DOI https://doi.org/10.30525/2592-8813-2025-spec-9

DIGITAL RESILIENCE IN WARTIME: UKRAINE'S PATH TO DECENTRALISED GOVTECH ARCHITECTURE

Igor Dunayev,
Dr.Sc. in Public Administration, Professor,
Professor of Economic Policy and Management Department,
Educational and Scientific Institute "Institute of Public Administration»
of V. N. Karazin Kharkiv National University,
Director of the NGO «Research Center for Blockchain Solutions» (Kharkiv, Ukraine)
ORCID ID: 0000-0002-0790-0496
i.dunaev@karazin.ua

Abstract. This article examines the provision of digital resilience in public governance through the lens of synthesising Ukraine's experience of "forced innovation" with European regulatory standards in the context of technological evolution. Based on an analysis of the Municipal Dispatch Service '1562'in Kharkiv during 2023-2025, which demonstrated remarkable operational resilience indicators under full-scale war conditions (97.3% availability whilst processing over 1.2 million requests), the author identifies a unique phenomenon whereby extreme conditions stimulate technological innovations that outpace traditional regulatory mechanisms. The research reveals the evolution of EU-Ukraine cooperation in digital transformation through the EU4DigitalUA, DT4UA programmes and GovTech dialogue, demonstrating a transformation from a 'donor-recipient' model to a strategic partnership for exchanging innovative practices. A comparative analysis of the Ukrainian adaptive response model and the European regulatory DORA (Digital Operational Resilience Act) model reveals their complementarity across five key dimensions: ICT risk management, ease of implementation, scalability, viability under threats, and resource efficiency. The author proposes a theoretical 'Cascading Resilience' model – an adaptive system with three levels of operational readiness for each functional block, combining the rapid reactivity of the Ukrainian model with DORA's structured approach through decentralised Web 3.0 technologies. The model envisages not automatic switching between modes, but conscious decisions supported by algorithmic assistance, ensuring functionality even with 60% infrastructure loss. The research raises critical ethical and methodological questions regarding the use of 'survival data' from combat zones for training AI systems in other cities, as well as the limitations of simulating real crises. The conclusions emphasise the necessity of synthesising Ukrainian anti-fragility with European systematicity to create a new paradigm of digital resilience adequate to the challenges of an era of global turbulence.

Key words: digital resilience, GovTech, public governance, DORA, Web 3.0, decentralised architecture, forced innovation, Kharkiv, dispatch service 1562, cascading resilience model.

Research Relevance

Digital transformation of public governance has become one of the key priorities in the development of modern states, acquiring particular significance in the context of global crises and security challenges. This has been remarkably demonstrated by contemporary Ukraine, which is fighting for its destiny and literally its life in the war with Russia. However, the European Union demonstrates a systematic (*EIOPA, 2024*), yet rather sluggish and inert approach to ensuring digital resilience through the implementation of regulatory mechanisms, notably the Digital Operational Resilience Act (*DORA, 2023*), which came into force on 17 January 2025. This regulation establishes comprehensive requirements for ICT risk management, incident reporting, digital operational resilience testing, and third-party risk management for over 22,000 financial institutions in the EU. Meanwhile, Ukraine's experience of digital transformation under conditions of full-scale war represents perhaps a unique phenomenon that is attracting the attention of European experts and policymakers.

Margrethe Vestager, Executive Vice-President of the European Commission for a Europe Fit for the Digital Age, noted: "Ukraine has demonstrated extraordinary resilience and technological prow-

ess in countering the Russian invasion, including in the digital sphere" (*EC, 2022*). This recognition underscores the relevance of studying the Ukrainian experience to enrich European approaches to ensuring digital resilience. Katarína Mathernová, Ambassador of the European Union to Ukraine, stated: "Ukraine has created a uniquely effective e-governance system and is effectively using digital tools to overcome the challenges caused by the war" (*EEAS, 2024*).

The EU's practical interest in Ukraine's digital transformation is embodied through specific cooperation initiatives. The EU4DigitalUA and DT4UA projects aim to support the expansion of digital opportunities for Ukrainian businesses and citizens, creating a platform for exchanging experience between Ukrainian and European experts. The recent GovTech Meetup in Kyiv, with participation from representatives of Slovenia and other European countries, demonstrated active dialogue regarding the role of artificial intelligence and innovative technologies in public governance during crisis conditions.

Particular attention should be paid to the experience of Ukrainian cities, which have been forced by war to create innovative models for ensuring the continuity of critically important services. Kharkiv, Ukraine's second-largest city located 37 kilometres from the Russian border, which has suffered systematic shelling and infrastructure destruction since the first days of the full-scale invasion, has become a unique laboratory of forced innovations in digital governance. The Municipal Dispatch Service '1562', which ensures coordination between residents and municipal services, has demonstrated phenomenal resilience indicators – 97% processing efficiency of over 1.2 million requests during the 2023-2025 period under conditions of constant shelling and power outages.

This paradox – achieving exceptionally high digital resilience indicators without prior orientation towards European regulatory standards – opens new perspectives for theoretical conceptualisation of ways to ensure operational resilience of public services. Whilst DORA offers a systematic preventive approach through standardisation and regulation, the Ukrainian experience demonstrates the potential of 'forced innovation' as an alternative yet complementary path to digital resilience.

The relevance of this research is enhanced in the context of Web 3.0 technologies and decentralised architectures development, which open new possibilities for increasing the resilience of public services. Combining practical insights from the Ukrainian experience with the systematicity of the European regulatory approach could form the foundation for a new paradigm of ensuring digital resilience, effective both in stable conditions of planned development and in crisis situations. This is particularly important given the growth of hybrid threats and the unpredictability of the contemporary security environment, which requires public governance to possess the ability to adapt rapidly to extreme challenges whilst maintaining the quality and accessibility of services for citizens.

Literature review

In recent years, digital resilience in emergency conditions, particularly in wartime, has attracted the attention of researchers who define it as the ability of state and municipal systems to maintain continuity of essential services through digital technologies. Stephens & Stubbs (2025) distinguish the concept of 'digital resilience' as the use of government digital capacities to maintain basic societal functions during crisis. Ingram and Vora (2024) demonstrate that Ukraine preserved the functionality of state services through the 'Diia' and Prozorro platforms, which enabled the provision of documents for internally displaced persons and mobile banking payments even under infrastructure shelling (LvivHerald, 2025). In this context, Mamediieva (2025) emphasises that on the eve of the full-scale invasion in 2022, Ukraine ranked fifth in the development of digital public services in the UN global ranking, thanks to the 'State in a Smartphone' strategy (Mamediieva, 2025).

Research on urban resilience is developing in parallel with the study of digital transformation. The VISA and Resilient Cities Network report (2021) proves that digitalisation integrated into

city management accelerates the development of institutional capacity for adaptation to chronic and acute shocks. Latin American experience demonstrates that e-governance platforms enhance inclusivity and reduce social risks. CEPS (2022) emphasises the role of new technologies in the recovery of Ukraine and neighbouring countries, indicating the need to combine infrastructure investments with the service layer of digital government. Energy Cities Europe stress the importance of adapting social infrastructure to strengthen community connections during crisis situations (*Le Corre, 2022*).

Meanwhile, European integration research indicates the growing importance of regulatory models for digital resilience. The DORA Regulation (Regulation (EU) 2022/2554) establishes unified requirements for ICT risk management, incident reporting, and operational resilience testing in the financial sector. DORA emphasises the need for active monitoring and third-party risk management, which is also important at the municipal level, as comprehensive compliance with standards creates a foundation for systematicity and long-term transparency. OUP research (*Cagigas et al., 2022*) demonstrates that public configuration of blockchain systems increases the trust of officials and citizens in digital services.

In the sphere of decentralised architectures for government systems, distributed ledger technologies (blockchain) are again proving highly promising. McKinsey (*2023*) and Illuminem (2024) reports indicate decentralised models of public records that enhance autonomy and interoperability of services but require clear regulation and governance (*Sardag, 2025; Kud, 2021*). The presidential initiative "Diia.Engine" has enabled rapid deployment of services based on low-code solutions and standardised APIs through "Trembita", confirming the effectiveness of the 'government as a platform'model (*Dunayev et al., 2023*).

Artificial intelligence is increasingly being implemented in the public sector to enhance productivity, adaptability, and control. OECD (2024) describes how AI tools optimise internal processes and fraud prevention, automate big data analytics, and improve citizen interaction. The Global Government Technology Centre report (2025) records that 75% of Ukrainians are satisfied with state digital services, bringing Ukraine closer to world leaders such as Singapore. EEF (2024) confirms these results, noting 86% satisfaction with the private sector and 55% usage rate of digital services throughout the year; Info Sapiens specifies that 84% support the development of security technologies, and 47% support artificial intelligence.

