24. The digital world has a long shadow

Serghei Ohrimenco, Grigori Borta and Valeriu Cernei

1. INTRODUCTION

In the transitional stage in scientific and technological development, the complex processes of adoption of modern innovations are associated with the implementation of the concept of the fourth industrial revolution "Industry 4.0". At this moment, its analogs and more advanced versions are being implemented all over the world. Having become the universally recognized management term, "Industry 4.0" is used much wider than its original meaning, encompassing many innovations. Among them are smart manufacturing, the Internet of Things, artificial intelligence (AI), a variety of nano-devices, Virtual and Augmented Reality (VR/AR), 3D printing (including food, organs and tissue), medical robotic surgeons, and many others. The emergence of new technologies is not an accident; it is an answer to the pressing problems of modern generations, who want to save time and money by receiving services in digital format.

The President of the European Commission Ursula 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 before in Davos, they intensively discussed digitalization processes, but the pandemic had accelerated these processes and in order to be successful it is necessary to pay attention to the "dark side" of the digital world (von der Leyen, 2022).

Specialists from the World Bank, the McKinsey Global Institute, and others, called such technologies "disruptive", because they create opportunities for radical changes (Daultrey, 2017; Petralia et al., 2019). These changes give rise to global fundamental transformations. The scale of innovation is unprecedentedly huge; it is being implemented at an ultra-high pace and is easily spreading around the world, ignoring borders. The classic business production and marketing model does not meet the modern requirements and requires a change in the principles of regulation of production; a completely new kind of competition arises between producers of goods and services.

All this has led to an increase in the need for a variety of information that characterizes almost all aspects of the activities of the individual, society and the state. Simultaneously with these processes, there has been an increase in the volume of illegal activities in relation to the information itself, the processes of its receipt and transmission through communication channels, places of concentration and storage of information resources. In other words, the extraction of information in all its forms, using various products and services, has turned into a highly profitable illegal business (Lusthaus, 2018) for a group of entrepreneurs.

The components of Industry 4.0 are used to commit a wide range of unlawful acts against the individual, society and the state. On their basis, illegal markets for products and services are formed satisfying the needs of both individual users, entire corporations, and government bodies. Thus, a "shadow" economy is formed, built on the modern achievements of human activity and functioning in parallel with the developed markets of scientific and technological achievements. Cybercrime as a form of "shadow digital economy" (SDE) has adopted many

characteristics from the classical criminal syndicates. Thus, cybercrime and SDE have adopted hierarchic structures, principles, role segregation, and so on. Classical techniques and artifacts have been updated and renewed so granting criminals a wider coverage and greater efficiency.

After the agricultural and industrial revolutions, the world community is experiencing a long-term information revolution, which has brought many positive things to individuals, companies and countries. It is already noted that the digital economy is superior to classic approaches and accounts for about 22.5 percent of the global economy. This is not the limit. There is enormous potential for further development due to the high speed of transactions, low costs, international coverage (Guo et al., 2017), etc.

The development and widespread adoption of Industry 4.0 components has generated a rapid increase in the need for a variety of information. At the same time, the volume of "illegal information" business has increased, and illegal markets for specific criminal products and services have formed. It is the latter circumstance that serves as the basis for the formation of a central energy center as a "parallel" and illegal economy of scientific and technological achievements.

2. LITERATURE OVERVIEW

There is no universally accepted definition of "shadow digital economy". Different definitions have been put forward by experts, the industry and the academic community. Most scientific research related to SDE starts with Shadow Information Technology (SIT / 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 (Serbia) (Raković, 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 on the shadow economy in developed and developing countries in collaboration with Rita Remeikiene, and Ligita Gaspareniene. Their work forms the basis of a new scientific field of research (see e.g. Gaspareniene, Remeikiene, & Schneider, 2015, 2017; Gaspareniene, Remeikiene, & Navickas, 2016; Gaspareniene, Remeikiene, Ginevicius, & Skuka, 2016; Remeikiene et al., 2017; Medina & Schneider, 2017, 2018, 2019; Wu & Schneider, 2019; Gaspareniene and Remeikiene, 2020).

Along with the cited works, it should be noted that one of the first authors to use the term "shadow information economy" was the author of the monograph *Rynok informacionnych uslug i produktov* [Market of Information Services and Products]. In chapter 5 of the monograph (Rodionov, 2002), paragraph 5.2.4, the "shadow information economy" is highlighted, which begins with the main premise of the research: "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 to the Russian budget due to the shadow nature of private business in the field of information services and products are not so great. In fact, 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 is in the shadow, but it does not have a criminal basis and is associated with

low efficiency of information activities, the level of development of which hinders financial growth, and makes it difficult 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 lacks a criminal basis. Over recent years, 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 Gaspareniene, Remeikiene, and Schneider (mentioned above; see also Schneider, 2017a, 2017b, 2017c) take a different approach, based 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" (Gaspareniene, Remeikiene, & Schneider, 2015).

The work of researchers from Brazil analyzed the approaches to the definition of Shadow IT (Mallmann et al., 2018), 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 is distinguished from closely related concepts such as workaround, bring-your-own, and IT consumerization; (3) individual shadow IT usage is "the voluntary usage of any IT resource violating injunctive IT norms at the workplace as reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization". Shadow IT classification is also included here, which includes the following:

- Cloud services in all its forms: IaaS, PaaS, SaaS (Internet-based infrastructure, platforms and software provided as a service, such as processing capacities, 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 are 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).
- 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).
- Self-installed (software installed by employees to perform their work tasks, on the company's computers. For example, downloading a freely available software from the web).
- Self-acquired devices (devices such as notebooks, servers, routers, printers, or other peripherals purchased by employees. These devices are purchased directly from retailers rather than being ordered through the official catalog of the IT department. It includes the use of applications in the employee's personal devices at the workplace. For instance, smartphones, notebooks, tablets, and so on).
- The authors completely agree with the opinion expressed in the work of Levene (2019) that the risk of malware is clearly 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, and their losses and recovery costs (if this was possible).

3. RESEARCH METHODOLOGY

The basis of this study is an approach based on the analysis of the qualitative characteristics of the SDE category as the subject of the study is not sufficiently defined and studied, either in theoretical or practical terms (Ohrimenco et al., 2019).

Most of the scientific developments related to shadow activities in the field of information and communication technologies and information confrontation are based on the research of Shadow IT and Shadow IS, but the category of SDE is currently misunderstood and remains insufficiently studied. Only a small part of publications considers SDE as an objective phenomenon, which is becoming more widespread in the world, and has a negative impact on the economies of developed and developing countries. That is why comprehensive research is needed for the emerging domain, since the relevance and importance of this new topic is constantly growing and affecting the relationships of citizens, society and the state, developing a new topic in the list of problems of international information security.

Another important drawback of the existing research methodology is the approach based on the thesis that Shadow IT is not always bad. Elements of shadow technologies are present in any information system, and the main task is to remove them from the shadows. Comments are made that the SDE can play a positive role in increasing revenues and improving the efficiency of the information system. The authors consider the thesis that Shadow IT is a user-only behavioral phenomenon and it all depends on the individuals, their specific needs and motivation. At the level of interaction between commercial structures, the behavioral phenomenon moves aside and is replaced by a well-designed and built-up company policy with the allocation of tactical and strategic goals, advertising campaigns, special events budget, etc. The presence of a complex of shadow information models forces the government and commercial structures information security and intelligence services to constantly review the composition and structure of countermeasures. They apply the same approaches and same shadow technologies to test their own security measures, and this is precisely what determines their "usefulness".

