POLITICAL ECONOMY ASPECTS OF THE SHADOW DIGITAL ECONOMY

UDC: 004.056+339.19:004
DOI: https://doi.org/10.53486/tids2025.15

DINARA ORLOVA
Financial University under the Government of the Russian Federation
DOrlova@fa.ru
ORCID ID: 0000-0002-2901-070X

SERGHEI OHRIMENCO
Academy of Economic Studies of Moldova
osa@ase.md
ORCID ID: 0000-0002-6734-4321

Abstract. The article analyzes the shadow digital economy (SDE) as a modern threat to cybersecurity. The article formulates and proposes definitions of the SDE, based on the specifics of software production and the life cycle of information services of a criminal nature.

In the course of the research, the political economy foundations and general features of the SDE were determined. These include latency, coverage of all phases of the process of social and economic reproduction, the parasitic nature of the activity, and others. Future cyber threats such as Quantum Computing Threats, AI-enabled cyberattacks, Internet of Things (IoT) vulnerabilities, Cyberwarfare, and political manipulation are presented.

Keywords: Digital Economics, Cybersecurity, Shadow Digital Economics, Digital Threats, Cyberattack.

JEL Classification: D74 E26 F51 K24

INTRODUCTION

The currently used and prevailing technical approach to covering cybersecurity issues ignores many crucial socio-economic aspects. We argue that a political economy approach should address the social relations developing within the shadow digital economy. This includes production, distribution, exchange, and consumption of information, software, and services with criminal intent, as well as their impact on the value chain.

The peculiarity of the political economy approach is, firstly, the analysis of objective production relations, the nature of man in the system of market relations, and his objective interests (maximization of value income and minimization of costs). Secondly, political economy assumes that the existing relations are limited through the regulation of the economy (including the structure of production, the quality of products, a range of prices, the introduction of environmental and social standards, the distribution of development funds in the spheres of education and health care, the establishment of progressive tax on income, etc.). Thirdly, political economy links economic decisions to the socio-economic and political interests of social groups.

1 Definition of the shadow digital economy

We define the shadow digital economy based on its specificity in the production of goods and services, and their life cycle.

In the context of rapid digitalization of all aspects of life, insufficient attention is paid to the emerging negative trends where the shadow digital economy and cybercriminals play a key role. That is why, with the widespread introduction of the latest information technologies into society's everyday life, a new branch of knowledge has arisen – the shadow digital economy (SDE), which combines activities to promote products and services with a "shadow" focus. We define the digital shadow economy as "all illegal and hidden products and services that use information technology." The most important economic elements of this area are the following: illegal economic relations, illegal activities associated with the production, distribution, and use of prohibited products and services (Ohrimenco, 2021), (Ohrimenco, 2020).

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 (Ohrimenco & Cernei, 2024).

From an economic perspective, the SDE represents a sector of economic relations that encompasses all types of production and economic activities which, by their nature, content, and form, contradict existing norms and legislation. These activities are carried out in violation of state regulation and bypass control mechanisms. The key economic elements of this sphere include: illegal economic and commercial relations, as well as illegal activities associated with the production, distribution, and use of prohibited or malicious products and services.

From a technological perspective, the SDE involves both individual and collective activities that are illegal, including the design, development, distribution, support, and use of information and technology components (such as processes, software, hardware, and communication systems), all of which are hidden from society. Thus, the SDE encompasses all illegal and concealed goods and services that rely on, are built upon, and operate with the support of information technology (IT) components.

A range of actions is undertaken by hacker groups, including targeted attacks, insider threats, social engineering, malicious mailings, espionage, and fraud. The main types involve hacking (e.g., credit card theft), denial-of-service attacks, identity theft, virus dissemination, online fraud, software piracy, and malicious code.

2. Cybercrime Economics

A separate and very important issue is the study of the economic foundations of cybercrime. In this regard, the data on the cybercrime economy looks stunning against the background of the collected statistics on the activities of the shadow digital economy. According to the study conducted by Bromium, cybercrime activity in 2018 was estimated at $1.5 trillion. This was the first study of its kind aimed at studying the "dynamics of cybercrime" in the context of revenue flow and profit distribution (Williams, 2019). In the course of the study, new criminal platforms and a thriving cybercrime economy were identified, which is self-sufficient and erases the boundaries of legality. Gregory Webb, CEO of Bromium, commented on the results of the study as follows: "It is shocking how widespread and profitable cybercrime has become. The crime model is to create malware and provide it to cybercriminals as easily as shopping online. Not only is it easier to access the tools, services and expertise of cybercriminals, it means that businesses and governments will face more

sophisticated, costly and destructive attacks as the profit-driven web gains momentum. We cannot solve this problem with old thinking or outdated technology. It is time for new approaches."

