METAMORPHOSES OF THE SHADOW DIGITAL ECONOMY

CZU: 343.9:004.056
DOI: https://doi.org/10.53486/tids2026.35

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

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

GHENADIE BELINSCHI
Academia of Economic Studies of Moldova
e-mail: gennadie.belinschi@ase.md
ORCID ID: 0009-0009-3361-9890

Abstract. This research analyses the shadow digital economy (SDE) as an ecosystem for the development of cybercrime. The SDE is viewed not as a collection of isolated illegal incidents, but as a digital shadow market environment in which illicit products, services, infrastructure and coordination mechanisms are organized in a quasi-market form. The term 'Metacrime' is used to denote the supra-systemic level of such an environment, understood as the service-market-based and reproducible criminal core of the SDE. The following are systematically explored: a research gap in the literature; the conceptual and methodological foundations of the study; umbrella models and the multi-level architecture of Metacrime; rent-seeking mechanisms and investment-reinvestment cycles; as well as the transformation of the classical SDE in immersive and virtual-active environments. Attention is also paid to the interpretation of Metacrime as crime in the Metaverse – a new segment of the SDE.

Keywords: Shadow Digital Economy, Cybersecurity, Metacrime, Metaverse

JEL Classification: D47, D74, D82, E26, K24, O17

INTRODUCTION

It should be noted that the digitalization of the global economy is having a direct impact on the development of platform markets, the proliferation of cloud services, artificial intelligence, blockchain solutions, digital twins, XR/AR/VR and next-generation communication networks. All of the above has led to the creation of a qualitatively new techno-economic environment, within which not only knowledge but also labor itself, identity, property, governance, payments, access to services and infrastructure, and much more are being transformed into digital form.

This environment is not limited to e-commerce or online communication in the traditional sense. It brings together hybrid industrial, medical, educational and social cyberspaces, where physical and virtual realms increasingly interact through digital twins, immersive technologies and interfaces, distributed data and platform coordination.

On the one hand, the growth and expansion of the legal digital economy also give rise to its shadow side. On the other hand, it is precisely where digital value is concentrated that forms of its covert appropriation, redistribution, blocking, imitation and monetization emerge. This is precisely why cybercrime, as a phenomenon and a product of the digital economy in the modern context, cannot

be adequately described and represented solely as a collection of cyberattacks, cyber incidents or computer offences. This phenomenon is increasingly taking on the characteristics of a service economy, in which complex unlawful activities are broken down into separate functions, packaged as products and services, supported by infrastructure, promoted through platforms, facilitated by intermediation and trust mechanisms, and then monetized and reinvested. Moreover, this phenomenon is successfully described by a set of simulation models, which will be discussed later.

I. ANALYSIS OF THE NEW ENVIRONMENT

The shadow digital economy is like an iceberg: only the tip is visible above the water, gleaming in plain sight. We have no idea what wave of technological processes is surging beneath the surface, how many people are working to sustain this hidden system, what management models are being devised to achieve its goals, or what abyss of human drama remains concealed beyond the boundaries of the conventional economy.

To analyses this environment, the concept of the shadow digital economy is used as an indirect shadow market environment in which illegal products, services, infrastructures and coordination mechanisms are organized in a quasi-market form. The supra-systemic level of this environment is designated as Metacrime — the criminal core of the SDE, in which disparate unlawful practices coalesce into a stable architecture of services, roles, markets, rent-seeking positions and investment-reinvestment cycles. In contrast to the narrow interpretation of Metacrime as crime in the Metaverse, as proposed in some contemporary literature, this article offers a broader political-economic interpretation of the concept.