In a completely different look and content take on confrontation at the geopolitical level, complex information security concepts are being developed, special services are being involved, and special operations are being run, etc.

Most scientific studies reflect the point of view that the activity of illegal collection, processing and storage of information, the development and use of malicious software, the organization of attacks on state and commercial information systems are associated with cybercrime and cybersecurity.

As the main methodological message, we have used the following thesis: "Crimeware in the Modern Era" (Levene, 2019). Levene makes the following points:

> Misconceptions around the severity of risk from financially motivated threat actors have hobbled enterprise defense efforts. Rates of losses due to crimeware are climbing, and countermeasures are decreasing in efficacy. Crimeware as a financial risk quantifiably outranks more sophisticated threats such as APTs (advanced persistent threats). Crimeware is underestimated. The ability of crimeware to disrupt businesses is tremendous and if efforts are not increased, there will be attacks greater in impact, scale and cost.

> Instances of crimeware have grown steadily, year over year and this leads to the conclusion that crimeware growth is enduring. The prevalence and frequency of crimeware have desensitized security teams and crimeware fatigue is a threat to organizations. As a result, crimeware poses a more likely business impact threat than sophisticated attacks.

Sophistication arose from the opportunity granted by volume – deploying crimeware is inexpensive and low-effort for financially-motivated actors. As a result, attackers have optimized for volume and speed. High volumes of broadly-cast attacks over time enabled financially motivated adversaries to optimize attack campaigns towards the most lucrative targets. Increased operationalization and strategy have resulted in increasingly sophisticated and targeted crimeware.

Financially motivated actors are able to adapt to countermeasures enforced by traditional law. Financially motivated actors are modeling risks based on law enforcement efforts, and adapting attack techniques based on profit. Having enough time, being geographically dispersed, the trans border and other factors that limit law enforcement efforts, crimeware operations have more time to adapt and make crimeware progressively more detrimental. Thus, the efficacy of law enforcement efforts decreases over time.

The bull market run of cryptocurrencies, as best mapped by the Bitcoin Index, reached its peak at the end of 2017 and began to crash by February of 2018. Following this trend, cryptominer activity dropped by more than 50% over the course of the year. The correlation between spikes in the Bitcoin Index and popularity of miners demonstrates that criminals viewed cryptocurrency as a fertile business opportunity.

As threat groups increased attack sophistication, organized criminal groups that initially targeted consumers switched to deploying new tactics to compromise corporate victims.

Crimeware is a business. Threat actors design their workflow and operate using traditional enterprise workplace standards in order to achieve maximum profit. For example, the push towards consolidation and "crimeware-as-a-service" demonstrates an ability to scale profitable enterprises while leveraging new infection methods. Typically, within a three-month period, cybercriminals are able to rapidly shift their toolsets to align with prime money-making opportunities.

4. OBTAINED RESULTS

This section goes into the results obtained in the process of the research: definitions of shadow information technologies are offered, the result of an analysis of organized criminal groups in shadow digital economy is provided along with their comparison to the "classic" criminal structures. Before going into the subject, we consider it important to provide a brief clarification of the term digital economy.

The digital economy is the main economic "form" that follows the agricultural economy and the industrial economy (Jiao & Sun, 2021). The digital economy is the focal point for governments, companies and citizens and includes several key subsectors: the infrastructure (equipment), operational and management information systems, processes, humans and the information.

Initially, information and communications technology (ICT) was seen as a sector of economy, particularly the sector that aimed to create and distribute digital content. Nowadays, when every economy sector implements new technologies and one cannot imagine them running without digital content, the ICT sector changed its focus, took over the classical economy and formed the digital economy which covers all other sectors as an umbrella.

4.1 Definitions and Principles

The starting point of the research is "Shadow IT" (Shadow IT, Stealth IT or Client IT). Various definitions are used and clarifications are required.

Shadow IT is all the third-party IT solutions, including cloud capacities, applications and services that are not controlled by a 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, as many IT and information security experts believed.

At the same time, from a security point of view, cloud applications and services are a "blind spot" (Oreshkina, 2017). Other definitions specify that "Shadow IT refers to IT devices, software and services outside the ownership or control of IT organizations" (Gartner, 2023) or "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). The above validates the information security rule that "everything not clearly permitted, is prohibited".

Other definitions reflect the business perspective. For example, Zimmermann and Rentrop state that shadow IT is when "Business units and users autonomously implement IT solutions that are not embedded in the organizational management of IT services" (Zimmermann and Rentrop, 2014). The same idea is proposed by Mallmann who states that "Shadow IT is any IT solution used by employees to perform their work tasks without the approval and official support of the IT department" (Mallmann, 2022).

In conclusion, the Shadow IT may be defined as third-party IT solutions that are not controlled by corporate governance. These solutions are not always clouds, it can be any information systems that are out of sight or control of the legitimate IT department.

Shadow IT infrastructure is not always evil, it often arises from "good" intentions to optimize legitimate business processes. 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. Therefore, Shadow IT must be identified and analyzed, and only if necessary, an alternative offered. This will help to keep the IT environment controlled, convenient and secure (Techopedia, 2022).

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 (Techopedia, 2022).

Accordingly, security policies and regulations 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 (JetInfo, 2017).

Even though these definitions touch upon very important points, in our 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, socio-psychological, organizational and managerial, economic and financial.

- The legal approach describes this category from the perspective of legal science, focusing on illegal activities.

- 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.
- 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.
- The organizational and managerial approach is to determine Shadow IT from the point of view of the organizational and legal form of interaction between participants.
- The economic and financial approach considers the financial impact because of improper use of information and communication within the organizations.

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 production 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 have a hidden, latent (secret) character, meaning the activity is not registered by the organizations or state authorities and is not reflected in the official reporting; it covers all phases of the process of social reproduction (production, distribution, exchange and consumption); and has a parasitic nature in 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 Gaspareniene and colleagues cited earlier, 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, 2022).

We agree with the thesis proposed by Fürstenau and colleagues (Fürstenau et al., 2016) that 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): It consists of all types of unregistered activity that contribute 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 different reasons like avoiding: taxes (for example, income or value added tax), social security contributions payments, using certain labor market standards, such as minimum wages, maximum working hours, safety standards, as well as avoiding adherence to certain administrative procedures.

Thus, summing up the analysis of existing approaches to the definition of SDE, the authors of this study propose their own definitions of SDE as being 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 economic activity and the concealment of income.

The definition has to be provided from at least two different perspectives: the economic and technological. From an economic point of view, the SDE represents a sector of economic rela-

tions, covering all types of production and economic activity, which, by their nature, content, and form, contradict the requirements of existing norms and legislation and are carried out contrary to state regulation of the economy and bypassing control over it. The most important economic elements of this sphere are the following: illegal economic and commercial relations, illegal activities related to the production, distribution and use of prohibited/bad intentioned products and services.

From a technological perspective, the SDE is an individual and/or collective activity that is illegal, associated with the design, development, distribution, support and use of information and relevant technology components (processes, software, hardware and communication), which is hidden from society. Thus, SDE is all illegal and hidden goods and services that use, are built on and run with the support of information technology (IT) components.

