TOPICAL SCIENTIFIC ISSUES

DOI https://doi.org/10.51647/kelm.2026.2.29

ODPORNOŚĆ OPERACYJNA MIEJSKIEJ INFRASTRUKTURY INFORMATYCZNEJ W CZASIE AKTYWNYCH DZIAŁAŃ WOJENNYCH: STUDIUM PRZYPADKU KIJOWA DOTYCZĄCE CIĄGŁOŚCI USŁUG CYFROWYCH, CYBERBEZPIECZEŃSTWA I ZARZĄDZANIA KRYZYSOWEGO

Pavlo Chernikov
Magister Służby Cywilnej, Specjalista ds. Prawa,
Niezależny Badacz, (Kijów, Ukraina)
ORCID ID: 0009-0006-7390-9698
pavlo.chernikov@gmail.com

Adnotacja. Artykuł przedstawia praktyczne studium przypadku dotyczące zarządzania miejskim przedsiębiorstwem informatycznym, które miało status przedsiębiorstwa o krytycznym znaczeniu zgodnie z ukraińskim prawem wojennym i odpowiadało za cyberbezpieczeństwo, infrastrukturę sieciową i ciągłość usług cyfrowych organów samorządu miejskiego Kijowa w czasie aktywnych działań wojennych (2021–2024). Analizuje on, w jaki sposób organizacja działająca pod wpływem jednoczesnych zagrożeń kinetycznych i cybernetycznych zapewniła dostępność usług, reagowanie na incydenty, strategiczną alokację zasobów i koordynację międzyresortową. W oparciu o bezpośrednie doświadczenia administracyjne zaproponowano koncepcję sześciu zasad zarządzania kryzysowego: priorytetyzacja sytuacyjna, redundancja wielopoziomowa, ciągłość kapitału ludzkiego, adaptacyjna struktura dowodzenia, komunikacja z interesariuszami oraz uczenie się o incydentach. Zasady te przyczyniły się do utrzymania dostępności kluczowych miejskich usług cyfrowych na poziomie około 99,9%, zgodnie z wewnętrznym monitoringiem operacyjnym. Chociaż studium przypadku opiera się na doświadczeniach Kijowa, uzyskane wnioski są istotne dla europejskich gmin borykających się z zagrożeniami hybrydowymi, cyberatakami, niestabilnym zaopatrzeniem w energię i fizycznym zniszczeniem infrastruktury miejskiej.

Słowa kluczowe: zarządzanie kryzysowe; miejskie IT; odporność operacyjna; infrastruktura krytyczna; cyberobrona; ciągłość usług; transformacja cyfrowa; administracja publiczna; SOC; SIEM.

OPERATIONAL RESILIENCE OF MUNICIPAL IT INFRASTRUCTURE UNDER ACTIVE HOSTILITIES: A KYIV CASE STUDY ON DIGITAL SERVICE CONTINUITY, CYBERSECURITY, AND CRISIS GOVERNANCE

Pavlo Chernikov
Master of Public Service, Specialist in Law
Independent Researcher, (Kyiv, Ukraine)
ORCID ID: 0009-0006-7390-9698
pavlo.chernikov@gmail.com

Abstract. This paper presents a practitioner's governance case study of municipal IT infrastructure resilience under active hostilities. The case is drawn from three years of leading a municipal information-technology enterprise in Kyiv that carried formal status as a critically important enterprise under Ukrainian wartime regulations and was responsible for cybersecurity, network operations, and digital-service continuity for urban government bodies. The study examines how an organization operating under simultaneous kinetic and cyber threats managed service availability, incident response, strategic resource allocation, and inter-agency coordination. Drawing on first-hand administrative experience, the paper proposes a framework of six governance principles – situational prioritization, layered redundancy, human capital continuity, adaptive command structures, stakeholder communication, and post-incident learning – that contributed to sustaining approximately 99.9% availability of selected critical city-government digital services, based on internal operational monitoring. The findings are relevant to public administrators, emergency managers, and policymakers responsible for digital resilience in high-threat urban environments. Although the case is based on Kyiv, the findings are relevant for European municipalities facing hybrid threats, cyberattacks, energy instability, and physical disruption of urban infrastructure.

