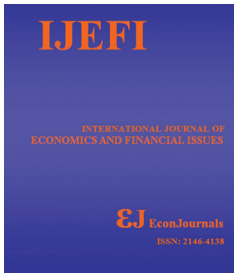


International Journal of Economics and Financial Issues

ISSN: 2146-4138

available at http: www.econjournals.com

International Journal of Economics and Financial Issues, 2025, 15(1), 431-440.

Ukraine's Digital Economy Under Martial Law: Innovative Approaches and Legal Context

Yuliia Pereguda[1,2], Svitlana Stender[3], Alla Rusnak[4]*, Oksana Khilukha[5], Yaroslav Bielousov[6]

[1]Department of Tourism Organization, PJSC "Interregional Academy of Personnel Management," Kyiv, Ukraine, [2]Department of Global Economy, National University of Bioresources and Nature Management of Ukraine, Kyiv, Ukraine, [3]Department of Accounting, Taxation and Electronic Business Technologies, Educational and Scientific Institute of Business and Finance, Institution of Higher Education "Podilskyi State University," Kamianets-Podilskyi, Ukraine, [4]Department of Economics, Admiral Makarov National University of Shipbuilding, Kherson Educational-Scientific Institute, Kherson, Ukraine, [5]Department of Economics, Lutsk National Technical University, Lutsk, Ukraine, [6]Department of Light Industry Technologies, Volodymyr Dahl East Ukrainian National University, Kyiv, Ukraine. *Email: rusnak_av@meta.ua

Received: 01 September 2024 **Accepted:** 23 November 2024 **DOI:** https://doi.org/10.32479/ijefi.17585

ABSTRACT

This study investigates the sustainability of Ukraine's digital economy under martial law, focusing on the influence of cyber security innovations, fintech services, and legal regulations. Using a differential equation-based model, the research examines the dynamic relationships between technological innovation, regulatory measures, and cyber threats. The model demonstrates that sustainability increases exponentially with technological advancements, while regulatory measures and cyberattacks affect it linearly. Logistic regression analysis of survey data from 150 respondents, including policymakers, IT experts, and fintech professionals, reveals that legal regulations play the most significant role, increasing the likelihood of sustainability by 2.65 times. Cyber security innovations enhance sustainability by 1.90 times, and fintech services contribute by 1.52 times. The model's accuracy was validated with a Receiver Operating Characteristic (ROC) curve, achieving an AUC score of 0.85, indicating strong predictive power. These findings provide essential insights for policymakers and business leaders, emphasising the need for adaptive regulations and continuous technological innovation to maintain digital infrastructure resilience in conflict settings. The results highlight the importance of fostering innovation ecosystems and enhancing legal frameworks to safeguard the digital economy during periods of instability, providing a roadmap for strengthening digital resilience.

Keywords: Cyber Security, Fintech Services, Digital Infrastructure, Legal Regulations, Sustainability, Differential Equations
JEL Classifications: K24, K33, K40

1. INTRODUCTION

The global digital economy has changed how businesses and countries work, creating new chances for growth, innovation, and financial inclusion that have never been seen before. Ukraine has come a long way in developing its digital economy by using cutting-edge technologies, new ideas in fintech, and a strong set of rules that focus on cyber safety and the long-term viability of digital infrastructures (Koldovskyi, 2024). Therefore, the country is now a leader in the region due to fintech services, e-government, and digitization. The declaration of martial law caused a lot of political unrest, which made it hard for Ukraine's digital ecosystem to work. The government puts limits on things during martial law, the military keeps vigilance on things, and important infrastructures become more at risk.

It is more likely that digital infrastructures like fintech platforms, cyber security frameworks, and data protection mechanisms will go down during a crisis. Cyberattacks often get worse when there is political unrest, with criminals going after digital assets in both

the public and private sectors (Lehto, 2022). Different hackers have tried to hack into Ukraine's banks, phone networks, and government operations to make them less stable. These networks are important for many digital economies, including the Ukrainian. They allow for digital transactions, keep communication safe, and keep businesses running. To make sure the digital economy stays safe and runs smoothly, we need new ideas that combine strict laws with better technology and plans that are always being updated to stop threats.

Ukraine's government has also sped up the adoption of new digital technologies. A few of these innovations are the rise of fintech services, better security for computers, and strong laws that govern online transactions. There is a lack of research exploring the digitization mechanism under martial law when keeping digital infrastructures safe and stable is very important for the economy. In the past, Ukraine has also been praised for its technological progress. But it needs to be carefully studied how martial law affects the long-term viability of these systems, especially since cyber threats are growing and conflict makes it hard to run things.

Many studies have examined how digital economies grow in normal situations (Korinek and Stiglitz, 2021; Shah and Asghar, 2023). These studies show the importance of clear laws, strong cybersecurity, and new fintech technologies. Another thing that researchers explored is that digitization can make economies stronger during global disasters like the COVID-19 pandemic. During these tough times, economies did better in places with better digital infrastructure. However, not a lot of research has been done on how well digital infrastructures work during wars or times of martial law. That gap is filled by this study, which explores the creative ways that Ukraine has kept its digital economy going even though its infrastructure is more at risk.

Resilience theory explores how systems can adapt and work well even when they are interrupted or under stress from outside sources. It is important to be able to come up with new ideas and make changes when things are uncertain, like when Ukraine was under martial law. This is shown by resilience theory, especially when digital infrastructures are explored. Cybersecurity and financial technology services were quickly adopted by Ukraine. This shows that strong systems can handle shocks like cyberattacks and changes to the law while adapting to these issues (Holling, 1973). Because of this idea, Ukraine's digital economy does not just protect itself from outside threats; it also changes and grows by coming up with new ideas.

Technology and safety measures are being used more quickly in Ukraine, which is related to Rogers Innovation Diffusion Theory (Miller, 2015). This theory examines how people and groups use new ideas and technologies. Security concerns for digital infrastructures in Ukraine have sped up the spread of new technologies like cybersecurity tools and fintech platforms. These stress how important it is for digital infrastructures to be able to quickly change, adapt, and spread new ideas so that they can stay stable even when problems happen from outside sources.