> There is a group of actions undertaken by hacker groups: targeted attacks, insiders, social engineering, malicious mailings, espionage and fraud. The main types are Hacking (credit card), Denial of Service Attacks, Identity theft, Virus Dissemination, Online Fraud, Software Piracy, Malicious Code, and so on. (Hutcheon, 2018)

The list can be enriched with technics and tools, however it is important to mention that they are being changed on a permanent basis and are being adapted by criminals according to each specific target, new technologies, new macro and micro-environment, etc. Taking into consideration the speed of new technologies as well as their high adoption rate, an analysis of those may become outdated in a 6- to 12-month period.

4.2 Analysis of Organized Criminal Groups in Shadow Digital Economy

To conduct an efficient struggle against shadow digital economy, complex research aims at outlining the most distinct features and characteristics of the interactions between separate criminal groups and individuals. Unfortunately, the research existing to date is focused on comparing the activity and structure of "traditional" organized crime groups and SDE goods and services.

The most prominent are the ones that make a comparison to actions of the Italian criminal syndicate "Cosa Nostra", Japanese "Yakuza", Russian mafia, etc. We can agree that "traditional" organized crime syndicates do employ information and communication technologies in their daily activity not only as a means of communication, but as a means of profiting and money laundering as well. The latter was prominent even before cryptocurrencies were introduced, but now it has grown to a larger extent.

Confrontation in the boundaries of criminal economics and law enforcement in the domain of information and communication technologies began with a change of paradigm, when the actions of individuals were aimed at gaining profits by means of developing specialized malicious software, etc. Emergence of malicious software at the early stages of development led to development of a market for computer viruses, worms, Trojan programs, fraudware, etc. While the scientific base of research has expanded, more complex mechanisms of influencing criminally aligned information systems emerged (e.g. the concept of GRID computing evolved into botnets). A gradual knowledge transfer, from information and computing services into the criminal domain, occurred. The impact of this process was partially exerted by specialized government structures by developing certain mechanisms of influence in the conditions of confrontation between countries (e.g. Stuxnet, DuQu, Flame). In some cases, these mecha-

nisms were officially activated to fight against cyber-terrorism. However, there are signs that these actions were just masks and used not only for the declared purpose.

4.2.1 The link between "classical" crime and SDE

In order to trace a link between "classical" crime and SDE, one would have to analyze a set of complex estimative criteria, including the form, typology, and many others.

The following forms are used:

- First form – organized groups acting on a certain territory and under a single law framework. They perform "regular" or economic crimes, and their authoritative leaders may or may not have previous criminal records.
- Second form – organized groups based on a certain territory and under a single law framework, performing economic crimes along with "regular" ones.
- Third form – organized groups that have international connections. They use law inconsistencies to organize and commit their illegal activities.
- Fourth form – organized groups of entrepreneurs, internationally connected, acting under different legal jurisdictions that perform illegal economic activity, and launder money via private organizations and banking systems.

The following typology of traditional criminal groups exists, defined further.

Simple organized group – a relatively primitive form of association into groups of around 2 to 4 people. They tend to have a common long-term criminal goal. Even though these groups are organized, stable, united, and their actions bear a premeditated, planned character, they do not have a complex structure, subordination, and no clear leader. The methods of criminal activity are usually similar, well thought out, and worked out. Decisions are made collectively and crimes are performed together. This group of criminals usually includes burglars, scammers, apartment thieves, street robbers, and minors. This kind of group tends to function no longer than three years due to change of members.

Structured (complex) organized group – compared to the previous group, this one is much more resistant, hierarchical, and tends to have a clear leader. This kind of groups tends to have 5 to 10 or even more members. Criminal activity tends to bear a regular character, more often than not, including property, mercenary, and violent crime.

Organized criminal group – multi-member criminal formation, encompassing tens or even hundreds of people actively partaking in criminal activity.

Criminal organization – a form of criminal activity that presumes formation of an armed group aiming to assault governmental structures, public and private companies, and individuals. The difference compared to the previous form is presence of arms and heavily criminal direction, including but not limited to open assault. Criminal organizations bear increased threat level.

Criminal syndicate – stable, complex, hierarchical criminal formation. Criminal syndicates tend to bear the following five defining characteristics:

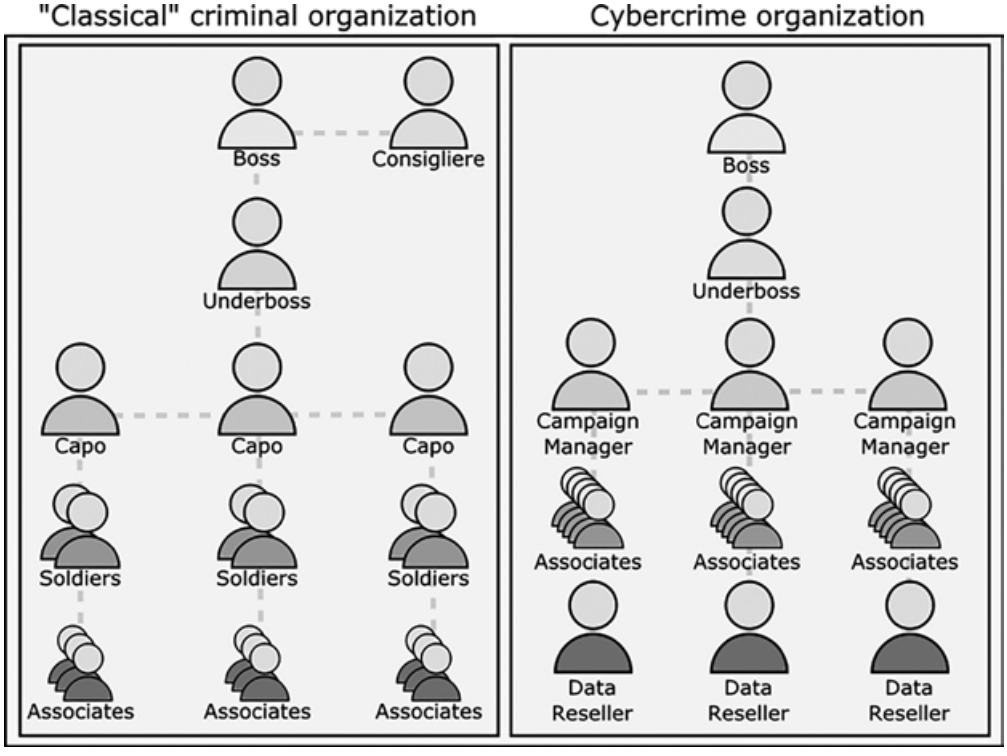
- Presence of a material base – common monetary funds used for mutual aid and bribing officials.
- Collegial form of leadership, when the management is performed by a circle of people having equal standing.
- A codex of informal behavior norms, laws, traditions, and sanctions for misconduct.

- Functional-hierarchic system – division of the organization to composite groups, presuming interregional connections and communication, clear separation of duties between the members (leading core, bodyguards, bank holders, communicators, controllers, etc.).
- Information base – intelligence and counter-intelligence, data gathering.

4.2.2 Types of criminal organizations and structures

Criminal syndicates are widely spread in the world, the most recognized among them being Camorra and La Cosa Nostra (LCN) in Italy, Yakuza in Japan, Triads in Hong-Kong, and Medellin Cartel in Columbia. Most of them deal in drugs, and have some influence over civil processes.