Key words: crisis governance; municipal IT; operational resilience; urban digital infrastructure; cyber defense; service continuity; wartime administration; public management; SOC; SIEM.

 © Knowledge, Education, Law, Management

ОПЕРАЦІЙНА СТІЙКІСТЬ МУНІЦИПАЛЬНОЇ ІТ-ІНФРАСТРУКТУРИ В УМОВАХ АКТИВНИХ БОЙОВИХ ДІЙ: КИЇВСЬКЕ КЕЙС-СТАДІ ЩОДО БЕЗПЕРЕРВНОСТІ ЦИФРОВИХ СЕРВІСІВ, КІБЕРБЕЗПЕКИ ТА КРИЗОВОГО УПРАВЛІННЯ

Павло Черніков
магістр державної служби, спеціаліст права,
незалежний дослідник, (Київ, Україна)
ORCID ID: 0009-0006-7390-9698
pavlo.chernikov@gmail.com

Анотація. У статті представлено практичне кейс-стаді з управління муніципальним ІТ-підприємством, що мало статус критично важливого підприємства згідно з українським законодавством воєнного часу та відповідало за кібербезпеку, мережеву інфраструктуру та безперервність цифрових сервісів органів міського самоврядування Києва в умовах активних бойових дій (2021–2024). Досліджено, як організація, що функціонувала під впливом одночасних кінетичних і кіберзагроз, забезпечувала доступність сервісів, реагування на інциденти, стратегічний розподіл ресурсів та міжвідомчу координацію. На основі безпосереднього адміністративного досвіду запропоновано концепцію шести принципів кризового управління: ситуаційна пріоритизація, багаторівнева надмірність, безперервність людського капіталу, адаптивна командна структура, комунікація зі стейкхолдерами та навчання за результатами інцидентів. Ці принципи сприяли підтриманню доступності ключових міських цифрових сервісів на рівні приблизно 99,9% за даними внутрішнього операційного моніторингу. Хоча кейс ґрунтується на досвіді Києва, отримані висновки актуальні для європейських муніципалітетів, що стикаються з гібридними загрозами, кібератаками, нестабільністю енергопостачання та фізичним руйнуванням міської інфраструктури.

Ключові слова: кризове управління; муніципальні ІТ; операційна стійкість; критична інфраструктура; кіберзахист; безперервність сервісів; цифрова трансформація; публічне управління; SOC; SIEM.

Introduction. Cities that have undergone rapid digital transformation over the past decade face a paradox: the same platforms that improve governance efficiency become vectors of vulnerability when the operating environment deteriorates. Under conditions of active armed hostilities, this vulnerability is compounded by physical threats to infrastructure, sudden changes in workforce availability, intermittent utility outages, and an adversarial cyber environment in which attacks are coordinated with kinetic events for maximum disruption.

This paper examines how a single municipal IT enterprise – one bearing formal legal responsibility for the cybersecurity and network infrastructure of more than 1,800 urban-government institutions – navigated these conditions across a three-year period that included the onset of full-scale armed conflict. The analysis draws on direct administrative experience accumulated during the enterprise's leadership from February 2021 to March 2024 to reconstruct decision-making processes, resource-allocation logic, and organizational adaptations that enabled service continuity.

The enterprise's responsibilities were broad: it operated approximately 1,500 kilometers of fiber-optic backbone connecting more than 1,800 Kyiv city-government institutions; managed a video-surveillance network of more than 8,000 cameras integrated into the city's public-safety system; administered an Internet-of-Things (IoT) sensor network based on LoRaWAN technology; and hosted the Security Operations Center (SOC) responsible for monitoring and incident response across the entire municipal digital ecosystem. These responsibilities placed the enterprise at the intersection of telecommunications, cybersecurity, and public governance – a convergence that shaped every management decision studied here.

The paper is structured as follows. Section 2 reviews relevant literature on crisis governance, organizational resilience, and public-sector IT management. Section 3 states the research problem and methodology. Section 4 describes the operating context. Section 5 presents the main governance findings organized around six principles. Section 6 discusses implications for policy and practice. Section 7 concludes.

