

Methods and Algorithms for Assessing the Resilience of Urban Information Infrastructure under Environmental Uncertainty

Valeriia Cherkasova¹, Maryna Novozhylova²

Modern cities function as complex cyber-physical systems (CPS), where digital technologies are integrated into all aspects of urban life. The urban information infrastructure (UII) forms the basis for the collection, processing, transmission, and storage of data critical to the continuous functioning of a city. Disruptions in UII operation can lead to failures in vital municipal processes, highlighting the importance of assessing its resilience.

This study aims to develop a methodological and algorithmic framework for assessing and forecasting the resilience of UII under multifactor uncertainty. It integrates probabilistic modeling, machine learning, and network analysis to evaluate risks, simulate cascading effects, and design adaptive systems capable of maintaining stability under external disruptions. The proposed approach combines systemic, risk-oriented, and computational methods to address hybrid challenges in wartime and post-war urban environments.

Keywords: urban information infrastructure, resilience, cyber-physical systems, uncertainty, artificial intelligence, digital twins, Ukraine.

1. Introduction

In the modern world, cities operate as complex cyber-physical systems (CPS), where digital technologies are present in all spheres of life – from transportation and energy to administrative services. Within this framework, the urban information infrastructure (UII) serves as the foundation for the collection, transmission, processing, and storage of data required for the uninterrupted functioning of a city.

The relevance of this topic for Ukraine is reinforced by several factors:

1. Military Challenges.

The large-scale Russian invasion involves not only the physical destruction of urban infrastructure but also massive cyberattacks on state and municipal information systems. Assessing UII resilience is essential during wartime and post-war recovery. According to the CERT-UA report, in 2024 over 4315 cyber incidents were recorded – almost 70% more than in 2023 – illustrating the rising threat level for governmental and municipal systems.

2. Environmental Uncertainty.

Unpredictable power outages, enemy cyberattacks, fluctuations in the socio-economic situation, and the destruction of critical facilities represent the diverse risks faced by Ukrainian cities. Classical vulnerability assessment methods fail to account for the dynamic, multifactor nature of these threats.

3. Digital Transformation and the Smart City Concept.

The UII is increasingly integrated into urban governance through the active implementation of e-government and digital services (e.g., Diia, Kyiv Digital, Kharkiv Smart City). Failures in these systems directly affect citizens and businesses.

4. European Integration.

Under the EU-Ukraine Association Agreement and European cybersecurity standards (NIS2, Cyber Resilience Act), Ukraine must ensure adequate resilience of critical and municipal information systems. This necessitates the adaptation of international methods and the

¹ PhD Student, O.M. Beketov National University of Urban Economy in Kharkiv, Ukraine
valeriia.cherkasova@kname.edu.ua

² DSc (Phys.-Math.), Head of the Department of Computer Science and Information Technologies, O.M. Beketov National University of Urban Economy in Kharkiv, Ukraine

5. Post-War Reconstruction and Public Safety.

Urban recovery requires not only rebuilding physical infrastructure but also establishing resilient digital systems capable of functioning under uncertainty and providing essential services during crises.

Traditional engineering and statistical approaches to reliability assessment assume environmental stability. However, under current Ukrainian conditions, new methods are needed that consider multifactor uncertainty, incomplete data, and dynamic dependencies within urban systems. Computational and AI-based modeling offers promising tools for this purpose.

2. Literature Review

In global research practice, various methodologies for assessing the resilience of critical infrastructure have been developed, integrating scenario-based analysis, risk modeling, and stress testing approaches. For example, the author of [6] emphasizes the importance of a multilevel risk management policy within dynamically changing environments. The NIST Cybersecurity Framework [7] provides a taxonomy of cybersecurity outcomes and governance functions (Govern, Identify, Protect, Detect, Respond, Recover) as a foundation for managing risks, yet it does not specify concrete algorithms for assessing the resilience of urban information infrastructure (UII) under uncertainty.

Methodologies used in other domains, such as energy and transport infrastructure [13; 14], demonstrate the potential of multi-factor analysis and Monte Carlo simulations to predict cascading effects. These approaches can be effectively adapted for the evaluation of UII resilience.

A significant part of contemporary research focuses on instruments and frameworks aimed at enhancing the resilience of critical infrastructure systems. The study [19], for instance, presents a classification of 161 analytical tools, including graph-theoretic algorithms for modeling interdependencies and stress-testing methods for verifying internal system robustness. Such approaches are directly relevant to digital urban systems, where the interconnectivity of services creates cascading failure risks.

