



THE POLITICAL-ECONOMIC NATURE OF THE SHADOW DIGITAL ECONOMY WITHIN THE SUSTAINABLE DEVELOPMENT PARADIGM

Serghei Ohrimenco

Laboratory of Information Security at the Academy of Economic Studies of Moldova, Chisinau, Moldova
<https://orcid.org/0000-0002-6734-4321>

Dinara Orlova

Financial University under the Government of the Russian Federation, Moscow, Russia
<https://orcid.org/0000-0002-2901-070X>

Valeriu Cernei

Partner, IT Audit&Advisory, BSD Management SRL, Chisinau, Moldova
<https://orcid.org/0000-0003-3300-334X>

ARTICLE INFO



Open access

JEL Category:
B51, D47, E11

Keywords:

shadow digital economy
sustainable development
political economy
cybersecurity
information and
communication
technologies

ABSTRACT

The paper examines the political-economic nature of the Shadow Digital Economy as an emerging structural phenomenon within the framework of sustainable development. The aim of the study is to develop a conceptual understanding of the Shadow Digital Economy as an adaptive subsystem of modern global capitalism and to identify its socio-economic and institutional consequences. The research applies critical political economy approaches, convergence theory, and structural and categorical analysis. It examines the impact of advanced digital technologies on the evolution of shadow activities. The findings demonstrate that the Shadow Digital Economy represents more than isolated cybercrime incidents; it forms hybrid value chains combining legal and illegal practices, contributes to institutional erosion, strengthens asymmetric power relations, and generates parasitic mechanisms of value extraction. The study concludes that the Shadow Digital Economy should be considered a latent form of digital conflict affecting economic resilience and sustainable development. The results are relevant for researchers, policymakers, cybersecurity professionals, and specialists in digital economy governance.

Address of the corresponding author:
Serghei Ohrimenco
osa@ase.md

Received: 24.05.2026
Revised: 16.07.2026
Accepted: 18.07.2026
Available online: 18.07.2026



1 INTRODUCTION

The rapid digitalization of the global economy has brought significant benefits in terms of innovation, productivity, and cross-border interactions. However, it has also given rise to a shadow digital economy (SDE), which constitutes a latent form of digital warfare. Unlike the traditional informal sector, SDE is deeply transnational, scalable, and technologically enabled. Its practices – ranging from cyberattacks and extortion to platform-based informal labor – reflect and intensify the contradictions of deregulated digital markets.

Existing literature on informal economies and network society has highlighted the structural role of informal and illicit activities in capitalism. However, studies of cybercrime often remain confined to technical or criminological approaches, neglecting the systemic and political-economic nature of SDE. This paper builds on critical political economy and digital capitalism studies to conceptualize SDE as an adaptive subsystem of the global economy, co-evolving with formal markets.

The aim of this study is to develop an original conceptual framework that interprets the Shadow Digital Economy (SDE) as a structurally adaptive subsystem of digital capitalism within the sustainable development paradigm. In doing so, the paper identifies the socio-economic and institutional consequences of SDE and proposes strategic directions for policy responses and future research.

2 THEORETICAL AND METHODOLOGICAL FRAMEWORK

The research is grounded in the traditions of critical political economy, drawing on post-Keynesian and neo-Marxist approaches to examine the contradictions of digital capitalism.

The framework extends heterodox economic theories of informality into the digital domain. SDE is viewed not as a collection of isolated crimes, but as a structurally adaptive subsystem of global capitalism that co-evolves with formal markets.

The methodological basis of the study includes:

- Critical political economy (post-Keynesian and neo-Marxist approaches), enabling analysis of SDE as part of global capitalism;

- Convergence theory, explaining the interpenetration of legal and illegal economic systems;
- Structural analysis of digital markets and illicit practices;
- Categorical analysis, justifying the inclusion of SDE in the domain of 'computer crimes';
- Examination of advanced IT technologies (AI, big data, blockchain, metaverse, deepfakes, etc.) as the key drivers of SDE.