The aim of this article is to develop and propose a comprehensive analytical model of the shadow digital economy (SDE) as an ecosystem for the development of cybercrime, and to demonstrate how it reproduces itself through service models, the life cycle of destructive digital value, rent-seeking mechanisms, and transformation in immersive and virtual-active environments. To achieve this objective, the following tasks have been set and are being addressed:

- to identify and define a research gap in the literature;
- to establish the conceptual and methodological foundations for the analysis of the SDE;
- to propose an aggregated architecture of Metacrime umbrella models;
- to describe the operational logic of the SDE by mapping out all stages of the product and service lifecycle;
- to reveal the rent-seeking nature and investment-reinvestment cycles of Metacrime;
- to demonstrate how the classical TCE model transforms into the Metaverse, the industrial Metaverse and other immersive environments.

II. LITERATURE REVIEW

This study employs a systematic review of scholarly and practitioner literature and reports from research organizations specializing in cybersecurity and its economic aspects. We use these sources to synthesize existing knowledge and identify emerging trends related to the shadow digital economy. The study included a review of scientific databases, including Google Scholar, IEEE, and Scopus. Keywords for identifying sources included terms such as Cybersecurity, Shadow Digital Economic, Cybercrime, Dark Markets, Metacrime, Metaverse and other.

The current literature on this subject can be divided into several groups, each of which covers only part of the subject area in question.

The first group consists of works directly devoted to Metacrime. There are not many of them as yet, which in itself indicates that the topic has not been explored in depth. Most notably, almost all of these publications consider Metacrime in a narrow sense — as crime in the Metaverse, in immersive environments and surrounding virtual assets, avatars, digital identity, virtual property and issues of legal regulation. Authors (Zhou, 2024) and (Tiwari, 2025) examine this topic in detail and link the emergence of the Metaverse to the rise of 'Metacrimes'—a new category of criminal activity taking place in the Metaverse, which poses a challenge not only to traditional cybercrime but also to existing law enforcement structures. Five general characteristics of these crimes are identified: classification of crimes, continuous evolution, hyperspatial-temporal scope (global scale), anonymity and governance issues. The second paper describes a mechanism whereby the Metaverse provides extensive and unique opportunities for committing crimes, or 'Metacrimes', which challenge existing law enforcement efforts and regulatory frameworks. Three main challenges in combating Metacrimes are identified: the lack of specialized jurisdictions, the absence of clear property rights, and difficulties regarding the liability of avatars.

Another piece of work that calls for greater attention to Metacrime is the article Andreas Karapatakis «Metaverse crimes in virtual (Un)reality: Fraud and sexual offences under English law» (Karapatakis, 2025), which states that the Metaverse is a virtual environment that uses technology to simulate the real world. The author examines issues related to criminal activity in the Metaverse. Given the potential applications of AI, cryptocurrencies and non-fungible tokens, he identifies three main problems: 1) decentralization, 2) user anonymity and 3) lack of regulation.

It is also worth highlighting the work G.M.Bovenzi (Bovenzi, 2023), which states that, as regards the topic of Metacrime, the precise boundaries have not yet been defined and there is no criminal liability for acts committed in the Metaverse.

It is worth noting this seminal work Eldar Haber "The Criminal Metaverse" (Haber, 2024), which demonstrates that virtual worlds are not mere fantasy; they open up new possibilities whilst simultaneously raising fears regarding criminal activity (financial and property crimes, crimes against the person, etc.). The author points out that immersive technologies may undermine criminal law, as they could lead to atypical crimes not described in the criminal code or in legal literature. In describing the taxonomy of crimes in the Metaverse, the author focuses on a fundamental conceptual question: is criminal law necessary to maintain order in a virtual society? His taxonomy relates both to behavior within the Metaverse and to explicit violations. In conclusion, the author puts forward the thesis that the Metaverse is unlikely to be free from crime. There should be no doubt that regulating the Metaverse, let alone its criminal aspects, will be no easy task. It will take time and effort before platforms, users and the state fully grasp the implications of using such technologies and their impact on our daily lives.