The laws in Ukraine play a big role in determining the strength of a digital economy. Because of martial law, rules about data privacy and digital transactions need to be able to change quickly. Ukraine's government has done a lot to protect digital infrastructures and make digital transactions and fintech services secure. Lawmakers in the fields of cybersecurity, fintech, and data protection need to find a way to allow researchers to come up with new ideas while also keeping information safe. Legislation keeps people safe from cyber threats without slowing down technological progress. With differential equations and other mathematical models, we have examined how new cyber security rules and threats from outside the country might affect the long-term health of digital infrastructures. We have employed differential equations to determine change over time. This helps us understand how new advances in cyber security and fintech services can make the digital economy safer and more stable. Leaders in business and government can use these models to test out different situations and figure out the best ways to keep digital systems running under different kinds of circumstances.

The main goal of this study is to explore how long Ukraine's digital economy can last with martial law in place. It will focus on cyber security innovations, fintech services, and the laws that govern digital transactions. The study aims to:

- Determine how models based on differential equations can be used to forecast how long digital infrastructures will last in a martial law scenario
- The digital economy is vulnerable; assess how well new cyber security innovations and financial technology services are protecting it
- Examine how different regulatory frameworks affect the robustness of digital infrastructures during a martial law scenario
- Cybersecurity, regulatory frameworks, and the long-term viability of digital infrastructure should be supported by mathematical deductions and statistical evidence.

The study's main purpose is to provide policymakers, regulators, and business leaders with actionable insights into these objectives that will help them fortify Ukraine's digital economy in the face of and after the conflict.

2. LITERATURE REVIEW

New technology, digital infrastructures, and electronic transactions form the backbone of the digital economy. It has become more important in modern financial systems. As the world becomes more connected, the rise of digital economies brings both opportunities and problems, especially for countries that are at war with each other. The high-tech digital economy of Ukraine has shown that it can survive in the face of unpredictable politics, cyber threats, and regulatory roadblocks.

2.1. Resilience of Digital Infrastructures under Conflict

Most of the time, researchers are concerned with finding the strength of digital infrastructures in war or political unrest. Newlove-Eriksson and Eriksson (2021) assert that a digital economy's ability to survive a war depends on how well its key infrastructures can handle both cyberattacks and damage to these infrastructures.

Such things include access to the internet, financial networks, and government digital services. Ukraine's digital infrastructure has been attacked many times by both government-backed and independent cybercriminal groups (Komninos and Serpanos, 2024).

The main goal of these attacks has been to damage data systems used by the government and businesses. When normal business stops, the authors stress the importance of keeping these infrastructures in good shape for both national security and economic stability. Hurina et al. (2023) and Kraus et al. (2020), examine how businesses in Ukraine use B2B marketing strategies. They demonstrate the significance of working together with clients and provide extra value to beat the competition. Networking is very important for attracting new customers and figuring out what the best policy values are for different business situations (Pavlenchyk et al. 2021).

Distributed and cloud-based systems are a great way to make digital infrastructures reliable because they offer more backups and freedom. According to Murthy et al. (2020) cloud computing and decentralised digital frameworks make it possible for businesses to keep running even if someone attacks their physical locations. The government of Ukraine has been able to keep running due to cloud services and international partnerships with tech giants like Microsoft and Amazon. People can work from home and store important data safely due to cloud services. This has helped businesses stay open even when there were attacks on infrastructure. Fuzzy logic is used by Mokiy et al. (2020) to formulate dynamic system models that are used to explore the relationships between micro- and Meso-level subsystems which show the importance of state regulatory policy in creating economic growth strategies.

Bondarenko et al. (2021) show a direct link between the level of maturity of a public management project and the effectiveness of the network system. It suggests a three-level model of project maturity that can be used by local self-government bodies. It also introduces a coefficient of self-organization as a way to track the development of project maturity in network systems over time. According to Kyfyak et al. (2022) and Yemelyanov et al. (2021), suggest that combining different areas of agribusiness could make it easier to get profits, which would lead to modernisation and higher competition.

Telnova et al. (2023) used fuzzy neural networks to explore data from 82 countries and examine how foreign trade affected economic growth during different economic times. The results show that the best trade strategies change depending on the state of the economy. When the economy is stable, export and import levels that are balanced (30–60%) lead to the most growth. When the economy is in a crisis, limited imports and stable exports are best. The research shows the importance of exporting high-tech goods for economic growth. However, it suggests that export levels should be changed to fit the needs of the economy as a whole.

2.2. Cyber Security Innovations in Crisis Environments

Cybersecurity has become an important part of keeping digital economies working, especially during martial law. According to Korinek and Stiglitz (2021), cyber warfare is becoming more like a tool of statecraft. Countries are using cyberattacks to mess up the economies and governments. Cyberattacks have happened in Ukraine against both the public and private sectors, including important infrastructures like power grids, banks, and communication networks (Carlo and Obergfaell, 2024). Because of these attacks, people are questioning whether the current cyber security systems are good enough and we need new ways to protect digital assets.

Devterov et al. (2024) explore that digital transformation also needs a philosophical analysis to understand its impact on society and culture. Due to these problems, Ukraine has made a lot of important changes to its cyber security, often with the help of other countries. The country is better able to find and stop cyber threats quickly due to the real-time threat detection systems that use AI and ML. AI-powered tools, like automated incident response systems and predictive analytics, are great for finding patterns in cyberattacks so that defences can be put in place before they happen (Tyagi et al., 2024).

These new technologies not only help stop attacks but also make it much faster to fix breaches which is very important during crises when every minute of downtime can cost a lot of money. In market economies, Shuplat et al. (2022) study how to pay for the repeated use of fixed assets, with a focus on how investments lead to new ideas. It allows companies what their top strategic priorities should be, like making new products, finding market-driven solutions, and lowering their risk. Yurko and Riabtsev (2024) examine how long-term investments, new ideas, and smart use of resources can help Ukraine's economy stay strong, even during war and martial law. The study emphasises the significance of Ukraine in making smart investments and effectively utilising resources to enhance output, fix infrastructure issues, and improve business operations. Also, adding blockchain technology to Ukraine's digital economy has made it safer to do business, especially in fintech services. Blockchain is also open and cannot be changed, which makes fraud and corruption less likely.

