Cybersecurity as a catalyst for digital transformation and economic development: A fuzzy system dynamics approach

Nataliia Kasianova[1,†], Berik Akhmetov[2,†], Serhii Koverha[3,†], Oleksandr Vovna[4,*,†], Anna Maryna[4,†] and Yaroslav Krutohorskyi[3,†]

[1]International Educators and Scholars Foundation, Zvirenetska Str., 63, Kyiv, 01014, Ukraine
[2]Yessenov University, Microdistrict, 32, Aktau, 130000, Kazakhstan
[3]SHEI "Donbas State Pedagogical University", Naukova Str., 13, Dnipro, 49107, Ukraine
[4]Taras Shevchenko National University of Kyiv, Volodymyrska Str., 60, Kyiv, 01033, Ukraine

Abstract

The article substantiates the strategic role of cybersecurity as a key driver of digital transformation and economic growth. The novelty of the study lies in the development of a comprehensive model based on Fuzzy System Dynamics (FSD), which for the first time integrates the Cybersecurity Index and the Digital Economy and Society Index through four integral dimensions: technological infrastructure, economic resilience, human capital, and institutional environment. The proposed model enables the simulation of complex, nonlinear interrelations among these parameters, taking into account the uncertainty of both qualitative and quantitative data. A causal diagram has been created to illustrate the impact of cybersecurity on digital development through feedback loops. Empirical modeling based on data from more than 80 countries has made it possible to form a matrix positioning them according to integral indicators. The results obtained expand the understanding of the role of digital security in economic policy and can be used for strategic planning and the formulation of national digital strategies.

Keywords

cybersecurity, digital transformation, economic development, modeling, fuzzy system dynamics, causal diagram

1. Introduction

The modern global economy is undergoing an unprecedented transformation driven by the rapid development of information and communication technologies (ICT) and the widespread implementation of digital innovations. The data-driven digital economy, based on network interactions and automated processes, opens up broad opportunities for enhancing productivity, creating new markets, and optimizing economic activity. However, this innovative paradigm generates complex digital risks, among which cyber threats are paramount. Economic losses from cybercrime, amounting to trillions of dollars annually, underscore the need to reconsider cybersecurity as a strategic economic asset that plays a central role in digital transformation and economic development. According to estimates by Cybersecurity Ventures, global losses from cybercrime exceeded $8 trillion in 2023, and are projected to grow to $10.5 trillion by 2025, surpassing the GDP of most countries worldwide [1]. According to the Global Risks Report 2023 prepared by the World Economic Forum, cyber threats have entered the top five most critical global challenges of our time [2].

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.
†These authors contributed equally.
nataliia.kasianova@npp.nau.edu.ua (N. Kasianova); berik.akhmetov@yu.edu.kz (B. Akhmetov); kovergaserg1970@gmail.com (S. Koverha); oleksandr.vovna@knu.ua (O. Vovna); annamarina197@gmail.com (A. Maryna); yarkrutogor@gmail.com (Y. Krutohorskyi)
0000-0001-7729-2011 (N. Kasianova); 0000-0003-2860-2188 (B. Akhmetov); 0000-0003-4094-8165 (S. Koverha); 0000-0003-4433-7097 (O. Vovna); 0000-0001-5634-9402 (A. Maryna); 0009-0003-4910-6877 (Y. Krutohorskyi)

The issue of digital security becomes particularly acute in the context of hybrid threats and cyberattacks targeting critical infrastructure. For instance, the large-scale attack on the Colonial Pipeline in the United States in 2021 resulted not only in disruption of energy supply but also caused direct economic damages estimated at over $200 million, including ransom payments, logistical losses, and a decline in public trust [3].

In Germany in 2020, an attack on the university hospital in Düsseldorf led to the shutdown of IT systems and ultimately the death of a patient – highlighting not only the economic, but also the humanitarian consequences of cyber incidents [4]. In the United Kingdom, the WannaCry ransomware attack on the National Health Service (NHS) in 2017 cost the budget over £92 million after 19,000 appointments were cancelled [5].

In Ukraine, the cybersecurity situation is no less critical due to the ongoing cyber warfare since 2022, which affects the public, military, and private sectors. According to expert estimates, in 2023, the vulnerability detection and response system processed about 18 billion information security events detected through monitoring tools and telemetry data analysis. Of these, 133 million were suspicious events, 148,000 were critical events indicative of potential cyber incidents, and 1,105 confirmed cyber incidents were recorded – 62.5% more compared to 2022 [6]. Cyberattacks have become a tool for destabilizing the macroeconomic situation, affecting the banking system, energy infrastructure, and information space.

The growth in the number, complexity, and international nature of cyberattacks, as well as the scale of their economic and social consequences, necessitate a deeper understanding of cybersecurity as a component of economic policy. Cybersecurity has become an integral part of national economic development. As digitalization advances, protecting information systems, data, and critical infrastructure acquires strategic importance for the modernization of economies and their integration into global digital markets. In this context, cybersecurity becomes a key precondition for investment attractiveness, innovation activity, and the economic resilience of a country in the face of global competition.

The complexity of interconnections between cybersecurity, digital transformation, and economic development, as well as the high level of uncertainty in assessing these processes, requires the application of innovative methodologies such as fuzzy system dynamics.

Fuzzy system dynamics, integrating the principles of system dynamics and fuzzy logic, enables the modeling of interrelations between system elements, taking into account qualitative data and uncertainty [7, 8, 9]. This approach makes it possible to analyze the impact of cybersecurity on the digital development of the national economy and propose an adaptive tool for shaping the state's digital policy.

2. Related work

Cybersecurity as a scientific category is increasingly viewed not in isolation within the protection of information systems but as an integral component of the digital economy. Its significance is manifested not only in safeguarding critical resources but also in influencing macroeconomic processes, particularly investment attractiveness, labor market stability, the development of innovation infrastructure, and the formation of institutional trust.

The studies of Li Shuzhun and M. Hadjieleftheriou deepen the understanding of cybersecurity by focusing on its regulatory and policy aspects. The authors emphasize that a comprehensive regulatory framework and strategic policy are key to building trust in digital markets, directly contributing to the competitiveness of the digital economy [10].

Significant contributions to the study of the economic aspects of cybersecurity have been made by R. Anderson, who argues that effective protection mechanisms are not only a technical issue but also an economic one, as low levels of cybersecurity lead to substantial economic losses and reduced economic activity. This underscores the need to integrate cybersecurity into economic strategies [11].

An innovative approach is represented by the cybersecurity investment model proposed by L. Gordon and M. Loeb [12]. The Gordon-Loeb model provides analytical tools for the optimal allocation of

resources, maximizing the benefits of cybersecurity investments while minimizing costs. This is crucial for managerial decision-making in digital security, allowing the assessment of risk-cost trade-offs/

In Ukraine, the issue of cybersecurity in the context of economic development is gaining increasing attention. In particular, Tkachuk L. and Movchanyuk M. substantiates the need for the formation of a national digital security strategy as a component of national security and economic growth. She emphasizes that without systematic management of digital risks, sustainable development during the country's digital transformation is impossible [13].