3. Taxonomy of cybercrime

The proposed taxonomy is based on approaches to defining a set of criteria, which include technical experience, behavior, motivation, and level of moral development. The proposed model includes seven categories and is based on the recording of behavior:

1. Script Kiddies (SK) - individuals with limited technical knowledge and abilities who run pre-compiled software to cause harm to individual users, systems, and networks.

2. Cyber-punks (CP) – these people have a clear disrespect for authority and its symbols and disregard for social norms. They are driven by the need for recognition or fame from peers and society. The moral level remains low.

3. Haktivist (H) – Calling yourself a hacktivist sounds more respectful than calling yourself a petty criminal. People tend to justify their destructive behavior, including defacing websites, by labeling it as civil disobedience and ascribing political and moral correctness to it.

4. Thief (T) – This group targets information systems for financial gain and as such, targets credit card and bank account numbers that can be used for immediate personal gain. This group can accurately be described as petty criminals, given that the activities of its members are usually not sophisticated, namely simple wire transfer fraud and fraudulent use of credit card numbers.

5. Virus Writers (VW) – This category of individuals can include both technically skilled and novices. This category includes four subcategories, namely: teenager, college student, adult, and former virus writer. Even though viruses have been around in one form or another for many decades, they still constitute a very profitable segment of the crimeware market.

6. Professionals (P) – This is the most elite of the cybercriminal groups and is associated with competitive intelligence and the activities of so-called "white hat" and "gray hat" hackers. Members of this group may be involved in sophisticated scams or corporate espionage. They will sell information and intellectual property to the highest bidder. Very little is known about this underground group as they use strict anonymity to hide their activities. For them, their criminal activities are a job and they are consummate professionals.

7. Cyber terrorist (CT) – members of this group may be part of the armed forces or paramilitary formations of a nation state and are considered soldiers or freedom fighters on the battlefield of the new cyberspace. Their activities are associated with the commission of terrorist acts in cyberspace.

Taking into account the motivation of criminals, cybercrimes can be divided into the following categories:

- cyber fraud with the purpose of acquiring funds;
- cyber fraud with the purpose of acquiring information (for personal use or for subsequent sale);
- interference with the operation of information systems with the purpose of gaining access to automated control systems (for intentional damage for a fee or to damage competitors).

4. The Future of Cybersecurity

We will assume that cybersecurity policies are aimed at ensuring the security and resilience of digital technologies. For this reason, cybersecurity is an integral part of any government strategy aimed at developing the digital economy: reducing risk means reducing the expected costs of the

economy and increasing the likelihood of adoption through greater trust. Cyber risk can entail huge costs for the economy, businesses, and ordinary users.

The main source of concern is purely technical: cybercriminals can exploit the limitations of software to hack it. Several factors support this thesis (Mariniello, 2022). It should be recognized that software is a very sensitive component and is subject to many errors. There are many reasons for this thesis. First, software code is extremely complex. Second, software always requires interaction with other software. Third, software code is necessarily built on previously coded software, which may have vulnerabilities that have never been fixed.

At the same time, users rely on other additional software such as antivirus, firewall, and traffic monitoring software (which may also be vulnerable to attacks) to track and counter potential attack attempts.

Thus, the cornerstone of cybersecurity effectiveness is the ability to withstand a variety of attacks. Historically, the evolution of cyberattacks spans from the emergence of simple malware to complex threats driven by artificial intelligence (Rusinova V., 2024), (Alaba, 2025), (S. Armstrong-Smith, 2024), (Shipley, 2024), (Kestner, 2024). Consider the evolution of cyberattacks, using et al.

Check Point experts identify five generations of cyberattacks. Generation 1 - late 1980s, virus attacks on autonomous personal computers affected all businesses and led to the first antivirus products. Generation 2 - mid 1990s, attacks from the Internet affected all businesses and led to the creation of the firewall. Generation 3 - early 2000s, exploitation of vulnerabilities in applications affected most businesses and led to the emergence of Intrusion Prevention Systems (IPS). Generation 4 - around 2010, the rise of targeted, unknown, evasive, polymorphic attacks affected most enterprises and led to the emergence of bot attack countermeasures (anti-bot) and sandboxes. Generation 5 - circa 2017, large-scale, multi-vector, mega-attacks using advanced attack tools and the introduction of advanced threat prevention solutions.