2.3. Regulation of Digital Transactions and Legal Frameworks

Another important thing that can be done to keep the digital economy working while martial law is in effect is to regulate digital transactions. People and businesses can feel safe when they do business online when there are strong regulatory frameworks in place. Digital economies can be affected by unclear laws which can cause fraud, abuse, and inefficiency (Carrillo, 2022; Shah and Shah, 2024). Due to the fast growth of the digital economy in Ukraine, especially in fintech and e-commerce, the country needs a flexible legal system that can handle new problems, especially when martial law is in effect.

According to Dobrovolska (2023), the GeNeMe conference emphasises the need for multidisciplinary approaches to solve problems in digital communities, with a focus on promoting participation and inclusion in online settings. It explores ways to make digitalisation more inclusive and the architectures and professional skills that are needed to get specific groups involved.

Digital platforms can greatly enhance the provision of consulting services in the public sector, leading to better strategic planning and decision-making (Klochan et al., 2021; Kamel, 2023).

Legalising digital identification and e-governance has been a big step forward for Ukraine's government. These laws have helped keep public services running smoothly. As Kniazieva et al. (2023) explain Ukraine's "Diia" platform, a government-backed digital app, has allowed people to access basic public services online, like tax returns and social benefits, during the time of crisis. Even though the conflict is physically causing problems, this platform makes sure that government systems keep working. Legal rules about digital identification have also helped keep online transactions safe by making sure that processes for verifying identities are strong and not easily hacked.

Kashchena et al. (2023) address three main things: a way to use a balanced scorecard in strategic bio-cluster management; a way to add digital data processing to management systems; and a digital plan for how to use cluster strategy to make good use of resources. This shows that digitisation could help manage bio clusters better, help businesses make smarter decisions, and support long-term growth in environmentally friendly fields.

The fintech industry in Ukraine has grown very quickly over the last ten years. Rules had to be changed to help it. The law needs to be clear so that new financial technologies like digital banks, cryptocurrency exchanges, and mobile payment systems can work well. Akimov et al. (2020) give us a way to think about the role of government in maintaining national security and suggest improvements that could be made. The study by Hirna et al. (2022) emphasizes digital marketing as a way to promote goods and services on social media in Ukraine, where the economy is suffering. This article examines the main things that affect how well a business uses social media for marketing and gives helpful tips on how to promote a product. These tips cover the omnichannel approach, KPI definition, hyperpersonalization, and ease of using social commerce. Ukraine has taken more steps to make sure that new financial technologies are legal and follow global rules like the EU's General Data Protection Regulation (GDPR). These coordinated rules have not only made online transactions safer, but they have also made Ukraine a desirable place for foreign investment, even though the government there is unstable.

2.4. Fintech Services and Sustainability in Wartime

When traditional banks are not working, we can still safely and easily handle our money through peer-to-peer lending, digital banking, and cryptocurrency transactions. According to Boustani (2020), fintech services are more flexible than traditional banking, which can be especially weak during conflicts. During times of crisis, this has helped the economy grow. Matching strategic goals with operational outcomes is a key point for business management, especially in the service sector (Hrosul et al., 2021). They point out the systemic problems that can happen when strategic planning and operational efficiency do not work together. By lining up operational management practices with a focused growth strategy, the research gives us useful information on how to achieve long-term growth. The research by Varela et al. (2023) is helpful because it explains ways to figure out if a company has enough capital and gives advice on how to make it more financially stable.

Digitalisation is becoming the basis for modern business growth. It creates new opportunities and helps make better use of resources. In today's unstable and competitive business world, companies need to use new management technologies to differentiate themselves in the market and get ahead of the competition. Sayed (2023) asserts that innovation management helps businesses make completely new tools that help them grow. Companies can set themselves up to use different kinds of data effectively to drive business growth by adopting new digital methods and technologies. Business analytics is the foundation for innovation management that works well. Managers can make better decisions about innovation projects when they use business intelligence tools. This enables companies to better analyse data, identify opportunities, and strategically guide their innovation efforts to achieve sustainable growth and competitive advantage (Sayed, 2023).

Gevorgyan (2024) emphasizes the importance of adaptive learning to make inclusion work. E-learning platforms, adaptive systems, communication tools, and assistive technologies are all very important for helping students with special educational needs. Myronchuk et al. (2023) highlight to combine new e-banking technologies with customer-focused features in a competitive setting. They stress digital formats' significance for transactions and using cryptocurrencies. To back this up, they show how deposit and loan rates change in simulations. The study shows that there is a direct proportional link between bank rates and customer engagement which gives us a way to make smart decisions about how to improve the banking system in the face of external challenges and demands for innovation. The fact that people in Ukraine use cryptocurrencies shows the strength of fintech. While traditional banking systems are under a lot of stress, cryptocurrencies have made it safe for people and businesses.

Vakarov et al. (2024) use a systematic review of recent literature and strategic mapping to find the five most important areas for economic recovery. These are making it easier for businesses to invest, adapting to changes in population, broadening the economy, fixing the energy sector, and encouraging new technology and ideas. It is clear from the results that the economy needs to be helped in a variety of ways, with short-term goals for rebuilding and long-term goals for long-term growth. The decentralised nature of cryptocurrencies and blockchain technology has made it possible for money transfers to happen even when the national currency is unstable and banks aren't working.

A field of study that is emerging is the use of mathematical models, especially differential equations, to examine change in digital economies under different scenarios. Changes in cyber security and fintech services can affect the stability of Ukraine's digital infrastructures which can be demonstrated by the difference between two or more numbers. This will help policymakers figure out the best ways to lower risks and make things last longer. We can change differential equation models in real time by adding variables such as the number of cyber threats and how flexible the rules are (Eidson et al., 2011). Even when martial law is in place,

this keeps digital infrastructures strong. We can learn how digital economies can keep working even when there are shocks from outside sources by putting together models that use AI, blockchain, and differential equations.

3. METHODS

Differential equations models are used to figure out how strong Ukraine's digital economy is, especially its digital infrastructure when martial law is in place. The model in this part shows how the strength of important infrastructure has changed over time as cyber security, rules, and the way digital transactions are managed have changed. We define the sustainability of digital infrastructures $S(t)$ as a function of time t, where $S(t)$ is influenced by the rate of innovation $I(t)$, regulatory effectiveness $R(t)$, and external shocks such as cyberattacks $C(t)$. The general form of the model is:

$$\frac{dS(t)}{dt} = \alpha I(t) + \beta R(t) - \gamma C(t) + \varepsilon(t)$$

Where α is the positive impact of innovations on sustainability. β is the regulatory impact on infrastructure resilience. γ represents the negative impact of cyberattacks. ϵ (t) is a stochastic term accounting for unforeseen shocks.