Yu. Kindzerskyi's research focuses on the economic consequences of cyber threats, highlighting their negative impact on investment and the development of digital infrastructure. He identifies institutional issues that slow down the mitigation of cyber risks and pose a threat to economic development [14].

One of the key ideas proposed by [15] is the distinction between digital security at the macro and micro levels, where the macro level refers to the security of the state's overall information-digital environment, and the micro level relates to the ability of enterprises to secure their own digital information . This approach enables the alignment of national cybersecurity policy with the practical needs of businesses, which is highly relevant in the context of hybrid threats and wartime.

Recent studies increasingly focus on the quantitative assessment of the impact of cybersecurity on digital development. For example, Y. Bilan et al. explored the impact of information and communications technology (ICT) on economic growth, showing that countries with high levels of cybersecurity (according to the National Cyber Security Index, NCSI) demonstrate higher digitalization and productivity indicators [16]. However, the authors note the lack of models linking cybersecurity with macroeconomic strategies.

The application of system dynamics allowed O. Rehman and V. Ali (2021) to model supply chain resilience to cyber threats, highlighting the capacity of this method to predict long-term economic consequences [17]. However, the proposed model does not account for the uncertainty inherent in cyber risks, limiting its practical applicability.

Despite significant progress, major gaps remain in the scientific literature. First, there is a lack of comprehensive metrics to assess cybersecurity in the context of a country's digital and economic development. For example, the NCSI developed by the e-Governance Academy [18] evaluates cybersecurity through 46 indicators but does not link it to economic indicators such as ICT investment or the Human Development Index. Second, regulatory mechanisms often lag behind the dynamics of digital threats, necessitating new approaches to cybersecurity management. Third, the shortage of cybersecurity specialists creates a bottleneck for implementing technologically complex projects. Finally, the absence of models integrating cybersecurity with the key dimensions of a country's digital development (technological infrastructure, economic resilience, human capital, institutional environment) limits forecasting and policy development opportunities.

This article aims to substantiate the fundamental relationship between cybersecurity and national economic development by developing a comprehensive model based on fuzzy system dynamics that integrates the cybersecurity indicator (National Cyber Security Index, NCSI) with an integral assessment of the country's digital development. The assessment covers key components of digital development: human capital (reflecting intellectual and educational potential), technological infrastructure (the foundation of digitalization), economic resilience (a prerequisite for financial and economic stability), and institutional factors (ensuring effective development management). The application of fuzzy system dynamics enables the modeling of complex interconnections while accounting for the uncertainty of qualitative and quantitative data, allowing forecasts of the impact of cybersecurity on digital transformation and economic growth. It provides recommendations for strategic digital development policy planning. Thus, the study is aimed at creating an analytical tool for assessing the contribution of cybersecurity to building a resilient economy and integrating the country into global digital markets.

3. Data and methodology

The methodological relationship between digital security and national economic development must be analyzed within a systemic context. In this framework, digital security emerges as a system of interconnected institutional, technological, legal, and social factors that ensure the continuity and security of digital interactions across all spheres of public life. Accordingly, any disruption of digital stability – whether caused by a cyberattack or the absence of regulatory oversight – can have systemic economic consequences. In particular, such disruptions may generate cascading effects that undermine macroeconomic stability by eroding trust in digital systems, reducing investment activity, and disrupting the functioning of critical infrastructure.

From the standpoint of institutional economics, digital security ensures the transparency and consistency of the "rules of the game" in the digital environment. It creates the preconditions for the effective enforcement of contracts, reduces transaction costs, and strengthens trust among investors and consumers of digital services. In this sense, digital security functions as an intangible institution that guarantees economic equilibrium under conditions of digital transformation. For instance, effective cybersecurity regulation helps to reduce information asymmetry between economic agents, which, according to the theory of institutional economics, enhances the efficiency of market interactions [19].

Moreover, a secure digital environment is essential for the development of digital infrastructure, including the Internet of Things, cloud services, mobile banking, and e-government. Any technical progress without an adequate security system increases risks, hampers the scaling of digital solutions, lowers the efficiency of public investments, and slows innovative growth. In particular, insufficient levels of cybersecurity can create barriers to the adoption of advanced technologies such as artificial intelligence or blockchain, which require high levels of data protection.

In the socio-economic dimension, digital security is closely linked to digital inclusion – the population's ability to fully access and utilize digital services regardless of age, income, or place of residence. Inadequate security in educational or medical digital services restricts citizens' participation in the digital economy, deepens inequality, and impedes human capital development. This link is confirmed by empirical data: countries with high levels of cybersecurity (as measured by NCSI) demonstrate higher levels of digital inclusion, correlating with the Human Development Index (HDI) [16].

At the macroeconomic level, digital security directly affects the economic security of the state. Strategically, it ensures the continuity of operations of critical infrastructure, including energy, transport, communications, and the banking sector. Its effective functioning is a prerequisite for the stability of public governance, capital markets, and fiscal policy implementation. For example, cyberattacks on critical infrastructure, as in the case of Colonial Pipeline [3] demonstrate how breaches of digital security can cause direct economic damage and destabilize markets.

Thus, digital security is an integral element of the national economic system, with a complex interdisciplinary nature and a multi-level hierarchy of influence – from the technological level to the level of strategic planning. Its methodological analysis requires the integration of principles from institutional, neoclassical, and digital economics, as well as national security theory. To model these complex relationships, it is advisable to apply fuzzy system dynamics (FSD), which accommodates data uncertainty and nonlinear interactions among technological infrastructure (TI), economic resilience (ES), human potential (HP), and the institutional environment (IE). This approach facilitates the creation of adaptive models that reflect causal relationships between cybersecurity (NCSI) and digital development (DESI), contributing to the design of strategies for enhancing economic competitiveness. Such an approach enables a comprehensive assessment of the role of digital security as an indicator of a state's economic maturity and as a guarantor of its competitiveness in the context of global digital transformation.

From an economic perspective, the chain "digital security $\rightarrow$ digital development $\rightarrow$ national economic development" follows the fundamental logic that security is a necessary precondition for the sustainable and effective deployment of digital technologies, which in turn become the main driver of economic growth. This chain reflects a causal relationship where digital security serves as a catalyst, ensuring the stability and trust necessary for scaling digital innovations [11].

First, digital security minimizes the risks of losses and disruptions associated with cyber incidents, which can cause significant direct and indirect economic damages—from the loss of consumer trust to the need for large financial expenditures to restore systems. Reliable security systems reduce uncertainty in the digital environment, stimulating trust from investors, users, and businesses. For example, according to [12], optimal cybersecurity investments can reduce economic losses from cyberattacks by up to 80%, confirming its role as an economic asset. Furthermore, a high level of cybersecurity helps lower insurance premiums for businesses and increases their readiness for digital transformation.

