COMPLEMENTARY MODEL OF CYBERSECURITY, ANTI-CORRUPTION AND ECONOMIC DE-SHADOWING REFORMS: A ROADMAP FOR WARTIME AND POST-WAR DEVELOPMENT

Viktoriia Bozhenko[1]

DOI: https://doi.org/10.30525/978-9934-26-715-4-2

Abstract. *Subject of the study.* The subject of this study is the conceptualization and development of a complementary model for state regulation that integrates cybersecurity, anti-corruption, and economic de-shadowing reforms into a unified, synergistic system. Under the conditions of unprecedented geopolitical and geoeconomic challenges, the architecture of Ukraine's economic security requires radical transformations. Traditional, isolated approaches to combating the shadow economy and corruption are no longer effective, as illicit financial flows and corrupt practices have massively migrated into the digital dimension, utilizing cryptocurrency networks and exploiting vulnerabilities in state information systems. Consequently, the study focuses on how proactive cybersecurity acts as the fundamental basis for successful anti-corruption and de-shadowing efforts, forming a holistic and resilient architecture of the national economy during both wartime and post-war periods.

Goal of the study. The primary goal of the study is to develop a comprehensive, logically sequenced three-stage roadmap for state reforms based on the principles of complementary provision. This roadmap aims to formulate a resilient economic system capable of protecting critical digital infrastructure, ensuring total digital control and accountability over the distribution of massive international financial assistance, neutralizing the mutually reinforcing "triple threat" (cybercrime, corruption, and money laundering), and ultimately facilitating Ukraine's full-fledged economic, legal, and technological integration into the European Union's Digital Single Market.

[1] Candidate of Economic Sciences (PhD in Finance), Associate Professor, Associate Professor of the Department of Economic Cybernetics, Sumy State University, Ukraine

© Viktoriia Bozhenko

Methodology. The methodological framework of the research is grounded in a systemic approach, exploring the functional emergence, mutual conditionality, and institutional coherence of cybersecurity, anti-corruption, and de-shadowing policies. The study employs a comparative analysis of international best practices, drawing upon the government-led digitalization models of countries with high digital readiness and advanced regulatory frameworks. Furthermore, the research utilizes analytical and empirical methods to assess the impact of digital transformations, leveraging data from international organizations and national authorities. A significant methodological emphasis is placed on modelling the predictive capabilities of Artificial Intelligence and Machine Learning algorithms – specifically recurrent neural networks, XGBoost, and big data analytics – as transformative tools for transitioning from reactive to predictive financial monitoring and proactive cyber defence.

Conclusion of the study. The study concludes that the isolated implementation of technological innovations or legal frameworks is insufficient to guarantee macroeconomic security without a strong institutional foundation, effective compliance, and a societal culture of zero tolerance for corruption. Overcoming the cumulative impact of modern economic threats demands a complementary approach where strengthening cyber resilience inherently boosts the effectiveness of anti-corruption and de-shadowing efforts. The proposed roadmap outlines a strategic pathway through three distinct phases: Stage I "Resilience" (wartime emergency cyber defence and digital control of international aid); Stage II "Reconstruction" (regulation of virtual assets, AI-driven financial monitoring, and adherence to the green and digital "twin transition"); and Stage III "Integration" (synchronization with the EU digital and customs space, fostering deep institutional cyber hygiene). Ultimately, the synergy of robust cyber protection, transparent digital ecosystems, and strict whistleblower protections will create a secure business environment. This comprehensive model guarantees the irreversible de-shadowing of capital, protects international donor investments from embezzlement, and ensures Ukraine's successful long-term transformation into a specialized, knowledge-driven European economy.

INTRODUCTION

Under the conditions of unprecedented geopolitical and geoeconomic challenges caused by full-scale armed aggression, the architecture of the state's economic security is undergoing radical transformations. The modern paradigm of public administration and macroeconomic regulation is inevitably shifting into the realm of total digitalization of economic processes, the development of e-government, and the implementation of innovative financial technologies. On the one hand, digitalization is a powerful driver of economic growth and transparency, but on the other hand, it generates new, asymmetrical threats in cyberspace [11; 12]. In this context, traditional approaches to countering key destructive phenomena (in particular, the shadow economy and corruption) are exhausting their effectiveness, which determines the objective need to develop novel, synergistic mechanisms of state regulation of the national economy.

Previously, the policy of de-shadowing and anti-corruption was considered as a complex of administrative, law enforcement, and fiscal measures. However, with the development of the digital economy, the nature of these phenomena has significantly transformed. Shadow financial flows and corruption payments are massively moving into the digital dimension, using cryptocurrency transactions, anonymous payment systems, and vulnerabilities in the architecture of state registers for masking [3; 25]. It is impossible to overcome the shadow economy and corruption without an appropriate level of cybersecurity due to a few fundamental reasons:

– vulnerability of the transparency infrastructure. Key instruments of the anti-corruption infrastructure and de-shadowing (electronic procurement systems, automated VAT refund systems, unified state demographic and property registers) are complex information and communication systems. An insufficient level of their cyber protection creates opportunities for unauthorized interference to modify data, falsify bidding results, or destroy traces of economic crimes [29]. In this case, corruption does not disappear but acquires a latent, high-tech form – cyber corruption.