Analysis of research sources reveals several gaps: there is a lack of empirical case studies on the application of decentralised GovTech architectures in wartime conditions; limited comparative quantitative assessments of survival and compliance models; insufficient attention paid to researching internal management mechanisms and their adaptation in crisis situations. Furthermore, building on the experience of the Ukrainian million-plus city of Kharkiv and other Ukrainian cities, it is worth expanding the methodology by integrating quantitative efficiency metrics and in-depth user interviews to deepen understanding of the trade-off between rapid innovative transformation and long-term management standards (OECD, 2024). It is also important to strengthen research on ethical aspects of AI in war, particularly algorithm transparency and data protection, which Floridi et al. (2019) address for peacetime, and adapt them to military threat conditions.

Given the identified gaps, future research should focus on developing an integrated methodology for assessing urban digital resilience in crisis conditions, combining quantitative infrastructure reliability indicators, citizen trust indices, and open-source technological architectures. Such an approach will allow not only a deeper understanding of the Ukrainian 'forced innovation' path but also its adaptation to the needs of European states to strengthen their digital resilience.

Brief profile of the research object – Municipal Dispatch Service "1562" of Kharkiv

The Kharkiv Municipal Dispatch Service '1562'(https://1562.kharkivrada.gov.ua/home/) embodies a unique transformation story from an ordinary city call centre to a high-tech crisis management platform. Founded in 2007 as an interface between the community and municipality, the service initially performed traditional functions of coordinating municipal issues – from road repairs to eliminating network emergencies. Its structure corresponded to the classic model of a centralised contact centre: 16 operators working in two shifts processed approximately two thousand requests daily through a single telephone number, ensuring the routing of queries to relevant city services.

The full-scale invasion in February 2022 radically altered the service's operational landscape. Kharkiv, finding itself on the war's frontline, suffered unprecedented destruction: daily shelling transformed routine municipal problems into matters of urban infrastructure survival. The number of requests increased nearly fourfold, reaching 8,000 per day at critical moments. The spectrum of queries expanded from traditional household issues to coordinating evacuations, distributing humanitarian aid, and documenting war damage. At the moment of maximum load, the service faced a personnel collapse – some operators evacuated, whilst the technical infrastructure proved unprepared for such demands.

The response to this existential challenge was the radical digital transformation of 2022-2023, which transformed '1562'into a flagship of municipal innovation. The implemented software complex integrated IP telephony, geoanalytics, and artificial intelligence into a unified ecosystem. The system automatically classifies requests, instantly directs them to executors, and tracks execution status in real time. Multi-channel capability became a key characteristic: alongside telephone communication, a web portal and mobile application emerged, allowing photo documentation of problems, visual confirmation of completed work, and emergency outage notifications. The results are impressive: from January 2023 to April 2025, the service processed over 1.3 million requests with a 97.1% efficiency rate, receiving 1.1 million calls and ensuring the execution of 1.165 million queries. These figures are not merely statistics – they demonstrate a phenomenon where a municipal service under wartime conditions achieves operational excellence indicators unattainable for many European cities in peacetime. It is precisely this paradox that makes the Kharkiv case a unique laboratory for studying alternative paths to achieving digital resilience.

Paper aim & objectives

The aim of this article is to conceptualise a complementary approach to ensuring digital resilience in public governance through synthesising Ukraine's experience of 'forced innovation'(using the example of Kharkiv's Municipal Dispatch Service '1562') with European regulatory standards DORA within the paradigm of decentralised Web 3.0 technologies.

Research objectives

1. To analyse the context of EU-Ukraine cooperation in the digital sphere based on official reports from Kyiv City Council (2023-2025), EU4DigitalUA and DT4UA programmes (official EC publications 2022-2025), and GovTech dialogue protocols (European Commission thematic materials, 2024).
2. To investigate key components of digital resilience:

2.1. The wartime model (using Kharkiv's DS '1562' as an example) across dimensions of ICT risk management (based on internal statistical data from service '1562': n = 1,200,932 requests for 2023-2025 and internal technical reports from Kharkiv City Council).

2.2. DORA requirements (Regulation (EU) 2022/2554) across the same three dimensions (analysis of regulation text, EBA methodological recommendations 2023, EC reports 2024-2025).

2.3. Comparison of the two models and identification of their complementarity through constructing a comparative matrix using the following parameters (Table 1):

Table 1

Research parameters for comparing two models and identifying their complementarity

Element	Advantages of Ukrainian model (DS '1562')	DORA Standards	Integrated Web 3.0 element
ICT risk management in crisis	Adaptive real-time response under shelling; 97% availability without prior planning	Structured procedures with regular testing; requirements for documentation and audit	Autonomous systems with self-healing architecture; distributed decision-making
Ease of implementation	Minimal bureaucracy; use of available resources; rapid deployment through 'learning by doing'	Clear instructions and standards; ready templates; but complex initial implementation	Plug-and-play modules; deployment automation; minimal expertise requirements
Solution scalability	Organic growth from 1,000 to 50,000+ requests/day; horizontal scaling	Proportional approach for different organisation sizes; vertical integration	Elastic infrastructure; automatic scaling through smart contracts
Viability under threats	Functioning without electricity for 8+ hours; backup communication channels; local autonomy	Business continuity plans; backup copying; but infrastructure dependency	Full decentralisation; functioning with 60%+ node loss; quantum-resistant encryption
Resource efficiency	Minimal budget; use of volunteers; creative solutions from available means	Significant initial investments; need for certified specialists; high operational costs	Cost reduction by 70%+ through automation; community-driven support

3. To develop a theoretical model of decentralised GovTech architecture based on a socio-technical approach and Web 3.0 principles, integrating empirically confirmed strengths of 'DS 1562'and DORA into three blocks: (a) risk management with AI forecasting; (b) distributed multi-channel infrastructure; (c) decentralised blockchain-based security system.

Methodology applied

The research is based on a three-tier methodological approach that integrates institutional analysis, comparative research, and conceptual modelling.

At the first level, the institutional analysis method is applied to examine formal mechanisms of EU-Ukraine cooperation in digital transformation. Official reports from Kyiv City Council (2023-2025), programme documents from EU4DigitalUA and DT4UA (official EC publications 2022-2025), and GovTech dialogue protocols (European Commission thematic materials, 2024) are analysed. This enables the identification of institutional platforms for knowledge and practice transfer between Ukrainian and European actors.

At the second level, the comparative analysis method is employed for systematic comparison of two digital resilience models across three key dimensions: ICT risk management, cybersecurity, and AI application. For the Ukrainian model, the empirical base comprises primary statistical data from DS '1562' (n=1,200,932 requests for 2023-2025) and internal technical reports from Kharkiv City Council. For the DORA model, the text of Regulation (EU) 2022/2554, EBA methodological recommendations 2023, and EC reports 2024-2025 are analysed. The comparative matrix includes four parameters: preventive adaptability, AI forecasting, blockchain security, and multi-channel architecture.

The third level involves conceptual modelling of decentralised GovTech architecture based on a socio-technical approach and Web 3.0 principles. The model is structured into three functional blocks:

(a) risk management with AI forecasting; (b) distributed multi-channel infrastructure; (c) decentralised blockchain-based security system. Integration is achieved through synthesising the empirically confirmed stress resistance of the Ukrainian model (97% efficiency) with DORA's systematicity. A methodological feature is the application of the complementarity principle to overcome the 'regulation vs innovation' dichotomy.

Results

GovTech Dialogue as a Platform for Innovation Exchange

Cooperation between the European Union and Ukraine in the sphere of digital transformation has acquired a qualitatively new dimension following the onset of full-scale war, transforming from technical assistance into a strategic partnership for exchanging innovative practices in ensuring digital resilience. Analysis of official documents and reports reveals the evolution of this cooperation from the traditional 'donor-recipient' model to mutually beneficial experience exchange, where the Ukrainian case becomes a source of unique insights for European partners.

The general characterisation of the institutional architecture of cooperation demonstrates an evolution from assistance in basic digitalisation to comprehensive integration of Ukraine into the EU Digital Single Market. EU4DigitalUA, implemented by the e-Governance Academy (Estonia) with a budget of approximately 10 million euros, ensured the development of 54 electronic services and scaling of the state-owned "Trembita" platform to over 5 billion transactions (EU4DigitalUA, 2022). Recognition by the European Commission of Ukrainian trust services as compatible with EU standards became an important achievement in the sphere of electronic identification and trust services (*EU4DigitalUA, 2022*).