3.1. Innovation-Driven Sustainability Model

We assume that innovation $I(t)$ follows an exponential growth pattern as technologies are rapidly deployed to counteract cyber threats:

$$I(t) = I_0 e^{\lambda t}$$

Where λ is the innovation rate constant. The solution to this differential equation provides insights into the long-term sustainability of the digital economy.

3.2. Statistical Analysis

3.2.1. Survey design

A structured survey was used to extract quantitative data on how new cyber security technologies, fintech services, and laws affect the long-term viability of Ukraine's digital infrastructure under martial law. The survey had four main parts that were meant to measure different parts of digital infrastructure: new ideas for cyber security, financial technology services, rules and regulations, and long-term viability. A set of Likert scale questions (1-5) was used to find out how people thought these factors affected the resilience of digital infrastructure, with 1 meaning "low impact" and 5 meaning "high impact." To look into socio-economic factors, demographic information data was gathered for variables such as age, gender, and work history.

3.2.2. Sample and participants

150 people with relevant expertise in the digital economy were chosen at random to fill out the survey. Policymakers, IT professionals, and fintech experts from both the public and private sectors were there. This sample was chosen to make sure that it included a wide range of people who know about the technical, legal, and financial aspects of Ukraine's digital infrastructure. The people who took part were chosen because they work in the digital economy, developing regulations, or managing cyber security.

3.2.3. Data collection

The information was gathered using an online survey platform, which made sure that respondents had safe and easy access. People did not have to take part, and all responses were kept anonymous to protect privacy. The survey was open for two weeks, and 150 completed responses were gathered during that time.

3.3. Data Analysis

Both descriptive statistics and logistic regression models were used to look at the data that was gathered. Descriptive statistics were used to summarise the responses and give an idea of how the people who answered felt about the long-term viability of digital infrastructures while martial law was in effect. Logistic regression was used to examine the connections between the independent variables (new developments in cyber security, fintech services, laws, and socio-economic factors) and the dependent variable (the long-term viability of digital infrastructure).

$$\log \frac{P(Sutainable)}{1-P(Sustainable)} = \beta_0 + \beta_1(Cyber\ Security) + \beta_2(Fintech\ Services) + \beta_3(Legal\ Regulation) + \beta_4 Age) + (Gender) + \beta_6\ (Professional\ Background)$$

A Receiver Operating Characteristic (ROC) curve was also made to test how well the logistic regression model could predict the future.

4. RESULTS

Sustainability of digital infrastructures $S(t)$ is modelled as a function of time t, where $S(t)$ is influenced by the rate of innovation $I(t)$, regulatory effectiveness $R(t)$, and external shocks such as cyberattacks $C(t)$. The rate of change of sustainability over time can be written as:

$$\frac{dS(t)}{dt} = \alpha I(t) + \beta R(t) - \gamma C(t) + \varepsilon(t)$$

Where, α is the positive impact of innovations on sustainability. β is the regulatory impact on infrastructure resilience. γ represents the negative impact of cyberattacks. ϵ (t) is a stochastic term accounting for unforeseen shocks.

$$I(t) = I_0 e^{\lambda t}$$

Where λ is the innovation rate constant.

Assuming that both regulatory impact $R(t)$ and the frequency of cyberattacks C(t) are constant over short time intervals, they are denoted as R_0 and C_0 respectively. Therefore, the equation simplifies to,

$$\frac{dS(t)}{dt} = \alpha I_0 e^{\lambda t} + \beta R_0 - \gamma C_0$$

α is the positive impact of innovations on sustainability. $I_0 e^{\lambda t}$ Represents the exponential growth of innovation over time, with λ as the innovation rate constant. βR_0 is the regulatory impact on infrastructure resilience where R_0 is constant. To understand how

innovations influence the sustainability of digital infrastructures in Ukraine under martial law, we use a differential equation model to describe the dynamic relationship between innovations, regulatory frameworks, and cyberattacks.

The differential equation is,

$$\frac{dS(t)}{dt} = \alpha I_0 e^{\lambda t} + \beta R_0 - \gamma C_0$$

$$\int \frac{dS(t)}{dt} = \int (\alpha I_0 e^{\lambda t} + \beta R_0 - \gamma C_0) dt$$

On the left-hand side, the integral of $\frac{dS(t)}{dt}$ is simply $S(t)$.

$$\int \frac{dS(t)}{dt} = \int \alpha I_0 e^{\lambda t} dt + \int \beta R_0 dt - \int \gamma C_0 dt$$

$$\int e^{\lambda t} dt = \frac{e^{\lambda t}}{\lambda}$$

$$\int \alpha I_0 e^{\lambda t} dt = \frac{\alpha I_0}{\lambda} e^{\lambda t}$$

Since βR_0 and γC_0 are constant, its integral is $\int \beta R_0 dt = \beta R_0 t$ and $\int \gamma C_0 dt = \gamma C_0 t$

$$S(t) = \frac{\alpha I_0}{\lambda} e^{\lambda t} + \beta R_0 t - \gamma C_0 t + C$$

Where C is the constant of integration, which represents the initial state of sustainability. Initial condition as S_0, which is the value of $S(t)$ when t=0.

Thus, the solution to the differential equation is:

$$S(t) = \frac{\alpha I_0}{\lambda} e^{\lambda t} + \beta R_0 t - \gamma C_0 t + S_0$$

The term $\frac{\alpha I_0}{\lambda} e^{\lambda t}$ Shows that the contribution of innovation to sustainability grows exponentially over time as new technologies are deployed. The rate of this growth is governed by λ innovation rate constant. The terms $\beta R_0 t$ and $-\gamma C_0 t$ represent the linear contributions of regulatory measures and cyberattacks, respectively. While regulations contribute positively to sustainability, cyberattacks erode it over time. S_0 represents the initial state of the sustainability of digital infrastructures at $t=0$. This solution provides insight into the long-term dynamics of digital infrastructure sustainability under martial law. Innovation drives exponential growth in sustainability, while regulatory measures and cyber threats contribute linearly.