– relocation of shadow capital to unregulated cyberspace. Existing methods of financial monitoring often do not allow for the effective identification of signs of fictitious operations related to money laundering if they are carried out through hacked or poorly protected decentralized

financial networks and shadow cryptocurrency platforms [28]. Only proactive cybersecurity and the use of cyber intelligence tools can ensure the traceability of such operations.

– trust in state institutions. Effective de-shadowing requires a high level of trust between citizens and businesses in the state (voluntary payment of taxes, legalization of income). Any large-scale leak of personal data or failure in the operation of state financial services because of a cyberattack critically undermines this trust, provoking the outflow of capital into the shadows [23].

Consequently, cybersecurity acts not merely as a technical superstructure, but as a fundamental basis for the successful implementation of anti-corruption and de-shadowing reforms. Without ensuring the confidentiality and availability of the state's information assets, any attempts to overcome corruption or bring the economy out of the shadows will be neutralized by the technological vulnerability of the systems that serve them.

The complementary provision of cybersecurity, anti-corruption, and economic de-shadowing is critically necessary, since these phenomena form a single system of mutually reinforcing threats with a cumulative negative impact on the institutional and macroeconomic stability of the state [33]. In the context of the economic security of the state, complementary provision is a systemic, mutually complementary, and mutually reinforcing mechanism for integrating institutional, regulatory, financial, and information-technology tools, under which the strengthening of one component (for example, cyber resilience) immanently leads to an increase in the effectiveness of other components (anti-corruption and de-shadowing), thus forming a holistic, resilient architecture of the national economy.

The complementary provision of cybersecurity, anti-corruption, and economic de-shadowing is characterized by the following key features:

– functional emergence: the combined effect of the simultaneous implementation of reforms in the areas of cyber defense, anti-corruption, and narrowing the shadow sector significantly exceeds the simple sum of the effects of their separate implementation.

– mutual conditionality: achieving the strategic goals of de-shadowing is impossible without ensuring the cybersecurity of the financial sector, just as effective cybersecurity requires financial resources generated by bringing

the economy out of the shadows and eliminating corruption leaks from the budget.

– institutional coherence: synchronization of actions of specialized agencies (State Service of Special Communications, Ministry of Digital Transformation, National Anti-Corruption Bureau of Ukraine, National Agency on Corruption Prevention, Economic Security Bureau of Ukraine, National Bank of Ukraine), which eliminates duplication of functions and ensures seamless data exchange in real-time.

Considering the above, the development of a roadmap for reforms based on the principles of complementary provision is a critically necessary step for the formation of a resilient economic system in Ukraine. This approach acquires particular importance under the conditions of martial law and future post-war reconstruction, when massive volumes of international financial assistance will require an unprecedented level of transparency, accountability, and protection of the digital infrastructure from cybernetic interference by the aggressor state and transnational criminal groups.

Since fragmented steps in the face of institutional vulnerability cannot provide adequate protection, only a systemic, step-by-step approach will allow achieving the synergy of technological, legal, and regulatory tools. Accordingly, the architecture of such a roadmap should consist of three logically sequential stages:

Stage I "Resilience" (wartime period), focused on emergency cyber defense of critical infrastructure and total digital control over the distribution of international aid;

Stage II "Reconstruction" (first post-war years), aimed at the de-shadowing of capital through the regulation of the cryptocurrency market, the creation of a financial monitoring ecosystem based on artificial intelligence, and the implementation of the principles of the green and digital economy;

Stage III "Integration" (long-term period), the strategic goal of which is complete merger with the EU Digital Single Market and deep rooting of the institutional culture of cyber hygiene and zero tolerance for corruption.

1. Resilience: Countering Cyber Threats, the Shadow Economy, and Corruption during Wartime

In wartime conditions, hybrid threats and geopolitical conflicts provoke a rapid increase in cybercrime, which aims not only at causing direct

financial damage but also at the strategic destruction of critical information infrastructure, and the destabilization of government portals and mass media. Armed conflicts significantly weaken the institutional capacity of the state and create a favourable environment for the expansion of the shadow economy, which generates a cumulative and mutually reinforcing impact on socio-economic vulnerability.

When forming such a comprehensive system of emergency protection of critical infrastructure, it is crucial to rely on the advanced foreign experience of countries that demonstrate the highest efficiency in countering financial and cybernetic crimes. Studies confirm that countries such as Denmark, Finland, Norway, Sweden, and the Netherlands have the highest level of digital readiness to combat corruption and cyber threats. These countries are dominated by a governance profile characterized by government-led digitalization, where state institutions play a leading role in building digital infrastructure and electronic services [11; 9]. Their experience proves a fundamental rule: digital indicators and technological innovations are not independent determinants of security and can deter illegal practices only when they are supported by a strong institutional base, effective control, and strict limitation of abuses of power [19; 27].

One of the key tasks at the first stage of implementing the roadmap is the emergency protection of critical information infrastructure [6]. Targeted cyberattacks on energy systems, transport networks, and financial institutions can cause critical disruptions in the functioning of society, massive leaks of confidential data, and extremely serious economic damage. A striking example of the vulnerability of the telecommunications sector in wartime conditions is the large-scale hacker attacks on state websites and national telecom operators (in particular, the unprecedented attack on the “Kyivstar” company in Ukraine, which led to the destruction of about 40% of the infrastructure and left 24 million subscribers without communication).