Systematic reviews [15–17] summarize resilience assessment approaches – from Dynamic Bayesian Networks for modeling technological resilience to quantitative methodologies based on damage accumulation models. These reviews also trace the evolution of resilience evaluation from simple vulnerability indices to integrated assessment systems capable of accounting for the complexity of modern threats.

Modern discourse in the field highlights that contemporary studies [20] often focus on cyber risk assessment, emphasizing algorithmic and AI-based approaches for improving regulatory frameworks related to information and urban infrastructures. However, despite considerable progress in risk modeling, studies that directly address urban information infrastructure resilience remain fragmented. Most concentrate on cybersecurity, data center reliability, or general smart city development, while comprehensive algorithmic solutions for resilience assessment under uncertainty remain underdeveloped.

The use of Complex Adaptive Systems (CAS) theory offers a conceptual foundation for describing urban dynamics, yet its integration into models of UII remains limited [8]. Similar constraints are observed in dynamic flow modeling research [9], which explores interdependencies among infrastructures but lacks a unified methodological approach for assessing UII resilience.

Furthermore, deep learning methods, including Diffusion Graph Convolutional Neural Networks, have been applied to predict failures in smart city systems, but primarily in the cybersecurity domain, without encompassing the broader resilience dimension [11].

The Information Security Strategy of Ukraine until 2025 [3] and the Digital Transformation Report by the Ministry of Digital Transformation [4] highlight the protection of telecommunication networks and public data infrastructures. However, systemic algorithms for assessing the resilience

of urban information systems – particularly under conditions of war or environmental uncertainty – remain insufficiently developed.

In summary, current international and national sources provide a solid methodological foundation adaptable to urban information infrastructure studies. Nevertheless, the research field remains fragmented, emphasizing the need for new, integrated methods tailored to Ukrainian urban realities and capable of predicting and enhancing the resilience of digital urban ecosystems.

3. Research Gaps

This analysis highlights that, although substantial theoretical and applied progress has been achieved in the field of infrastructure resilience, the research on urban information infrastructures remains fragmented and insufficiently formalized. Therefore, it is necessary to identify the unresolved aspects that hinder the development of comprehensive algorithmic solutions for resilience assessment in uncertain and rapidly changing environments.

- Lack of holistic algorithmic approaches that ensure comprehensive assessment of UII resilience under multifactor uncertainty caused by military, technological, and environmental risks.
- Limited adaptation of dynamic and complex adaptive system models (CAS) to the specificity of urban information systems that combine multidimensional digital and socio-organizational elements.
- Fragmentary application of artificial intelligence methods – deep learning algorithms are mostly used for cybersecurity tasks, not for modeling interdependencies across urban subsystems.
- Deficit of standards and quantitative methodologies: International frameworks (UNDRR, OECD, NIST) offer mainly risk management recommendations but lack the analytical instruments required for quantitative modeling of resilience under uncertainty.
- Underdeveloped Ukrainian context: While national policies and CERT-UA statistics highlight information security challenges, systematic algorithms for complex resilience prediction and assessment of UII are still absent.

Based on the analysis of current international and Ukrainian research, as well as the practical implementation gaps, it can be concluded that this scientific direction holds **high potential for further development** and the creation of new methodological foundations for ensuring urban information infrastructure resilience.

4. Research Objectives

The aim of the research is to develop a scientific, methodological, and algorithmic framework for designing adaptive methods of assessing and forecasting the resilience of urban information infrastructure (UII). This framework is intended to automate the processes of risk analysis, identification of cascading effects, and decision support aimed at improving the reliability of urban information systems under external uncertainty. It also involves the application of artificial intelligence (AI) methods for predicting the development of crisis scenarios in urban digital environments.

To achieve this aim, the following **objectives** are set out, structured by research stages:

1) Analytical Stage

- Conduct a comprehensive review of scientific sources and practical approaches to resilience assessment of urban information infrastructure.
- Analyze the impact of military and hybrid threats on the functioning of urban information systems in Ukraine.
- Identify the key gaps in current methods of resilience assessment under conditions of uncertainty.

2) Methodological Stage

- Develop a conceptual model for assessing the resilience of UII as a cyber-physical system.
- Define criteria and indicators for both quantitative and qualitative assessment of resilience.
- Justify a methodological approach that accounts for uncertainty, cascading effects, and cross-sectoral interdependencies in urban systems.

3) Algorithmic Stage

- Develop resilience forecasting algorithms for UII using probabilistic methods, machine learning, and artificial intelligence.
- Design methods for modeling cascading failures and for assessing long-term risks in municipal information systems.