Another significant piece of work is an article by a group of authors «A scoping study of crime facilitated by the Metaverse» (Gómez-Quintero, 2024). The authors note that the Metaverse represents an emerging convergence of technologies and, unfortunately, the implications of these new technologies for crime and security are often overlooked. The authors anticipate the types of crime that the Metaverse may facilitate and present the results of a study conducted using the nominal group technique (NGT). Their findings provide a better understanding of the most dangerous and likely criminal threats that the Metaverse may give rise to and, consequently, help stakeholders priorities the crimes on which they should focus.

The second group comprises works that explore issues relating to cybercrime and digital forensics. These include works such as (Steinmetz, 2023), Author advances a theoretically informed realist criminology of computer crime. In other book (Baker, 2020), presents new research in artificial intelligence (AI) and law, with special reference to criminal justice. Next book "Cybercrime: An encyclopedia of digital crime" (Marion, 2020), is an encyclopedia that systematically examines Ransomware, Phishing, Identity Theft, Viruses, DDoS Attacks, Malware, Cyberterrorism, Hacking and etc. Pall Watters in the book "Cybercrime and cybersecurity" (Watters, 2023). indicates: "The field of cybersecurity and cybercrime is a critical and rapidly evolving area of study. As our society becomes more and more reliant on technology, the risks of cybercrime increase. This book provides a comprehensive introduction to the field, covering both cybercrime and cybersecurity."

A wonderful textbook has been prepared Alex Alexandrou "Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices" (Alexandrou, 2021). It states many books cover investigations, forensic recovery, and presentation of evidence, and others explain computer and network security, this book explores both, explaining the essential principles governing computers, wireless and mobile devices, the Internet of Things, cloud systems, and their significant vulnerabilities. This book deserves special attention Pierre Skorich and Matthew Manning "Insider Threat: A Systemic Approach" (Skorich, 2024), in which the authors establishing a new framework for understanding insider risk by focusing on systems of organization within large enterprises, including public, private, and not-for-profit sectors, this book analyses practices to better assess, prevent, detect, and respond to insider risk and protect assets and public good. Researchers are particularly interested in Nir Kshetri's book on the global cybercrime industry (Kshetri, 2010). Specifically, he points out «The cybercrime industry is a comparatively young area of inquiry. While there has been an agreement that the global cybercrime industry is tremendously huge, little is known about its exact size and structure. Very few published studies have examined economic and institutional factors that influence strategies and behaviors of various actors associated with the cybercrime industry. Theorists are also debating as to the best way to comprehend the actions of cyber criminals and hackers and the symbiotic relationships they have with various players».

The third group relates to literature on the shadow economy and its digital representation Works F. Schneider (Schneider, 2013) subsequent studies show that the shadow economy has a solid institutional foundation, whereas research by a group of authors (Ohrimenco, 2026), (Ohrimenco, 2023) allows us to directly refer to the SDE as a specific form of a digitally mediated shadow market embedded in information ecosystems.

The fourth group includes research on the metaverse, digital twins, blockchain, Web3, Industry 4.0/5.0, and the industrial metaverse. These sources are important because they demonstrate the emergence of new objects of digital value—virtual property, NFTs, digital real estate, self-identity authentication, digital twins, tokenized assets, and new platform-based frameworks for ownership and exchange. However, even within this group, the technological, legal, or industry-specific perspective predominates.

III. KEY BUSINESS MODELS AND ARCHITECTURE

The most common mistake in describing cybercrime is when researchers either focus solely on specific cyberattack techniques or reduce the topic to a mere list of X-*as-a-Service* models. However, the service format alone does not constitute a complete business model. Within the digital crime ecosystem, it is necessary to distinguish between:

- forms of packaging the function (e.g., *as-a-Service*);
- mechanisms for its operational implementation;
- the business models themselves, as sustainable schemes for the production, coordination, and extraction of destructive digital value.

At the *micro level*, Metacrime can be represented by individual tools, access points, a set of malicious functions, service units, infrastructure modules, and individual exchange entities. This is where the primary "commodity form" of illicit activity emerges: access, a malicious module, a bypass scheme, a concealment service, a distribution channel, a digital identity, an asset, or a data fragment.