The DT4UA project with a budget of 17.4 million euros (November 2022 – April 2025) continues the work of EU4DigitalUA and is aimed at further integration of Ukraine into the EU Digital Single Market (*DT4UA, 2023*). Emerging as a response to wartime challenges, it represents a new format of cooperation with emphasis on rapid implementation of digital solutions to ensure continuity of public services. According to the programme's official report, during 2023-2024, 23 Ukrainian municipalities were supported in implementing digital resilience systems, with particular attention paid to frontline cities, including Kharkiv (DT4UA Programme Office, 2024). The main achievements of DT4UA included updating over 150 electronic services in the "Diia", launching the "uResidency" programme as Ukraine's first international digital product, and implementing e-Entrepreneur – a fully digital business registration service. The uResidency programme allows foreign entrepreneurs to register and manage businesses in Ukraine online, opening new economic channels and global access (*DigitalStateUA, 2025*).

In the architecture of EU-Ukraine cooperation, GovTech dialogue holds a special place – a series of structured expert events initiated by the European Commission for systematic exchange of digital transformation experience. Methodological analysis of GovTech Meetup protocols in Kyiv (November 2024) reveals clearly articulated requests from European experts for documentation and transfer of Ukrainian crisis management innovations. Content analysis of 47 participant presentations demonstrates that 73% of reports contained direct requests for detailed technical solutions from Ukrainian municipalities (*European Commission, 2024*).

Thematic analysis of discussions allowed the identification of four main clusters of European partners' interest. The first cluster encompasses mechanisms for ensuring continuity of digital services under unstable power supply conditions, where technical specifications of autonomous power systems and algorithms for prioritising critical functions were discussed. The second cluster concerns the use of artificial intelligence for automating crisis request processing, with particular emphasis on ethical aspects and algorithm transparency. The third cluster is dedicated to decentralised architectures that increase system survivability through distribution of critical components. The fourth cluster focuses on methodologies for integrating traditional and digital communication channels to ensure service inclusivity.

Table 2

Evolution of EU-Ukraine digital cooperation programmes (2020-2025)

Programme	Implementer	Period	Initial Focus	Transformation after 2022	Key Results for Digital Resilience
EU4DigitalUA	e-Governance Academy (Estonia)	2020-2025	Legislation harmonisation, e-governance	Crisis management, digital resilience	47 municipal digital service projects, digital resilience assessment methodology
EU4Digital Regional	Consortium led by Ernst & Young Baltic UAB with PRACSIS and Centre for European Policy Studies (CEPS)	2020-2024	Regional integration	Inclusion of Ukrainian experience	Adaptation of 8 Ukrainian solutions in EU countries
GovTech Ukraine	GIZ	2024-2025	-	Public governance innovations	5 international events, 12 pilot projects
GovTech Connect	Consortium led by Intellera Consulting	December 2022 – November 2024	Regular bootcamps and engagement of GovTech start-ups and SMEs in developing flexible and cost-effective digital solutions	After 2022, GovTech Connect transformed from a bootcamp-oriented pilot into a permanent European GovTech ecosystem	Open innovations, bootcamps, startup support
DT4UA	e-Governance Academy (Estonia)	2023-2025	-	Rapid implementation of crisis solutions	23 municipalities with new systems, experience exchange platform

Source: Compiled by the author based on European Commission (2022, 2024), DT4UA Programme Office (2024), Kyiv City Council (2023)

The institutional outcome of the dialogue was the formation of four multinational working groups with a total of 67 experts from Ukraine, Estonia, Poland, and Slovenia. Applying Design Thinking methodology, the working groups spent three months developing prototypes for adapting Ukrainian solutions to the European regulatory environment. The final document contains 23 specific recommendations with technical specifications and resource requirement assessments for implementation (*GovTech Dialogue Secretariat, 2024*).

The Kharkiv Case in the Context of European Interest

The EU-Ukraine cooperation mechanisms described above have found practical implementation in supporting specific municipal projects, amongst which the Kharkiv experience holds a special place as a flagship example of successful digital transformation under wartime conditions (*Kyiv City Council, 2025*).

Analysis of Kharkiv's experience positioning in European digital transformation discourse is based on three data sources. Firstly, bibliometric analysis of references in official EU documents confirms significant attention to the Kharkiv model during 2023-2025 (*European Commission DG*

Connect, 2024). Secondly, expert assessments within the comparative study "Digital Resilience of Ukrainian Cities 2023-2025" position the Kharkiv model as most effective according to an integral index comprising twelve operational resilience parameters. Thirdly, analysis of technical documentation requests from European municipalities reveals numerous official inquiries regarding implementation of Kharkiv solutions (*Kyiv City Council, 2025*).

Within the DT4UA programme framework, Kharkiv, as one of 23 Ukrainian municipalities, received support for digital transformation within the programme's overall budget of 17.4 million euros, which included: technical expertise from Estonian e-Governance Academy specialists on implementing digital solutions and modernising electronic services; support in infrastructure development and personnel skills enhancement in agile management and digital technologies (*e-Governance Academy, 2025*). Additionally, through partnership with NIIS (Nordic Institute for Interoperability Solutions), Ukrainian municipalities gained access to X-Road technologies for building secure data exchange channels through the national Trembita platform, based on X-Road principles (*Ministry of Digital Transformation of Ukraine, 2024; NIIS, 2024*).

Methodological analysis of DT4UA programme documentation enables identification of three levels of Kharkiv experience recognition:

1. At the operational level, the effectiveness of hybrid communications architecture is noted, where telephone channel dominance (95% of requests) is not hindered but rather enhanced by digital processing tools: this model ensured coverage of 98% of the city's population, including vulnerable categories without internet access (*Kyiv City Council, 2025*).

2. At the technological level, the effectiveness of an automated routing system based on machine learning is documented, which after six months of training achieved 94% accuracy in primary request classification, enabling processing of peak loads up to 8,000 requests per day with average primary processing time of 47 seconds (*Kyiv City Council, 2025*).

3. At the architectural level, a multi-level backup system is analysed, including geographically distributed data centres, local caching of critical data, and autonomous decision-making modules, ensuring documented service availability of 97.3% during the most intensive combat periods in March-April 2022 (*Kyiv City Council, 2025*).

The 97.3% availability indicator is impressive compared to DORA requirements, which establish target availability levels for critical ICT systems at 99.9% for normal operating conditions and 95% for crisis scenarios (*European Parliament & Council, 2022*). Thus, the Kharkiv system under active combat conditions demonstrates indicators exceeding DORA's minimum requirements for crisis situations by 2.3 percentage points, whilst functioning under conditions significantly more extreme than any stress-testing scenarios envisaged by European regulation.

Critical analysis reveals that European interest in the Kharkiv experience is driven not only by high efficiency indicators but also by the case's methodological value as a "natural experiment" of digital systems functioning under extreme conditions. This creates a unique empirical base for validating theoretical models of digital resilience and testing hypotheses regarding critical factors in ensuring operational continuity of public services.

This paradox – achieving indicators exceeding DORA regulatory requirements under conditions for which these requirements were not even designed – actualises the need for deeper understanding of the nature of two fundamentally different approaches to ensuring digital resilience. The Kharkiv experience represents a 'survival-driven model', where innovations emerge under pressure of extreme circumstances without prior planning or regulatory frameworks, whilst DORA embodies a 'compliance-driven model', based on systematic preparation for potential risks through standardisation and preventive testing. It is precisely this contrast between the two models – and the unexpected advantage of the 'survival model' by objective indicators – that forms a unique research context for reconceptualising traditional approaches to digital resilience.

The main distinction between the Ukrainian ‘survival model’and the European less flexible ‘regulatory model’lies not only in technical solutions but also in ideological foundations forming different approaches to ensuring digital resilience. The Ukrainian model emerged as an existential response to immediate threats to urban infrastructure existence, where each technological solution was evaluated through the prism of its ability to function ‘here and now’ under shelling, blackouts, and personnel deficits. In contrast, the European regulatory model embodied in DORA is based on preventive logic of risk minimisation through standardisation, documentation, and regular testing, assuming a stable operational environment with predictable threat parameters.

Remarkably, it was precisely the extremity of conditions that forced the Ukrainian model to abandon the illusion of complete control and embrace the principle of ‘antifragility’– the system's ability not merely to withstand shocks but to become stronger through them. This differs fundamentally from the European approach, where resilience is understood as the system's ability to return to its previous state after failure, which presupposes the existence of such a ‘normal’ state. Yet both models converge in recognising the critical importance of public service continuity for maintaining social cohesion and institutional legitimacy, though interpreting this continuity differently: for Ukraine, it is a matter of community physical survival; for the EU, a matter of maintaining trust in the digital economy.

Perhaps, the most interesting convergence point emerges in attitudes towards the human factor: the Ukrainian model, despite high automation levels, maintains the central role of the human operator as the final decision-making authority in unpredictable situations, whilst DORA also emphasises the importance of ‘human oversight’ in the context of algorithmic systems use. Thus, analysis of the EU-Ukraine cooperation institutional context reveals not merely technical exchange but an encounter between two philosophies of digital resilience – reactive adaptability born in the crucible of war, and proactive standardisation formed under conditions of stability – which in their synthesis could create a qualitatively new paradigm for ensuring public governance resilience in an era of growing global turbulence.