The research design follows a qualitative conceptual approach aimed at constructing a theoretical interpretation of the Shadow Digital Economy. The analytical procedure consists of three interconnected stages: (1) identification of structural characteristics of digital capitalism; (2) examination of the interaction between formal digital markets and shadow practices; (3) synthesis of identified mechanisms into a conceptual framework explaining the role of SDE within sustainable development challenges.

Conceptual analysis is applied to clarify the theoretical boundaries of SDE and distinguish it from traditional informal economy and isolated cybercrime phenomena. The study examines relationships among digital infrastructures, economic incentives, institutional mechanisms, and forms of value extraction.

The reviewed literature was selected according to three analytical criteria: relevance to digital capitalism and political economy; contribution to understanding informal, illegal, or technologically mediated economic practices; and relevance to cybersecurity and sustainability challenges.

Despite extensive research on cybercrime, informal economies, and digital transformation, existing approaches often examine these phenomena separately. Cybersecurity studies primarily focus on technical vulnerabilities, while economic analyses of informality rarely consider technologically mediated and transnational forms of value extraction. This study addresses this gap by conceptualizing the Shadow Digital Economy as a systemic phenomenon emerging at the intersection of digital capitalism, institutional transformation, and cybersecurity challenges.

The theoretical contribution of this study consists in proposing a conceptual framework that interprets SDE not as a collection of illegal

activities but as an adaptive subsystem of digital capitalism characterized by hybrid value chains, institutional erosion, asymmetric power relations, and parasitic mechanisms of value extraction.

As a conceptual study, this research does not provide a statistical measurement of the SDE scale or empirical testing of causal relationships. The proposed framework should therefore be considered an analytical model that requires further empirical validation.

One of the most significant achievements of modern science has been the development of the concept of sustainable development (SD). Today, SD has become an indispensable requirement of the current stage of global progress, representing a fundamentally new and still-evolving field of synthetic knowledge.

The emergence of this concept should be understood as the outcome of a broad set of studies across natural sciences, the social sciences, and economics. Scholars emphasize both the novelty and the inherently interdisciplinary nature of this field, which calls for systematic research in order to more accurately reflect and integrate the results already achieved.

In this context, the subject of sustainability science has begun to take shape—a developing field that rethinks the interconnections between different domains and scales. At its core, it explores the interaction between nature and society, between science and practice, and between the global and the local. At the same time, it reflects on the relationship between the past, the present, and potential futures. Experts emphasize that, in the search for sustainable solutions, the structuring of knowledge within this complex and interdisciplinary domain is of fundamental importance (Danilina & Gerbina, 2024; Jerneck *et al.*, 2011; Komiya & Takeuchi, 2006).

Regarding the intellectual heritage of sustainable development, it should be noted that it has been shaped over a long period of time and can be divided into several distinct stages. The first stage, which dates back to the 19th century, reflects the emergence of a conscious approach to interaction with the environment and the rational use of natural resources. This period is represented in the works of T. Malthus, K. Marx, A. Comte, H. Spencer, and others. The philosophical and

worldview foundation of the concept of sustainable development is often associated with the doctrine of the *noosphere*, developed by the French thinkers É. Leroy and P. Teilhard de Chardin, as well as the Russian scientist V. Vernadsky.

The second stage is linked to the 1960s, when the global scale of emerging challenges became increasingly evident, and the search for collective solutions gained momentum. During this time, social and economic crises became a subject of systematic investigation by scientists, policymakers, business leaders, and civil society. In order to analyze the pressing issues of energy and raw materials, particularly in the context of the growing automobile industry, the Club of Rome was established. Its activities had a significant impact on the development of the concept of sustainable development. A milestone in this regard was the 1972 report *The Limits to Growth*, which is often considered one of the key stages in shaping the concept (Meadows *et al.*, 1972). The report presented computer modeling of global system dynamics, taking into account trends in industrialization, population growth, food production, environmental pollution, and the scarcity of resources.

Although the report was widely criticized for its methods and conclusions (Robinson, 1973), it drew much-needed attention to the idea that delaying responses to global problems and failing to take preventive measures in time leaves fewer viable options for development. The 1972 Stockholm Conference reinforced this perspective by highlighting the necessity of shifting priorities toward the ecological and economic sustainability of society. One of its outcomes was the creation of the United Nations Environment Program (UNEP), which stimulated new developments in environmental law, international cooperation, and global environmental policy.