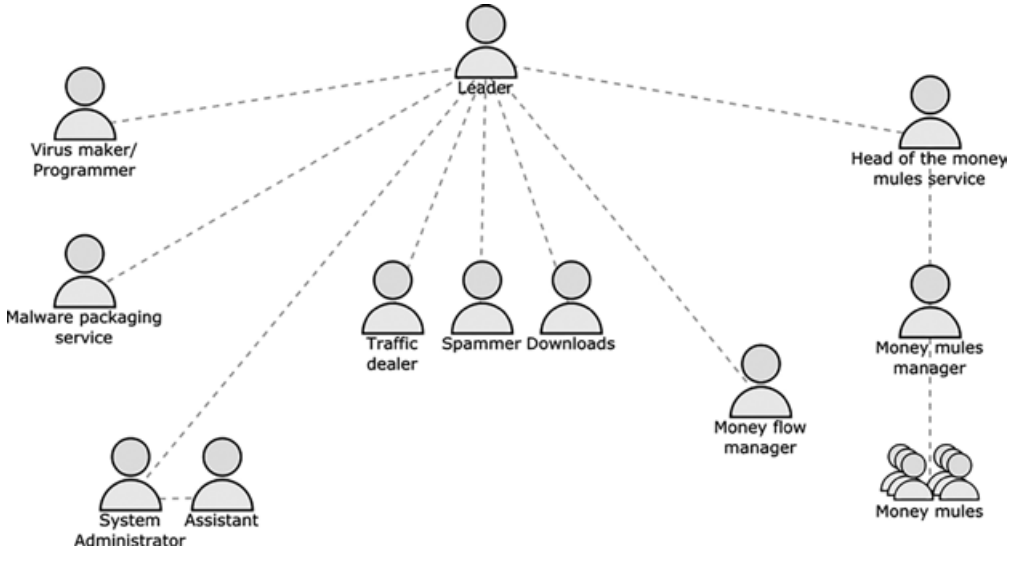
We state that the organizational structures and processes of interaction have been "lent" from criminal syndicates and had been implemented by the SDE actors. With relevant adjustments, cybercrime organizations implemented a similar, hierarchical approach. A graphical comparison of "classical" and "cybercrime" organization structure is represented in Figure 24.1.



Source: Prepared by authors.

Figure 24.1 The pyramidal structure of a criminal syndicate

Another view of this type of research represents a paper by Kaspersky Lab, which is related to organized financial cybercriminal groups, and the result is presented in Figure 24.2.



Source: Prepared by authors.

Figure 24.2 How a financial cybercrime group is organized.

We can see different actors, organized hierarchically and having specific and clear roles, which is very close to the "classic" way of structuring.

The comparison between "classical" crime and cybercrime demonstrates that the same type of crime remains, but it is performed at different levels using information technologies, granting a wider coverage and greater efficiency.

An analysis of key differences is represented in Figure 24.3.

The next model, represented in Figure 24.4, thoroughly represents the possibilities of criminals in the conditions of appearance and development of SDE.

It is easy to observe that we have an interconnection between "cyber" and "classic" organized criminal groups. More than that, the "classic" criminal groups became centric to the SDE in majority of cases – they, having resources and criminal products, switched to online and transformed their processes in order to align to the new reality.

The authors propose a new model describing current organization of SDE from the point of view of criminal organization, represented in Figure 24.5.

We state that the SDE is not something chaotic and unorganized. We see that diverse specialization groups are being formed with the aim to ensure maximum efficiency and efficacy. The following groups of participants are outlined:

- Research
- Development
- Spread
- Profiteering
- Laundering.

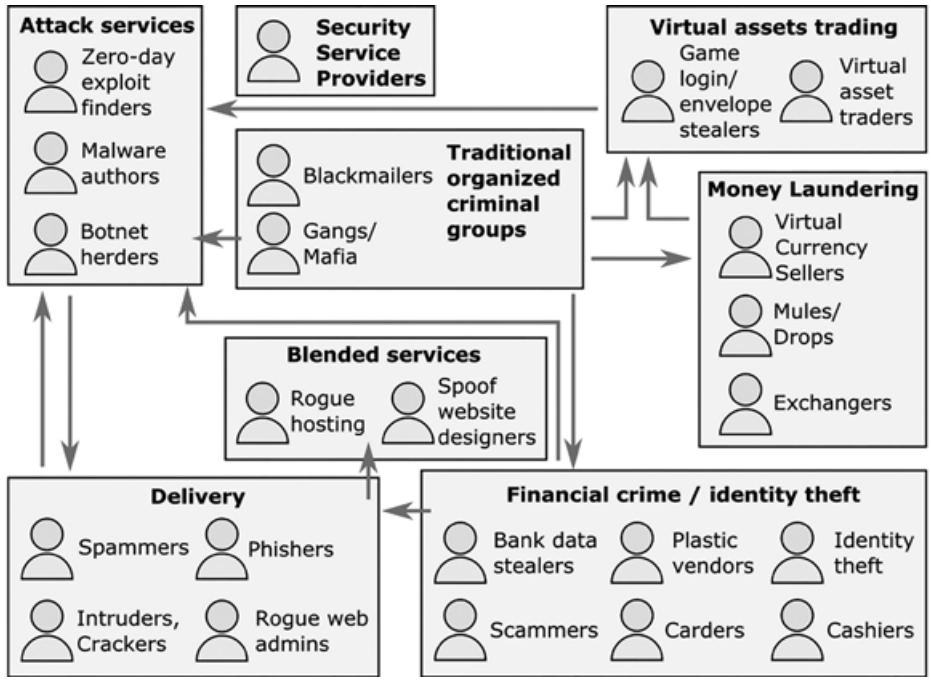
Traditional criminal techniques	Cybercrime
Burglary: Breaking into a building with the intent to steal.	**Hacking:** Computer or network intrusion providing unauthorized access.
Deceptive callers: Criminals who telephone their victims and ask for their financial and/or other personal information	**Phishing:** A high-tech scam that frequently uses unsolicited messages to deceive their financial and/or personal identity information.
Extortion: illegal use of force or one's official position or powers to obtain property, funds or patronage.	**Internet extortion:** Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.
Fraud: Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.	**Internet fraud:** A broad category of fraud schemes that use one or more components of the internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.
Identity theft: Impersonating or presenting oneself as another in order to gain access, information, or reward.	**Identity theft:** The wrongful obtaining and using of another person's identifying informtion in some way that involves fraud or deception, typically for economic gain.
Criminal exploitation: Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.	**Child exploitation:** Using computers and networks to facilitate the criminal victimization of minors.

Figure 24.3 Comparison between traditional criminal and cybercrime techniques

We supplement this list with, from our point of view, some important categories. The following include stealthy and targeted cyber attacks (Check Point Research, 2019):

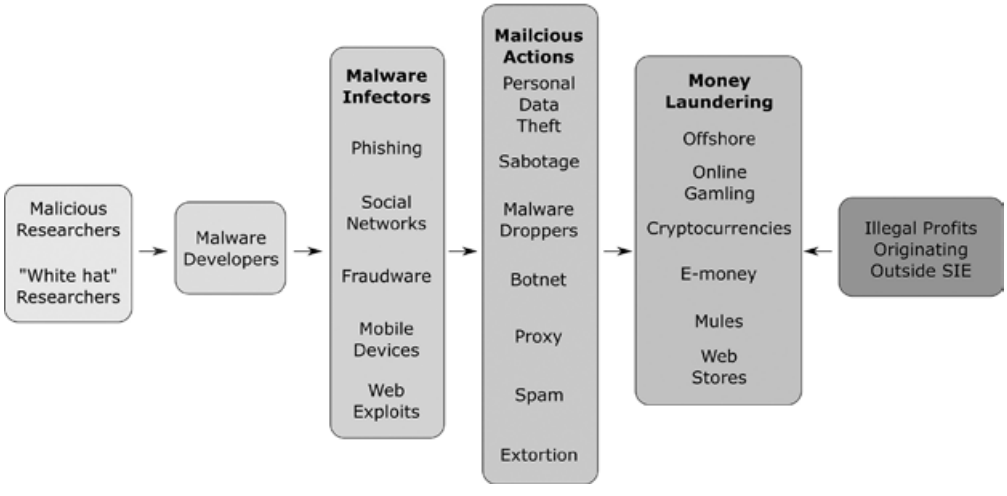
- Management. They search for new team members, form teams in relevant areas and manage the implementation of operations.
- IT Technicians. They have a support function aimed to create and maintain the infrastructure (networks, servers, databases, etc.) for the SDE.
- Merchants. This category is the last link in the software product development process. They sell software abuse and stolen victim data. At the same time, they provide feedback between the developer and the user.