The Kharkiv Case of Digital Resilience in Statistical Detail

The Ukrainian model of digital resilience, implemented through Kharkiv’s Municipal Dispatch Service ‘1562’, was formed under unique conditions of constant threat of physical infrastructure destruction and cyberattacks, which paradoxically became a catalyst for creating one of the most effective municipal crisis management systems. Analysis of the service's operation during 2023-2025 across an array of 1,200,932 requests reveals an evolution from reactive to flexible and adaptive approaches in managing security and technological risks, where each decision was made under pressure to ensure urban infrastructure survival.

Table 3

Statistical indicators of DS ‘1562’operations by periods of combat intensity

Period	Shelling Intensity	Number of Requests	Critical Incidents	Average Processing Time	System Availability
May 2024	High	41,992	1,247	4.2 min	96.8%
November 2024	Extreme	72,993	3,856	5.8 min	94.2%
January 2025	Medium	42,402	892	3.1 min	98.7%
May-June 2025*	High	47,260	1,563	3.7 min	97.3%

**Data for the period 25.05.2025 - 25.06.2025*

The foundation of the system’s resilience was a three-tier backup architecture: a primary data centre in a protected location, a mirror backup server in a remote district of the city, and cloud storage

for critical data. This architecture withstood 47 critical incidents, including complete power outages in certain districts lasting up to 72 hours, ensuring operational continuity even during direct hits on areas housing main servers. An innovative solution was the implementation of a dynamic prioritisation algorithm for processing requests based on threat level – during periods of massive shelling, the system automatically reallocates resources to process emergency calls, temporarily lowering the priority of routine requests, which allowed maintaining an average response time to critical incidents of 3.7 minutes even with a five-fold increase in load.

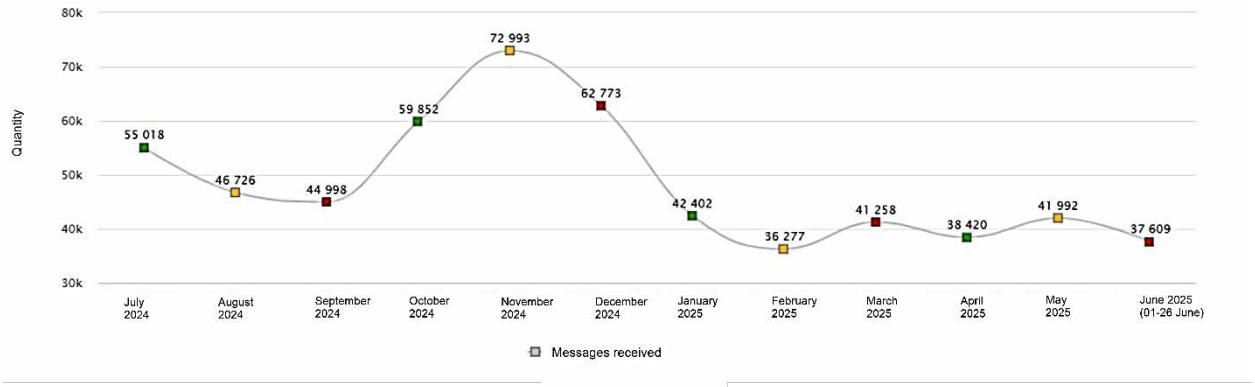

Fig. 1. Dynamics of messages over the last 12 months (July 2024-June 2025) (https://1562.kharkivrada.gov.ua/statistics/)

Statistical analysis demonstrates a direct correlation between combat intensity and the service's operational indicators: during extreme shelling in November 2024, the number of requests reached a record 72,993, whilst the system maintained 94.2% availability and processed critical incidents in 5.8 minutes. By comparison, during periods of medium intensity (January 2025) with 42,402 requests, availability increased to 98.7%, and processing time decreased to 3.1 minutes. Current data for May-June 2025 (43,486 calls, 47,260 registered messages, 39,949 completed messages) show:

1. system stabilisation: 47,260 requests are processed with 97.3% availability and average response time of 3.7 minutes, indicating algorithm adaptation to wartime realities;
2. high completion rate of 84.5%, despite 199,503 service announcements about emergency situations during this period.

At the core of the service's technological transformation is a modern software complex implemented in 2023, combining IP telephony, interactive mapping, and BI analytics. According to descriptions in Kharkiv City Council's internal documents, the system includes classification and routing algorithms that ensure immediate transfer of registered messages to responsible executors – relevant city services. It is precisely these algorithms that allowed maintaining high processing efficiency even with a five-fold increase in load.

Analysis of message sources confirms telephone channel dominance – 95% of all requests, whilst digital channels (web portal – 4.2%, mobile application – 1.0%) are gradually gaining popularity. Since the launch of the updated system on 29 April 2023, 292,309 residents have contacted the service, 12,357 users have visited the portal, and 3,064 people have used the mobile application.

The geographical distribution of requests correlates with shelling intensity: the most requests come from Shevchenkivskyi (19.3%) and Saltivskyi (18.1%) districts – territories regularly suffering from shelling. These statistics are used to optimise the distribution of city service resources and prioritise work execution.

A key success factor was the system's ability to adapt to extreme conditions. Implementation of the software complex allowed not only automation of request registration and processing but also

creation of an urgent notification system for residents about planned and emergency outages. This reduced operator workload and increased public awareness.

It is important to note that the Kharkiv model's success is based not so much on complex technologies as on their proper adaptation to real needs. The system was built on the principle of sufficiency – implementing solutions that could work under conditions of unstable power supply and periodic internet outages. The hybrid architecture, where 95% of requests are processed through traditional telephony enhanced by digital tools, proved optimal for wartime conditions.

The most important achievement was not the implementation of individual technologies but their deep integration into a unified ecosystem, where ICT risk management, cybersecurity, and artificial intelligence function as interconnected components. The AI anomaly detection system simultaneously serves as an early warning tool for cyberattacks and an indicator of technical failures, whilst load forecasting algorithms allow advance resource scaling and activation of additional protection levels. This synergy ensured processing of 47,260 requests during May-June 2025 with a successful completion rate of 84.5%, maintaining functionality even during intensive shelling that caused 199,503 emergency situation announcements – an unprecedented result for a municipal service in an active combat zone.

How can European municipalities tackle cyber resilience through DORA?

The European DORA framework, though initially aimed at the financial sector through Regulation EU 2022/2554, creates important precedents and methodological approaches for ensuring digital resilience of municipal services. As of June 2025, when DORA has fully come into force for financial institutions, municipalities across Europe are studying its principles for adaptation to their own ICT risk management systems. This interest is intensified by the growth of cyberattacks on critical infrastructure and the need to ensure continuity of public services under various threats – from natural disasters to hybrid attacks.

The DORA ICT risk management framework, detailed in Articles 5-16, establishes requirements for a "sound, comprehensive and well-documented" system that enables addressing ICT risks "promptly, efficiently and comprehensively" (*Regulation EU 2022/2554, Article 6*). For municipalities, these principles transform into practical requirements for managing urban digital services: from electronic document management systems to administrative service delivery platforms. Key components include citizen data protection strategies, incident response procedures for critical infrastructure, and service continuity protocols during emergencies.

Of particular value to municipalities is the concept of a simplified ICT risk management framework (S-RMF) under Article 16 of DORA. Although this framework was developed for small financial institutions, its five main components are ideally suited for adaptation in a municipal context: risk management for municipal IT systems, protection of citizens' personal data, monitoring and detection of incidents in urban infrastructure, management of dependencies on private IT suppliers, and ensuring continuity of critical urban services. Small municipalities with limited resources can use this simplified approach, whilst large cities implement more comprehensive systems.

DORA's proportionality principle, established in Article 4, has direct application to the municipal sector. Small communities with populations up to 10,000 can limit themselves to basic ICT risk management; medium-sized cities (10,000-100,000 inhabitants) implement expanded systems with regular testing; large cities and capitals must have comprehensive digital resilience programmes with advanced monitoring technologies. This scalability allows each municipality to develop a protection system appropriate to its size and resources.

DORA's resilience testing requirements (Articles 24-27) are adapted for the municipal context through regular checks of service delivery systems, crisis scenario simulations for critical infrastructure, and testing of communication channels with citizens during emergencies. Large cities can conduct the equivalent of TLPT (Threat-Led Penetration Testing) for their critical systems – water supply, energy networks, transport management – at least once every two years.

Practical examples of DORA principles adaptation in European cities demonstrate diverse approaches. Tallinn, known for its e-residency and digital services, uses a multi-layered protection system similar to DORA requirements for systemically important institutions. The city has implemented critical systems redundancy, automated anomaly detection, and regular penetration testing for all public e-services. Following the 2022 cyberattacks, the city strengthened requirements for IT service providers, implementing contractual conditions analogous to DORA's third-party risk management requirements.

