



CONVERGENCE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Serghei Ohrimenco¹, Zoran Čekerevac²

osa@ase.md, zoran@cekerevac.eu

ORCID ID: 0000-0002-6734-4321, 0000-0003-2972-2472

¹Academy of Economic Studies, Chisinau, B-Bodoni 59, Chisinau, MD 2005
REPUBLIC OF MOLDOVA,

²MESTE – Belgrade, Knez Mihailova 33, Belgrade
SERBIA

Abstract: The convergence of information and communication technologies (ICT) represents a transformative force reshaping modern digital economies, including their shadow counterparts. This paper continues the author's prior research on the shadow digital economy (SDE), examining how the integration of advanced technologies — such as artificial intelligence, blockchain, and the Internet of Things — contributes to new digital infrastructures while simultaneously spawning hidden, often illicit, economic activities. Through exploration of the 3C innovation framework and technological granularity, the study emphasizes how convergence amplifies both progress and vulnerability. The SDE is defined considering multiple perspectives, from socio-economic impact to its association with corruption and digital currencies. The paper also analyzes the emergence of criminal products and services — malware, espionage tools, and monetization models within the DarkNet — resulting from this convergence. Risks such as cybersecurity threats, digital inequality, and erosion of regulatory visibility are addressed, positioning the SDE as a parasitic construct embedded in legal digital ecosystems. Ultimately, the paper argues that digital convergence not only accelerates technological integration but simultaneously demands critical rethinking of transparency, accountability, and control within increasingly porous digital environments.

Key words: Information and Communication Technologies, CyberSecurity, Shadow Digital Economics, Digital Economics, CyberThreats, Convergence of ICT.

1 INTRODUCTION

This paper is a logical continuation of the research on the shadow digital economy (SDE), reflected in several publications [1-4].

Information and communication technologies have entered modern life and have a positive impact on all aspects of existence. There are many similar examples. For example, the use of artificial intelligence, blockchain, machine learning in education, medicine, industry, etc.

One of the latest achievements can be considered a trend reflected in the report of the world economic forum, which presents the 3c framework 3c, which reveals the patterns driving innovative transformation. It is a map for navigation in the conditions of a modern technological explosion, where breakthroughs do not exist on their own, but merge to transform markets [5].

Specifically, the report points out that technological innovation is driven by combination: the integration of individual complementary technologies to create something fundamentally new. To understand this process, it is important to consider granularity, or the degree to which technologies can be analyzed at the subcomponent level. For example, artificial intelligence (AI) is a catch-all term for many subcomponents, such as machine learning (ML), natural language processing (NLP), large language models (LLM), neural networks, and others. When progress in a technology area like AI occurs, it occurs at the subcomponent level, as each develops at a different rate, driving the technology area forward.

It should be considered that the process of IT convergence, i.e. the convergence of individual components, generates not only new areas of research, but also problems. Thus, in [6,7], it is indicated

that high-performance computing has recently faced a challenge due to the emergence of artificial intelligence. Artificial intelligence has become quite popular in recent years and has achieved certain success in solving current scientific problems in various fields. High-performance computing and artificial intelligence are two technologies that work well together, and they are complemented by the Internet of Things, which contributes to the creation of a concept called digital convergence. And this digital convergence is already shaping the future of computer modeling today.

It seems necessary to consider the process of convergence of ICT components. In the context of information and communication technologies, convergence can characterize the unification of different technologies or platforms, for example, the merger of telecommunications, information technologies and media. In our case, we consider the convergence of ICT for the formation and promotion of products and services of the shadow digital economy.

2 DEFINITIONS OF THE SHADOW DIGITAL ECONOMY

The digital economy is a new form of economic and social development of society after the agrarian and industrial economy. It refers to several economic activities with digitalized knowledge and information as key factors of production, a modern information network as their main carrier, and the effective use of information and communication technologies as the main driving force for increasing efficiency and optimizing the economic structure.

The digital economy implies total globalization, creates an extremely competitive environment, provides a new quality of life, business and public services. At the same time, many traditional spheres of activity are being destroyed. Based on the digital economy, as a result of the development of the information society, a shadow sector or "shadow digital economy" has formed. Let us give definitions of this category.

The most significant contribution to the SDE definition has been made by Friedrich Schneider, who has an undoubted primacy in the field of research on the shadow economy in the developed and developing countries [8,9,10,11]. Certain "new" features of SDE are defined through the connection between corruption, the shadow economy and digital currencies [12].

In [13-16], the ICT is defined as a specific sphere of economic activity with its inherent structure and system of economic relations. The specificity is determined by illegality, informality, as well as the criminal nature of economic activity and concealment of income. From an economic point of view, the ICT is a sector of economic relations covering all types of production and economic activity that, by their focus, content, nature and form, contradict the requirements of existing legislation and are carried out despite state regulation of the economy and bypassing control over it. And the last definition is individual and collective activity that is illegal, related to the design, development, distribution, support and use of components of information and communication technologies, hidden from society. Thus, the ICT is all illegal and hidden products and services used and based on information technologies. The following are identified as the most important economic elements in this area: illegal economic relationships, illegal activities related to the production, distribution and use of prohibited products and services.