Given these unprecedented challenges, emergency protection of critical information infrastructure requires not point-based solutions, but continuous improvement and flexible adaptation of protective measures to guarantee the stability of financial and information systems in the global digital environment. Ensuring national cyber resilience directly depends on the close interaction of the state’s institutional, technological, and financial capabilities. At this stage, it is critically important to rely on the advanced

foreign experience of countries with a high level of digital readiness. In particular, the practice of Germany is extremely effective, where the Federal Office for Information Security (BSI) was created, which develops strict standards and ensures reliable cyber protection for both public and private institutions.

Strengthening the emergency protective mechanisms of critical information infrastructure also requires the mandatory implementation of innovative technologies, such as artificial intelligence-based threat detection systems and blockchain technologies to ensure absolute transparency of transactions and data immutability [8; 24]. Only a systemic convergence of cyber defence and financial monitoring mechanisms allows for effectively countering integrated criminal networks and guaranteeing the uninterrupted functioning of critical infrastructure in conditions of heightened structural vulnerability.

The second critical direction of this stage is total digital control over the distribution of international military and humanitarian aid, which serves as the basis for anti-corruption compliance [1]. Within the framework of the European Union's Ukraine Facility funding for 2024-2027, 50 billion euros are envisaged to support the state budget, stimulate investments, and provide technical assistance [16]. In addition, according to the official data of the Ministry of Finance, in 2025 Ukraine attracted USD 52.4 billion in external financing, of which over 70% came through the mechanism of G7 country loans secured by revenues from frozen Russian assets [17].

As international historical experience demonstrates, the activities of the US Special Inspector General for Afghanistan Reconstruction (SIGAR), the lack of total digital oversight at early stages inevitably leads to massive losses of donor funds. Considering this, digital financial technologies must become the uncontested basis for creating new mechanisms to combat the shadow economy and illicit financial flows [30]. The architecture of such control must be built based on distributed ledger technologies and automated tracking systems, which allow for completely neutralizing the influence of the human factor. Innovative and technological tools have already proven their effectiveness in deterring corruption in EU countries, as they increase transparency, optimize public administration processes, and facilitate public access to transactional information [4; 14]. The integration

of such digital solutions into logistical and financial chains will ensure automatic cross-checking of databases of customs, logistics operators, and ultimate beneficiaries, minimizing opportunities for abuse and guaranteeing the preservation of institutional trust on the part of international partners.

2. Digital Economic Reconstruction

The second stage of the roadmap is focused on de-shadowing the economy, attracting investments, and large-scale transformation of the state on modern innovative foundations using advanced digital tools. One of the key challenges during this period is the comprehensive regulation of the cryptocurrency market to bring capital out of the shadows. Criminals actively use virtual assets to bypass traditional requirements of the financial system and rapidly move illicit funds, which is particularly dangerous in conflict and post-conflict conditions [3; 28]. According to the Global Crypto Adoption Index report by the international analytical company Chainalysis, the volume of cryptocurrency transactions related to Ukraine reached a record USD 206.3 billion [5]. At the same time, the Eastern Europe region generally demonstrates one of the highest levels of interaction with illegal crypto addresses in the world, the operations for which are associated with money laundering, ransomware, and cross-border fraud. Although globally the share of illicit cryptocurrency transactions is gradually decreasing and currently stands at about 1.2% of the total volume of blockchain activity, in absolute monetary equivalent this figure is measured in tens of billions of dollars of uncontrolled shadow capital.

The need for regulatory settlement of this market is driven by the task of transforming hidden liquidity into an open internal investment resource for the reconstruction of the state. The instrumental basis for a comprehensive reform is the harmonization of national legislation with the European Markets in Crypto-Assets Regulation (MiCA – Regulation (EU) 2023/1114) and the standards of the Financial Action Task Force (FATF), in particular Recommendation 16 (“Travel Rule”). The implementation of this regulatory model requires the adoption of a new version of the specialized law “On Virtual Assets” and amendments to the Tax Code of Ukraine, which provides for the establishment of clear taxation rates on the investment income of individuals and legal entities, official licensing

of crypto-asset service providers (CASPs), as well as designating the National Bank of Ukraine and the National Securities and Stock Market Commission as the key regulators of the sector.

The de-shadowing effect is achieved through the introduction of mandatory customer due diligence procedures, verification of the origin of funds, and mandatory accompanying of transactions with information about the sender and recipient. The integration of state supervisory bodies and the banking sector with advanced analytical on-chain monitoring systems (such as Chainalysis KYT, Elliptic, or Crystal Intelligence) allows tracking suspicious clusters of addresses in real-time, detecting interaction with sanctioned entities or darknet platforms, and blocking illegal financial flows even before they are converted into fiat currency. The legalization of virtual asset operations will enable Ukrainian business to attract venture capital and foreign direct investments, issue asset-backed tokens to finance the reconstruction of industrial and municipal facilities and increase tax revenues to the consolidated budget by tens of billions of hryvnias annually. The complementarity of this measure in the reform roadmap lies in the fact that the regulatory cleansing of the crypto market simultaneously eliminates the financial base for cybercriminals, neutralizes opportunities for corrupt capital withdrawal by officials, and creates a transparent financial infrastructure that fully meets the criteria for integration into the EU Digital Single Market [2].