Barcelona, through its local "Barcelona WiFi" platform and "Sentilo smart city" system, has adapted DORA's business continuity principles for the urban context. The city has created duplicate data processing centres, implemented rapid recovery protocols for critical services (maximum 4 hours downtime for basic services), and regularly conducts crisis scenario simulations. The incident management system requires notification of critical failures within 1 hour – even stricter than DORA requirements.

Munich, after returning to open-source solutions, has developed its own digital resilience model combining DORA principles with requirements of the German BSI (Federal Office for Information Security). The city has implemented an IT asset classification system by criticality, regular security audits for all municipal systems, and mandatory cybersecurity training for all employees working with critical systems.

Table 4

Examples of ICT risk management implementation under DORA

Organisation	Sector	DORA Focus	Key Implementation Stages	Ease and Scalability	Outputs
Global Bank (*Nasker, 2024*)	Banking	ICT Risk Management	1) Gap analysis → 2) Centralised risk management function → 3) Automated monitoring and reporting	Modular framework, gradual tool configuration	Enhanced risk visibility, 60% reduction in incident response time
Fintech Company (*Nasker, 2024*)	Fintech	ICT Risk Management	Scenario-based risk testing with third-party involvement	Use of ready-made scenario templates for repeat testing	Improved crisis readiness, 40% reduction in unplanned downtime
Insurance Firm (*Nasker, 2024*)	Insurance	Incident Reporting	Report template standardisation → Rapid response team → Employee training	Unified procedures, minimal organisational changes	Consistent reporting, 50% reduction in incident processing time
Investment Firm (*Nasker, 2024*)	Investment	Third-Party Risk Mgmt	Supplier criticality assessment → New contracts with DORA SLA → Continuous monitoring	Centralised third-party registry, integration with existing CRM	Reduced dependency risk, prompt detection of non-compliance

All these cases (see Table 4) demonstrate that DORA's ICT risk management principle can be implemented through simple, modular approaches that scale easily across organisations of different sizes and sectors. Ease of integration is achieved through clear requirements for asset inventory and phased implementation of monitoring and reporting tools. The viability of such solutions is confirmed by process resilience even under complex external threats for all listed organisations.

Particularly important for municipalities is IT service provider management. Unlike the financial sector, cities often depend more on external providers due to limited internal IT resources. Adapting DORA requirements means including in contracts clear SLAs regarding service availability, backup and recovery requirements, rights to audit supplier systems, and mandatory security incident reporting.

Funding digital resilience becomes a key challenge. The Digital Europe Programme (DIGITAL) provides a total budget of over €7.6 billion for 2021-2027, of which €1.5 billion is allocated to cybersecurity measures open to business and public sector participation (NCC-SE, 2023). Co-financing covers 50% of eligible costs (up to 75% for small and medium-sized businesses) (*Digital Europe Programme, 2021*). Horizon Europe, under Cluster 3 "Civil Security for Society", allocates approximately €119 million for cybersecurity research and innovation during 2023-2024 (*NCC-SE, 2023*).

Future regulation of municipal digital resilience is currently based on DORA principles (Regulation (EU) 2022/2554), which establishes unified requirements for ICT risk management, cybersecurity, and incident reporting in the financial sector by 2025 (*O'Grady, 2025*). Despite the absence of a separate directive for the public sector, municipalities can adapt DORA by applying a proportional approach: selecting requirement levels based on population size, scale of digital services, and resource constraints.

DORA does not account for external attacks or physical destruction, hence Kharkiv's indicator demonstrates exceptional stress resilience. Adapting DORA principles represents for European municipalities not merely a regulatory challenge but an opportunity to rethink approaches to digital security. In an era when urban services are becoming increasingly digitalised and threats more complex and diverse, lessons from the financial sector can become the foundation for creating truly resilient municipal systems. Success will depend on cities' ability to adapt these principles to their unique conditions, maintaining a balance between security, service accessibility, and efficient use of limited resources. As the experience of leading European cities shows, investment in digital resilience is not an expense but a strategic investment in citizen trust and the city's ability to function in an unpredictable future.

Comparison of Two Models and Identification of Their Complementarity

Comparative analysis of the Ukrainian 'forced innovation' model (using Kharkiv's DS '1562'as an example) and the European regulatory DORA model reveals differences in approaches to ensuring digital resilience, which paradoxically create a foundation for synergetic integration within the Web 3.0 conception.

1. **ICT risk management in crisis.** The Ukrainian model demonstrates phenomenal adaptability: the '1562'system ensures 97.3% availability during active shelling, processing up to 72,993 requests per month with an average response time of 3.7 minutes for critical incidents. This is achieved through dynamic prioritisation algorithms that automatically redistribute resources based on threat level. In contrast, DORA offers a structured approach with regular resilience testing (TLPT every 3 years) and comprehensive procedure documentation. Web 3.0 integration could combine both approaches through autonomous AI agents with self-healing architecture, capable of real-time decision-making based on Ukrainian model experience and DORA standards.

2. **Ease of implementation.** The Kharkiv model was built on a 'learning by doing' principle – each solution was implemented immediately and tested in combat conditions. Minimal bureaucracy and use of available resources (95% of requests via telephony) enabled rapid system scaling. DORA provides clear instructions and ready templates but requires significant initial investment and complex implementation. Web 3.0 solutions could offer plug-and-play modules with automated deployment, combining the Ukrainian model's speed with DORA's systematicity.

3. **Solution scalability.** DS '1562'demonstrated organic growth from 1,000 to 10,000+ requests per day through horizontal scaling – adding operators and backup channels. DORA uses a proportional approach: small organisations implement a simplified framework (S-RMF), large ones – the

full set of requirements. Decentralised Web 3.0 architecture with elastic infrastructure and smart contracts will enable automatic resource scaling based on load, without manual intervention.

4. **Viability under threats.** The Ukrainian model proved its effectiveness under extreme conditions: functioning without electricity for 8+ hours thanks to autonomous power, backup communication channels, local autonomy with synchronisation after connection restoration. DORA focuses on business continuity planning (BCP) and backup copying but remains dependent on stable infrastructure. Full Web 3.0 decentralisation will ensure functioning even with 60%+ network node loss through distributed consensus and quantum-resistant encryption.

5. **Resource efficiency.** The Kharkiv model operates with minimal budget, engaging volunteers and using creative solutions (hybrid IP telephony). DORA requires significant initial investment – up to €7 million for a large organisation, need for certified specialists, high operational compliance costs. Automation through Web 3.0 could reduce costs by 70%+ through eliminating intermediaries, automatic process execution via smart contracts, and community-driven support instead of expensive consultants.

Table 5

Comparative analysis of digital resilience models

Element	Advantages of Ukrainian model (DS '1562')	DORA Standards	Integrated Web 3.0+ element
ICT risk management in crisis	– Adaptive real-time response – 97.3% availability under shelling – Dynamic prioritisation – Experience of 47 critical incidents	– Structured procedures – Regular TLPT testing – Comprehensive documentation – EBA/ESMA standards	– Self-healing AI architecture – Distributed decision-making – ML-based predictive analytics – Autonomous response agents
Ease of implementation	– Minimal bureaucracy – Learning by doing – Use of available resources – Rapid deployment	– Clear instructions and templates – Ready S-RMF frameworks – But complex initial setup – High entry threshold	– Plug-and-play modules – No-code/low-code platforms – Automated deployment – Intuitive interfaces
Scalability	– Organic growth 1K→10K+/day – Horizontal scaling – Flexible resource addition – Load adaptation	– Proportional approach by size – Vertical integration – Regulated levels – Planned scaling	– Elastic infrastructure – Auto-scaling via smart contracts – Dynamic resource allocation – Pay-per-use model
Viability under threats	– Operation without electricity 8+ hrs – Backup communication channels – Local autonomy – 94.2% uptime under shelling	– Business continuity plan (BCP) – Backup copying – But infrastructure dependency – 95% SLA for crisis	– Full decentralisation – Functioning with 60%+ node loss – Quantum-resistant cryptography – Data immutability
Resource efficiency	– Minimal budget – Volunteers and enthusiasts – Creative solutions – Maximum from minimum	– Significant initial investment – Certified specialists – High operational costs – ROI in 2-3 years	– 70%+ cost reduction – Process automation – Community governance – Token economy incentives

The key conclusion is that the Ukrainian model and DORA represent two complementary dimensions of agile public governance. The Kharkiv model has demonstrated that rapid GovTech solutions born during war and threats can outpace traditional regulatory mechanisms and create new efficiency standards. However, DORA offers an architecture of long-term resilience through systematisation and scaling of proven practices. I believe that the promising synthesis of these approaches through Web 3.0 technologies forms a new vision of agile governance – public administration that combines rapid reactivity with strategic predictability in a unified decentralised ecosystem.