In the authors' opinion, existing attempts at combining "traditional" crime and SDE are far from perfect and require further research. In spite of the fact that at the top level they look similar, it is important to trace the differences at a lower level, by analyzing used tools and techniques.



Source: Prepared by authors.

Figure 24.4 The underground economy ecosystem



Source: Prepared by authors.

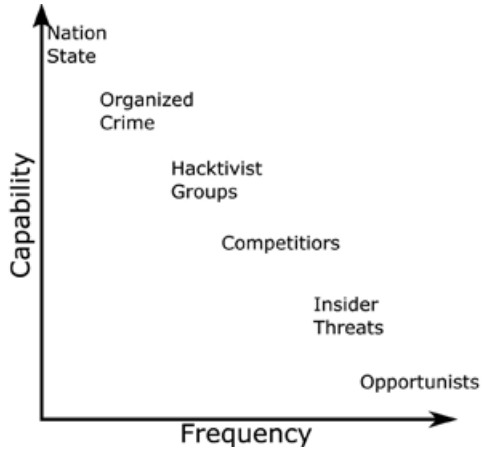
Figure 24.5 SDE structure

4.2.3 Actors and tools in the confrontation

With the rise of cyber threats, cybersecurity spending is constantly growing (including spending on firewalls and threat analysis) from governments and the private sector, and it is estimated (Lee-Makiyama, 2018) that the cost is approaching 0.1% of global GDP. Some researchers argue that the risks and costs associated with cloud and 5G outweigh the benefits of digitalization (Verizon, 2017; Atlantic Council, 2015).

Another important aspect is the amount of losses from cyber espionage. For example, according to the Center for Strategic and International Studies (CSIS, https://www.csis.org), in 2014 the global cost of cybersecurity amounted to 575 billion dollars (or 0.8% of global GDP). For the European Union (EU), the cost is estimated at 0.41% of GDP or $55 billion per year. According to the calculations of Lloyd's insurance company, disruption of the cloud service can lead to significant economic losses, which can vary from 4.6 up to 53.1 billion dollars, which amounts to 0.07% of world GDP (Lloyd's, 2017). Cyber espionage is very expensive for the European Union: 55 billion euros are lost annually as a result of such actions, and 289,000 jobs are in danger. Such significant losses will increase with the expansion of digitalization processes (5G generation, Industry 4.0), and it is predicted that 26,000,000,000 new devices (Lee-Makiyama, 2018) will appear on the network. Naturally, we can assume that attacks on information systems and resources will increase; their composition and quantity will change.

There are several groups of actors that act at different levels. These groups, based on their capabilities, plan and realize cyber-attacks with different frequencies. As presented in Figure 24.6 (see also McKinsey, 2019) many countries announced the establishment of specialized cyber defense / attack units. Among the countries that officially announced the presence of special units, whose activities are associated not only with cyber defense, but also with cyber offense, are the following: USA, UK, Russian Federation, France, Germany, Estonia, Iran, Israel, South and North Korea, China, Australia and others.



Source: Prepared by authors.

Figure 24.6 Cyberthreat capability and frequency by threat actor

Other threat actors are considered the organized crime, hacktivist groups, competitors or economic espionage, as well as opportunists. From a capability point of view, each significant group will act with different frequency. Nation-state actors will plan for and realize complex, well targeted attacks while opportunists, as they have fewer capabilities, will conduct simple, but more frequent attacks.

We ascertain that more and more cases of nation-state actors are being identified. One of the main features of such attacks is a narrow focus, unlike cybercriminals who seek to infect as many victims as possible. Most often, such developments are sponsored or conducted by government agencies. The most striking example is of this is the development of specialized software, used by intelligence services like Stuxnet, Falme, Duqu, Gauss. Usually, such malware exploits zero-day vulnerabilities.

Table 24.1 describes cyber-attacks (ATP) targeting EU interests together with potential sponsors, target country and a brief description.

It can be concluded that states initiate cyber-attacks against other states, however, these attacks often target major companies and industries with an objective to get access to know-how, IP, develop strategic plans, and so on.

The list of organized targeted attacks can be extended. However, one specific characteristic of these attacks is the secrecy – rarely does the related information become known and public.

According to Figure 24.6, the rest of the actors could be grouped as being non-state. All these sub-groups have different capabilities and motivation. However, in most cases their motivation is financial.

Table 24.2 presents a classification of non-state actors in terms of their motivation, goals and methods of influence. It should be noted that pure state actors and non-state actors often act together and use the same methods. We conclude that the motivation is the only differentiator – states create their own units and/or sponsor hacking groups to get access to information (key motivation) while non-state groups follow mainly the financial gain and sometimes are driven by patriotism/idealism/curiosity.

Of great interest for scientific research is a series of reports on the leading countries of the world in the field of cybersecurity, prepared by Anomali. In particular, the main performance indicators of such countries as the USA, China, Great Britain, Republic of South Africa (RSA), Islamic Republic of Iran, and Russian Federation are given. The reports contain information on the following sections: Current Landscape – International Relations, Domestic Security, National Cyber Strategy, Intelligence and Cyber Services, Activity Overview, and Future Concerns. For some countries, information about organized crime (Anomali, 2018a–2018f, 2019) is provided. The information provided can be used to conduct research on the interaction of key actors in the field of cybersecurity at several levels.

Table 24.1 Examples of cyber-attacks targeting EU interests

Incident, threat	Estimated government sponsor	Year	EU countries with affected interests	Notes
APT 10	China	2017	Great Britain, France, Sweden, Finland	The group steals information that characterizes intellectual property and other confidential data from several information systems of service providers regarding energy, finance, technology, and medical institutions.
OPERATION BUGDROP	Russia	2017	Austria	US and European media reported that the target was to collect information in various fields, including data on critical infrastructure, media and research, including audio recordings of conversations, screenshots, documents and passwords.
"OCEAN LOTUS"	Vietnam	2015	Germany	The group disclosed information to weaken the competitive advantage (data from the private sector, law enforcement agencies, intellectual property theft and anti-corruption measures) of foreign companies interested in consumer goods from Vietnam, manufacturing, hotel business, technological infrastructure and banking sectors.
UPS	China	2015	Great Britain	The goal was gathering information from aerospace, defense, construction, engineering, technological, telecommunication and transport companies.
EMISSARY PANDA	China	2015	Great Britain, France	Their actions targeted companies in the aerospace, automotive, technological, energy, and other sectors of production and defense, as well as obtaining political and commercial information about competitors, innovations, financial, price opportunities and development plans.
ÄXIOM	China	2014	Great Britain, Germany, Netherlands, Belgium, Italy	The group had as a target organizations related to strategic technologies, telecommunications, infrastructure, environmental and energy policies to develop competition and get rid of foreign technology as part of a special plan.
CARETO	Spain	2014	Great Britain, France, Spain, Germany, Poland	Dedicated to the activities of energy, oil, and gas companies, research institutes and private investment companies. A sophisticated program has been created and used that is capable of intercepting and collecting important information through communication channels.