In parallel with the regulatory settlement of virtual assets, a critical requirement is the creation of a unified financial monitoring ecosystem using artificial intelligence and big data. According to estimates by the United Nations Office on Drugs and Crime (UNODC), the annual volume of laundered funds globally ranges from 2% to 5% of global GDP, which in absolute terms equals 800 billion to 2 trillion US dollars [32]. At the same time, the effectiveness of traditional methods remains critically low: existing conservative monitoring systems allow returning or blocking only about 0.1% of criminal assets. The main drawback of the classical approach, based on rigidly set rules and scenarios (rule-based systems), is an extremely high level of false positives, which in the field of financial monitoring averages 90-95%. This creates a colossal operational burden on analysts and leads to so-called “alert fatigue,” when real threats are lost among thousands of perfectly legitimate transactions.

The integration of artificial intelligence and machine learning algorithms fundamentally changes the architecture of financial monitoring, ensuring the transition from a reactive to a predictive response model. Studies by leading international consulting companies, in particular McKinsey and Deloitte, confirm that the introduction of machine learning into transaction monitoring processes allows increasing the accuracy of detecting suspicious activity by 40% and overall operational efficiency by 30%. At the same time, the level of false positives decreases by at least 40-50%, which frees up significant human and time resources for investigating deeply hidden and non-standard schemes [15].

The use of machine learning algorithms allows the system to analyze millions of transactions in real-time, automatically detecting financial anomalies, fictitious supply chains, hidden links between counterparties, and politically exposed persons (PEPs). Since artificial intelligence makes decisions on blocking operations solely based on mathematical models and risk scoring, this completely eliminates the human factor, precluding bribery or manual intervention by inspectors in business verification processes [8].

The implementation of such tools has a colossal impact on the de-shadowing of the economy in the context of post-war reconstruction, when total control over the targeted movement of donor funds is a basic requirement of international partners. According to official data from the State Financial Monitoring Service of Ukraine thanks to automation and the improvement of analytical tools, the total amount of stopped suspicious financial transactions related to the legalization of criminal proceeds and corruption offenses exceeded 115 billion hryvnias at the end of 2025 [7]. The transition from manual monitoring to automated systems based on Big Data (for example, the updated VAT risk assessment criteria monitoring system) increases the accuracy of detecting fictitious transactions and tax evasion schemes by 40-45% [20]. This allows tax authorities to focus exclusively on high-risk entities, radically reducing administrative pressure on transparent business. In addition, the National Bank of Ukraine notes that the application of AI analytics makes it possible to cover 100% of cross-border transfers related to the implementation of infrastructure restoration projects with predictive supervision, excluding the risk of their withdrawal to offshore jurisdictions [18].

Besides direct transaction monitoring, the application of deep learning, in particular recurrent neural networks and XGBoost algorithms, demonstrates unprecedented efficiency in macroeconomic forecasting. The integration of indicators of corruption, cyber vulnerability, and money laundering risks into predictive AI models increases the accuracy of forecasting GDP per capita dynamics by 43.96%, and political stability by 38.41% for countries experiencing intensive conflict and migration burdens [36].

The AI-based financial monitoring ecosystem can analyse massive, big data arrays in real-time, recognizing hidden behavioural patterns, processing natural language to monitor open sources and PEP registries, and automatically verifying clients using biometric analysis tools. The creation of such an ecosystem is a non-alternative step to minimize corruption risks, rapidly detect shadow flows, and ensure absolute financial transparency, which is critically necessary to attract massive international investments during the reconstruction stages.

At the same time, the concentration of such an unprecedented volume of sensitive financial and personal data in a single data lake requires the complementary provision of the highest level of cybersecurity [29]. In this ecosystem, artificial intelligence works in two directions simultaneously: as a financial auditor and as a cyber defender of the infrastructure. Neural networks continuously analyse access patterns to state registers and can identify and block unauthorized access attempts, spoofing of payment details, or data leaks in milliseconds. According to analytics from the Computer Emergency Response Team of Ukraine (CERT-UA), the integration of proactive AI cybersecurity systems successfully neutralized more than 3,500 targeted cyberattacks on the financial and public sectors over the past year. This guarantees the immutability and integrity of digital data on which the entire modern anti-corruption architecture of the state is based.

Successful reconstruction is also impossible without the deep implementation of the principles of a green and digital economy directly into recovery projects. The scale of destruction requires radically new approaches to attracting private and public capital. According to updated estimates by the World Bank as of 2026, the total cost of rebuilding and recovering Ukraine over the next decade has grown and stands at nearly 588 billion US dollars [34]. Since such unprecedented needs cannot be covered

solely by the state budgets of donor countries, a fundamental prerequisite for attracting international investments is the strict implementation of the European paradigm of the "twin transition." This approach views environmental sustainability and digitalization as inseparable processes, where digital tools act as the main catalyst and guarantor of transparency for green reconstruction.

The financial architecture of international support already strictly links the provision of macro-financial assistance to the fulfilment of environmental and digital criteria. The main support instrument is the European Union's Ukraine Facility program with a total volume of 50 billion euros, aimed at the rebuilding, reconstruction, and modernization of Ukraine in the period 2024-2027. The regulation of this European mechanism establishes a strict investment quota: at least 20% of the total funding under the Ukraine Investment Framework and the Ukraine Plan must be directed exclusively toward the green transition, environmental protection, and climate change mitigation. This means that a significant portion of European funds will be available only to those initiatives that can prove their compliance with decarbonization standards and European climate goals.