Second, digital development is a consequence of investments in digital technologies, infrastructure, human capital, and innovation. This development directly depends on effective digital security: businesses and public institutions are more likely to adopt new digital solutions, expand e-services, and create innovative products when confident in the protection of information assets. This generates a multiplier effect for the economy, increasing productivity and competitiveness. In particular, countries with a high level of cybersecurity (according to NCSI) demonstrate higher ICT investment and innovation activity, which correlates with the Digital Economy and Society Index (DESI) [16]. This effect is especially pronounced in data-dependent sectors such as fintech and e-commerce.

Third, digital development transforms the national economy by expanding access to global markets, creating new areas of activity, increasing resource management efficiency, and stimulating innovation. As a result, the country achieves sustainable economic growth, GDP growth, and improved social welfare. Digital development also promotes integration into global value chains, which, according to OECD [20], can increase national GDP by 1–2% provided an adequate level of digital security. For example, countries with advanced digital infrastructure and high NCSI levels, such as Singapore and Denmark, demonstrate higher economic growth rates compared to countries with low levels of cybersecurity.

Thus, digital security creates the conditions for uninterrupted and reliable digital development, which in turn forms the basis for modernization and national economic growth. This relationship forms a reinforcing loop, where improvements in cybersecurity stimulate digital development, and digital development, in turn, generates demand for enhanced security systems.

However, despite the obvious importance of this aspect, a unified approach to quantitatively measuring digital security and digital development as components of a state's economic resilience is still absent in both scientific and applied fields. Most existing approaches focus either on purely technological indicators or on formal legal criteria, which does not fully capture the complex interrelations between digital security and national economic development. For example, the Global Cybersecurity Index (GCI) focuses on technical and legal aspects but ignores socio-economic factors such as human capital or institutional trust. Similarly, DESI covers digital development but does not integrate cybersecurity as a key factor. To overcome these gaps, it is proposed to use fuzzy system dynamics (FSD), which allows the modeling of nonlinear interconnections between technological infrastructure (TI), economic resilience (ES), human potential (HP), and the institutional environment (IE), while accounting for uncertainty and qualitative data [7].

Assessing a country's digital development is a key component in analyzing modern economic transformation and integration into the global digital space. Several methodological approaches exist for measuring this phenomenon, each with its advantages and limitations that determine its applicability in various contexts. Moreover, digital development, as a complex phenomenon, encompasses not only technological aspects but also socio-economic, institutional, and security factors, requiring an integrative assessment approach [21].

First, the index-based approach relies on the formation of composite digital development indices that aggregate various indicators – from Internet accessibility and digital infrastructure to levels of digital literacy and the use of digital technologies in business. One of the best-known is the Digital Economy and Society Index (DESI) developed by the European Commission [22]. The advantage of this approach is its comprehensiveness and the ability to compare across countries, as well as the dynamic nature of the index, which is updated annually. However, the index approach is often criticized for excessive universality, which may not reflect the specifics of national economies, and for requiring a large volume of data that may not always be available or of sufficient quality [23]. Furthermore, DESI does not fully integrate cybersecurity indicators, such as the National Cyber Security Index (NCSI), limiting its ability

to assess the security dimension of digital development.

Second, a systems approach views digital development through the lens of interactions among infrastructure, the regulatory environment, human capital, and innovation culture. R. Atkinson and A. McKay [24] emphasize the importance of comprehensive analysis of systemic factors shaping a country's digital ecosystem. This approach enables a deeper understanding of the relationships and factors that promote or hinder digital transformation. At the same time, its disadvantages include the complexity of modeling and quantitatively assessing all systemic components simultaneously. The systems approach also complicates the accounting of nonlinear effects, such as cascading failures from cyberattacks, which requires dynamic modeling. In an increasingly turbulent economic environment characterized by digital transformation and environmental challenges, the concept of balanced national economic development is acquiring new strategic significance. The focus is shifting from linear planning to an integrated, multifactor assessment of economic resilience and adaptability under dynamic conditions. At the same time, classical strategic analysis tools are unable to adequately account for the fuzziness, contradictions, ambiguity, and nonlinearity of interrelations between economic, social, environmental, and innovation determinants of digital development. For example, traditional models, such as regression analysis, do not account for qualitative variables, such as trust in digital systems or subjective perceptions of cyber threats. This necessitates intelligent models based on processing linguistic variables, weakly structured data, feedback dynamics, and development scenarios.

Fuzzy logic makes it possible to formalize complex managerial assessments based on expert judgments, while system dynamics helps identify delayed effects of strategic decisions and feedback loops in governance. The combination of these approaches creates the foundation for building an integral model of balanced digital development, relevant to contemporary challenges. This combination, known as fuzzy system dynamics (FSD), enables the modeling of complex interconnections between cybersecurity (NCSI) and digital development (DESI), accounting for data uncertainty and nonlinear effects [25].

System Dynamics as a Tool for Strategic Modeling was initiated by J. Forrester [8] and later adapted to the management of large-scale economic systems in the works of K. Richardson [26] and J. Sterman [27]. These studies emphasize the significance of nonlinear interdependencies between subsystems, time delays, amplification (or attenuation) effects, and similar dynamics. Particularly promising is the policy design through feedback loops approach, which facilitates the evaluation of long-term effects of strategic decisions (e.g., the implementation of a cybersecurity enhancement policy may have a delayed effect on ICT investment growth through increased business trust).

On the other hand, fuzzy logic methods are increasingly employed to formalize complex managerial assessments, especially under conditions of information scarcity or vague definitions of strategic parameters. These approaches are based on the ideas of L. Zadeh [7] and are applied in the assessment of innovation activity, environmental load, financial sustainability, among other areas [28, 29]. Fuzzy logic allows for the processing of qualitative assessments such as "high/medium/low protection level", which is especially critical for countries with limited data availability.

The integration of fuzzy logic and system dynamics remains at the conceptual development stage; however, selected studies have demonstrated the effectiveness of this combined approach in modeling strategic interactions among digital development factors. The fuzzy system dynamics (FSD) approach integrates:

1) system dynamics – to represent dynamic interrelationships through stocks, flows, and feedback loops (reinforcing and balancing);

2) fuzzy logic – to handle uncertainty in qualitative or imprecise data (e.g., "high / medium / low level of cybersecurity") via membership functions and Fuzzy Inference Systems (FIS) [Zadeh, 1965]. FSD enables the construction of causal loop diagrams that illustrate interconnections among technological infrastructure (TI), economic sustainability (ES), human potential (HP), and institutional environment (IE).

In the process of formalizing a methodology for assessing digital development, particular importance is placed on the selection of indicators that can serve as generalized (integral) metrics for specific assessment dimensions. Given the multidimensional nature of digital security, the substantiated choice of such indicators ensures a balance between analytical depth and practical model applicability. This selection

is based on criteria of international standardization, data availability, and relevance to cybersecurity and digital development.