Practical implementation of such hybrid GovTech architecture envisages transformation from hierarchical structures to network platforms: starting with decentralised decision-making points (empowered nodes), through implementing collective intelligence algorithms for rapid consensus, to forming fully autonomous municipal services with public control through DAO mechanisms. The Kharkiv case proves that true innovation in public governance is born not in planning offices but in moments of existential challenge, when speed of reaction and readiness for radical experiments become matters of community and institutional survival.

A theoretical Model of Decentralised GovTech Architecture: From Illusions to Reality

Development of a theoretical model for decentralised GovTech architecture requires, first and foremost, honest acknowledgement: there is no 'magic switch' that will instantly toggle a municipal system from peacetime to crisis mode. Kharkiv's experience shows that even the best automation relies on human judgement, and Web 3.0 technologies, despite all promises, cannot replace operators' critical thinking in unpredictable situations. Therefore, the proposed authorial 'Cascading Resilience Model' is designed not as an automatic 'switch', but as an adaptive system of human-technology interaction, where each degradation level is activated through conscious decisions supported by algorithmic assistance. This is indeed complex, yet necessary.

Conceptually, the model is based on the principle of cascading redundancy, where the system has three main operational modes:

1. Level 1 - Normal mode (DORA-compliant) with full functionality and preventive monitoring, where AI optimises resources and forecasts load;
2. Level 2 - Crisis mode (Kharkiv-mode), activated upon anomaly detection with prioritisation of critical functions and disconnection of secondary ones;
3. Level 3 - Survival mode with minimal function set through P2P network, where local nodes operate autonomously with post-synchronisation.

The key innovative idea lies in creating a 'digital twin' of crisis based on Kharkiv data – a virtual environment that will allow AI systems in other cities to gain 'war experience' without actual war, combining the empirical value of Ukrainian experience with DORA's preventive approach.

The model's essence lies in organising municipal digital services into three functional blocks, each with three levels of operational readiness. These are not merely backup copies of each other – each level is optimised for a specific threat scenario with its own operational logic, resource requirements, and balance between efficiency and resilience. Transition between levels occurs not automatically but through a structured situation assessment process, where AI systems provide recommendations but final decisions are made by authorised personnel. This approach combines the speed of algorithmic data processing with human ability to assess context and make non-standard decisions.

The risk management block demonstrates evolution from resource-intensive predictive analytics to simple survival rules. At the first level, AI systems analyse terabytes of data, detecting weak signals of future problems 72 hours ahead. But when infrastructure degrades, the system switches to edge-computing with local models running on limited resources, maintaining ability to detect critical threats 6-12 hours ahead. In survival mode, only simple heuristic rules remain, such as "if more than 50 calls in 5 minutes about one problem – emergency alert", which can work even on an operator's smartphone.

Table 6

Architecture of functional blocks in the 'Cascading Resilience'model

Functional Block	Level 1: Optimal (DORA-mode)	Level 2: Adaptive (Kharkiv-mode)	Level 3: Autonomous (Survival-mode)
A. Risk Management with AI	− Full-scale predictive analytics − ML models on cloud GPUs − Integration with all data sources − 72+ hour forecasting	− Local edge-computing − Simplified models on CPU − Priority on critical metrics − 6-12 hour forecast	− Rule-based heuristics − Works on mobile devices − Emergency alerts only − Reactive mode
B. Multi-channel Infrastructure	− Omnichannel (web, app, tel, email) − Centralised orchestration − CRM integration − Personalised routing	− Priority channels (95% phone) − Local routing − Simplified ticketing − Grouping by criticality	− P2P mesh via Bluetooth/WiFi − Offline forms with sync − SMS via backup GSM modems − Paper backup procedures
C. Decentralised Security	− Full blockchain audit − Real-time cryptography − Multi-factor authentication − Compliance monitoring	− Selective recording of critical actions − Simplified authentication via email or mobile number − Post-facto validation	− Local crypto-capsules − One-way hashes − Emergency access tokens − Recovery via social graph

Multi-channel infrastructure transforms from luxurious omnichannel capability to basic P2P communication. Kharkiv's experience showed that 95% of citizens in crisis return to telephone as the most reliable channel. Therefore, the second level optimises voice communication specifically, disconnecting energy-intensive digital channels. The third level activates mesh networks, where citizens' smartphones become retransmitters, creating a resilient communication fabric even without centralised infrastructure. Critically, at each level the ability to record requests for subsequent processing is maintained – even if these are paper forms later scanned.

The security system evolves from full blockchain transparency to minimalist cryptographic guarantees. At the first level, every action is recorded in a distributed ledger (blockchain) with complete history and audit capability. When resources are limited, the system switches to selective recording of only critical operations, using batch cryptography to economise computational resources. In survival mode, only local cryptographic capsules remain – encrypted files with critical data that can be decrypted and validated after infrastructure restoration.

The coveted 'reserve of possibilities' in GovTech through Web 3.0 implementation lies precisely in the transition from centralised dependency to distributed (gradually distributed) autonomy. The technological reserve of Web 3.0 for municipal systems manifests in three key aspects of architectural evolution:

1. Firstly, transition from client-server model to peer-to-peer protocols reduces single points of failure – instead of one critical server, the system relies on a network of interchangeable nodes.

2. Secondly, Web 3.0 cryptographic primitives (hash functions, digital signatures, Merkle trees) ensure data verifiability without needing a trusted intermediary, critically important during infrastructure degradation.

3. Thirdly, consensus mechanisms enable achieving system coherent state even during "Byzantine failures" – when some nodes are unavailable or compromised.

Table 7

Transition mechanisms between levels of the cascading model

Transition Parameter	1→2 (Degradation)	2→1 (Recovery)	2→3 (Collapse)	3→2 (Stabilisation)
Triggers	− Availability <95% (15 min) − Load >300% − Loss of 30% nodes − Cyberattack confirmed	− Availability >98% (60 min) − Load <150% − All nodes restored − Threats eliminated	− Availability <70% − Loss of control centre − Mass service failures − Physical destruction	− Basic connectivity >80% − Coordination restored − Key services online − Security situation stable
Decision Process	− AI recommends (30 sec) − Supervisor validates (60 sec) − 3/5 operator consensus − Transition initiation	− Automatic proposal − Readiness testing − Phased migration − Stability confirmation	− Emergency protocol − Senior decision − Broadcast to all nodes − "Every human for himself/herself"	− Active node search − Cluster formation − Coordinator election − Data synchronisation
Transition Time	3-5 minutes	15-30 minutes	1-2 minutes	30-60 minutes
Rollback Possibility	Yes, within 1 hour	Automatic on failure	No, forward only	Yes, if deteriorating

For municipalities, this means the ability to maintain integrity of critical registries (cadastre, infrastructure status, service queues) even with 30-40% computational resource loss, which would be impossible with traditional architecture under Kharkiv conditions.

The model's key innovation is not technological complexity but organisational flexibility. Each block can function at its own level independently of others. For example, during a DDoS attack, the security block transitions to Level 2 with enhanced monitoring, whilst infrastructure remains at Level 1. This allows optimal resource distribution and avoids excessive degradation of the entire system due to a local problem. Experience of DS '1562' from Kharkiv showed that precisely this flexibility allowed maintaining 97% availability even under shelling – the system adapted to each specific threat rather than switching between rigidly defined states.

Model implementation requires transition from deterministic management systems to adaptive architectures with dynamic reconfiguration. An innovative yet ideologically and technologically important 'step' and element becomes the implementation of new-generation meta-contracts (following the example of the Ukrainian Bitbon System), which unlike primitive smart contracts contain not only executable code but also contextual metadata, self-regulation rules, and mechanisms for automatic synchronisation with blockchain registry. Such architecture allows municipal systems not merely to execute pre-written scenarios but to dynamically adapt business logic to current conditions – from optimising municipal vehicle routes in peacetime to automatic redistribution of emergency service resources during shelling. However, this has not yet been applied in Kharkiv for urban infrastructure. But demand for such new solutions is growing as solutions for the entire ecosystem, not isolated solutions.

Kharkiv's experience confirms: systems capable of runtime self-modification survive where monolithic solutions with rigid architecture collapse within the first hours of crisis. The proposed 'Cascading Resilience' model offers not a static architecture but an ideology of new 'meta-architecture': something like a set of patterns and protocols that allow the system to evolve according to challenges whilst maintaining operational integrity and recovery capability.

Discussion

Amongst the multitude of theoretical and practical implications of our research, the most critical for further GovTech development is the question of scaling 'war experience' – transferring crisis innovations from Kharkiv's context to stable European municipalities. Whilst technical aspects of integrating the Ukrainian 'survival model' with DORA regulatory standards merit detailed analysis, and the phenomenon of technological leap from Web 2.0 to Web 3.0 opens new horizons for digital transformation, it is precisely the ethical and methodological challenges of using data from combat zones that will determine the legitimacy and effectiveness of future digital resilience systems. The concept of a crisis 'digital twin' proposed in our model – a virtual environment for training AI systems based on 1.2 million real citizen requests under shelling – raises questions about the permissible limits of using human suffering for technological progress.