A further landmark in the evolution of the concept was the 1987 publication of the report «Our Common Future», prepared by the independent Brundtland Commission after 900 days of work. The Commission's primary task was to identify practical ways of addressing global challenges. The report introduced the now-classic definition of sustainable development: *development that meets the needs of the present without*

compromising the ability of future generations to meet their own needs.

This conceptualization was further advanced at the 1992 Earth Summit in Rio de Janeiro (Brundtland, 1987). The Rio Declaration outlined methods and strategies for achieving sustainable development and identified its three fundamental pillars: social, economic, and environmental (UN, 2000). This declaration later served as the foundation for the formulation of the eight Millennium Development Goals (MDGs), which were set to be achieved by 2015:

- Eradicate extreme poverty and hunger.
- Achieving universal primary education.
- Promote gender equality and empower women.
- Reduce child mortality.
- Improve maternal health.
- Combat HIV/AIDS, malaria, and other diseases.
- Ensure environmental sustainability.
- Develop a global partnership for development.

The Sustainable Development Goals (SDGs), also known as the Global Goals, are a set of 17 ambitious objectives adopted by all United Nations Member States in 2015 as part of the 2030 Agenda for Sustainable Development. These goals provide a shared blueprint for peace and prosperity for people and the planet, aiming to achieve sustainable development in a balanced and integrated manner.

In recent years, the world has been navigating a global polycrisis characterized by the COVID-19 pandemic, escalating geopolitical tensions, armed conflicts, and the application of sanctions aimed at isolating individual countries. These developments have created a new, challenging reality, imposing additional constraints on our civilization's ability to achieve the Sustainable Development Goals.

Among the recent developments, the Fourth United Nations Conference on Financing for Development, held in Seville, Spain, and concluded on July 4, 2025, stands out. The conference outlined concrete measures to translate ambitious goals into tangible actions to overcome the financial crisis and accelerate the achievement of the SDGs. The adopted resolutions identify specific steps to reduce the

financing gap for sustainable development, which amounts to approximately 4 trillion dollars annually (UN, 2025; Wells, 2025) in developing countries.

3 LITERATURE REVIEW

The literature review can be structured along three main directions: digital capitalism and transformation of value relations; informality, cybercrime, and hybrid economic structures; cybersecurity as an institutional sustainability challenge.

3.1 Digital Capitalism and the Transformation of Value Relations

An important perspective is also presented in Christian Fuchs's «Digital Labor and Karl Marx» (Fuchs, 2014). The author draws on Marx's labor theory of value, where value is determined by the number of labor hours socially necessary for producing a commodity. Since the actual labor time for each item is difficult to measure, what matters economically is the average labor time required during a given period (for example, one year). This average can be calculated at the level of a single firm, an industry, or even internationally. Capital constantly seeks to reduce the value of commodities in order to increase profit margins. Reducing value means accelerating production, so that the same number of labor hours, which are tied to a certain monetary value, suddenly produces more goods. Although labor costs do not increase, surplus profit accumulates more rapidly.

The article by Andreas Wittel (2017) examines the political economy of digital technologies (PEDT) as an emerging but increasingly significant field, rooted in the political economy of media and communication (PEMC).

In essence, PEDT represents a contemporary strand of critical economic thought, examining how digital technologies integrate into the capitalist system and reshape socio-economic relations. Emerging from PEMC, PEDT significantly broadens the analytical lens: whereas PEMC traditionally treated media—television, radio, print, and later online media—as separate industries, PEDT views digital technologies as structural foundations of the entire economy.

Digitization today spans industry, transportation, education, healthcare, and social services, erasing distinctions between “media technologies” and other forms of technological innovation.

The theoretical framework of PEDT also deepens the analysis of digital capitalism through Marxist categories of labor, value, property, and alienation. Particular attention is paid to how value is created in the digital economy through immaterial and “free” labor, such as content creation, commenting, liking, and the generation of massive personal data sets. The processes through which platforms appropriate the results of collective activity are scrutinized, revealing new forms of labor and data alienation, alongside the phenomenon of digital rent—profit extracted through the monopolization of infrastructure, standards, and ecosystems. PEDT emphasizes that digital technologies are not neutral tools but socially embedded relations capable of reinforcing or transforming capitalism.