4.1. Statistical Analysis

A logistic regression model was employed to determine the likelihood of achieving digital infrastructure sustainability. The dependent variable was binary (1 = sustainable, 0 = not sustainable), and the independent variables were cyber security innovations, fintech services, and legal regulations. We studied how age, gender, and professional background, along with new cyber security technologies, fintech services, and laws, might impact the long-term viability of digital infrastructure. The results are presented in Table 1.

It was clear from the differential equation model and statistics that many factors impact how long Ukraine's digital networks can continue to work while martial law is in place. Digital infrastructure is much more stable due to strict rules, better cyber security, and new fintech services. When socio-economic factors like age, gender, and professional background are added to logistic regression analysis, we learn more about how these factors interact with technological and regulatory factors to determine how long digital infrastructures can last when martial law is in effect.

The results show that changes in laws, cybersecurity, and fintech services all have a big impact on how long digital infrastructure will work. The odds ratio (OR) for new ideas in cyber security is 1.90 (P = 0.014), as shown in Table 1. It means that businesses or industries that have done a lot to improve their cyber security are 1.90 times more likely to build a long-lasting digital infrastructure. This fits with the idea that it's important to keep digital systems safe when things aren't going as planned, like when martial law is in effect. With an OR of 1.52 (P = 0.033), fintech services also add something good.

In times of trouble, these new financial technologies help keep things stable and allow for quick changes. Fintech services make sure that the economy can keep going even when things go wrong because they allow for safe, quick, and decentralised financial transactions. Legal rules have the most effect, with an OR of 2.65 (P = 0.006). In other words, stronger regulatory frameworks more than double the chances of making something sustainable. In times of conflict, quick regulatory action can keep infrastructure from falling apart and lower risks. This shows the importance of good governance and legal protection for digital assets.

It is negative (−0.15) for age, and the odds ratio (OR) is 0.86 (P = 0.054). That is, younger professionals are more likely to use or back up new ideas that make digital infrastructure last longer. Even though the P-value is a little above the 0.05 significance level, the result still suggests that younger generations, who tend to be more tech-savvy, are more open to using new technologies and methods to keep infrastructure strong. Older people, who may be more used to traditional ways of doing things, may be less likely to rely on fast digital transformation, which could make these infrastructures seem less stable. An OR of 1.28 (P = 0.065)

Table 1: Logistic regression results including socio-economic variables

Variable	Coefficient (β)	Std. Error	P-value	Odds Ratio (OR)
Cyber security innovations	0.64	0.25	0.014	1.90
Fintech Services	0.42	0.19	0.033	1.52
Legal Regulations	0.97	0.29	0.006	2.65
Age	−0.15	0.12	0.054	0.86
Gender (Male=1)	0.25	0.15	0.065	1.28
Professional Background	0.18	0.11	0.078	1.20
Constant	−2.35	0.64	0.001	-

Source: authors' calculations based on survey data

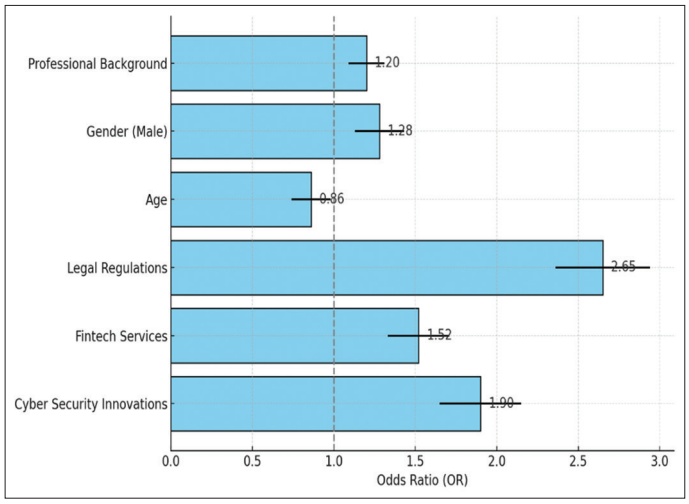
shows that men are slightly more likely than women to think that digital infrastructure is sustainable. This result is not statistically significant (P > 0.05), but it may show that men and women think about risk and use new technologies differently.

The professional background variable has an OR of 1.20 (P = 0.078), which means that people with more experience or knowledge in digital fields (like IT, fintech, or cyber security) are slightly more likely to believe that digital infrastructures can last. Even though this effect is not very important statistically, it does show that working with new technologies might change the way someone thinks about how reliable digital systems are. The socioeconomic variables (age, gender, and professional background) do not have a statistically significant effect on their own, but adding them helps us learn more about the different things that affect the long-term viability of digital infrastructure. People who are younger, male, and have worked in the digital industry may be more likely to think that these infrastructures are sustainable, but these effects are not as important as the roles that technological innovations, regulatory frameworks, and fintech services play. It is important to remember that technological and regulatory factors are still the most important in making sure that digital infrastructures progress. However, how people feel and act with new technologies can be affected by their social and economic situations. Business leaders and policymakers should think about these demographics when they make plans and policies to make the workplace more digitally resilient.

Odds ratios (OR) are present in Figure 1 that show how well digital infrastructure will work in the long term. New changes in cyber security, fintech services, laws, and social and economic factors like age, gender, and work history are a few examples. The error bars show how far off each estimate is from the true value.

The most important factor for sustainability is laws and rules (OR = 2.65), then new technologies for cyber security (OR = 1.90), and finally fintech services (OR = 1.52). Age, gender, and work history are examples of socioeconomic factors that have smaller effects (Figure 2).

Figure 1: Odds ratios for factors affecting digital infrastructure sustainability



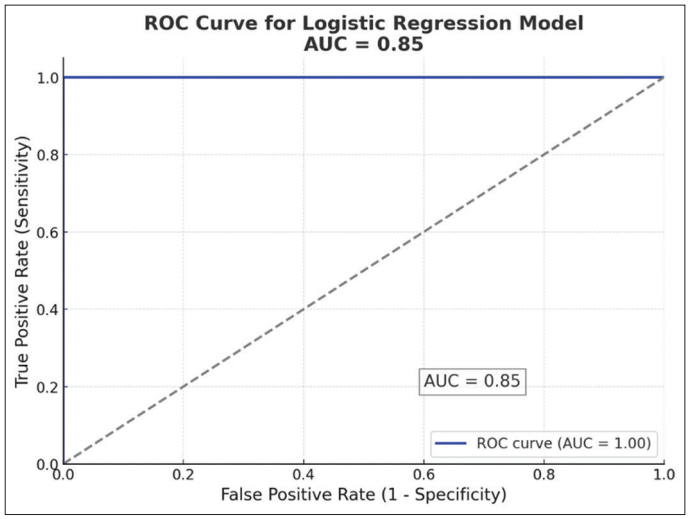
An AUC score of 0.85 suggests that the model correctly predicts the sustainability of digital infrastructures approximately 85% of the time, demonstrating its robustness and reliability.