Let's consider expert assessments. Thus, Steve Morgan, editor-in-chief of Cybercrime Magazin, presented to the experts' judgment an article describing the five most significant facts on cybersecurity (Morgan, 2021). In particular:

1. Global cybercrime costs are projected to reach $10.5 trillion per year by 2025.Cybersecurity spending will exceed $1 trillion from 2017 to 2021. Experts predict that the global cost of cybercrime will grow by 15 percent per year over the next five years, reaching US$10.5 trillion per year by 2025, up from US$3 trillion in 2015. Innovation and investment in cybersecurity will significantly exceed the damage caused by natural disasters in a year, and will be more profitable than the global trade in all major illicit products combined (including drugs, pornography, arms trafficking, etc.). The costs of cybercrime include the cost of data damage and destruction, theft of money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, disruption to normal business operations following an attack, forensic investigation, recovery and removal of hacked data and systems, and reputational damage.

2. Global cybersecurity spending between 2021 and 2025 will total more than $1.75 trillion. The increasing pace of digitalization will drive global spending on cybersecurity products and services to a combined $1.75 trillion over the five-year period from 2021 to 2025. By comparison, the global cybersecurity market was valued at just $3.5 billion in 2004, and is now one of the largest and fastest-growing sectors of the information economy. The cybersecurity market is expected to grow at a compound annual growth rate of 15 percent from 2021 to 2025.

3. By the end of 2021, there will be 3.5 million unfilled cybersecurity jobs worldwide. Every IT job is also a cybersecurity position. Every IT worker, every technology worker, must play a role in protecting applications, data, devices, infrastructure, and people. According to Cybersecurity Ventures, there will be 3.5 million unfilled cybersecurity jobs worldwide in 2021. That's up from Cisco's previous estimate of 1 million unfilled cybersecurity jobs in 2014. The cybersecurity unemployment rate in 2021 will be zero percent (for experienced workers, not entry-level positions), where it has been since 2011. The rise in cybercrime will lead to just as many unfilled positions over the next 5 years.

4. Global ransomware damage is projected to exceed $265 billion by 2031. Global ransomware damage is projected to reach $20 billion per year in 2021, up from $325 million in 2015, a 57-fold increase. Ten years from now, costs will exceed $265 billion. Experts expect that by 2021, a business will fall victim to a ransomware attack every 11 seconds, up from 14 seconds in 2019. This makes ransomware the fastest growing form of cybercrime. The frequency of ransomware attacks on governments, businesses, consumers, and devices will continue to increase over the next 5 years, reaching every two seconds by 2031. The average ransom amount is estimated (Report, 2021), to be a significant $220,298 ($220,298 vs. $154,108, up 43% from Q4 2020), with the median ransom amount being $78,398 ($78,398 vs. $49,450, up 59% from Q4 2020), foreshadowing a quantitative and qualitative increase in new attacks.

5. The average ransom amount estimated by (Schwartz, 2021), is a significant $220,298 ($220,298 vs. $154,108, up 43% from Q4 2020), with the median ransom amount being $78,398 ($78,398 vs. $49,450, up 59% from Q4 2020), suggesting a quantitative and qualitative increase in new attacks.

Leading experts make an interesting suggestion that if cybercrime, from an economic point of view, were a sovereign country, it would rank 13th in the world by GDP. The total revenue, according to rough estimates, is $1.5 trillion and includes: $860 billion - activities in illegal, illicit online markets; $500 billion - theft of trade secrets, IP; $160 billion - data trading; $1.6 billion - cyber fraud and cybercrime as a service; $1 billion - ransomware. The report indicates that cybercrime operates on several levels, with some large "corporate" style trading operations bringing in more than $1 billion, and "small and medium business" style orders - from $30,000 to $50,000.

As information and communication technologies evolve, so too do the strategies used by cybercriminals. Cyber attacks have evolved significantly since the first computer viruses emerged. Experts note that the spectrum of cyber risks is constantly changing – from sophisticated malware to state-sponsored cyber warfare (cyber blockades).

Historical context includes: The Morris worm (1988); email-borne viruses (1990s); phishing attacks (early 2000s) to expropriate passwords and financial data.