The first key group of indicators characterizes the state of digital transformation's technological infrastructure, as the technical foundation is critical for all digital processes, including those related to security. Within this group, the level of broadband Internet access is proposed as a core indicator. It captures both physical accessibility to digital resources and the population's potential to participate in the digital environment. Broadband connectivity underpins not only the digital economy but also the effective operation of defensive infrastructures that must respond to threats in real time. Furthermore, this indicator is internationally standardized and widely available in open databases from ITU and the World Bank. For instance, countries with high broadband coverage (over 80% of households) demonstrate higher NCSI scores, indicating their capacity to maintain digital security [23].

The second dimension involves the economic capacity of the state to ensure digital security. Here, the key indicator is gross national income per capita (GNI per capita). This metric reflects not only overall welfare levels but also the availability of resources for investing in complex digital protection systems, human capital development, and infrastructure modernization. Countries with high GNI exhibit greater expenditure capacity for digital security in both the public and corporate sectors. Globally, GNI is often used as a proxy indicator of investment potential in innovation-driven sectors, including cybersecurity. Notably, the correlation between GNI per capita and cybersecurity spending reaches 0.75 among OECD countries, highlighting the economic dimension of digital security [20].

Equally important is human potential, which shapes the quality of users' digital behavior, threat awareness, and, consequently, the overall vulnerability of a country to cyberattacks and lapses in information hygiene. In this context, the Human Development Index (HDI) – which includes life expectancy, education level, and income – is the most comprehensive representation. It consolidates key social aspects that determine not only digital literacy but also the overall societal capacity to adapt to digital challenges. HDI also correlates with digital inclusion indicators ($r = 0.65$), confirming its role in reducing cyber risk through education [30].

The fourth component is the institutional environment, which influences the effectiveness of digital security policy implementation, transparency of processes, and responsiveness to cyber threats within public governance. The most informative indicator in this case is the Worldwide Governance Indicators (WGI), developed by Transparency International. Among them, the indicator of government effectiveness was selected. It reflects perceptions of the quality of public services, the civil service's quality and its independence from political pressure, the quality of policy formulation and implementation, and confidence in the government's commitment to these policies. Government effectiveness strongly correlates ($r = 0.82$) with NCSI, underscoring its key role in building institutional trust in cybersecurity [31].

Thus, for each of the four domains – technological, economic, social, and institutional – a representative integral indicator has been substantiated, capable of meaningfully reflecting the essence of the corresponding component of digital security. The subsequent combination of these variables within a fuzzy logic model enables the construction of an adaptive index of digital development relevant to the conditions of a specific country or region. These indicators form the basis for developing an adaptive digital development index via a Fuzzy Inference System (FIS), which integrates NCSI and DESI within the FSD model. Further formalization of the model involves building a causal loop diagram to depict feedback between these variables and performing scenario analysis to evaluate the impact of cybersecurity policy on economic development.

Based on a comparative analysis of the literature, recommendations from international organizations (ITU, World Bank, UNDP, OECD), and the logic of structural modeling of digital environments, a generalized indicator system was developed, consisting of logical blocks presented in Table 1. This system reflects a multidimensional approach to assessing digital development by integrating quantitative and qualitative aspects, aligned with the contemporary challenges of global digital transformation [32].

Table 1: Indicators for Assessing the Digital Development of the Country by Group

№	Indicator	Code	Use in the Model	Type of Impact	Brief Description
			Technological Infrastructure (TI)		
1.1	Broadband penetration	BRA	Direct use	Level of basic internet access	Essential for the development of e-government, online services, and digital commerce.
1.2	Fixed-broadband Internet (5GB), Speed Mbit/s	FBS	Direct use	Average speed of fixed broadband (5GB minimum plan)	A basic level of digital access enabling online learning, e-commerce, and digital services. 10 Mbit/s is the minimum quality threshold.
1.3	Fixed-broadband Internet (5GB), as % of GNI p.c.	FBI	Requires inversion	Relative cost of 5GB fixed broadband package as % of GNI per capita	Reflects affordability of basic internet access. <2% GNI p.c. is considered affordable by ITU; >5% is a significant barrier.
1.4	ICT trade balance	ICTB	Direct use	Level of digital economy development	Indicates the country's capacity to produce and export ICT products. A higher balance reflects technological maturity.
1.5	ICT Development Index	IDI	Direct use	Composite index	An aggregated measure of a country's technological potential.
			Economic Stability (ES)		
2.1	Public debt (% of GDP)	DEBT	Requires inversion	Excessive debt reduces investment potential	Higher debt limits strategic investments in security, infrastructure, and digital projects.
2.2	Inflation (%)	INF	Requires inversion	Macroeconomic instability	High inflation devalues resources, limits planning, and hinders digital project financing.
2.3	Unemployment rate (%)	UER	Requires inversion	Limits domestic digital market and inclusion	Reflects low employment and productivity, limiting tax revenue and demand for digital services.
2.4	Foreign Exchange Reserves (% of GDP)	FXR	Direct use	Financial flexibility for digital challenges	High reserves act as a buffer during crises, including cyber threats. Indicator of macroeconomic resilience.
2.5	Gross national income per capita	GNI	Direct use	Country's capacity to invest in digitalization	Key indicator of prosperity. Higher GNI reflects greater ability to invest in infrastructure and digital security.
			Human Potential (HP)		
3.1	Years of education	YE	Direct use	Educational level as a driver of digital literacy	Reflects the quality and accessibility of education, impacting digital competencies.
3.2	Life expectancy at birth	LEB	Direct use	Well-being and social capital indicator	Represents health, welfare, and social stability—factors influencing digital adoption.
3.3	Multidimensional Poverty Index	MPI	Requires inversion	Social vulnerability and barrier to digital inclusion	Higher MPI indicates limited access to basic resources, restricting digital inclusion and increasing cyber risks.
3.4	Public spending on education (% of GDP)	GEE	Direct use	Priority of human capital development	Shows national commitment to education, including development of digital skills.
3.5	Human Development Index	HDI	Direct use	Composite of education, income, and health	Strongly correlates with digital literacy, responsibility, and institutional capacity.
			Institutional Environment (IE)		
4.1	Corruption Perceptions Index	CPI	Direct use	Transparency and trust in governance	High CPI suggests transparent processes—vital for trust in digital services and data protection.
4.2	Happiness Index	HI	Direct use	Trust marker for state and digital services	Reflects public trust, well-being, and willingness to use e-services.
4.3	Environmental Performance Index	EPI	Direct use	Indicator of responsible governance	High EPI suggests mature institutions, often correlating with digital maturity.
4.4	Gini index	GI	Requires inversion	Social inequality limiting digital access	Higher values reflect inequality, reducing digital inclusiveness and increasing social risks.