4) Applied Stage

- Implement a prototype software system or digital module for resilience assessment and risk forecasting.
- Conduct testing and validation of the proposed algorithms using open data from Ukrainian cities.
- Develop practical recommendations for enhancing the resilience of urban information infrastructures in wartime and post-war contexts.

5. Methodology

The methodological foundation of this research lies in the combination of systemic, risk-oriented, and algorithmic approaches to analyzing urban information infrastructure (UII) as a complex cyber-physical system (CPS). The study considers the multilevel structure of UII, its cross-sectoral dependencies, and the influence of external uncertainty factors, including military and hybrid threats. The proposed methodology focuses on developing an integrated resilience assessment model that combines mathematical modeling, algorithmic solutions, and modern computational technologies.

The research employs the following methods:

1) System Approach

System analysis enables the examination of UII as a socio-technical system that includes transportation, energy, communication, and digital service subsystems. It allows the identification of intersectoral dependencies and the modeling of cascading effects within the urban infrastructure network.

2) Probabilistic and Mathematical Modeling

Statistical methods, probability theory, and risk analysis are used to conduct quantitative assessments of risks and to forecast UII behavior under various operational and disruptive scenarios.

3) Network Analysis

The network approach is applied to explore the interconnections between subsystems, identify critical nodes, and assess potential cascading failures. Network modeling forms the basis for analyzing the interdependencies between information and physical components of urban infrastructures.

4) Artificial Intelligence Methods

The study employs machine learning and artificial intelligence (AI) techniques to construct adaptive algorithms for resilience assessment. These methods enable the processing of incomplete, fuzzy, and large-scale data, allowing for real-time prediction and the identification of hidden patterns in system behavior. Classification, forecasting, and optimization algorithms enhance the accuracy and speed of computations in dynamic urban environments.

5) Simulation Modeling and Digital Twins

To validate and test the proposed methods, digital twin technology is utilized to create virtual models of urban infrastructure systems. This approach enables the simulation of crisis scenarios, modeling of system behavior under damage or attack conditions, and the evaluation of algorithmic effectiveness in ensuring resilience.

6) Computational Experiment

A key element of the methodology is the implementation of computational experiments, providing empirical validation of the developed algorithms using real and simulated datasets from Ukrainian cities. This approach allows for the evaluation of the applicability, scalability, and performance of the proposed model and the development of practical recommendations for improving UII resilience in wartime and post-war contexts.

6. Expected Results

Theoretical outcomes: a conceptual model integrating systemic, probabilistic, and AI-based components to evaluate UII resilience; a set of criteria and indicators for quantitative assessment; and a method for modeling cascading and long-term risks.

Algorithmic outcomes: development of AI-enhanced predictive algorithms, probabilistic risk models, and a simulation prototype to test resilience under varying uncertainty conditions.

Practical outcomes: creation of a prototype digital tool for municipal resilience evaluation, validated using Ukrainian urban datasets, with recommendations for post-war reconstruction and sustainable digital governance.

Scientific novelty: integrated approach to UII resilience modeling that accounts for cascading effects, incomplete data, and stochastic impacts in uncertain environments.

References:

- [1] Verkhovna Rada of Ukraine. (2021). *Law of Ukraine on Critical Infrastructure* (No. 1882-IX). <https://zakon.rada.gov.ua/laws/show/1882-20#Text>
- [2] President of Ukraine. (2021a). *On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"* (Decree No. 447/2021). <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
- [3] President of Ukraine. (2021b). *On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy"* (Decree No. 685/2021). <https://zakon.rada.gov.ua/laws/show/685/2021#Text>
- [4] Ministry of Digital Transformation of Ukraine. (2024). *Digital transformation results in regions of Ukraine for 2024*. <https://thedigital.gov.ua/news/rezultati-tsifrovoi-transformatsii-v-regionakh-ukraini-za-2024-rik>
- [5] CERT-UA. (2024). *CERT-UA processed 4315 cyber incidents last year*. State Service of Special Communications and Information Protection of Ukraine. <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv>
- [6] OECD. (2024). *Good governance for critical infrastructure resilience*. https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html
- [7] National Institute of Standards and Technology. (2024). *NIST cybersecurity framework 2.0*. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [8] United Nations Office for Disaster Risk Reduction. (2023). *Global methodology for infrastructure resilience review*. <https://www.undrr.org/publication/global-methodology-infrastructure-resilience-review>
- [9] Shi, Y., et al. (2021). Assessment methods of urban system resilience: From the perspective of complex adaptive system theory. *Cities*, 112, 103141. <https://doi.org/10.1016/j.cities.2021.103141>
- [10] Goldbeck, N., Angeloudis, P., & Ochieng, W. Y. (2019). Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models. *Reliability Engineering & System Safety*, 188, 62–79. <https://doi.org/10.1016/j.ress.2019.03.007>
- [11] Han, X., et al. (2022). Research progress and framework construction of urban resilience computational simulation. *Sustainability*, 14(19), 11929. <https://doi.org/10.3390/su141911929>