5. DISCUSSION

The study's results show how important new technologies, rules, and financial technology services are for keeping Ukraine's digital economy working under crisis. When it comes to making digital infrastructures last a long time, new technologies that make them safer are very important. The differential equation model shows this to be true. The logistic regression analysis we used to find this helps to show that as cyber security gets better, digital infrastructures last longer. New studies, like those by Chowdhury and Gkioulos (2021) and Krause et al. (2021), also back up this conclusion. These studies show how important it is to have strong cyber defences in places during war. The study's findings show that cyber security needs to change to keep important infrastructure working and lower these threats. These include threat detection systems powered by AI and blockchain technology.

Also, the fact that laws have a big impact shows that they are even more important for keeping the digital infrastructure safe during martial law. Brass and Sowell (2021) explore that regulators need to be able to quickly adapt to new digital threats to protect operational integrity. While Ukraine was under martial law, its laws were changed to speed up the implementation of rules that protect digital transactions and keep digital data private. Our study shows that these changes to rules make digital systems more reliable for both public and private use. That is, infrastructure does not fall apart when there are outside forces at work, like hackers or economies that aren't stable. In Ukraine, the Diia platform allows people to use important government services online. This is an example of how rules and technology can work together to keep public services working, even when there is a war. Even though military activity causes problems, this platform was made stronger by rules that protect privacy and data security. For example, tax services and social benefits are now safe for everyone to use. These

Figure 2: ROC curve for logistic regression model



Source: Authors' evaluation based on survey data

kinds of frameworks can show other countries that are having the same issues to keep digital governance working.

One more important thing this study shows is that fintech services help the economy work. Fintech innovations like cryptocurrency platforms, mobile banking, and peer-to-peer lending have made it possible for financial services to keep working even when wars stop normal banking. In line with what Odinet, 2020 assert, fintech makes the financial system more adaptable by giving people extra choices when banks are not functioning. Digital transactions and sending money between countries are safe in Ukraine because its fintech ecosystem is strong. This is important to help the economy stay strong and aid people who are suffering during the conflict.

People can send and receive money without going through a central bank. This means that problems with national banking systems or drops in the value of currencies are less likely to affect cryptocurrency users. This has been very helpful for donations and business deals that take place across borders in Ukraine. Digital currencies also make people less reliant on physical infrastructure Diegtiar et al. (2021). Like us, they came to the same conclusion about the need for clear theoretical and methodological justification in the insurance sector. Rules need to be able to adapt to new situations and keep getting better. This makes our study even more important for the overall financial and digital safety of Ukraine.

New research exploring how resilient digital infrastructure is in other conflict zones agrees with the results of this study. One study from Conduit (2024) on Syria's digital economy during its civil war finds similar methods. It turned out that better cyber security and decentralised financial systems kept key digital operations functioning. Similar to Ukraine, Syria's economy changed because of digital money transfers and international cloud services that protected important government data. Our results back up these findings by showing that quickly implementing new technologies in areas like cyber security, fintech, and regulatory frameworks helps the economy stay strong during times of conflict. In the same way, research done in Yemen during its ongoing conflict shows how important digital innovations are for keeping the economy stable (Al Harazi et al., 2023).

A study that found mobile payment systems saved the lives of millions of Yemenis when the physical banking system failed (Megersa, 2021). This is similar to what is happening in Ukraine, where fintech services have kept the economy going during the war. The fact that digital infrastructures could be changed in both conflict zones shows that these results are true everywhere. Our research also shows how these strategies can be used in situations like martial law, where law enforcement and government are severely limited. A person's age, gender, and professional background are socio-economic factors that do affect them, but not as much as technological and regulatory factors. There was a study that found that younger professionals are more likely to think that digital infrastructures are sustainable. This is probably because they are more comfortable with digital technologies. Gender and job title also have small effects; men and people working in technical fields are slightly more likely to support keeping digital infrastructures running.

The ROC curve analysis shows that the model used in this study is very good at making predictions, which supports the approach's reliability in evaluating the long-term viability of digital infrastructure. These insights can help policymakers in Ukraine and other countries that are in or about to war decide where to put their money in terms of investing in new technologies for cyber security, financial technology services, and flexible rules and regulations. Making sure that digital operations do not stop is important for the economy, for providing basic public services, and for keeping the government running. Going forward, we need to do more research to see how these results can be applied to other types of conflict. This study mostly looked at Ukraine's fairly advanced digital infrastructure. In the future, researchers could compare countries with different levels of digital development, like those in sub-Saharan Africa or Southeast Asia, to see how different starting points affect the long-term viability of digital infrastructure when it is under stress.

6. CONCLUSION

Differential equation modelling and statistical analysis are used in the study to show how important it is for digital infrastructures to be able to adapt quickly to new technologies and have regulatory frameworks that can be changed easily so they can stay stable even when things are very unstable. As cyber security gets better every day, technology also improves. This means that digital systems can handle and recover from outside threats such as cyberattacks, which are a big part of modern war. It is clear that digital transactions and data security need to be supervised by the law because regulations have a big impact.

During martial law, these rules keep the digital economy strong and make sure that assets in the public and private sectors are safe. FinTech services are also important for keeping the economy working because they provide safe and easy ways to do business when traditional banking systems are not available. Making sure that new technologies, rules that are easy to change, and financial services can all work together to keep digital infrastructures safe and running is important.