Source: Lee-Makiyama (2018).

Table 24.2 Main non-state actors in cyber conflict

Actor	Motivation	Target	Method
Ordinary citizens	None (or weak)	Any	Indirect
Script kiddies	Curiosity, thrills, ego	Individuals, companies, governments	Previously written scripts and tools
Hacktivists	Political or social change	Decision makers or innocent victims	Protests via web page defacements or DDoS (distributed denial of service) attacks
Black-hat hackers	Ego, personal animosity, economic gain	Any	Malware, viruses, vulnerability exploits
White-hat hackers	Idealism, creativity, respect for the law	Any	Penetration testing, patching
Grey-hat hackers	Ambiguous	Any	Varies
Patriot hackers	Patriotism	Adversaries of own nation-state	DDoS attacks, defacements
Malicious insiders	Financial gain, revenge, grievance	Employer	Social engineering, backdoors, manipulation
Cyber terrorists	Political or social change	Innocent victims	Computer-based violence or destruction
Malware authors	Economic gain, ego, personal animosity	Any	Vulnerability exploits
Cyber scammers	Financial gain	Individuals, small companies	Social engineering
Organized cyber criminals	Financial gain	Individuals, companies	Malware for fraud, identity theft, DDoS for blackmail
Corporations	Financial gain	ICT-based systems and infrastructures (private or public)	Range of techniques for attack or influence operations
Cyber espionage agents	Financial and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber militias	Patriotism, professional development	Adversaries of own nation-state	Based on the group capabilities

Source: Sigholm (2013).

5. CONCLUSIONS

Security is a business, and information security is a large business. There is a good reason to believe that the future state of the information security system will directly depend on individual market segments, innovation capability and investment volume. To identify promising areas for future research, the authors have collected and processed statistics on information security market segments. The information is presented in Appendix Table 24A.1. It presents cost indicators of the main segments of the information technology and security market.

It is a challenge to collect for analysis realistic and valid data related to Information Technology and Security indicators. This information is not always public and, even if some is being disclosed, it is not structured and ready for analysis. Appendix Table 24A.1 includes information from different sources, for different periods and may have an error rate due to approximations.

As information security is tightly connected to market mechanisms, it is necessary to comprehend the prospects. The global cybersecurity market value stood at USD 112.01 billion in

2019 and is projected to reach USD 281.74 billion by 2027, exhibiting a CAGR – Compound Annual Growth Rate – of 12.6% during the forecast period from 2020 to 2027 (Fortune Business Insights, 2020).

Future research could be associated with the cost characteristics of the market. It is considered that presented segments and figures in the Appendix represent a strong starting point for further research. Potential investments are directly related to the need for objective indicators to measure information security.

A first step would be to validate cost indicators and structure, including allocating to right groups, periods and values. Another step would be to align periods and amounts. As a result, we will see trends and, by applying certain indicators, we admit that there is space to have an idea of SDE dimensions.

Another area, as noted in (Oltsik, 2019), the cybersecurity skills and human capacity, is important. A survey has been conducted for several years, and as a result, the percentage of organizations reporting a problematic lack of cybersecurity skills continues to grow. Below are the results of the last four polls:

- 2018–2019: 53 percent of organizations report a problematic shortage of cybersecurity skills;
- 2017–2018: 51 percent of organizations report a problematic shortage of cybersecurity skills;
- 2016–2017: 45 percent of organizations report a problematic shortage of cybersecurity skills;
- 2015–2016: 42 percent of organizations report a problematic shortage of cybersecurity skills.

It is necessary to determine how many and what kind of specialists are needed by governmental, corporate, and private information systems, how to retrain them and attract new specialists to this area.

Cybercrime and SDE is everywhere. Effects of a single criminal attack (for example, DDoS or MIM (Man-in-the-Middle) and others) are felt in supply chains beyond the realm of cyberspace.

We consider it necessary to pay attention to the low level of knowledge of the following research areas: the possibility of implementing threats to medical equipment (in particular, in relation to cardiac pacemakers); cryptomania – as a socio-economic phenomenon; Wetware – computer technologies integrated with the biological organism; Digital Twin concept, etc.

A review of the content (qualitative and quantitative) is required using relevant cybersecurity assessment metrics (Daultrey, 2017). These are related to legal aspects, including laws and regulations, the organizational area which targets national strategies and all forms of cybersecurity cooperation, industry standards development, as well as training for cybersecurity professionals, and public awareness.

From a different point of view, relatively new directions of threats were identified. The most topical threats foreseen by the authors are personal data, socially dangerous content (cyberbullying, calls for suicide), attacks on IoT and supporting electronic systems, attacks on electronic voting systems and information processing.

And the last but not the least area is that of new technologies. New technologies, like 5G communication networks, malware, AR/VR, and AI bring expansion of capabilities for implementing various attacks.

According to UN Secretary-General António Guterres (United Nations, 2020), the main threats to our society are geostrategic tension, climate change, growing distrust at the global level and the danger of new technologies ("Reverse side" of the digital revolution) the "Four Horsemen of the Apocalypse" (United Nations).

Even though the technologies bear multiple benefits, they can facilitate incitement, the spread of false information, interference in private life, exploitation of people, and committing crimes.

Finally, the closest attention should be paid to Marc Goodman's prediction: "The future of cybercrime will be exponential, automated and three-dimensional" (Goodman, 2016). The processing power and the adoption rate of new technologies is doubling every two to three years. The criminal world, along with the "normal" world is taking advantage of them. It could be stated that criminals adopt new technologies even faster than cybersecurity professionals. Cybercriminals automate their activities and this facilitates them to be more efficient in all relevant aspects: organization, management and operational. Finally, they cooperate to keep a "one step ahead" advantage.

REFERENCES

Anomali (2018a). Anomali Labs Threat Landscape: Republic of South Africa (RSA). https://www.anomali.com.

Anomali (2018b). Islamic Republic of Iran Cybersecurity Profile. https://www.anomali.com.

Anomali (2018c). North Korea Cybersecurity Profile. https://www.anomali.com.

Anomali (2018d). People's Republic of China (PRC) Cybersecurity Profile. https://www.anomali.com.

Anomali (2018e). United Kingdom Threat Landscape. https://www.anomali.com.

Anomali (2018f). United States of America Cybersecurity Profile. https://www.anomali.com.

Anomali (2019). Russian Federation Cybersecurity Profile. https://www.anomali.com.

Atlantic Council (2015). *Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures*. https://www.atlanticcouncil.org/in-depth-research-reports/report/risk-nexus-overcome-by-cyber-risks-economic-benefits-and-costs-of-alternate-cyber-futures/.

Check Point Research (2019). *Under the Hood of Cyber Crime: The Rise of Stealthy and Targeted Cyber Attacks*. https://bezpecneit.cz/wp-content/uploads/2019/03/SR2019_Single-Pages_Vol-2_R2.pdf.