The common features of the TCE are the following:

- hidden, latent nature of the activity, which is not registered by government agencies and is not reflected in official reporting.
- covers all phases of social reproduction (production, distribution, exchange and consumption).
- parasitic nature of all processes, from the formation of the source code of software abuse to the monetization of individual products and services.

3 "CONVERGENCE" AND ITS PRODUCTS AND SERVICES

Thus, ICT convergence is the process of combining different technologies and platforms to create more efficient and integrated solutions. Examples include the following:

- Modern smartphones combine the functions of a phone, computer, camera and multimedia player, which provides the user with a solution to many user tasks.
- The use of cloud services provides the ability to store data and access it using various devices.
- Game consoles act as multifunctional devices, in addition to computer games, provide access to streaming services, social networks and Internet browsers.

- Smart TVs integrate many functions from various sources on one device (streaming video functions, Internet surfing, access to applications, etc.).
- Smart Home and Smart Office are systems that combine control of lighting, climate, security and other aspects to improve the efficiency of work and living.

Along with the benefits, the convergence process brings certain risks and threats. The main ones are the following: data security (data leaks and cyber-attacks), privacy (use of personal data without the consent of users), dependence on technology (various failures can lead to serious problems), job losses (the integration of technologies can lead to job losses in some industries, which causes social and economic problems), digital inequality (unequal access to new technologies can lead to the exclusion of certain groups of the population from the digital economy).

Software abuse is a problem that has existed almost since the first computers appeared. Some of the first computer viruses appeared in the 1970s, but they were quite simple and did not pose a major threat. As computer technology developed in the 1980s, more complex viruses emerged that could cause serious damage to computer systems. In the 1990s, new threats emerged in the form of worms and Trojans. With the development of the Internet in the early 2000s, new threats such as phishing and pharming emerged. Today, software abuse remains a serious threat to computer systems and information security in general.

Convergence also gives rise to new products and services, and they are of a clearly criminal nature [17-20]. The following products should be considered: SpySoft, AdWare, Virus, FraudWare, Crimeware, Worm, Trojan horse, Botnet and others. The distribution of malicious software is carried out using social networks, phishing, email, mobile devices, exploits, as well as due to the carelessness and negligence of users. In turn, the range of services is constantly expanding and DarkNet [21] is full of offers for services provided, from selling credit card data, gaming credentials, spying on a specific person or company, to blackmail and extortion based on DDOS attacks. A separate group can be distinguished spy hardware, that is, hidden equipment used for surveillance and reading signals (for example, keyloggers).

A special place in the list of services is occupied by such operations as money laundering. These include the following: organization of online casinos, lotteries, transfer of funds to offshore stores, opening of online stores, resale of stolen goods and others. Other examples of services in the field of TCE are: analytical information containing search and analysis of software vulnerabilities, analysis of various market segments, etc.; theft of personal data (identification data, logins and passwords); Fishing - mass mailing of emails with a malicious attachment; Farming - a type of attack that redirects traffic to a fake website; creation of bot networks; leasing of proxy servers, illegal mining, organization of attacks and many others.

Thus, the first example of such a "negative" convergence is the creation of a computer virus for a PC. The basis for its creation was knowledge of the Windows PC operating system and its design errors, the interruption system used (INT) and a great desire to force the user to perform actions that are not typical for him or to deprive the user of the ability to control the information processing process.

4 SPECIALIZED MODELS AND SERVICES

The main services in TCE are the following:

- Cybercrime-as-a-Service (CaaS) – is the provision of services to others to facilitate their commission of cybercrimes. This service is also called by names such as Attacks-as-a-Service, Malware-as-a-Service and Fraud-as-a-Service. This is a set of models for developing criminal functions that cybercriminals supply to their clients (customers) in exchange for payment for their services and products. The logical continuation is the following services:
- Ransomware-as-a-service (RaaS) – Cybercriminals offer ransomware packages that other individuals or groups can use to infect and encrypt their targets' data. The attackers then demand a ransom from the victim to decrypt the data. Ransomware programs are constantly evolving through the development of additional features and are turning into a sophisticated mechanism for targeted and successful attacks.
- Phishing-as-a-Service (PhaaS). PhaaS offers a phishing kit for a certain price. This kit contains the tool and knowledge to carry out a phishing attack. Cybercriminals have access to already-made phishing pages, phishing messages, a list of potential victims, etc. Cybercriminals offer a user-friendly interface for even non-technical individuals to create and manage phishing

campaigns. These services typically provide pre-built phishing templates, hosting services for the phishing sites, and tools to collect victim's data.