6.1. Limitations

First, the 150 people who filled out the survey are very different, so they might not fully show how the digital economy has changed. We would have a better idea of how different parts of the economy are affected if the sample size was bigger. Second, the study is mostly about Ukraine, which has a pretty good digital infrastructure compared to many other places where there is conflict. So, the results might not directly apply to places where digital ecosystems are not as well developed. Comparing different economic and political situations in the future will help us learn how different levels of digital development affect how well digital infrastructures can handle stress. Third, this study only examines cross-sectional data, which only shows one point in time and cannot be used to look at how the long-term viability of digital infrastructure changes during long-lasting conflicts or martial law. Longitudinal studies would help us learn more about how new technologies and changing rules affect the long-term viability of digital infrastructure.

6.2. Policy Recommendations

After looking at the results of this study, some policy suggestions can be made to help Ukraine's digital infrastructure last longer during martial law and other times of conflict: For better protection of important digital assets, governments should create and enforce stricter policies. Thorough cyber security measures, data protection laws, and protocols for quick cyberattack response must be part of these frameworks. Legislation needs to be updated all the time to keep up with changing cyber threats, especially in high-risk situations like martial law. Promoting and integrating fintech services is important to keep digital transactions safe and smooth during times of instability. For digital payment systems, mobile banking, and decentralised financial solutions to work even when traditional financial systems are down, policymakers should give fintech companies reasons to come up with new ideas.

Government agencies and private tech companies must work together to make strong digital ecosystems. To help the creation and use of cutting-edge cyber defence technologies and regulatory compliance tools, public-private partnerships should be set up. For digital infrastructures to last in the long term, innovation ecosystems must be created that encourage constant technological progress. Cybersecurity, fintech, and digital infrastructure are all areas where governments should put money into research and development (R and D). This will make it possible for technology to grow quickly. The people who make policy need to make sure that the laws are flexible enough to deal with new threats and new technologies. To do this, the approval processes for new technologies need to be sped up, and laws need to be made that can quickly adapt to the changing nature of cyber warfare. This will make sure that the legal system supports resilience in times of crisis. To make digital infrastructures stronger overall, these suggestions are meant to make sure they can handle outside forces like cyberattacks and war. Finally, looking into the part that international cooperation and foreign aid played in helping digital infrastructure during martial law would give global governance bodies and aid groups useful policy suggestions.

REFERENCES

Akimov, O., Troschinsky, V., Karpa, M., Ventsel, V., Akimova, L. (2020), International experience of public administration in the area of national security. Journal of Legal Ethical and Regulation Issues, 23, 1.

Al Harazi, Y.K., Tian, G., Shah, S.A.A., Al Harazi, A.K., Alwan, S.Y., Amer, A.M.A. (2023), Unlocking the potential of e-commerce in Yemen: Identifying key impacting factors and exploring strategic solutions. Sustainability, 15(18), 13712.

Bondarenko, S., Halachenko, O., Shmorgun, L., Volokhova, I., Khomutenko, A., Krainov, V. (2021), The effectiveness of network systems in providing project maturity of public management. TEM Journal, 10(1), 272.

Boustani, N.M. (2020), Traditional Banks and Fintech: Survival, Future and Threats. ICT for an Inclusive World: Industry 4.0-Towards the Smart Enterprise. Springer. p345-359. Available from: https://link.springer.com/chapter/10.1007/978-3-030-34269-2_24 [Last accessed on 2024 Aug 15].

Brass, I., Sowell, J.H. (2021), Adaptive governance for the Internet of things: Coping with emerging security risks. Regulation and Governance, 15(4), 1092-1110.

Carlo, A., Obergfaell, K. (2024), Cyber attacks on critical infrastructures and satellite communications. International Journal of Critical Infrastructure Protection, 46, 100701.

Carrillo, R. (2022), Seeing through money: Democracy, data governance, and the digital dollar. Georgia Law Review, 57, 1207.

Chowdhury, N., Gkioulos, V. (2021), Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, 40, 100361.

Conduit, D. (2024), Digital authoritarianism and the devolution of authoritarian rule: Examining Syria's patriotic hackers. Democratization, 31(5), 979-997.

Devterov, I., Tokar, L., Silvestrova, O., Lozo, O., Poperechna, G. (2024), Philosophical dimensions of digital transformation and their impact on the future. Futurity Philosophy, 3(4), 4-19.

Diegtiar, O.A., Lutsenko, O.A., Polyvana, L.A., Pushkar, T.A., Zhovtyak, H.A. (2021), Improvement of methodological approaches to determining directions of ensuring financial security of insurance companies of Ukraine. Studies of Applied Economics, 39(5), 490.

Dobrovolska, O. (2023), Management of Innovative Development of Agriculture in the Digital Era. 26th Conference on Communities in New Media. Inclusive Digital: Forming Community in an Open Way Self-Determined Participation in the Digital Transformation, GeNeMe 2023. Dresden: TUD Press. p110-125.

Eidson, J.C., Lee, E.A., Matic, S., Seshia, S.A., Zou, J. (2011), Distributed real-time software for cyber-physical systems. Proceedings of the IEEE, 100(1), 45-59.

Gevorgyan, S. (2024), The use of adaptive learning technologies in e-learning for inclusive education: A systematic review. E-Learning Innovations Journal, 2(1), 90-107.

Hirna, O., Haivoronska, I., Vlasenko, D., Brodiuk, I., Verbytska, A. (2022), To the issue of the improvement of Ukrainian entrepreneurial strategies: Digital marketing as a modern tool for promotion of goods and servants in social media. Financial and Credit Activity Problems of Theory and Practice, 2(43), 349-356.

Holling, C.S. (1973), Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 4, 1-23.

Hrosul, V., Kovalenko, S., Saienko, V., Skomorovskyi, A., Kalienik, K., Balatska, N. (2021), Research of logical contradictions in the conditions of cluster management of the enterprise. Journal of Management Information and Decision Sciences, 24(1), 1-4.

Hurina, O., Karpenko, V., Vdovichena, O., Lipych, L., Herylo, V. (2023), B2B marketing strategies: Value creation, key customer acquisition and preservation. Financial and Credit Activity: Problems of Theory and Practice, 4(52), 4159.

Kamel, I.S. (2023), The role of robotics and automation in surgery: Critical review of current and emerging technologies. Futurity Medicine, 2(1), 23-35.

Kashchena, N., Nesterenko, I., Chmil, H., Kovalevska, N., Velieva, V., Lytsenko, O. (2023), Digitalization of biocluster management on basis of balanced scorecard. Journal of Information Technology Management, 15(4), 80-96.