Simultaneously with environmental requirements, European partners oblige the state to implement end-to-end digital solutions to ensure accountability. The central element of this architecture is the Digital Restoration Ecosystem for Accountable Management (DREAM). As of mid-2026, this platform covers 100% of public investment projects, uniting over 12,000 reconstruction projects at the local and regional levels with a total value exceeding 1.06 trillion hryvnias. The integration of such tools allows effectively overcoming information asymmetry between international creditors and local implementers, providing donors with objective data on the rational use of resources. The synergy of green standards and total digitalization minimizes corruption risks, guarantees investment accountability, and creates a solid foundation for building a high-tech economy [21].

3. European Digital Integration

The third stage of the roadmap involves the complete synchronization of the national economic and legal system with the European space and deep integration into the EU Digital Single Market. To achieve this strategic goal,

the state must transition from transit mixed models to clearly specialized digital development profiles, such as the "Digital Service Economy" or "Knowledge-driven Economy," which have proven their success in advanced European countries [35]. The foreign experience of leading states like Denmark, Finland, Sweden, and the Netherlands demonstrates the undeniable effectiveness of the Government-led Digitalization model, where institutional stability and a high level of digital competence and business innovations act as key drivers of macroeconomic growth.

A fundamental element of Ukraine's integration into the EU Digital Single Market is joining the European trust services area in accordance with the eIDAS regulation. The mutual recognition of qualified electronic signatures (QES) allows Ukrainian business to conclude cross-border agreements, register companies in the EU, and pay taxes in a unified digital environment without using paper documents. According to the Ministry of Digital Transformation of Ukraine, the full-fledged launch of cross-border document sharing and electronic contracts has eliminated opportunities for forging foreign economic agreements, which were previously used for fictitious VAT refunds and capital withdrawal to offshore zones.

In the customs sphere, the key anti-corruption tool was Ukraine's integration into the New Computerized Transit System (NCTS), which is the foundation of the European digital customs space. Operating on the principle of "one vehicle – one declaration – one guarantee," the system ensures automated information exchange between the customs of Ukraine and 35 participating countries of the Convention on a Common Transit Procedure. This eliminates the human factor and precludes common corruption schemes, such as altering product nomenclature or understating customs value when crossing the border. According to reports from the State Customs Service of Ukraine, as of the beginning of 2026, over 210 thousand electronic transit declarations were successfully processed through the NCTS system. By precluding contraband "interrupted transit," the level of customs revenues to the state budget increased by 18%, which is direct statistical confirmation of the large-scale de-shadowing of import-export operations.

The security foundation of this digital openness is guaranteed by synchronization with the European cybersecurity architecture, in particular the implementation of the requirements of the NIS2 Directive and deep

sectoral cooperation with the EU Agency for Cybersecurity (ENISA). Since digital customs, tax databases, and cross-border e-government systems become critical nodes of the economy, their protection according to NATO and European standards is a mandatory EU condition. The implementation of European Threat Intelligence sharing protocols has allowed state registers to automatically block anomalous cross-border requests. According to analytics from the National Institute for Strategic Studies, the transition to NIS2 standards has increased the operational resilience of state digital services to hacker attacks by 75%, guaranteeing the continuity of anti-corruption services even amid systemic information warfare.

A fundamental prerequisite for the irreversibility of European integration reforms is the formation of a strong culture of cyber hygiene and zero tolerance for corruption at the institutional and societal levels. The results of large-scale cross-country studies convincingly prove that the implementation of advanced digital technologies alone cannot guarantee the overcoming of corruption or absolute protection against cyber threats unless it is supported by a strong institutional base, effective control, and a strict limitation of abuses of power [19; 27; 24].

Institutional cyber hygiene serves as the first line of defense for state registers against insider threats and social engineering methods. According to statistics from the Computer Emergency Response Team of Ukraine (CERT-UA), about 75% of successful cyberattacks on Ukraine's public sector begin specifically with phishing emails or the use of compromised passwords by agency employees. As successful foreign experience, Ukraine is actively implementing the model of Estonia. In Estonian government practice, over 95% of civil servants annually pass certification on the Cyber Hygiene platform, which has reduced the rate of successful phishing intrusions into their government networks to almost zero. Through the adaptation of this experience via the "Diia. Education" programs and internal training by the National Agency on Corruption Prevention (NACP), the level of basic cyber literacy among Ukrainian officials involved in reconstruction processes increased by 40% as of 2026, significantly minimizing the risks of leaking sensitive procurement data.

In parallel with strengthening digital discipline, the institutionalization of zero tolerance for corruption is taking place, which is a fundamental factor in the de-shadowing of the economy [26]. A key tool in this process was

the launch and expansion of the functionality of the Unified Whistleblower Reporting Portal by the NACP. This portal guarantees complete anonymity and the highest level of cyber protection for communication channels for citizens reporting financial abuses. Drawing on advanced US experience, particularly the SEC whistleblower reward programs, Ukraine institutionalized the payment to whistleblowers of 10% of the value of the subject of a corruption crime. Such financial motivation, combined with robust data encryption, fundamentally changed the societal paradigm and reduced the fear of reporting. According to studies by the USAID "ENGAGE" program, as of 2026, the share of Ukrainian citizens declaring their readiness to actively report corruption cases reached a historical maximum of 62% (whereas before the start of the full-scale invasion, this figure barely reached 40%). Thanks to safe reporting through a secure portal, anti-corruption bodies received over 18 thousand substantiated signals, which helped prevent the embezzlement of hundreds of millions of hryvnias in regional reconstruction projects.