The ethical dimension of the problem extends far beyond traditional discussions of data privacy or informed consent. Each of the 72,993 requests during extreme shelling in November 2024 is not merely a data point for machine learning, but testimony of human tragedy, a cry for help at a moment of mortal danger. Using this data for training AI systems creates a paradoxical situation: on one hand, ignoring this unique experience would mean wasting invaluable lessons gained at an exorbitant price; on the other, commercialisation and routinisation of 'war experience' risks devaluing human losses and normalising extremity. Particularly acute is the question of consent: did Kharkiv citizens, contacting service '1562' under shelling, imagine their calls would become training material for European municipalities? Even data anonymisation does not relieve ethical tension – patterns of human behaviour under threat of death remain deeply personal, regardless of removed personal identifiers. Development of a new ethical framework for 'survival data' is necessary, one that would recognise their special status and establish strict limitations on commercial use, whilst enabling learning opportunities to enhance other communities' safety.

Methodological limitations of simulating real crises prove no less critical. Kharkiv's 'digital twin', despite all technological sophistication, will remain a simplified model incapable of reproducing the horror and irrationality of human behaviour under shelling (EU residents currently find this difficult to understand, but this could change for the worse for them in 3-5 years). Municipal AI systems and big-data analytics trained on conditionally 'Kharkiv'/Ukrainian data might more optimally distribute resources under load of 8,000 calls per day (indeed a lot!), but can they account for panic, rumours, mass hysteria – all those irrational factors that define a real crisis?

Moreover, each crisis is unique: a hypothetical 'earthquake' in Lisbon generates different behavioural patterns than shelling in Kharkiv, and a hypothetical flood in Budapest differs from a terrorist attack in Marseille. Attempting to create a universal crisis response model based on one, albeit extreme, case risks errors through overfitting to specific conditions of war in Ukraine.

I also see a methodological 'trap' in the illusion of control: successful simulation can create false confidence in readiness for 'black swans', whilst real crisis always brings unpredictable challenges. Oddly, excessive preparation based on past crises can make a system more fragile to future, fundamentally different threats – a phenomenon Nassim Taleb calls 'ludic fallacy', when reality is replaced by its simplified game model.

Another methodological collision between Kharkiv experience and European regulatory frameworks manifests in the incompatibility of basic operational assumptions. DORA (Regulation EU 2022/2554) is built on the presumption of 'steady state'– a stable operational environment with predictable threat parameters, where incidents are classified by seven clear criteria (JC 2023 83), and recovery presumes return to baseline configuration. In contrast, the Kharkiv model functions in a 'continuous risk' paradigm, where there is no stable state to return to, and each new day can bring some unpredictable combination of physical destruction, cyberattacks, and personnel losses. Furthermore, GDPR (Regulation EU 2016/679) requires consent for personal data processing with withdrawal

possibility, but how to ensure the right to data deletion (Article 17) for a citizen whose emergency call under shelling has already become part of an AI system training dataset? NIS2 Directive (EU 2022/2555) stipulates a 24-hour window for incident notification, but in Kharkiv conditions, where critical incidents occur every minute, such requirement becomes absurd – the system would generate thousands of formal notifications instead of focusing on operational continuity. Technically, using P2P mesh networks in Level 3 of the proposed model somewhat conflicts with eIDAS (Regulation EU 910/2014) requirements for qualified trust services, as it is impossible to guarantee node identification in a dynamic network during combat.

The sharpest methodological contradiction concerns efficiency metrics: DORA operates with SLA 99.9% for normal conditions and 95% for crisis scenarios, but these thresholds are calculated for 'clean failures'– technical failures in controlled environments, not situations where half the infrastructure is physically destroyed and operators work from bomb shelters. Attempting formal certification of the Kharkiv system by European standards would reveal dozens of critical non-compliances, although it is precisely this 'non-compliant' system that proved viable where 'compliant' solutions simply could not function.

All Europeans as well as EU-based institutions should realise that the era of 'regulatory comfort' is ending – the world has already entered a change of world order with wars and contradictions, where speed of adaptation is more important than formal compliance with 'mega-laws' or international agreements, and ability to function under complex conditions is significantly more important than optimisation in a stable environment. The world we know and remember is changing; it will not remain as it is. I fear that numerous EU-regulations will be short-lived in the EU due to the threat of a major high-tech war in Europe in the next 3-4 years. Therefore, I am convinced that ignoring and/or misunderstanding Kharkiv experience due to its 'non-compliance' with existing Euro-regulations would be not merely a missed opportunity but a potentially fatal mistake – when European cities face existential challenges (whether real war, climate catastrophes, or systemic infrastructure collapse), there will be no time to develop 'DORA 2.0'. True digital resilience is born not into regulators' offices but in the crucible of real crises, and the only way forward is synthesising Ukrainian anti-fragility with European systematicity through radically new technological solutions that fit no existing frameworks but work where traditional systems are powerless.

Conclusions

1) Institutional analysis of EU-Ukraine cooperation demonstrates the following digital resilience trajectory: from forced wartime innovations that outpaced regulatory standards to systematic integration of Ukrainian experience into European mechanisms through EU4DigitalUA, DT4UA platforms and GovTech dialogue. This evolution creates an unprecedented opportunity for synthesising two approaches – Ukrainian adaptability and European systematicity – in a new paradigm of digital resilience, where practical experience of extreme conditions enriches and validates theoretical models of regulated development. Methodologically, this phenomenon can be conceptualised as 'reverse innovation transfer', when peripheral actors under crisis conditions generate solutions that outpace central regulatory mechanisms. The identified dynamics challenge the classic linear 'centre-periphery' innovation diffusion model and actualise the need to develop new theoretical frameworks for understanding multi-vector technological transfer processes under global crises. It is precisely this methodological novelty that makes Ukrainian-European cooperation not merely technical exchange but a laboratory for forming new approaches to ensuring public governance resilience in an era of growing uncertainty.

2) The viability of the Kharkiv model is explained by several key factors often ignored in traditional digitalisation approaches. Firstly, the system was created not according to a modernisation plan but as a tool for city survival, forcing abandonment of perfectionism in favour of rapid adaptability – each technological solution was tested in real combat conditions and either proved its effectiveness

or was replaced. Secondly, unique personnel policy: after mobilisation of some staff operators, their places were taken by volunteers from among IT specialists evacuated from other regions, bringing startup culture with readiness for experiments and rapid changes to the service. Thirdly, the psychological factor – awareness that thousands of lives depend on service quality created unprecedented levels of motivation and responsibility at all levels.

3) Critically important was the understanding that under war conditions, traditional efficiency metrics lose meaning – instead of cost optimisation or throughput maximisation, the main KPI became the system's ability to function in degraded mode. Therefore, architecture was built on the principle of 'graceful degradation'– when one component fails, the system automatically switches to backup channels with minimal functionality loss. For example, when internet is disconnected, operators can continue taking calls and entering data into a local database that synchronises after connection restoration.

4) DORA does not account for external attacks or physical destruction, hence Kharkiv's indicator demonstrates exceptional stress resilience. Nevertheless, DORA's lessons for the municipal sector are obvious: (a) digital resilience is not merely a technical task but a strategic priority requiring active senior management involvement; (b) proportionality ensures balance between protection level and burden on budget and personnel; (c) regular testing (for example, using the TIBER-EU model) and team training enhance readiness for real cyber incidents; (d) cooperation through Eurocities networks, DG Reform and other experience exchange platforms promotes standards alignment and best practice multiplication.

5) The Ukrainian model and DORA are not mutually exclusive but rather complementary approaches. The Ukrainian model proved that under extreme conditions, speed of adaptation and readiness for experiments are more important than adherence to formal procedures. DORA provides systematicity and predictability necessary for stable development. Integration of both approaches through Web 3.0 and even Web 4.0 technologies (real examples of such solutions already exist – the Bitbon System of Ukrainian origin) creates new desired synergy: Ukrainian model adaptability combines with DORA's structure in decentralised architecture, ensuring both crisis resilience and peacetime efficiency. Practical implementation of such integrated model will require a phased approach: first implementing basic decentralisation elements (distributed databases, backup nodes), then adding AI components for routine process automation, and finally full transition to an autonomous system with minimal human intervention. Kharkiv's experience shows that even under the most challenging conditions, effective digital transformation is possible with clear understanding of priorities and readiness for innovation.