At the *meso-level*, which is structurally dominant, the division of labor and the organization of collaboration occur simultaneously. It is here that access providers, developers, operators, intermediaries, call centers, consultants, infrastructure providers, trust actors, and financial executors transform individual functions into a coordinated service economy. In this environment, tasks are broken down and passed between specialized participants, while the platform or marketplace serves as the assembly point for the operation.

At the *macro level*, stability mechanisms are taking shape: trust, arbitration, quasi-market rules, reputation standards, platform governance, principles of inclusion and exclusion, and, in the long term, unique forms of digital governance. It is precisely here that Metacrime ceases to be a strictly organizational and technical environment and begins to manifest itself as an institutionally rich system.

IV. RESULTS AND DISCUSSION

Based on the results of their research, the authors propose, for the sake of analytical clarity and transparency, to consolidate the models listed above and reduce them to nine broad archetypes of criminal business models. This approach avoids the need to create a voluminous catalog of dozens of disparate services and instead focuses on describing the underlying structural logic. Each archetype will be represented by two data sets: the key function and the dominant revenue logic. Let us examine them in the following order.

1. R&D and optimization: vulnerability research, testing, tool refinement; service and consulting revenue.
2. Access and access brokering: acquiring, verifying, and reselling access; access revenue, revenue-sharing model.
3. Infrastructure, evasion, and resilience: hosting, anonymization, obfuscation, resilience; infrastructure and rental revenue.
4. Payload and malicious execution: infection, drainage, sabotage, encryption; subscription and performance-based revenue.
5. Operational outsourcing: call centers, solver functions, consulting, support; fee-based and service rent.
6. Markets, trust, and governance: escrow, ratings, arbitration, market-making; commission and intermediary rent.
7. Monetization, cash-out, and laundering: conversion, routing, mixing, drops; financial-routing rent.
8. Influence, deception, and reputation: deepfakes, bot farms, disinformation, review manipulation; information and reputation rent.

9. Meta-strategies and systemic reproduction: dual-use, digital reincarnation, adaptation, parasitic models; strategic and investment rent.

The most important feature of the proposed architecture is that the same solution can simultaneously function as a technical module, a service, and an element of a broader business model. For example, access can be the product of a direct transaction (sale), an entry point into a more complex operation, or part of a revenue-sharing scheme. Infrastructure can be a standalone entity—a service for sale, a hidden support circuit, or a node through which rent is captured. Consequently, Metacrime can be viewed as a construction set where individual modules are combined into new configurations, and economic sustainability is achieved through their reusability and interoperability.

V. CONCLUSIONS

The Metacrime architecture shows what the system consists of, but does not explain how it operates. This requires an analysis of the life cycle of destructive digital value. In the proposed model, this cycle includes the following interconnected phases: idea—research—development—testing—productization—service packaging—market coordination—monetization—profit distribution—reinvestment.

But this is not merely an abstract intention on the part of the offender; rather, it is the identification of a technological or organizational opportunity that can be economically rationalized as a source of future profit. In this sense, a Metacrime participant acts not only as a technical actor but also as an entrepreneur: they assess whether there is demand, whether they have sufficient resources of their own, whether they can rent the necessary functionality, acquire an intermediate asset, or integrate into an existing service chain.

The research phase transforms fragmented knowledge into a designable function. This stage involves analyzing vulnerabilities, competitor practices, existing services, technical constraints, market niches, and monetization options. Development then gives the idea a technical, organizational, or infrastructural form. This could be code, an access scenario, an obfuscation scheme, a financial roadmap, a consulting package, or a service module. Testing serves as a filter and initial validation of the business model: can the feature be scaled, is there sufficient demand, and how sustainable and compatible is it with other modules.

Productization refers to the process of transforming a project solution into a marketable product. As soon as a feature becomes transferable, rentable, updatable, and maintainable, it ceases to be a one-off initiative and becomes a marketable product. This is where the service layer comes into play: support, updates, training, consulting, customization, help desk, and sometimes—a guarantee of results. It is precisely in this phase that Metacrime definitively transcends the scope of individual criminal activity and becomes a service-oriented platform environment.