[12] Wu, P., et al. (2024). Deep learning solutions for smart city challenges in urban development. *Scientific Reports*, 14(1). <https://doi.org/10.1038/s41598-024-55928-3>

[13] Links, J. M., et al. (2017). COPEWELL: A conceptual framework and system dynamics model for predicting community functioning and resilience after disasters. *Disaster Medicine and Public Health Preparedness*, 12(1), 127–137. <https://doi.org/10.1017/dmp.2017.39>

[14] Kichata, N., et al. (2024). Methodological approach to enhancing the security and resilience of critical infrastructure objects. *Technogenic and Ecological Safety*, 16(2), 3–10. <https://doi.org/10.52363/2522-1892.2024.2.112>

[15] Kichata, N., et al. (2025). Implementation of a risk assessment methodology for emergency situations at critical infrastructure objects. *Journal of Ecological Engineering*, 26(7), 286–294. <https://doi.org/10.12911/22998993/203529>

[16] Sathurshan, M., et al. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures*, 7(5), 67. <https://doi.org/10.3390/infrastructures7050067>

[17] Tretyakov, O., Khalmuradov, B., Pukha, M., Sydorenko, V., Chubko, L., & Nechiporuk, V. (2025). Methodology for quantitative assessment of critical infrastructure resilience. <https://ceur-ws.org/Vol-3925/short05.pdf>

[18] Kour, R., Patwardhan, A., Karim, R., Dersin, P., & Kumari, J. (2022). A cybersecurity approach for improved system resilience. In *Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)* (pp. 2514–2521). https://doi.org/10.3850/978-981-18-5183-4_S13-03-586-cd

[19] Rehak, D., et al. (2025). Critical entities resilience strengthening tools to small-scale disasters. *International Journal of Critical Infrastructure Protection*, 100766. <https://doi.org/10.1016/j.ijcip.2025.100766>

[20] Santos, P., et al. (2025). A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors*, 25(14), 4272. <https://doi.org/10.3390/s25144272>

[21] Cherkasova, V. V., & Kostenko, O. B. (2023). The role of information technologies in the social and economic spheres in supporting Ukraine's European integration. In *Information Technologies: Theory and Practice: Proceedings of the VI All-Ukrainian Scientific and Practical Internet Conference of Higher Education Students and Young Scientists* (pp. 28–31). <http://ir.nmu.org.ua/handle/123456789/163340>

[22] Novozhylova, M., & Cherkasova, V. V. (2025). Integrated approach to change management. In I. V. Kononenko (Ed.), *Integrated strategic management, portfolio, program, and project management: Abstracts of the XV International Scientific and Practical Conference* (p. 32). NTU “KhPI”. <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/0122a9ff-3da8-45e7-8e13-ed55fd61045b/content>

[23] Cherkasova, V. V., & Bashyrov, Ye. T. (2025). Secure storage and processing of citizens' data. In *Sustainable urban development: Post-war period: Proceedings of the XVIII All-Ukrainian Scientific and Technical Conference* (Part 2, pp. 164–165). O.M. Beketov National University of Urban Economy in Kharkiv. https://science.kname.edu.ua/images/dok/konferentsii/stalyirozvytok2019/2025/C.%20Energetica%20informacijna%20ta%20transportna%20infrastruktura_25.pdf

[24] Cherkasova, V. V., & Lykova, V. (2025). Inclusive web design as a tool for developing innovative interfaces under conditions of change. *Information Technology: Computer Science, Software Engineering and Cyber Security*, (2), 195–203. <https://doi.org/10.32782/IT/2025-2-20>

[25] Cherkasova, V. V. (2024). Assessing sustainability of educational information infrastructure. In *Higher technical education of the XXI century: Challenges, problems, prospects* (Vol. 3). ДОННАБА.

[26] Cherkasova, V. V., Bredikhin, V. M., & Didok, O. V. (2025). *Convolutional neural networks (CNN): Development of neural network architectures from classical to innovative*. O.M. Beketov National University of Urban Economy in Kharkiv.