4.5	Government Effectiveness	WGI	Direct use	Institutional ability to lead digital transformation	Measures reliability and competence of public administration—crucial for digital security.
Integral indicator of digital development					
5	Digital Economy and Society Index	DESI	Direct use	Integral indicator of digital development	Composite index assessing national digital readiness. Higher values indicate stronger digital development.

The application of this particular system of indicators, in combination with fuzzy logic methods (FIS modeling), facilitates the construction of an adaptive, multidimensional framework for assessing digital security and development. This framework captures both quantitative and qualitative aspects of the functioning of the digital environment at the national level. At its core, the model is structured around two key variables – the Digital Economy and Society Index (DESI) and the National Cyber Security Index (NCSI). These variables function as stocks, synthesizing the contributions of four principal dimensions: technological infrastructure (TI), encompassing metrics such as broadband access, the development of e-government, ICT investment, and related indicators; economic sustainability (ES), reflecting macroeconomic variables including public debt, investment in cybersecurity, and economic losses stemming from cyber threats; human potential (HP), capturing indicators of education, well-being, poverty levels, and workforce development in the field of cybersecurity; institutional environment (IE), which comprises corruption levels, government effectiveness, legislative frameworks for cybersecurity, and indices of trust and happiness. As detailed in Table 1, these dimensions constitute a comprehensive system of indicators that reflect both direct and mediated influences on cybersecurity and digital development, thereby ensuring their relevance across countries with diverse economic and social contexts.

4. Experimental results

A causal diagram enables the modeling of interrelationships between cybersecurity— quantified via the National Cyber Security Index (NCSI) – and a country's digital development, structured according to the four dimensions outlined in Table 1. This diagram, partially presented in graphviz.pdf, reveals nonlinear interactions among TI, ES, HP, and IE. These relationships are empirically validated by observed correlations between NCSI and DESI (r = 0.68 for 93 countries, 2023) [23].

The causal scheme (Figure 1) illustrates both reinforcing and balancing feedback loops among these dimensions. Specifically, an increase in cybersecurity capacity (NCSI) contributes to the advancement of the digital economy (DESI) through enhancements in technological infrastructure, growth in investment, human capital development, and the reduction of corruption. Conversely, higher levels of digital development increase investment attractiveness, stimulate economic growth, and create favorable conditions for the further strengthening of cybersecurity. For instance, countries with high NCSI scores, such as Estonia, demonstrate more rapid DESI growth, driven by the synergistic interplay between cybersecurity and e-governance [22].

The proposed causal diagram represents the dynamic interdependence between cybersecurity – measured by the National Cyber Security Index (NCSI) – and digital development, evaluated through the Digital Economy and Society Index (DESI). The diagram integrates the fuzzy system dynamics (FSD) approach, which combines classical system dynamics – characterized by stocks, flows, and feedback loops – with fuzzy logic, thus enabling effective analysis under uncertainty and when working with qualitative data [7]. This hybrid approach offers deeper insights into the manner in which each of the four dimensions affects DESI and NCSI, and how these indices interact, forming a complex system of interdependencies.

System dynamics models the flows of investment into technology, education, and cybersecurity, as well as feedback mechanisms, which can be either reinforcing (positive) or balancing (negative). For example, an increase in NCSI may stimulate digital development, which in turn fosters economic growth and encourages further investment in cybersecurity. Simultaneously, cyber threats or economic

constraints can act as limiting factors within this process.

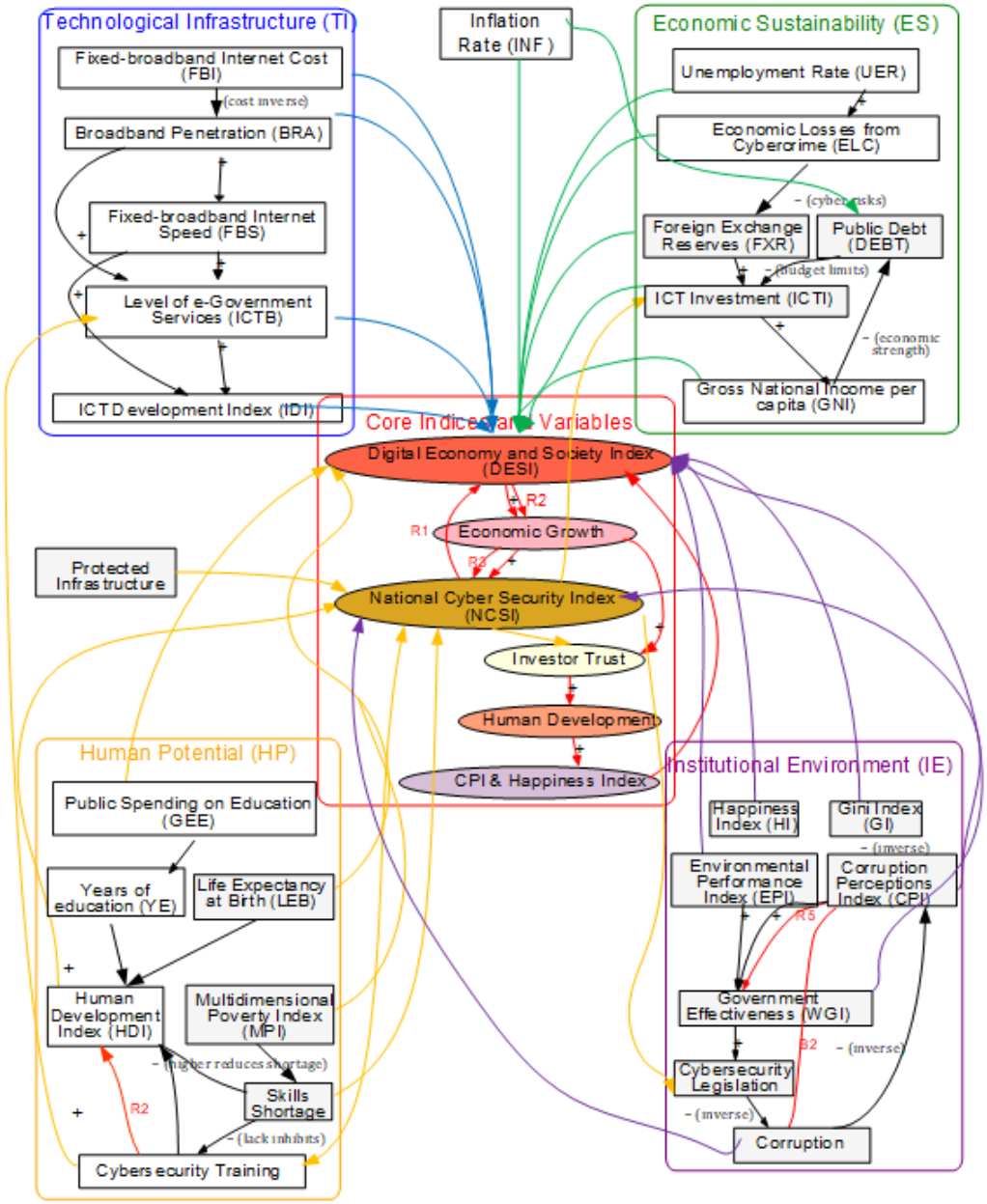

Figure 1: Causal diagram of national digital development.