- Distributed Denial of Service-as-a-Service (DDoSaaS). In this service, cybercriminals provide tools and infrastructure for launching distributed denial of service (DDoS) attacks on websites or online services, causing them to become unavailable to legitimate users.
- Botnets-for-hire. Cybercriminals may rent out their botnets, which are networks of compromised computers or devices controlled by a central entity (the botmaster). Cybercriminals can use these botnets to send spam, conduct DDoS attacks, or spread malware.
- Credential theft services. Some cybercriminals offer services to steal login credentials (e.g., usernames and passwords) from individuals or companies. Other cybercriminals.
- Research-as-a-Service (ReaaS). Research consumed as a service will be the new digital-era application-programming interface that can help companies connect better with their customers. Information instability forces cybercriminals to analyze and understand the complex real-time events that shape their business.

5 CONCLUSIONS

The analysis presented in this article underscores the intricate balance between technological rigor and interpretative nuance in the application of industrial safety standards. While the ATEX and IEC frameworks offer structured methodologies for hazard prevention, their deployment in real-world scenarios often reflect deeper epistemological tensions: between precaution and pragmatism, codification and cognition.

This tension, rather than being a flaw, emerges as a productive site for reflection—one that invites engineers, policymakers, and scholars to re-evaluate the scope and intent of regulation. Safety, as argued, is not a static concept codified solely through normative texts, but a dynamic interplay of contextual judgment, ethical responsibility, and systemic transparency.

Ultimately, the path forward lies in fostering integrative thinking: where standardization coexists with critical autonomy, and where the architecture of risk management is viewed not merely as compliance, but as a reflection of collective reason and institutional trust. This, perhaps, is the truest safeguard, not just against physical hazards, but against the conceptual fragility that underpins our technological environments.

REFERENCES:

- [1] RYBALCHENKO L., OHRIMENCO S., "The impact of cybersecurity and crime on national security". – 2024.
- [2] OHRIMENCO S., CERNEI V., Shadow digital technologies—threats to national security //International Scientific Conference on Economic and Social Development – "Economics, Management, Finance and Banking". – 2022. – pp. 343-349.
- [3] OHRIMENCO S., ORLOVA D., CERNEI V., Cyber Threats Modeling: An Empirical Study //Business Management. – 2023. – T. 33. – №. 3. – pp. 90-106.
- [4] OHRIMENCO S., BORTA G., CERNEI V., "The digital world has a long shadow" //The Elgar Companion to Information Economics. – Edward Elgar Publishing, 2024. – pp. 481-504.
- [5] Technology Convergence Report. <https://www.weforum.org/publications/technology-convergence-report-2025/>.p.60 [Accessed 27 7 2025]
- [6] RESCH, M.M., ·GEBERT, J., KOBAYASHI, · H., TAKIZAWA, H., BEZ, ·W. (Editors). "Sustained Simulation Performance", 2022
- [7] HUANG, I. et al., "The convergence of information and communication technologies gains momentum" //The global information technology report. – 2012. – p. 35-45.
- [8] ENSTE, D. H., SCHNEIDER, F., "The shadow economy: an international survey". – Cambridge University Press, 2013.
- [9] SCHNEIDER, F. "Estimating the size of the shadow economies of highly-developed countries: Selected new results" //CESifo DICE Report. – 2016. – T. 14. – №. 4. – pp. 44-53.

- [10] SCHNEIDER, F., “Shadow economy //Encyclopedia of Law and Economics”. – Springer, New York, NY, 2014. – pp. 1-13.
- [11] SCHNEIDER, F., “Size and measurement of the informal economy in 110 countries” //Workshop of Australian National Tax Centre, ANU, Canberra. – 2002. – T. 17. – pp. 1-50.
- [12] BERDIEV, A. N., GOEL, R. K., SAUNORIS, J. W., “Global cryptocurrency use, corruption, and the shadow economy: New insights into the underlying linkages” //American Journal of Economics and Sociology. – 2024. – T. 83. – №. 3. – pp. 609-629.
- [13] OHRIMENCO, S., BORTA, G., CERNEI, V., “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). – IEEE, 2021. – pp. 103-107
- [14] OHRIMENCO, S., BORTA, G., “The Nature Of Shadow Digital Economics” //MEST Journal. – 2021. – T. 9. – №. 1.
- [15] OHRIMENCO, S., BORTĂ, G. “The Structure of Shadow Information Economics” //Information Technologies and Security. – 2012. – C. 278-283.
- [16] OHRIMENCO, S., BORTĂ, G. “Informal Economics of Information Threats” //Application of information and communication technology and statistics in economy and education. – 2013. – C. 27-33.
- [17] CZABAŃSKI, J., “Estimates of cost of crime: history, methodologies, and implications”. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2008
- [18] TROIA, V., “Hunting cyber criminals: a hacker's guide to online intelligence gathering tools and techniques”. – John Wiley & Sons, 2020.
- [19] MEHAN, J., “CyberWar, CyberTerror, CyberCrime and CyberActivism: An i-depth guide to the role of standards in the cybersecurity environment”. – IT Governance Publishing, 2014.
- [20] CLOUGH, J. “Principles of cybercrime”. – Cambridge University Press, 2015
- [21] ČEKEREVAC, Z., DVORAK, Z., ČEKEREVAC, P., “Is the ‘Dark Web’ Deep and Dark?”, 2016, *FBIM Transactions*, pp. 53-65,