A defining feature of PEDT is its dual orientation toward critique and transformation. Research in this area examines cooperative platforms where users and workers co-own digital infrastructure, supports initiatives promoting open access and open source, and explores the development of digital commons as alternatives to corporate ownership. Democratic models for managing digital technologies, both locally and globally, and activist movements advocating digital justice and data protection are increasingly recognized as integral to the pursuit of social justice in a digitalized economy. In this way, PEDT combines classical political-economic analysis of capital, labor, and property with critical engagement with digital infrastructures, while also proposing practical strategies aimed at creating more equitable and democratic models for the use of digital technologies.

Finally, Gillian Youngs, in “Global Political Economy in the Information Age: Power and Inequality” (Youngs, 2007), presents a framework for understanding global political economy in the digital era. ICT infrastructures and their global spread have reshaped how we conceive of states and markets. ICT networks operate at multiple levels, within and across states and markets, linking public and private spaces, institutions and corporations, businesses with one another (B2B),

and companies with their customers (B2C) in real-time transactions across the globe. Youngs emphasizes that communication is not only a matter of technology but also of a social process. It concerns both organizational dynamics and the creation of specific products and services. Above all, this approach foregrounds communication as the fabric of social coexistence—the medium through which action is mediated and through which individuals and groups experience identity and belonging.

Digital capitalism transforms traditional mechanisms of value creation and creates new forms of dependence on digital infrastructures.

3.2 Informality, Cybercrime, and Hybrid Economic Structures

A further example is white-collar cybercrime (Gottschalk & Gunnesdal, 2018), associated with occupational and corporate misconduct. In their research, the authors employ the iceberg metaphor: the visible tip represents only a small fraction of the problem, while the full extent lies largely beneath the surface. This study is particularly valuable as crimes involving social security fraud compete with other forms of financial crime. Social security fraud often involves individuals in need of financial assistance to maintain a decent standard of living, whereas other white-collar crimes are perpetrated by elites who exploit their positions for personal or organizational gain, amplifying societal harm.

Another significant work, Grady and Parisi (2006), highlights that cybercrime imposes enormous economic costs and is highly resistant to conventional prevention and deterrence strategies. Unlike traditional crime, which typically targets certain individuals but results in relatively few direct victims, cybercrime impacts virtually all citizens and organizations, influencing everyday life on a broad scale.

Another study turns to the concept of “cybershadows” (Nordstrom, 2014), with findings that are striking in scope. The book surveys the darker dimensions of the digital world, mapping threats and innovations in cybercrime, espionage, and surveillance, as well as new forms of attack that move beyond data theft to target behavioral

patterns, neurological processes, and even DNA, all within lucrative markets for exploitation.

Despite a substantial body of literature, this field remains insufficiently equipped to respond effectively within the context of the shadow digital economy (SDE), due to significant theoretical and practical gaps. Nevertheless, it is important to reference the most influential studies. Among them is (Moallem, 2025), where the author explores the human factor underpinning cyberattacks, as well as the behavioral patterns that contribute to their success.

The starting point of this study lies in identifying the macro-trends that shape contemporary business. For instance, Stephen J. Andriole (Andriole, 2005) highlights two central tendencies:

- The first, or business trend, is collaboration. This refers to companies engaging with employees, customers, suppliers, and partners in new and ongoing ways.
- The second trend is technological integration. Systems once used for accounting, customer communication, or employee information management are now increasingly interconnected, exchanging data and building on each other's analyses to drive and expand collaboration.

According to the author, the intersection of these two trends produces a powerful business-technology synergy. The crucial point is that collaboration and technological integration are tightly intertwined. Collaboration is becoming ever more dependent on technology, while technologies themselves are increasingly integrated, thereby enabling and reinforcing collaborative business models. Such models require not only process integration but also data integration. Business technologies remain "tactical" and "operational"—computers and networks still need to function reliably—but they have also become highly "strategic." They now have the potential to make or break a company, particularly as the pace of collaborative and integrative trends accelerates. Organizations are discovering ways to enhance the efficiency of existing processes while simultaneously adding new, cooperative ones.