Daultrey, S. (2017). Cybercrime: Invisible problems, imperfect solutions. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3803735.

Fortune Business Insights (2020). *Cyber Security Market Overview by Size, Growth & Trends, 2029*. https://www.fortunebusinessinsights.com.

Fürstenau, D., Sandner, M., & Anapliotis, D. (2016). Why do shadow systems fail? An expert study on determinants of discontinuation. Research.cbs.dk. Association for Information Systems. AIS Electronic Library (AISeL). https://research.cbs.dk/en/publications/why-do-shadow-systems-fail-an-expert-study-on-determinants-of-dis.

Gartner (2023). *Gartner Definition of Shadow IT*. https://www.gartner.com/en/information-technology/glossary/shadow.

Gaspareniene, L. & Remeikiene, R. (2020). Digital shadow economy: A critical review of the literature. *Mediterranean Journal of Social Sciences*, 6(6). https://www.richtmann.org/journal/index.php/mjss/article/view/8577.

Gaspareniene, L., Remeikiene, R., Ginevicius, R., & Skuka, A. (2016). Critical attitude towards the theory of digital shadow economy: Literature review and new foundations. *Terra Economicus*, 14(4), 156–172.

Gaspareniene, L., Remeikiene, R., & Navickas, V. (2016). The concept of digital shadow economy: Consumer's attitude. *Procedia Economics and Finance*, 39, 502–509.

Gaspareniene, L., Remeikiene, R., & Schneider, F. G. (2015). The factors of digital shadow consumption. *Intellectual Economics*, 9(2), 108–119.

Gaspareniene, L., Remeikiene, R., & Schneider, F. G. (2017). Concept, motives and channels of digital shadow economy: Consumers' attitude. *Journal of Business Economics and Management*, 18(2), 273–287.

Goodman, M. (2016). *Future Crimes: Inside the Digital Underground and the Battle for our Connected World*. New York: Anchor Books.

Guo, S., Ding, W., & Lanshina, T. (2017). Global governance and the role of the G20 in the emerging digital economy. *International Organisations Research Journal*, 12(4), 169–184.

Hutcheon, S. (2018). *Cyber Crime & IT Fraud*. https://www.acwa.asn.au/wp-content/uploads/2018/02/ACW-StewartBrown-Cybercrime-Presentation-Feb-2018.pdf.

JetInfo (2017). ИТ-портал компании Инфосистемы Джет [Shadow IT или как стоит обращаться с теневыми ИТ, кейсы и примеры]. https://bit.ly/2YqYeOm.

Jiao, S. & Sun, Q. (2021). Digital economic development and its impact on economic growth in China: Research based on the perspective of sustainability. *Sustainability*, 13(18), 10245. https://doi.org/10.3390/su131810245.

Lee-Makiyama, H. (2018). *Stealing Thunder*. https://ecipe.org/wp-content/uploads/2018/02/ECIPE_Occasional0218_HLM_V7.pdf.

Levene, B. (2019). *Crimeware in the Modern Era*. https://github.com/Blevene/Crimeware-In-The-Modern-Era/blob/master/%5BFINAL%5D%20Crimeware%20in%20the%20Modern%20Era.pdf.

Lloyd's (2017). *Counting the Cost – Lloyd's*. https://www.lloyds.com/countingthecost.

Lusthaus, J. (2018). *Industry of Anonymity: Inside the Business of Cybercrime*. Cambridge, MA: Harvard University Press.

Mallmann, G. (2022). Can shadow IT facilitate knowledge sharing in organizations? An exploratory study. *17th European Conference on Knowledge Management*. https://www.academia.edu/34196339/Can_Shadow_IT_Facilitate_Knowledge_Sharing_in_Organizations_An_Explorator.

Mallmann, G. L., Maçada, A. C. G., & Oliveira, M. (2018). The influence of shadow IT usage on knowledge sharing. *Business Information Review*, 35(1), 17–28.

McKinsey (2019). *The Approach to Risk-Based Cybersecurity*. https://mck.co/35spU6Z.

Medina, L. & Schneider, F. (2017). *Shadow Economies around the World: New Results for 158 Countries over 1991–2015*. https://ideas.repec.org/p/ces/ceswps/_6430.html.

Medina, L. & Schneider, F. (2018). *Shadow Economies Around the World: What Did We Learn Over the Last 20 Years?* IMF Working Paper 18(17). https://doi.org/10.5089/9781484338636.001.

Medina, L. & Schneider, F. (2019). *Shedding Light on the Shadow Economy: A Global Database and the Interaction with the Official One*. CESifo Working Paper No. 7981. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3502028.

Ohrimenco, S., Borta, G., & Tetiana, B. (2019). Shadow of digital economics. *2019 IEEE International Scientific-Practical Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. https://doi.org/10.1109/picst47496.2019.9061545.

Oltsik, J. (2019). The cybersecurity skills shortage is getting worse. *CSO Online*. https://www.csoonline.com/article/569723/the-cybersecurity-skills-shortage-is-getting-worse-2.html.

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

Petralia, K., Philippon, T., Rice, T., & Veron, N. (2019). *Banking Disrupted? Financial Intermediation in an Era of Transformational Technology*. Geneva: ICMB.

Raković, L. (2020). Shadow IT: Systematic literature review. *Information Technology and Control*, 49(1), 144–160.

Remeikiene, R., Gaspareniene, L., & Schneider, F. G. (2017). The definition of digital shadow economy. *Technological and Economic Development of Economy*, 24(2), 696–717.

Rodionov, I. I. (2002). *Rynok informacionnych uslug i produktov*. Moscow: Mk-Periodika.

Schneider, F. (2017a). Implausible large differences in the sizes of underground economies in highly developed European countries? A comparison of different estimation methods. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2999761.

Schneider, F. (2017b). Restricting or abolishing cash: An effective instrument for fighting the shadow economy, crime and terrorism? Frankfurt a. M.: Deutsche Bundesbank. https://www.econstor.eu/handle/10419/162914.

Schneider, F. (2017c). Countries? A comparison of different estimation methods. https://ssl-administracja.sgh.waw.pl/en/cpm/Documents/EstShadEc_OECDCountries_prof_Schneider.pdf.

Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, 4(1), 1–37.
Silic, M. & Back, A. (2014). Shadow IT: A view from behind the curtain. *Computers & Security*, 45, 274–283.
Techopedia (2022). *What is Shadow IT? Definition from Techopedia*. https://bit.ly/30xJhYv.
United Nations (2020). Глава ООН рассказал о своих приоритетах на 2020 год. Новости ООН. https://bit.ly/3bEt8Gu.
Verizon (2017). *Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/2017/2017_dbir.pdf.
Von der Leyen, U. (2021). Ursula von der Leyen's message to Davos Agenda in full. World Economic Forum. https://bit.ly/3h9CtLw.
Wu, D. F. & Schneider, F. (2019). *Nonlinearity Between the Shadow Economy and Level of Development*. IMF Working Paper. https://www.imf.org/en/Publications/WP/Issues/2019/03/01/Nonlinearity-Between-the-Shadow-Economy-and-Level-of-Development-46618.
Zimmermann, S. & Rentrop, C. (2014). On the emergence of shadow IT: A transaction cost-based approach. *ECIS 2014 Proceedings*. http://aisel.aisnet.org/ecis2014/proceedings/track15/11.