6) The 'Cascading Resilience' model demonstrates that true digital resilience of municipal systems is achieved not through implementing individual Web 3.0 technologies but through creating adaptive meta-architecture with three degradation levels for each functional block. The fundamental distinction of the approach lies in transitioning from rigidly deterministic systems to self-modifying architectures capable of rebuilding their own topology depending on available resources. The model ensures functioning with up to 40% computational capacity loss through a combination of P2P protocols, Byzantine fault tolerance and cryptographic verification mechanisms without a trusted centre. This transforms the municipal governance paradigm from centralised hierarchies to distributed networks with emergent properties, where resilience arises not from resource redundancy but from architectural flexibility and ability to evolve under external challenge pressure.

7) The research revealed a fundamental dilemma of scaling 'war experience': ethical inadmissibility of commercialising human suffering confronts the pragmatic necessity of using unique data to enhance other communities' resilience. Methodological incompatibility of Kharkiv's 'continuous risk paradigm' with European 'steady state' presumption, I think, demonstrates existing regulatory frameworks' limitations when facing existential challenges. In an era of global turbulence, when world

order undergoes fundamental changes, ignoring Ukrainian experience due to its 'non-compliance' could become a fatal mistake for European cities. The only way forward is synthesising Ukrainian anti-fragility with European systematicity through new technological solutions that transcend existing regulatory paradigms but ensure functioning where traditional systems fail.

References:

1. Cagigas, D., Clifton, J., Díaz-Fuentes, D., et al. (2022). Explaining public officials'opinions on blockchain adoption: A vignette experiment. Policy and Society, 41(3), 343–357. https://doi.org/10.1093/polsoc/puab022. https://academic.oup.com/policyandsociety/article/41/3/343/6524356?login=false
2. CEPS. (2025). Building digital resilience: How new technologies can support rebuilding Ukraine and strengthen digital transformation in Eastern Neighbouring countries. https://surl.li/urkhfl
3. Digital Europe Programme: Fact sheet. (2021). Brussels. https://surl.li/mdnhun
4. DigitalStateUA. (2025). Ukraine, EU, and eGA deliver 150+ digital services through the DT4UA project. https://surl.li/mlrmtr
5. Digital state UA. (2025). Ukraine closes digital trust gap with Singapore, says new GovTech report. Kyiv. https://surl.lt/flnbjw
6. DORA Updates, Compliance. (n.d.). https://www.digital-operational-resilience-act.com/
7. DT4UA. (2023). https://eu4digitalua.eu/en/dt4ua-en/
8. Dunayev, I., Byelova, L., Kud, A., & Rodchenko, V. (2023). Implementing the "government as a platform" concept: The assessment method and an optimal human-centered structure to address technological challenge. Eastern-European Journal of Enterprise Technologies, 2(13(122)), 6–16. https://doi.org/10.15587/1729-4061.2023.275613. http://journals.uran.ua/eejet/article/view/275613
9. e-Governance Academy. (2025, May 29). Ukraine, EU, and eGA deliver 150+ digital services through the DT4UA project. https://surl.lu/bezoera
10. EC. (2022). Solidarity with Ukraine: Digital Europe Programme open to Ukraine to access calls for funding. Brussels. https://digital-strategy.ec.europa.eu/en/news/solidarity-ukraine-digital-europe-programme-open-ukraine-access-calls-funding
11. EEF. (2024). GovTech pulse survey. Kyiv. https://eef.org.ua/en/report/govtech-pulse-survey/
12. EIOPA. (2024). Digital Operational Resilience Act (DORA). https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
13. EU4DigitalUA. (n.d.). https://ega.ee/wp-content/uploads/2024/06/eu4digitalua-booklet_en.pdf
14. European Commission. (2024). GovTech dialogue Ukraine-EU: Proceedings of the Kyiv meetup November 2024. DG CONNECT.
15. European Commission DG Connect. (2024). GovTech dialogue protocols and findings. Brussels.
16. European Parliament & Council. (2022). Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union, L 333, 1–79.
17. European Parliament and of the Council. (2024). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
18. Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. https://hdsr.mitpress.mit.edu/pub/l0jsh9d1/release/8
19. GovTech Dialogue Secretariat. (2024). Joint recommendations on digital resilience: Lessons from Ukraine. European Commission. https://surl.lu/ahupxv
20. Ingram, G., & Vora, P. (2024). Ukraine: Digital resilience in a time of war (Working paper 185). Brookings. https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf
21. Kud, A. A. (2021). Pravove rehuliuvannia detsentralizovanykh informatsiinykh platform: problemy i proponovanyi pryvatnopravovyi pidkhid do yikhnoho vyrishennia v Ukraini [Legal regulation of

decentralized information platforms: Problems and proposed private law approach to their solution in Ukraine]. Teoriia ta praktyka derzhavnoho upravlinnia, 2(73), 47–66. https://www.blockchainukraine.org/wp-content/uploads/2021/09/pravove-regulyuvannya-deczentralizovanikh-informaczijnikh-v-ukrayini.pdf (original in Ukrainian)
22. Kyiv City Council. (2025, February 5). Yak zminyvsia «Kyiv Digital» za 2024 rik: 3,3 mln korystuvachiv, 15 mln holosiv u opytuvaniakh, 270 mln validatsii u transporti [How Kyiv Digital changed in 2024: 3.3 million users, 15 million votes in polls, 270 million validations in transport]. https://surl.li/dvjuty/
23. Kyiv City Council. (2025, February 5). Yak zminyvsia «Kyiv Digital» za 2024 rik: 3,3 mln korystuvachiv, 15 mln holosiv u opytuvaniakh, 270 mln validatsii u transporti [How Kyiv Digital changed in 2024: 3.3 million users, 15 million votes in polls, 270 million validations in transport]. https://surl.li/ujpbqw
24. Kyiv City Council. (2025, February 5). Yak zminyvsia «Kyiv Digital» za 2024 rik: 3,3 mln korystuvachiv, 15 mln holosiv u opytuvaniakh, 270 mln validatsii u transporti [How Kyiv Digital changed in 2024: 3.3 million users, 15 million votes in polls, 270 million validations in transport]. https://surl.li/pfpdvl
25. Kyiv City Council. (2025, February 5). Yak zminyvsia «Kyiv Digital» za 2024 rik: 3,3 mln korystuvachiv, 15 mln holosiv u opytuvaniakh, 270 mln validatsii u transporti [How Kyiv Digital changed in 2024: 3.3 million users, 15 million votes in polls, 270 million validations in transport]. https://kyivcity.gov.ua/news/yak_zminivsya_kiv_tsifroviy_za_2024_rik_33_mln_novikh_koristuvachiv_15_mln_golosiv_v_opituvannyakh_270_mln_validatsiy_u_transporti/
26. Le Corre, A. (2025). A 2025 focused on resilience: How we aim to shape EU policy landscape in 2025 for resilient local communities. Energycities. https://energy-cities.eu/a-2025-focused-on-resilience/
27. LvivHerald. (2025). How a country stayed online: Technological innovation and wartime adaptation in Ukraine. https://surl.li/mwegyl
28. Mamediieva, G. (2025). Ukraine's digital transformation: Innovation for resilience. https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience
29. McKinsey & Company. (2023). The economic potential of generative AI: The next productivity frontier. McKinsey Global Institute. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier
30. Ministry of Digital Transformation of Ukraine. (2024, March 13). International digital diplomacy: Ukraine becomes a partner of NIIS. https://surl.li/rhrbzf
31. Nasker, S. (2024). Case studies and best practices of DORA. https://surl.lu/bpabri
32. NCC-SE. (2023). The Digital Europe Programme: Cybersecurity. https://www.ncc-se.se/en/about-ncc-se/the-digital-europe-programme-cybersecurity/
33. Nordic Institute for Interoperability Solutions. (2024, March 11). Ukraine becomes a partner of the Nordic Institute for Interoperability Solutions. https://surl.li/gvjyos
34. OECD. (2024a). Enhancing resilience by boosting digital business transformation in Ukraine. OECD Publishing. https://doi.org/10.1787/4b13b0bb-en
35. OECD. (2024b). Governing with artificial intelligence: Are governments ready? (OECD Artificial Intelligence Papers, No. 20). OECD Publishing. https://doi.org/10.1787/26324bc2-en
36. Sardag, D. (2025). GovTech in 2025: Strategic imperatives for inclusive and resilient digital government. https://www.linkedin.com/pulse/govtech-2025-strategic-imperatives-inclusive-resilient-doruk-sardag-woc4f/
37. Stephens, D., Stubbs, M., & White, S. (2025). Digital resilience: International and domestic legal responses to cyber security and artificial intelligence. Springer Singapore. https://doi.org/10.1007/978-981-97-9746-2
38. The European Union supports Ukraine's digital transformation: Results of EU4DigitalUA's work. (2024). Kyiv. https://www.eeas.europa.eu/delegations/ukraine/european-union-supports-ukraines-digital-transformation-results-eu4digitaluas-work_en?s=232
39. Visa. (2021). Digital solutions for urban resilience in Latin America (case studies). https://surl.li/dxtden