Existing studies explain specific forms of cybercrime but rarely conceptualize them as a systemic economic phenomenon.

3.3 Cybersecurity as an institutional sustainability challenge

The Shadow Digital Economy (SDE) is defined in this study as a technologically mediated sphere of economic activity that operates partially outside formal institutional regulation while remaining structurally connected with legitimate digital markets. The rise of the SDE, characterized by hidden, unregulated, and often illicit digital activities, intensifies the complexity of cybersecurity. As evidenced by China's experience, rapid digitalization, while fostering innovation and growth, also amplifies systemic exposure to cyber threats that erode economic resilience. These threats are not merely technical disruptions but manifestations of deeper structural vulnerabilities within digital ecosystems.

This convergence of SDE and cybersecurity concerns also transcends the economic domain, as Olejnik and Kurasiński (2023) highlight: the societal implications of cybersecurity failures—from critical infrastructure to democratic institutions—are profound. Authors Olejnik and Kurasiński (2023) argue that cybersecurity cannot be reduced to data or computer protection alone; rather, it encompasses the security of society as a whole. They stress that cybersecurity concerns affect almost everyone, including individuals who may not actively use computers, smartphones, or social networks. Their analysis begins with the concept of risk and its typologies and continues through discussions of cyberattacks. Importantly, they examine the vulnerabilities of users and the exposure of critical social domains such as infrastructure, healthcare, military and strategic systems, and the state itself. Their conclusion is unequivocal: as digitalization advances, the challenges of cybersecurity cannot be avoided, as cybercrime advances, as well.

Author (Cobos, 2024) emphasizes that the importance of cybersecurity cannot be overstated, particularly for developing countries, which face heightened exposure to cyber threats. Vulnerability in these countries is often exacerbated by a combination of factors: limited resources, underdeveloped infrastructure, political

instability, inefficient cybersecurity markets, a shortage of qualified specialists, legal gaps, and the rapid pace of digital technology adoption. The consequences of cyber incidents can be profound, ranging from economic downturns that destabilize entire economies to disruptions in the provision of critical services, thereby hindering socio-economic development. The book is structured into three sections: The Threat Landscape, The Economic Costs of Cyber Incidents, and The Cybersecurity Market. The author prefaces the material with a clear call to action: "Securing our digital future hinges on our commitment to efficient cybersecurity. It is not just an option. It is a vital imperative."

A collective of authors, Pal et al. (2023), investigates contemporary cybersecurity challenges using advanced technologies such as artificial intelligence, quantum cryptography, and blockchain. They analyze quantum computing, post-quantum digital signatures, and AI applications for securing modern networks, while also reviewing various cyberattacks, protective measures, strategies, and countermeasures. The book presents novel approaches for intelligent, proactive responses to today's cyber threats, emphasizing both technological innovation and strategic foresight.

Heikki Patomäki's book (Patomäki, 2007) offers a pioneering investigation into the future of wars, crises, and transformations within the global political economy. Bringing together economic theory, political economy, peace and conflict studies, philosophy, and historical analogy, the work explores alternative futures (Patomäki, 2007). Patomäki develops an original and thought-provoking political-economic critique of neoliberalization and globalization at the end of the twentieth century, describing their real-world consequences as a twenty-first century form of imperialism. He argues that even a partial return to nineteenth-century ideals and practices would likely be profoundly counterproductive today, potentially setting the stage for a global catastrophe.

Cybersecurity failures represent not only technological risks but institutional and developmental challenges.

4 RESULTS AND CONCLUSIONS

The influence of SDE on sustainable development can be observed through three major mechanisms: institutional degradation, unequal distribution of digital value, and increased vulnerability of critical infrastructures.

Figure 1 presents the conceptual model developed in this study. It illustrates how digital capitalism and technological infrastructures create conditions for the emergence of SDE, which subsequently affects institutional stability, cybersecurity, and sustainable development trajectories.