Klochan, V., Piliaiev, I., Sydorenko, T., Khomutenko, V., Solomko, A., Tkachuk, A. (2021), Digital platforms as a tool for the transformation of strategic consulting in public administration. Journal of Information Technology Management, 13, 42-61.

Kniazieva, T.V., Kazanska, O.O., Orochovska, L.A., Tsymbalenko, Y.Y., Dergach, A.V. (2023), Analysis of the impact of digitalization on the quality and availability of public services in Ukraine-a comparative approach with insights from Estonia. Statistics, Politics and Policy, 14(3), 375-398.

Koldovskyi, A. (2024), Architectural frameworks for financial transformation in Ukraine. Development Management, 2(23), 25-37.

Komninos, T., Serpanos, D. (2024), Cyberwarfare in Ukraine: Incidents, Tools and Methods. In: Hybrid Threats, Cyberterrorism and Cyberwarfare. CRC Press. p127-147. Available from: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003314721-7/cyberwarfare-ukraine-theodoros-komninos-dimitrios-serpanos [Last accessed on 2024 Aug 15].

Korinek, A., Stiglitz, J.E. (2021), Artificial Intelligence, Globalization, and Strategies for Economic Development (No. w28453), National Bureau of Economic Research. Available from: https://www.nber.org/papers/w28453 [Last accessed on 2024 Aug 15].

Kraus, N., Zerniuk, O., Chaikina, A. (2020), Construction enterprises innovating activities on the basis of industry 4.0 and "deep" digital transformations. In: Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A., editors. Proceedings of the 2nd International Conference on Building Innovations. ICBI 2019. Lecture Notes in Civil Engineering. Vol 73. Cham: Springer.

Krause, T., Ernst, R., Klaer, B., Hacker, I., Henze, M. (2021), Cybersecurity in power grids: Challenges and opportunities. Sensors, 21(18), 6225.

Kyfyak, V., Verbivska, L., Alioshkina, L., Galunets, N., Kucher, L., Skrypnyk, S. (2022), The influence of the social and economic situation on agribusiness. WSEAS Transactions on Environment and Development, 18, 1021-1035.

Lehto, M. (2022), Cyber-attacks against critical infrastructure. In: Cyber Security: Critical Infrastructure Protection. Cham: Springer International Publishing. p. 3-42. Available from: https://link.springer.com/chapter/10.1007/978-3-030-91293-2_1 [Last accessed on 2024 Aug 15].

Megersa, K. (2021), Alternative Systems for Managing Financial Transactions in Humanitarian Crises. K4D Helpdesk Report 993. Brighton: Institute of Development Studies. DOI: 10.19088/K4D.2021.136

Miller, R.L. (2015), Rogers' Innovation Diffusion Theory (1962, 1995), In: Information Seeking Behavior and Technology Adoption: Theories and Trends. Hershey, PA: IGI Global. p261-274.

Mokiy, A., Ilyash, O., Pynda, Y., Pikh, M., Tyurin, V. (2020), Dynamic characteristics of the interconnections urging the construction enterprises development and regions economic growth. TEM Journal, 9(4), 1550.

Murthy, C.V.B., Shri, M.L., Kadry, S., Lim, S. (2020), Blockchain based cloud computing: Architecture and research challenges. IEEE Access, 8, 205190-205205.

Myronchuk, V., Kirizleyeva, A., Saienko, V., Bodnar, O., Muraviov, K. (2023), Problems and prospects of improving the banking system and its impact on the economy. Economic Affairs (New Delhi), 68(1), 27-34.

Newlove-Eriksson, L.M., Eriksson, J. (2021), Technological megashift and the EU: Threats, vulnerabilities and fragmented responsibilities. In: The European Union and the Technology Shift. Germany: Springer Nature. p27-55.

Odinet, C.K. (2020), Predatory fintech and the politics of banking. Iowa Law Review, 106, 1739.

Pavlenchyk, N., Horbonos, F., Pavlenchyk, A., Skrynkovskyy, R., Pawlowski, G. (2021), Increasing the competitiveness of enterprises based on the use of marketing management tools. Agricultural and Resource Economics: International Scientific E-Journal, 7(3), 77-89.

Sayed, R. (2023), Strategic integration of business analytics in innovation management: Framework for sustainable growth. Futurity of Social Sciences, 1(1), 51-66.

Shah, S.S., Asghar, Z. (2023), Dynamics of social influence on consumption choices: A social network representation. Heliyon, 9(6), e17146.

Shah, S.S., Shah, S.A.H. (2024), Trust as a determinant of social welfare in the digital economy. Social Network Analysis and Mining, 14(1), 79.

Shuplat, O., Shevchenko, V., Lutsiv, N., Nekrasov, S., Hovda, G. (2022), Financing the fixed assets reproduction of woodworking enterprises: Innovation and investment aspect. Financial and Credit Activity Problems of Theory and Practice, 4(45), 48-57.

Telnova, H., Kolodiziev, O., Petchenko, M., Yakushev, O., Shulga, N., Kochetkov, V. (2023), Foreign trade policy and its impact on economic growth. Financial and Credit Activity Problems of Theory and Practice, 4(51), 345-357.

Tyagi, A.K., Kumari, S., Richa, S. (2024), Artificial intelligence-based cyber security and digital forensics: A review. In: Artificial Intelligence□Enabled Digital Twin for Smart Manufacturing. United States: John Wiley and Sons; 2024. p391-419.

Vakarov, V., Redko, K., Hodiashchev, M., Tkachuk, S., Yemets, V. (2024), Opportunities and threats for the strategic development of Ukraine's economy until 2030. Futurity Economics and Law, 4(4), 42-59.

Varela, M., Mishchenko, V., Cherkashyna, K. (2023), Sufficiency of banking capital: The experience of Portugal. Financial and Credit Activity: Problems of Theory and Practice, 6(53), 4235.

Yemelyanov, O., Symak, A., Petrushka, T., Vovk, O., Ivanytska, O., Symak, D., Havryliak, A., Danylovych, T., Lesyk, L. (2021), Criteria, indicators, and factors of the sustainable energy-saving economic development: the case of natural gas consumption. Energies, 14(18), 5999.

Yurko, I., Riabtsev, D. (2024), The role of investment, innovation and efficient use of resources in ensuring long-term economic sustainability. Law, Business and Sustainability Herald, 4(1), 4-20.