Fuzzy logic allows the incorporation of linguistic variables such as "low", "medium", and "high" levels of specific indicators through a system of fuzzy inference rules (FIS). This feature is especially critical when working with incomplete or subjective data – such as corruption indices or education levels.

To synthesize the multifactorial characteristics within each of the four domains, FIS modeling is applied using the Matlab programming environment (Figure 2). For each block (TI, ES, HP, IE), a separate FIS is specified, receiving a set of input indicators. Membership functions describe the degree to which each input indicator is classified as "low", "medium", or "high". FIS rules define the logical integration and conditional relationships between input variables and the resulting aggregate indicator for each dimension. For instance, within the TI block, a FIS rule might state: "If BRA is high and IDI is high, then TI is high", reflecting the synergy between broadband access and ICT development.

The composite Digital Economy and Society Index (DESI) is formulated as a function of four integral FIS-derived indicators, each representing a key national component: technological, economic, human,

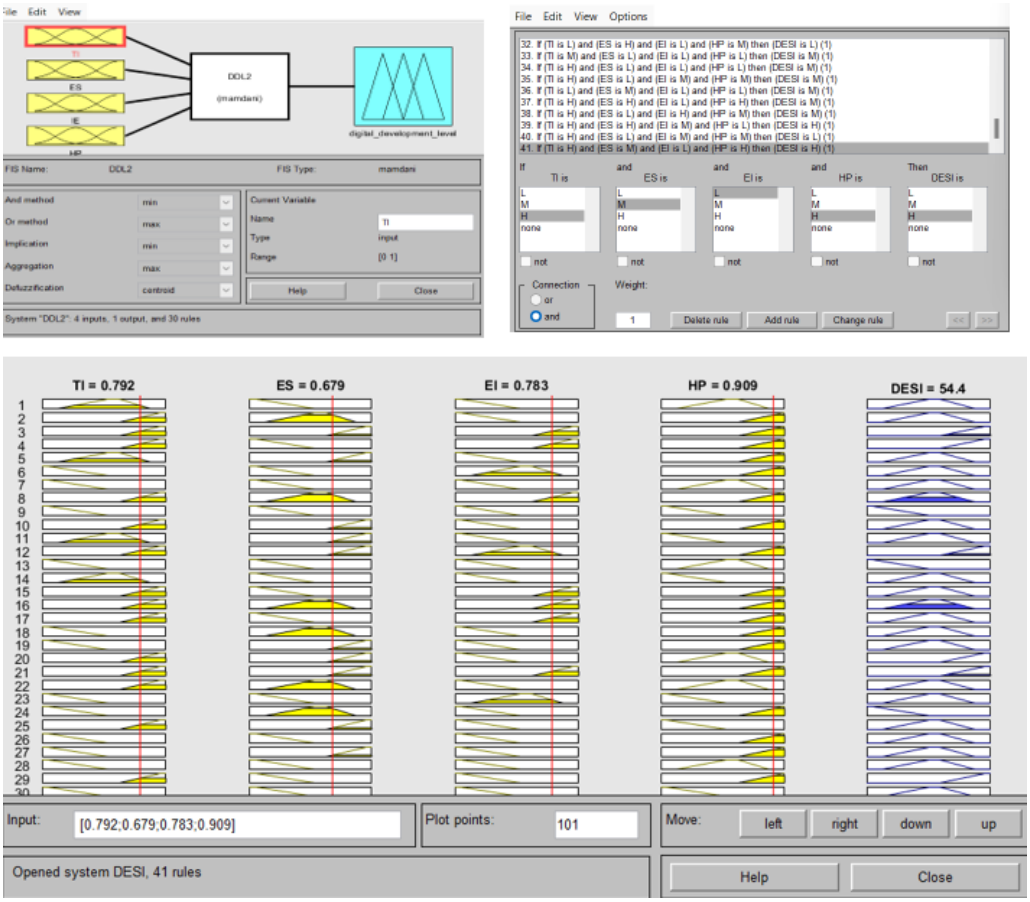

Figure 2: FIS modeling in the Matlab environment.

and institutional. These aggregated indicators capture the overall condition of a country within each dimension. The interrelation with the National Cyber Security Index (NCSI) is twofold: beyond its direct influence on these four components, the integral indicators also interact with NCSI through DESI via feedback loops, either reinforcing or offsetting the impact of cybersecurity on digital development. For instance, a low level of institutional environment (IE) – reflected in a high Corruption Perceptions Index (CPI) – may introduce a balancing feedback loop, thereby constraining the effect of a high NCSI score on DESI due to corruption-related barriers. The application of fuzzy logic enables the qualitative assessment of indicator states using the categories "low/medium/high". This capability is particularly critical in contexts where precise data are unavailable, or where multi-component socio-economic processes must be evaluated under uncertainty. The results of the fuzzy modeling of the digital development index across countries are presented in Table 2.

In parallel, the level of cybersecurity is assessed using the National Cyber Security Index (NCSI), which is based on 46 indicators covering legislative, organizational, educational, and technical aspects of cyber protection. The obtained DESI and NCSI values for various countries are used to construct a positioning matrix, where the horizontal axis represents the level of digital development and the vertical axis represents the cybersecurity index (Figure 3). The matrix is divided into nine quadrants, allowing for a classification of countries based on their degree of digital maturity and cybersecurity. This segmentation enables a more nuanced classification, which is critical for differentiated strategic management.

1. Low DESI / Low NCSI: Countries with limited digital development and low cybersecurity levels, such as Mauritania, Mozambique, and Guatemala. These nations exhibit weak infrastructure, low investment in digital technologies, and insufficient legal frameworks for cyber protection. Strategic challenges: Development of basic digital infrastructure, legislative formation, and improving cyber