The model conceptualizes digital capitalism as the macro-level environment that stimulates the expansion of digital infrastructures and creates conditions for technological innovation, platformization, and data commodification. These infrastructures simultaneously enable legitimate economic activities and generate structural vulnerabilities associated with regulatory asymmetries, technological complexity, and cross-border digital interactions. Within this environment, the Shadow Digital Economy emerges as an adaptive subsystem that exploits existing digital infrastructures through hybrid legal-illegal value chains, cybercrime ecosystems, informal digital labor, and illicit digital markets. The functioning of SDE produces institutional consequences, including the erosion of governance capacity, declining public trust, regulatory fragmentation, and weakened fiscal sovereignty, while simultaneously increasing cybersecurity risks through the expansion of the cyberattack surface and systemic vulnerabilities. These interconnected processes ultimately undermine the economic, institutional, and social dimensions of sustainable development, reducing societal resilience and impeding progress toward the Sustainable Development Goals. The framework emphasizes that these relationships are dynamic and mutually reinforcing, suggesting that SDE should be understood not as a collection of isolated illegal activities but as a structural phenomenon embedded within the contemporary political economy of digital capitalism.

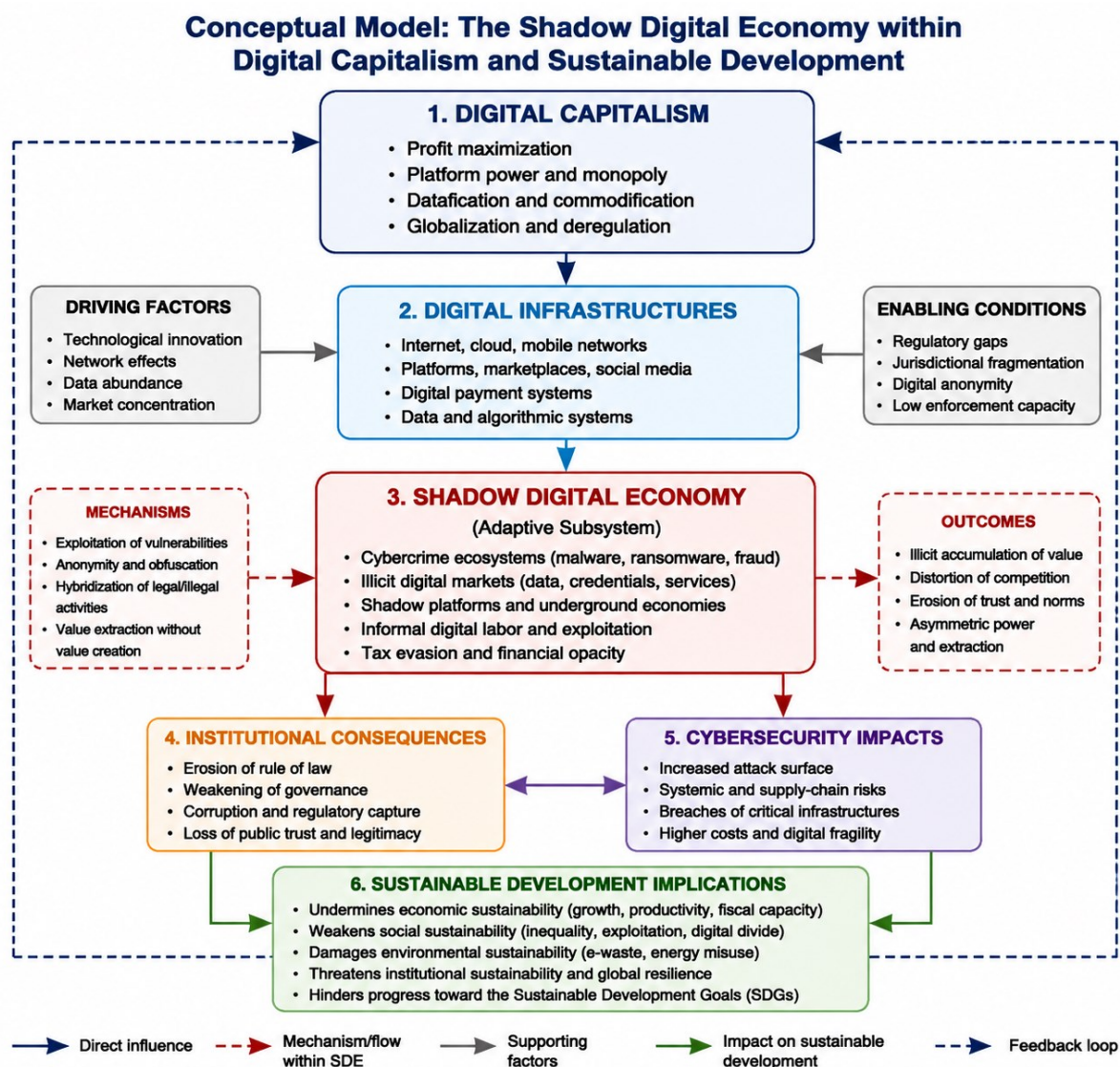


Figure 1. The SDE within Digital Capitalism and Sustainable Development

Source: elaborated by the authors

The analysis yields several key findings regarding the structural nature and consequences of SDE:

1. **Dual Value Chains:** Legal and illegal digital markets increasingly overlap, creating hybrid chains of value. Shadow actors exploit the same infrastructures—telecommunications, cloud services, and financial systems—relied upon by legitimate enterprises. This entanglement blurs regulatory boundaries and normalizes shadow practices.