The synergy of these two cultures creates an environment in which the digital traces of transactions cannot be hidden due to the cyber hygiene of state database administrators, and any attempts at shadow agreements are instantly exposed by a conscious society. Such a comprehensive approach guarantees the stability of the transparency architecture and forms an impeccable reputation for Ukraine before international donors financing national reconstruction.

CONCLUSION

The conceptualization and implementation of the proposed complementary roadmap serve as a critically necessary condition for overcoming the cumulative and mutually reinforcing impact of the modern "triple threat," which consists of cybercrime, corruption, and shadow economy. Traditional, isolated approaches to combating the shadow economy and corruption have exhausted their effectiveness, primarily because illicit financial flows and corrupt practices have massively migrated into the digital sphere. Criminal actors now routinely exploit cryptocurrency networks, anonymous payment systems, and vulnerabilities in the architecture of state registers to mask their illicit activities. Therefore, overcoming these integrated economic threats demands a complementary approach characterized by functional

emergence, mutual conditionality, and institutional coherence. Within this regulatory framework, strengthening cyber resilience immanently boosts the effectiveness of anti-corruption and de-shadowing efforts.

Comprehensive studies and international experiences confirm that technological innovations and the development of digital infrastructure, in and of themselves, are fundamentally incapable of guaranteeing macroeconomic security. The isolated implementation of legal frameworks or technological tools is insufficient to overcome the shadow economy if it is not firmly underpinned by a strong institutional foundation, effective anti-corruption compliance, and rigorous control over authoritative powers. Digital transformation must be coupled with a societal culture of zero tolerance for corruption to be truly effective. Proactive cybersecurity acts not merely as a technical superstructure, but as the fundamental basis for successful anti-corruption and de-shadowing reforms, forming a holistic and resilient architecture of the national economy. Without ensuring the confidentiality and availability of the state's information assets, attempts to bring the economy out of the shadows are neutralized by technological vulnerabilities, allowing corruption to bypass traditional oversight and acquire a latent, high-tech form.

To achieve this resilient architecture, the sequential passing of three logically structured stages of reforms (Resilience, Reconstruction, and Integration) is fundamentally required. The first stage, "Resilience," addresses the wartime emergency period by focusing on the vital cyber defense of critical digital infrastructure and the establishment of total digital control over the distribution of massive international financial and military aid. This emergency protection is necessary to prevent the strategic destruction of critical infrastructure by targeted cyberattacks and to ensure absolute accountability. By utilizing digital financial technologies and automated tracking systems, the state can completely neutralize the human factor, thereby protecting international donor investments from embezzlement and maintaining institutional trust on the part of global partners.

The second stage, "Reconstruction," focuses on the immediate post-war years and aims at the irreversible de-shadowing of capital through the comprehensive regulation of virtual assets and the cryptocurrency market. A pivotal component of this phase is the creation of a sophisticated

financial monitoring ecosystem driven by artificial intelligence, machine learning algorithms, and big data analytics. The deep integration of artificial intelligence into national financial monitoring systems facilitates a crucial transition from reactive to predictive response models. This provides the ability to proactively detect hidden financial anomalies, recognize shadow flows, and effectively counter illicit practices by making blocking decisions based solely on mathematical models, which strictly precludes bribery or manual intervention by inspectors. Furthermore, this reconstruction phase mandates adherence to the principles of the green and digital "twin transition," ensuring that environmental sustainability and digitalization remain inseparable in recovery projects to meet the rigorous investment criteria of European partners.

The third and final stage, "Integration," involves the complete synchronization of the national economic, legal, and customs systems with the European Union's Digital Single Market. This long-term strategic goal requires the state to qualitatively transform its economic structure, transitioning from mixed transitional models to highly specialized and resilient profiles, such as a "Digital Service Economy" or a "Knowledge-driven economy," which are characteristic of advanced European states. A fundamental prerequisite for the success and irreversibility of this integration is the deep rooting of an institutional culture of cyber hygiene and the institutionalization of strict whistleblower protections.

Ultimately, the synergy of reliable cyber protection, transparent digital ecosystems, and an institutionalized societal culture of zero tolerance for corruption will create a stable, secure, and transparent business environment. This comprehensive and complementary model guarantees the irreversible de-shadowing of capital, completely neutralizes the risks of embezzlement of international aid, and ensures the country's successful, long-term economic, legal, and technological transformation into a specialized, knowledge-driven European economy.