Table 2
Results of Fuzzy Modeling of Global Digital Development

Country	TI	ES	HP	IE	DESI	NCSI
Czechia	0,803	0,43	0,78	0,623	42,2	98,33
Canada	0,621	0,725	0,455	0,522	50,2	96,67
Finland	0,853	0,779	0,78	0,905	60,8	93,33
Belgium	0,792	0,546	0,725	0,919	50,7	92,50
Poland	0,69	0,795	0,51	0,911	71,9	92,50
Estonia	0,802	0,636	0,472	0,609	52,6	88,33
Italy	0,725	0,924	0,474	0,45	61,7	88,33
Australia	0,835	0,792	0,725	0,817	63,8	87,50
Austria	0,916	0,471	0,725	0,744	50,5	85,00
Lithuania	0,881	0,691	0,912	0,61	50	85,00
Singapore	0,905	0,793	0,575	0,514	80,1	85,00
Portugal	0,792	0,782	0,469	0,607	57,7	84,17
United States	0,918	0,792	0,619	0,183	83,9	84,17
Croatia	0,918	0,5	0,78	0,677	50,2	82,50
Netherlands	0,792	0,792	0,78	0,914	60,9	81,67
Slovak Republic	0,905	0,575	0,5	0,347	50,1	80,83
Ukraine	0,792	0,679	0,783	0,909	54,4	80,83
Latvia	0,683	0,646	0,798	0,639	57	79,17
Ireland	0,917	0,474	0,907	0,621	50,5	77,50
United Kingdom	0,92	0,611	0,472	0,916	57,7	75,00
Serbia	0,918	0,5	0,725	0,537	43	72,50
Brazil	0,433	0,44	0,469	0,499	50,1	71,67
Turkiye	0,435	0,909	0,327	0,424	42,6	71,67
Morocco	0,434	0,5	0,392	0,5	43	70,00

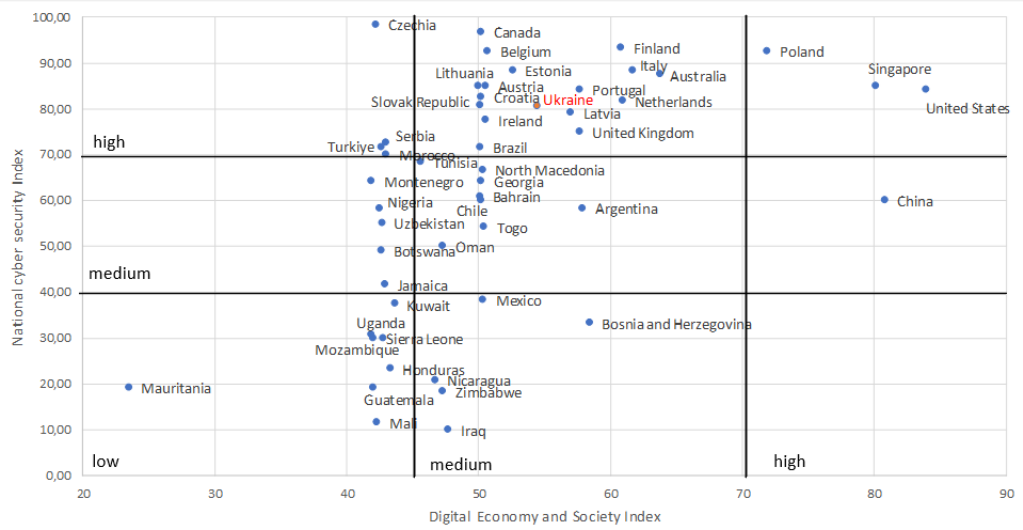

Figure 3: Country positioning matrix based on integral indicators.

literacy.

2. Low DESI / Medium NCSI: Countries with low digital integration but moderate cybersecurity levels (Nigeria, Botswana, Montenegro), possibly due to targeted cybersecurity initiatives. Strategic challenges: Accelerating digital transformation while maintaining and enhancing cybersecurity.

3. Low DESI / High NCSI: Countries with limited digital development but high cybersecurity levels (e.g., Czech Republic, Turkey, Serbia), indicating a prioritization of security even amid limited resources. Strategic challenges: Leveraging cybersecurity strengths to accelerate digital transformation.

4. Medium DESI / Low NCSI: Countries with moderate digital development but insufficient cyberse-

curity (Mexico, Zimbabwe, Bosnia and Herzegovina). Strategic challenges: Strengthening cybersecurity to ensure the stability of digital services.

5. Medium DESI / Medium NCSI: Countries with moderate levels of both digital integration and cybersecurity (Chile, Argentina, Oman). Strategic challenges: Balancing digital infrastructure development with improved cyber resilience.

6. Medium DESI / High NCSI: Countries with strong cybersecurity and medium levels of digital development (Estonia, Croatia, Ukraine). Strategic challenges: Using cybersecurity as a competitive advantage to stimulate the digital economy.

7. High DESI / Low NCSI: Countries with high digital integration but inadequate cybersecurity (none identified). Strategic challenges: Immediate enhancement of cybersecurity to prevent major cyber incidents.

8. High DESI / Medium NCSI: Countries with an advanced digital economy but moderate cybersecurity levels (China). Strategic challenges: Increasing cyber resilience to maintain user and investor trust.

9. High DESI / High NCSI: Countries with high levels of both digital development and cybersecurity, representing leaders in digital transformation (USA, Singapore, Poland).

Strategic challenges: Sustaining leadership through innovation, continuous cybersecurity improvement, and human capital development.

Thus, the causal diagram and the country positioning matrix based on the Digital Economy and Society Index (DESI) and the National Cyber Security Index (NCSI) constitute two complementary components of an integrated study of digital development and cybersecurity.

The causal diagram models the deep cause-effect relationships among the key components of digital transformation – technological infrastructure, economic resilience, human capital, and institutional environment – and their influence on the integral indices DESI and NCSI. It reflects dynamic processes, including investment flows, reinforcing and balancing feedback loops, and accounts for data uncertainty using fuzzy logic. This systems-based approach allows for a better understanding of how interactions among these factors shape a country's level of digital development and cybersecurity, as well as their mutual impact. The positioning matrix, in turn, is a practical tool based on modeling results and empirical data that enables the classification of countries by digital maturity (DESI) and cybersecurity (NCSI) into nine quadrants (low, medium, high for each dimension). It visualizes countries' current states, identifies their strengths and weaknesses, and helps prioritize strategic development areas.

Therefore, the causal diagram provides the theoretical and methodological foundation by explaining the mechanisms of index formation and interaction, while the positioning matrix transforms this knowledge into a practical format for analysis, comparison, and decision-making. Together, they form an integrated system that combines deep systems analysis with applied analytics, supporting effective digital transformation planning and cybersecurity enhancement at both national and international levels.

5. Conclusions

This study proposes an innovative approach to assessing the impact of cybersecurity and digital development in countries using a Fuzzy System Dynamics (FSD) model. The core of the approach lies in integrating fuzzy logic with system dynamics to model the nonlinear interdependencies between cybersecurity and digital development across four dimensions: technological infrastructure, economic resilience, human capital, and institutional environment. The novelty of the approach lies in:

1. Using Fuzzy Inference Systems (FIS) to manage data uncertainty, allowing the model to adapt to countries with incomplete statistical data.

2. Creating a causal diagram that models reinforcing and balancing feedback loops.

3. Unlike traditional index-based or regression-based methods, FSD accounts for nonlinearity, dynamics, and qualitative variables, enabling a deeper understanding of complex interrelations.