APPENDIX

Table 24A.1 Cost indicators of the main segments of the information technology and security market

No.	Category / Segment	Min	Max	CAGR
I	**Segments "Cybersecurity":**			
1	Database Encryption Market	261.8 million in 2015	968.3 million by 2020	29.9%
2	Cloud Encryption Market	645.4 million in 2017	2,401.9 million by 2022	30.1%
3	Managed Detection and Response Market	419.7 million in 2017	1,658.0 million by 2022	31.6%
4	Runtime Application Self-Protection Market	294.7 million in 2017	1,240.1 million by 2022	33.3%
5	Security Assessment Market	1.26 billion in 2017	4.03 billion by 2022	26.1%
6	User Activity Monitoring Market	1,071.3 million in 2018	3,335.7 million by 2023	25.5%
II	**Segments "Network Security":**			
1	CDN Security Market	1.93 billion in 2017	7.63 billion by 2022	31.6%
2	Cloud IDS IPS Market	600.9 million in 2017	1,764.7 million by 2022	24.04%
3	Security Analytics Market	2.83 billion in 2016	9.38 billion by 2021	27.1%
4	Software-Defined Perimeter (SDP) Market	992.8 million in 2016	4,396.1 million by 2021	34.7%
5	Microsegmentation Market	670.3 million in 2017	2,038.7 million by 2022	24.9%
6	Managed Detection and Response Market	419.7 million in 2017	1,658.0 million by 2022	31.6%
7	Perimeter Security Market	110.64 billion in 2017	196.60 billion by 2022	12.2%
8	Perimeter Intrusion Detection Systems Market	4.12 billion in 2016	5.82 billion by 2021	7.1%
9	Deep Packet Inspection and Processing Market	7.01 billion in 2016	18.60 billion by 2021	21.6%
10	Web Application Firewall Market	2.37 billion in 2017	5.48 billion by 2022	18.3%.
III	**Segments "Analytics":**			
1	Cognitive Analytics Market	1.84 billion in 2017	10.95 billion by 2022	42.9%
2	Enterprise AI Market	845.4 million in 2017	6,141.5 million by 2022	48.7%
3	Recommendation Engine Market	801.1 million in 2017	4414.8 million by 2022	40.7%
4	AI in Education Market	537.3 million in 2018	3,683.5 million by 2023	47.0%
5	User and Entity Behavior Analytics Market	131.7 million in 2016	908.3 million by 2021	47.1%
6	Artificial Intelligence in Healthcare Market	667.1 million in 2016	7,988.8 million by 2022	52.68%
7	Big Data Market	28.65 billion in 2016	66.79 billion by 2021	18.45%
8	Geospatial Analytics Market	40.65 billion in 2018	86.32 billion by 2023	16.3%
9	Embedded Analytics Market	26.77 billion in 2017	51.78 billion by 2022	14.1%

No.	Category / Segment	Min	Max	CAGR
10	High Performance Data Analytics (HPDA) Market	25.71 billion in 2016	78.26 billion by 2021	24.9%
11	Data Science Platform Market	19.58 billion in 2016	101.37 billion by 2021	38.9%
IV	**Segments "Data Centre & Networking":**			
1	Software-Defined Networking and Network Function Virtualization Market	3.68 billion in 2017	54.41 billion by 2022	71.4%
2	Software-Defined Wide Area Network (SD-WAN) Market	738.9 million in 2016	9,066.2 million by 2021	65.11%
3	SDN Orchestration Market	214.7 million in 2017	4,458.5 million by 2022	83.4%
4	Service Market for Data Center	39.68 billion in 2017	77.51 billion by 2022	14.33%
5	Managed Network Services Market	38.60 billion in 2016	59.38 billion by 2021	9.0%
6	Data Center Colocation Market	31.52 billion in 2017	62.30 billion by 2022	14.60%
7	High Performance Computing Market	32.11 billion in 2017	44.98 billion by 2022	7.0%
8	Data Center Rack Server Market	36.47 billion in 2016	90.56 billion by 2021	19.95%
V	**Segments "Mobility & Telecom":**			
1	Network Automation Market	2.32 billion in 2017	16.89 billion by 2022	48.7%
2	Virtualized Evolved Packet Core (vEPC) Market	968.9 million in 2017	7,975.3 million by 2022	52.4%
3	Low Power Wide Area Network Market	1.01 billion in 2016	24.46 billion by 2021,	89.3%
4	Network Transformation Market	6.01 billion in 2017	66.86 billion by 2022	61.9%
5	BYOD & Enterprise Mobility Market	35.10 billion in 2016	73.30 billion by 2021	15.87%
6	Telecom IT Services Market	67.38 billion in 2014	233.05 billion in 2019	28.2%
7	Premium A2P and P2A Messaging Market	55.49 billion in 2016	71.60 billion by 2021	5.23%
8	Mobile Enterprise Application Market	48.24 billion in 2016	98.03 billion by 2021	15.24%
9	Telecom API Market	93.69 billion in 2016	231.86 billion by 2021	19.87%
VI	**Segments "Cloud Computing":**			
1	Integration Platform as a Service Market	528.0 million in 2016	2,998.3 million by 2021	41.5%
2	Disaster Recovery as a Service Market	2.19 billion in 2017	12.54 billion by 2022	41.8%
3	Personal Cloud Market	12.02 billion in 2015	80.02 billion by 2020	46.1%
4	Cloud/Mobile Backend as a Service (BaaS) Market	1.32 billion in 2015	28.10 billion by 2020	84.2%
5	Integration Platform as a Service Market	528.0 million in 2016	2,998.3 million by 2021	41.5%
6	Cloud Storage Market	30.70 billion in 2017	88.91 billion by 2022	23.7%
7	Cloud Managed Services Market	27.15 billion in 2017	53.78 billion by 2022	14.6%
VII	**Segments "Software & Services":**			
1	Blockchain Market	411.5 million in 2017	7,683.7 million by 2022	79.6%
2	Artificial Intelligence as a Service Market	1.52 billion in 2018	10.88 billion by 2023	48.2%
3	Blockchain Government Market	162.0 million in 2018	3,458.8 million by 2023	84.5%
4	Social Customer Relationship Management (CRM) Market	2.22 billion in 2014	17.92 billion in 2019	51.9%
5	Gamification Market	1.65 billion in 2015	11.10 billion by 2020	46.3%

No.	Category / Segment	Min	Max	CAGR
6	3D Mapping and 3D Modeling Market	1.90 billion in 2015	16.99 billion by 2020	55.0%
VIII	**Segments "Application Security":**			
1	Application Security Market	2.79 billion in 2017	9.0 billion by 2022	26.4%
2	Microsegmentation Market	670.3 million in 2017	2,038.7 million by 2022	24.9%
3	Managed Detection and Response Market	419.7 million in 2017	1,658.0 million by 2022	31.6%
4	Runtime Application Self-Protection Market	294.7 million in 2017	1,240.1 million by 2022	33.3%
5	Dynamic Application Security Testing Market	736.0 million in 2017	2,398.5 million by 2022	26.7%
6	Encryption Software Market	3.87 billion in 2017	12.96 billion by 2022	27.4%

Source: Calculated by the authors based on: Most Promising Segments "Cybersecurity". https://www.mnmks.com/subscribers/mnm/industry_trends/cyber_security?isguest=true; https://www.marketsandmarkets.com/top-market-reports.asp?utm_source=TopReports&utm_medium=TopReportsBranding&utm_campaign=KSBrandingCampaign.