References:

1. Abdullahi, A. O., & Ali Mohamed, I. S. (2025). E-Government as a tool to combat corruption in post-conflict Somalia. *Journal of Somali Studies*, 12(1), 9–30. https://doi.org/10.31920/2056-5682/2024/v12n1a1

2. Baskoro, A. (2025). Combating corruption in procurement: The synergy of law enforcement, civil society, and digital oversight. *Jurnal Pengadaan Indonesia*, 4(1), 24–39. https://doi.org/10.59034/jpi.v4i1.59

3. Berdiev, A. N., Goel, R. K., & Saunoris, J. W. (2024). Global cryptocurrency use, corruption, and the shadow economy: New insights into the underlying linkages. *American Journal of Economics and Sociology*, 83(3), 609–629. https://doi.org/10.1111/ajes.12566

4. Bojan, A., & Achim, M. V. (2025). Does information and communication technology influence the shadow economy? A panel data analysis for EU countries. *Proceedings of the International Conference on Business Excellence*, 19(1), 2843–2862. https://doi.org/10.2478/picbe-2025-0219

5. Chainalysis. (2025). Crypto adoption in Europe: Global crypto adoption index. Chainalysis Blog. https://www.chainalysis.com/blog/europe-crypto-adoption-2025/

6. Cheng, S., Li, J., Luo, L., & Zhu, Y. (2024). Cybersecurity governance and digital finance: Evidence from sovereign states. *Finance Research Letters*, 65. https://doi.org/10.1016/j.frl.2024.105533

7. Derzhavna mytna sluzhba Ukrainy [State Customs Service of Ukraine]. (2026). Pidsumky zastosuvannia Novoi kompiuteryzovanoi tranzytnoi systemy (NCTS) v Ukraini: statystyka ta antykoruptsiinyi efekt [Results of the application of the New Computerized Transit System (NCTS) in Ukraine: Statistics and anti-corruption effect]. Ofitsiinyi vebportal Derzhmitsluzhby [Official web portal of the State Customs Service]. https://customs.gov.ua

8. Habiburrochman, H., Saa, S., Indrayana, D., Khairunnisah, K., & Rahma, F. (2024). Tackling corruption in the public sector: Innovative approaches and policy reforms. *Join: Journal of Social Science*, 1(6). https://doi.org/10.59613/ejan4589

9. Kelemen, R. (2026) The Cyberfare state: divergent models of digital governance and control. *Frontiers in Political Science*, 8. https://doi.org/10.3389/fpos.2026.1748562

10. Kormych, L., Krasnopolska, T., & Zavhorodnia, Y. (2024). Digital transformation and national security ensuring. *European political and law discourse*, 11(1), 29–37. https://doi.org/10.46340/eppd.2024.11.1.4

11. Leheza, Y., Kulinich, O., Zhuravlova, T., Khainatskyi, Y., & Sainchyn, S. (2025). Combating Corruption Offenses: Foreign Experience, Theoretical, Practical, Legal Regulations, and Improvement. *Jurnal Hukum Islam*, 23(1), 305–335. https://doi.org/10.28918/jhi.v23i1.10

12. Lesmana, D., Afifuddin, M., & Adriyanto A. (2023). Challenges and cybersecurity threats in digital economic transformation. *International Journal of Humanities Education and Social Sciences*, 2(6). https://doi.org/10.55227/ijhess.v2i6.515

13. Lyeonov, S., Yarovenko, H., Reshetniak, Y., & Bilan, Y. (2025). The triple threat: Understanding the effects of cyber threats, corruption, and money laundering on the business environment. Equilibrium. *Quarterly Journal of Economics and Economic Policy*, 20(3), 1087-1129. https://doi.org/10.24136/eq.3846

14. Mara, E. R. (2025). Quo Vadis Shadow Economy in A Digitalized World? Evidence from Panel Cointegration for EU Countries. Journal of Innovation Economics & Management, Prépublication (0), I179-XL. https://doi.org/10.3917/e.jie.pr2.0179

15. McKinsey. (2022). The fight against money laundering: Machine learning is a game changer. New York: McKinsey Risk Practice. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer

16. Ministerstvo finansiv Ukrainy [Ministry of Finance of Ukraine]. (2024). Rada YeS zatverdyla instrument Ukraine Facility obsiahom 50 mlrd yevro na 2024-2027 roky [The EU Council approved the Ukraine Facility instrument in the amount of EUR 50 billion for 2024-2027]. Uriadovyi portal [Government portal]. https://eu-ua.kmu.gov.ua/news/rada-yes-zatverdyla-instrument-ukraine-facility-obsyagom-50-mlrd-yevro-na-2024-2027-roky/

17. Ministerstvo finansiv Ukrainy [Ministry of Finance of Ukraine]. (2025). U 2025 rotsi Minfin zaluchyv 52,4 mlrd dolariv SShA zovnishnoho finansuvannia, z yakykh ponad 70% - za rakhunok dokhodiv vid zamorozhenykh aktyviv RF [In 2025, the Ministry of Finance attracted USD 52.4 billion in external financing, of which over 70% came from the revenues of frozen Russian assets]. Uriadovyi portal [Government portal]. https://www.kmu.gov.ua/news/u-2025-rotsi-minfin-zaluchyv-524-mlrd-zovnishnoho-finansuvannia-iz-iakykh-ponad-70-za-rakhunok-dokhodiv-vid-zamorozhenykh-aktyviv-rf

18. Natsionalnyi bank Ukrainy [National Bank of Ukraine]. (2025). Stratehiia rozvytku finansovoho sektoru Ukrainy: napriam tsyfrovizatsii, kiberzakhystu ta finmonitorynhu v umovakh vidnovlennia [Strategy for the development of the financial sector of Ukraine: Direction of digitalization, cyber defense, and financial monitoring in the context of recovery]. Kyiv. https://bank.gov.ua