2. **Institutional Erosion:** SDE erodes state capacity by shrinking tax revenues, incentivizing corruption, and weakening enforcement. This institutional degradation is most visible in areas where regulatory frameworks lag behind technological change, but even advanced economies have diminished fiscal sovereignty.
3. **Asymmetric Power Relations:** The results highlight stark asymmetries between states and private actors. While governments face jurisdictional limits, transnational corporations and shadow networks exploit digital flows across borders, deepening inequalities both domestically and internationally.
4. **Parasitic Dynamics:** SDE exemplifies a parasitic relationship with the formal economy, extracting value without contributing to the maintenance of public infrastructure. The concept of parasitic mechanisms refers to forms of value extraction where shadow

actors benefit from existing digital infrastructures and institutional resources without proportionally contributing to their maintenance. The costs of policing, cybersecurity, and institutional repair are externalized to the state, while shadow actors capture rents with near impunity.

5. Latent Digital Warfare: Finally, SDE functions as a form of low-visibility digital conflict, providing 'Shadow Fog' on economic activities. Shadow fog is a condition of reduced transparency and uncertainty within

digital economic interactions. Rather than dramatic, one-time cyberattacks, their impact accumulates gradually through lost revenues, weakened trust, systemic data breaches, and widening inequalities, constituting a chronic mode of institutional disruption.

6. Together, these findings underscore that SDE is not reducible to isolated cybercrime events but should be understood as an evolving subsystem of global capitalism with long-term destabilizing effects.