Market coordination integrates the service into a broader exchange ecosystem. At this stage, suppliers, intermediaries, operators, buyers, trusted parties, financial service providers, and infrastructure nodes come together. Intermediate assets—such as initial access—become a distinct liquid commodity. The better the mechanisms for trust, rating, and arbitration are established, the lower the transaction costs of illicit exchange. Specific markets for semi-finished products also emerge here: not for an unfinished attack, but for access, a route, a spoofed identity, a consulting service, a tool, or a monetization channel.

Monetization is the conversion of destructive digital value into a liquid form. Revenue can be generated through subscriptions, rentals, pay-per-use models, commissions, revenue shares, premium

services, consulting fees, or hybrid schemes. It is important to note that a significant portion of revenue is generated not at the level of the final malicious action, but at the level of control over the intermediate conditions that enable it: access, infrastructure, anonymization, trusted intermediation, routing, and cash-out.

Profit distribution within Metacrime is determined not only by participation but also by control over a critical node in the chain. The scarcity of a function, the supplier's reputation, the exclusivity of access, the degree of risk, and the ability to retain customers within the service loop define the revenue hierarchy. Therefore, a stable position in the ecosystem is not necessarily held by those who carry out the most "visible" attacks, but by those who control a recurring and scarce segment of the circulation of destructive digital value.

REFERENCES

Alexandrou, A., 2021. Cybercrime and information technology: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices.: CRC Press.

Baker, D. J. &. Robinson. P. H., 2020. Artificial intelligence and the law: Cybercrime and criminal liability.: Routledge.

Bovenzi, G. M., 2023. MetaCrimes: Criminal accountability for conducts in the Metaverse. In: Companion Proceedings of the ACM Web Conference 2023, April, pp. 565-567.

Gómez-Quintero, J., Johnson, S. D., Borrion, H., & Lundrigan, S., 2024. A scoping study of crime facilitated by the metaverse. Futures, Volume 157, p. 103338.

Haber, E., 2024. The Criminal Metaverse. Indiana Law Journal, Vol 99. (Iss 3).

Karapatakis, A. 2025. Metaverse crimes in virtual (Un) reality: Fraud and sexual offences under English law. Journal of Economic Criminology, 7, 100118.

Kshetri, N., 2010. The global cybercrime industry: economic, institutional and strategic perspectives.: Springer Science & Business Media.

Marion, N. E., & Twede, J., 2020. Cybercrime: An encyclopedia of digital crime.: Bloomsbury Publishing USA.

Ohrimenco, S., Orlova, D., & Cernei, V., 2026. The Shadow Digital Economy: Threats and Challenges for the Information Ecosystems. In: Value Creation in Digital Platforms and Business Ecosystems.: Routledge., pp. 50-72.

Ohrimenco, S., Orlova, D., & Cernei, V., 2023. Cyber threats modeling: An empirical study. Business Management/Biznes Upravlenie., 33(3), pp. 90-106.

Schneider, F., & Enste, D. H., 2013. The shadow economy: An international survey.: Cambridge University Press.

Skorich, P., & Manning, M., 2024. Insider Threat: A Systemic Approach.: Routledge.

Steinmetz, K. F., 2023. Against cybercrime: Toward a realist criminology of computer crime.: Routledge.

Tiwari, M., Zhou, Y., Gilmour, P., & Bernot, A., 2025. Confronting metacrime: complexities, enforcement challenges, and regulatory pathways. Law, Innovation and Technology., Vol 17. (1), pp. 159-176.

Watters, P. A., 2023. Cybercrime and cybersecurity.: CRC Press.

Zhou, Y., Tiwari, M., Bernot, A., & Lin, K., 2024. Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. Asian Journal of Criminology., Vol. 19(3), p. 419–439.