19. Nguyen, C. P., Schinckus, C., Nguyen, Q. B., & Le Tran, D. T. (2024). Digitalization and informal economy: a global evidence of internet usage. Journal of Industrial and Business Economics, 51(1), 1–37. https://doi.org/10.1007/s40812-023-00278-w

20. Ningsih, D. N. C., Rokhimakhumullah, D. N. F., Suryani, Y., & Mahendra, I. I. (2025). An effectiveness analysis of tax administration digitalization reducing the shadow economy in Indonesia. KnE Social Sciences, 10(13), 93–117. https://doi.org/10.18502/kss.v10i13.18943

21. Omotoye, A. M., & Holtzhausen, N. (2025). Integration of digital technologies in anti-corruption initiatives in Botswana: lessons from Georgia, Ukraine and South Africa. Transforming Government: People, Process and Policy, 19(1), 22–36. https://doi.org/10.1108/TG-01-2024-0002

22. Prohrama spryiannia hromadskii aktyvnosti “Doluchaisia!” (USAID/ENGAGE) [Civic engagement promotion program “Join in!” (USAID/ENGAGE)]. (2026). Zahalnonatsionalne opytuvannia shchodo hromadskoho zaluchennia: dynamika tolerantnosti do koruptsii v umovakh vidbudovy [National survey on civic engagement: Dynamics of tolerance to corruption in the context of recovery]. Pact Ukraine.

23. Przekota, G., Kowal-Pawul, A., & Szczepańska-Przekota, A. (2025). Determinants of the Shadow Economy – Implications for Fiscal Sustainability and Sustainable Development in the EU. *Sustainability*, 17(20). https://doi.org/10.3390/su17209033

24. Rahmafillah, R., Yuliandari Aida Putri, R., & Sartika, R. (2025). The effectiveness of anti-corruption policies in the digital age: a literature review on the use of technology in the eradication of corruption. *Hermeneutika : Jurnal Ilmu Hukum*, 9(2), 146-150. https://doi.org/10.33603/hermeneutika.v9i2.10043

25. Remeikiene, R., Gaspareniene, L., & Schneider, F. G. (2018). The definition of digital shadow economy. *Technological and Economic Development of Economy*, 24(2), 696–717. https://doi.org/10.3846/20294913.2016.1266530

26. Rudiyansah, M. M. D. H., & Rezki, Moch. G. F. (2025). The impact of corruption on economic development and community welfare from local and national perspectives. *Abdurrauf Social Science*, 2(2), 138–158. Retrieved from https://journal.abdurraufinstitute.org/index.php/arsos/article/view/349

27. Santiso, C. (2022). Govtech against corruption: What are the integrity dividends of government digitalization? *Data and Policy*, 4(3). https://doi.org/10.1017/dap.2022.31

28. Saputra, D. H., & Kusumah, F. (2025). Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries. *Indonesian Journal of Criminal Law Studies*, 10(2), 615-658. https://doi.org/10.15294/ijcls.v10i2.28795

29. Stefanchuk, M., Polyvoda, V., Kikalishvili, M., Bodunova, O., & Yermolenko-Kniazieva, L. (2021). Digitalization of public services in countering criminal corruption offenses. *Estudios de Economia Aplicada*, 39(7). https://doi.org/10.25115/eea.v39i7.5012

30. Syed, A. A., Ahmed, F., Kamal, M. A., & Trinidad Segovia, J. E. (2021). Assessing the role of digital finance on shadow economy and financial instability: An empirical analysis of selected South Asian countries. *Mathematics,* 9(23). https://doi.org/10.3390/math9233018

31. TRM Labs. (2026). 2026 crypto crime report: Illicit activity on the blockchain. TRM Labs Insights. https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

32. United Nations Office on Drugs and Crime. (n.d.). Money laundering. URL: https://www.unodc.org/unodc/en/money-laundering/overview.html

33. Velchev, A. (2025). Role of economic sustainability in strengthening national security: Case of post-soviet countries. International Journal of Accounting and Economics Studies, 12(2), 361–371. https://doi.org/10.14419/zf7kfx55

34. World Bank. (2026). Ukraine Fifth Rapid Damage and Needs Assessment (RDNA5), February 2022 – December 2025. World Bank. https://doi.org/10.1596/44369

35. Yarovenko, H., Bozhenko, V., Lešetický, J., & Oláh, J. (2026). Configurational analysis of digital transformation profiles across European countries. *Journal of International Studies*, 19(2), 117-150. https://doi.org/10.14254/2071-8330.2026/19-2/6

36. Yarovenko, H., Hurochkina, V., Cugova, A., & Mohylna, K. (2026). Forecasting Illicit Practice Impacts on Economies of Conflict Countries: XGBoost Approach. *Business Ethics and Leadership*, 10(1), 105-129. https://doi.org/10.61093/bel.10(1).105-129.2026

37. Yarovenko, H., Pakhnenko, O., Riabushka, L., Tarasenko, I., & Khmurova, V. (2026). GRU-based forecasting of conflict-related socio-economic vulnerabilities under illicit practices. *Problems and Perspectives in Management*, 24(3), 15-36. https://doi.org/10.21511/ppm.24(3).2026.02