Current status: Modern attacks are becoming increasingly sophisticated, using artificial intelligence, automation, and social engineering to evade detection. Key trends include:

Ransomware as a Service (RaaS), where criminal organizations provide ransomware toolkits that allow individuals with little or no technical knowledge or skills to carry out large-scale attacks;

Advanced Persistent Threats (APT): state-sponsored intrusions that infiltrate networks to spy or sabotage infrastructure;

Cloud Security Threats: as enterprises migrate to the cloud, attackers are taking advantage of misconfigurations and inadequate authentication protocols;

Deepfakes and AI-powered attacks: cybercriminals are using AI-generated audio and video to deceive individuals and organizations.

Future Cyber Threats: As technology evolves, cyber threats will also adapt, and potential future attacks include:

Quantum Computing Threats: quantum decryption has the potential to undermine existing encryption methods, thereby compromising sensitive information;

AI-enabled cyberattacks – cybercriminals will use AI to automate and optimize attacks, making them more difficult to detect;

Internet of Things (IoT) vulnerabilities: the proliferation of connected devices will create new attack vectors, especially in smart homes and industrial systems;

Cyberwarfare and political manipulation: nation-state actors will continue to use cyber strategies for espionage, sabotage, and influence operations.

CONCLUSIONS

The processes of digitalization have affected all leading economies, on the one hand, and the availability of modern tools and the growth of criminal competencies, on the other hand, are accelerating the criminalization trend, turning the underground infrastructure of the digital economy into an influential force capable of generating new threats at cosmic speed. This is why the shadow digital economy is now seen as a powerful, financially sustainable catalyst for cybercrime, providing attackers with access to services, resources, and technologies, thus expanding the scale and complexity of global attacks.

Additional difficulties were created by the COVID-19 pandemic, which revealed many problems related to remote user access and "home" work. First of all, these are information security problems - connecting personal computing devices to information networks, which activated phishing, which exploited the COVID-19 problem, and others. Additional threats were the remote access devices used, the volume of work performed using cloud technologies increased and, as a result, the number of DDOS attacks increased. The goals of cybercriminals have changed - if earlier financial organizations were considered the main target of cyberattacks, then during the pandemic there was a shift and the main targets became government organizations, industrial enterprises, energy, and medical institutions.

REFERENCES

1. Alaba, F. A. &. R. A., 2025. *The Implication of Cyberattacks on Big Data and How to Mitigate the Risk.*. s.l.:Springer.
2. Kestner, P., 2024. *The Art of Cyber Warfare.*. s.l.:Springer.
3. Mariniello, M., 2022. *Digital economic policy: The economics of digital markets from a European Union perspective.* s.l.: Oxford University Press.
4. Morgan, S., 2021. *Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021.* [Online] Available at: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/ [Accessed 25 June 2025].
5. Ohrimenco, S. &. B. G., 2020. Challenges for Digital Transformation in the Manufacturing Industry. In: *Socio-Economic Development-Interdisciplinary Ecosystems Perspective,.* Krakov: s.n., pp. 139-154.
6. Ohrimenco, S. B. G. &. C. V., 2021. *Estimation of the key segments of the cyber crime economics..* Harkiv, IEEE.
7. Ohrimenco, S. B. G. &. T. B., 2019. *Shadow of digital economics..* Harkiv, IEEE.

8. Ohrimenco, S. & Cernei., G. B. &. V., 2024. The Digital World Has a Long Shadow.. In: D. R. R. a. J. WŁODARCZYK, ed. *The Elgar Companion to Information Economics.* s.l.:Edward Elgar Publishing, pp. 481-.
9. Report, 2021. *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound.* [Online]. Available at: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound [Accessed 25 June 2025].
10. Rusinova V., &. M. E., 2024. Fighting cyber attacks with sanctions: Digital threats, economic responses. *Israel Law Review.,* 57(1), pp. 135-174.
11. S.Armstrong-Smith, 2024. *Understand the Cyber Attacker Mindset: Build a strategic security programme to counteract threats.* s.l.: Kogan Page Limited.
12. Schwartz, M. J., 2021. *Cyber Extortion Thriving Thanks to Accellion FTA Hits.* [Online] Available at: https://www.bankinfosecurity.com/blogs/cyber-extortion-thriving-thanks-to-accellion-fta-hits-p-3024 [Accessed 25 June 2025].
13. Shipley, T. G. &. B. A., 2024. *Surviving A Cyberattack: Securing Social Media and Protecting Your Home Network.* s.l.: Stylus Publishing, LLC.
14. Williams, J., 2019. *Cybercrime as an Economy.* [Online] Available at: https://thefintechtimes.com/cybercrime-economy/ [Accessed 25 June 2025].