Another fundamentally new aspect is the combination of quantitative data normalization with fuzzy set theory, which avoids rigid threshold-based decisions and better reflects the real functioning of

digital systems. Traditional methods often ignore the non-linear nature of digital development, which depends on the dynamic interaction of factors that cannot always be precisely measured. Therefore, the model is built as a Fuzzy Inference System (FIS) to formalize the causal relationships between input variables (e.g., institutional trust, digital accessibility, macroeconomic stability) and the resulting level of digital security. Moreover, the proposed system is open to extension and adaptation, as each group of indicators can be detailed or replaced depending on the specific country, its strategic priorities, or available statistical sources. The model can also be integrated with existing digital indices such as the Global Cybersecurity Index, Network Readiness Index, or Digital Economy and Society Index (DESI) — serving not as an alternative, but as an analytical supplement focused on deeper internal evaluation.

Key contributions of scientific novelty:

1. Systemic structuring of digital development across functional dimensions, covering both technological and socio-institutional aspects.
2. Use of internationally recognized composite indicators as a representative foundation.
3. Application of fuzzy logic methods to model complex inter-factor relationships under uncertainty.
4. Adaptability of the model to various strategic analysis scenarios and digital transformation policy monitoring.

The proposed model can serve as a basis for developing national digital capacity rankings, as a tool for rapid diagnostics of the digital environment, and for evaluating the effectiveness of public policies in the field of cybersecurity and digital development. This approach demonstrates strong potential as a tool for shaping effective digital policy. The FSD model provides a comprehensive view of the interrelations between cybersecurity and digital development, contributing to enhancing the competitiveness of countries in the global digital landscape.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] S. Morgan, Cybercrime to cost the world $10.5 trillion annually by 2025, 2021. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

[2] World Economic Forum, Global Risks Report 2023, 2023. URL: https://www.weforum.org/reports/global-risks-report-2023.

[3] The New York Times, Cyberattack Forces a Shutdown of a Top U.S. Pipeline, 2021. URL: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

[4] DW News, Police probe lethal cyberattack on hospital, 2020. URL: https://www.dw.com/en/german-police-probe-negligent-homicide-in-hospital-cyberattack/a-54970859.

[5] National Health Executive, WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled, 2018. URL: https://surl.lu/rrjkqw.

[6] State Service for Special Communications and Information Protection of Ukraine, Report of the Cyber Incident Response Center of the State Cyber Security Center, 2023. URL: https://surl.li/yglmbx.

[7] L. A. Zadeh, Fuzzy sets, Information and Control 8 (1965) 338–353. doi:10.1016/S0019-9958(65)90241-X.

[8] J. W. Forrester, Industrial Dynamics, Pegasus Communications, Waltham, MA, 1961. URL: https://surl.lu/bbgxxt.

[9] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, in: S. Shukla, A. Unal, J. V. Kureethara, D. Mishra, D. Han (Eds.), Data Science and Security, volume 290 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2021, pp. 258–265. doi:10.1007/978-981-16-4486-3_28.

[10] F. Li, M. Hadjieleftheriou, G. Kollios, L. Reyzin, Dynamic authenticated index structures for outsourced databases, IEEE Transactions on Information Forensics and Security 13 (2017) 70–84. URL: https://www.cs.bu.edu/~reyzin/papers/auth-db.pdf.
[11] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2008. URL: https://www.cl.cam.ac.uk/~rja14/book.html.
[12] L. A. Gordon, M. P. Loeb, The economics of information security investment, ACM Transactions on Information and System Security 5 (2002) 438–457. doi:10.1145/581271.581274.
[13] L. M. Tkachuk, M. T. Movchanyuk, Information security as a component of the national security of ukraine, in: Abstracts of the reports of the All-Ukrainian scientific and practical Internet conference of students, postgraduates and young scientists "Youth in science: research, problems, prospects" (MN-2021), Vinnytsia, 2021. URL: https://surli.cc/bbvjye.
[14] Y. V. Kindzerskyi, Cybersecurity and the formation of the digital economy: problems of interconnection, Economics Bulletin 3 (2020) 18–26. URL: https://doi.org/10.33271/ebdut/71.018. doi:10.33271/ebdut/71.018.
[15] N. Kasianova, M. Bilichenko, A. Severynenko, Modeling digital security of an enterprise, Modern Economics 39 (2023) 54–61. doi:10.31521/modecon.V39(2023)-08.
[16] Y. Bilan, O. Oliinyk, H. Mishchuk, M. Skare, Impact of information and communications technology on the development and use of knowledge, Technological Forecasting and Social Change 191 (2023). doi:10.1016/j.techfore.2023.122519.
[17] O. Rehman, Y. Ali, Enhancing healthcare supply chain resilience: decision-making in a fuzzy environment, The International Journal of Logistics Management 33 (2022) 520–546. doi:10.1108/IJLM-01-2021-0004.
[18] National Cyber Security Index, National Cyber Security Index Methodology, 2025. URL: https://ncsi.ega.ee/methodology/.
[19] D. C. North, Institutions, institutional change and economic performance, Cambridge University Press, 1990. URL: https://doi.org/10.1017/CBO9780511808678.
[20] OECD, Digital Economy Outlook 2020, 2020. URL: https://doi.org/10.1787/bb167041-en.
[21] D. P. Möller, Guide To Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices, Springer, 2024.
[22] European Commission, Digital Economy and Society Index (DESI), 2020. URL: https://digital-strategy.ec.europa.eu/en/policies/desi.
[23] ITU, Measuring digital development: Facts and Figures 2024, 2024. URL: https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-4/.
[24] R. D. Atkinson, A. S. McKay, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution, 2007. URL: http://dx.doi.org/10.2139/ssrn.1004516.
[25] B. Kosko, M. Toms, Fuzzy thinking: The new science of fuzzy logic, Flamingo, London, 1994. URL: https://reasonpapers.com/pdf/19/rp_19_20.pdf.
[26] G. P. Richardson, Feedback Thought in Social Science and Systems Theory, University of Pennsylvania Press, 1991.
[27] J. D. Sterman, Business dynamics: Systems thinking and modeling for a complex world, Irwin/McGraw-Hill, 2000. URL: https://surl.li/wqtqhw.
[28] H. J. Zimmermann, Fuzzy set theory – and its applications, 4th ed., Springer Science & Business Media, 2010. URL: https://doi.org/10.1007/978-94-007-0849-0.
[29] C. Kahraman, Fuzzy multi-criteria decision making, Springer, 2008. URL: https://surli.cc/jaguxd.
[30] UNDP, Human Development Report 2021/2022, 2021. URL: https://hdr.undp.org/en/content/human-development-report-2021-22.
[31] World Bank, Worldwide Governance Indicators 2023, 2023. URL: https://info.worldbank.org/governance/wgi/.
[32] S. Saeed, S. A. Altamim, N. A. Alkayyal, E. Alshehri, D. A. Alabbad, Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations, Sensors 23 (2023). doi:10.3390/s23156666.