratory Study. https://www.semanticscholar.org/paper/Can-Shadow-IT-Facilitate-Knowledge-Sharing-in-An-Oliveira-Mallmann/d4eedb9ae760b22a5f5c98991f6e686b0e361000
10. Gartner Says Every Employee Is a Digital Employee. Analysts to Discuss the Workplace of the Future at the Gartner Digital Workplace Summit 2015, September 21-22, in London https://www.gartner.com/en/newsroom/press-releases/2015-08-20-gartner-says-every-employee-is-a-digital-employee
11. Serghei Ohrimenco, Grigori Borta, Bochulia Tetiana (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. ISBN 978-172-8141-855
12. Serghei Ohrimenco, Grigori Borta, Valeriu Cernei (2022). Estimation of the Key Segments of the Cyber Crime Economics. 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). ISBN:978-1-6654-0682-6
13. Gregory J. Skulmoski (2022). Shields Up: Cybersecurity Project Management. Business Expert Press. ISBN-13: 978-1-63742-290-8
14. World Economic Forum. 2020. “Digital Transformation: Powering the Great Reset.” World Economic Forum. www3.weforum.org/docs/WEF_Digital_Transformation_Powering_the_Great_Reset_2020.pdf, (accessed July 26, 2021).
15. Microsoft. 2020. “Microsoft Digital Defense Report.” Microsoft. www.microsoft.com/en-us/download/details.aspx?id=101738, (accessed July 7, 2021).