REFERENCES

- Andriole, S. J. (2005). *The 2nd digital revolution*. IGI Global. ISBN 978-1591408017
- Balbi, G. (2023). *The digital revolution: A short history of an ideology* (B. McClellan-Broussard, Trans.). Oxford University Press, 159 pp. <https://doi.org/10.1515/commun-2024-0116>
- Brecher, C., Padberg, M., Jarke, M., Aalst, W.v.d., Schuh, G. (2024). The internet of production: Interdisciplinary visions and concepts for the production of tomorrow. In: Brecher, C., Schuh, G., van der Aalst, W., Jarke, M., Piller, F.T., Padberg, M. (eds) *Internet of Production. Interdisciplinary Excellence Accelerator Series*. Springer, Cham. https://doi.org/10.1007/978-3-031-44497-5_1
- Brundtland, G. H. (1987). Our common future world commission on environment and development. 20 March 1987. Retrieved from <https://www.are.admin.ch/en/1987-brundtland-report>
- Cobos, E. V. (2024). *Cybersecurity economics for emerging markets*. World Bank Publications. <https://doi.org/10.1596/978-1-4648-2120-2>
- Danilina, Y. V., & Gerbina, T. V. (2024). Sustainable Development. Systematization of Subject Domain. *Scientific and Technical Information Processing*, 51(4), 329-339. <https://doi.org/10.3103/S0147688224700709>
- Fuchs, C. (2014). *Digital labour and Karl Marx*. Routledge. <https://doi.org/10.4324/9781315880075>
- Gottschalk, P., & Gunnesdal, L. (2018). *White-collar crime in the shadow economy: Lack of detection, investigation and conviction compared to social security fraud*. Springer. <https://doi.org/10.1007/978-3-319-75292-1>
- Grady, M. F., & Parisi, F. (Eds.). (2006). *The law and economics of cybersecurity*. Cambridge University Press. <https://doi.org/10.2139/ssrn.622985>
- Hahnel, R. (2017). *Radical political economy: Sraffa versus Marx*. Routledge. <https://doi.org/10.4324/9781315169149>
- Jerneck, A., Olsson, L., Ness, B., Anderberg, S., Baier, M., Clark, E., ... & Persson, J. (2011). Structuring sustainability science. *Sustainability science*, 6(1), 69-82. <https://doi.org/10.1007/s11625-010-0117-x>
- Kitsing, M. (2021). *The political economy of digital ecosystems: Scenario planning for alternative futures*. Routledge. <https://doi.org/10.4324/9781003129264>
- Komiyama, H. & Takeuchi, K. (2006) Sustainability Science: Building a New Discipline. *Sustainability Science*, 1, 1-6. <https://doi.org/10.1007/s11625-006-0007-4>

- Meadows, D. H., Meadows, D. L., Randers, J., & Behrens, W. W. III. (1972). *The limits to growth*. Universe Books. Retrieved from <https://www.donellameadows.org/wp-content/userfiles/Limits-to-Growth-digital-scan-version.pdf>.
- Moallem, A. (2025). *Human Factors Analysis of 23 Cyberattacks*. CRC Press. <https://doi.org/10.1201/9781003461739>
- Nordstrom, C., & Carlson, L. (2014). *Cyber shadows: Power, crime, and hacking everyone*. ACTA Publications. ISBN 9780991245109
- Olejnik, L., & Kurasiński, A. (2023). *Philosophy of Cybersecurity*. CRC Press. <https://doi.org/10.1201/9781003408260>
- Pal, O., Kumar, V., Khan, R., Alam, B., & Alam, M. (Eds.). (2023). *Cyber Security Using Modern Technologies: Artificial Intelligence, Blockchain and Quantum Cryptography*. CRC Press. <https://doi.org/10.1201/9781003267812>
- Patomäki, H. (2007). *The political economy of global security: War, future crises and changes in global governance*. Routledge. <https://doi.org/10.4324/9780203937464>
- Robinson, W.C. The limits to growth: A report for the club of rome's project on the predicament of mankind Donella H. Meadows, Dennis L. Meadows, Jergen Randers, and William W. Behrens, III. *Demography* **10**, 289–299 (1973). <https://doi.org/10.2307/2060819>
- Schmitt, M., & Koutroumpis, P. (2025). Cyber shadows: Neutralizing security threats with AI and targeted policy measures. *IEEE Transactions on Artificial Intelligence*, 6(7), 1697-1705. <https://doi.org/10.1109/TAI.2025.3527398>
- Spread, P. (2018). *Economics for an information age: money-bargaining, support-bargaining and the information interface*. Routledge. ISBN:9780429792687
- UN. (2025, 06 30). *Special Coverage of Fourth International Conference on Financing for Development*. Retrieved from UN: <https://news.un.org/en/events/ffd4-sevilla/date/2025-06-30>
- Wells, M. (2025, 07 02). *Drowning in debt*. Retrieved from UN News: <https://news.un.org/en/story/2025/07/1165196>
- Wittel, A. (2017). The political economy of digital technologies: Outlining an emerging field of research. *Digitisation*, 251-275. <https://doi.org/10.4324/9781315627731-14>
- Youngs, G. (2007). *Global political economy in the information age: Power and inequality*. Routledge. <https://doi.org/10.4324/9780203964064>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs. ISBN 978-1-61039-570-0