The Kyiv case is relevant beyond Ukraine because European municipalities increasingly operate under conditions of hybrid risk: cyberattacks, infrastructure sabotage, energy instability, disinformation pressure, and emergency-service overload. The article therefore treats Kyiv not as an exceptional case only, but as an extreme case from which transferable governance principles can be derived for European urban digital resilience.

Literature review. Organizational resilience – broadly understood as the capacity to anticipate, absorb, adapt to, and recover from disruptions – has accumulated a substantial literature since Wildavsky's foundational treatment (Wildavsky, 1988). In the public-sector context, Boin and colleagues have distinguished between organizational robustness (resistance to disruption) and adaptive capacity (the ability to reconfigure under novel conditions), arguing that high-reliability governance requires both (Boin, Hart, Stern, Sundelius, 2016). More recent scholarship has extended these concepts to cyber-physical systems, recognizing that digital and physical infrastructure are so deeply intertwined that threats to one propagate to the other, as demonstrated by cyberattacks that produced physical power outages in Ukraine (Liang, Weller, Zhao, Luo, Dong, 2017); systematic reviews of cyber resilience for critical infrastructure have since consolidated this body of work and emphasized the role of situational awareness in sustaining essential services (Naserinia, Ekstedt, Asplund, 2021), (Bellini, Marrone, Di Mauro, 2025).

Research on municipal IT governance during crises is comparatively sparse. Much of the existing work focuses on disaster recovery following natural events (Kapucu, Hu, 2016), (Comfort, Boin, Demchak, 2010) or on cybersecurity incident response in isolation from broader administrative context (Touhill, Touhill, 2014). Studies that

address both cyber and kinetic threats concurrently remain rare, in large part because such conditions have historically been unusual in the settings most studied by organizational scholars.

The concept of continuity of operations (COOP) originated in military doctrine but has been adapted for civilian government, particularly in the United States following post-2001 reforms (Circular, 2017). The European regulatory landscape has converged on a layered model of resilience. The NIS2 Directive establishes a high common level of cybersecurity across the Union and imposes risk-management, incident-reporting, and supervisory obligations on essential and important entities – a category into which municipal IT operators of the kind studied here naturally fall (Directive (EU), 2022). Complementing it, the Critical Entities Resilience (CER) Directive addresses the broader, non-cyber dimensions of resilience, requiring critical entities to withstand and recover from disruptions including physical attacks, natural disasters, and hybrid threats (Directive (EU), 2022). Together, these instruments frame digital and physical resilience as a single governance obligation rather than two separate technical concerns. However, implementation guidance at the municipal level remains uneven, and the administrative literature offers little on how such obligations function in practice when an entity is simultaneously subject to cyber and kinetic attack.

Ukrainian regulatory frameworks similarly define categories of critical infrastructure and critically important facilities, imposing continuity and protection obligations broadly analogous to the EU model, and recent comparative analyses have examined the alignment between Ukrainian legislation and the EU directives (Zubok, Davydiuk, Klymenko, 2023 : 59).Yet the gap between regulatory requirement and operational reality is precisely where the present study is situated: how a designated critical entity actually sustains its obligations under sustained hostilities.

The empirical scale of the threat environment in which such entities operate is documented in two complementary bodies of evidence. At the European level, the ENISA Threat Landscape report identifies threats against availability – principally distributed denial-of-service attacks – and ransomware as the dominant categories, with public administration the single most-targeted sector, and explicitly links the escalation to ongoing regional conflict (ENISA Threat Landscape, 2024.). At the national level, the operational reporting of Ukraine's State Service of Special Communications and Information Protection (SSSCIP) and its Government Computer Emergency Response Team (CERT-UA) documents a sharp year-on-year rise in processed cyber incidents, with local-government bodies, the energy sector, and telecommunications among the most frequently targeted, and with attacks repeatedly timed to amplify the effect of kinetic strikes on infrastructure (Analytics, 2025). This body of reporting establishes that the conditions analyzed in the present case study were not anomalous but representative of a systematic, sustained threat directed at exactly the class of municipal critical entity examined here.

On the technical side, the NIST Cybersecurity Framework (CSF) 2.0 provides a widely adopted structure for organizing security functions across the Identify–Protect–Detect–Respond–Recover cycle (NIST Cybersecurity White Paper, 2024). SIEM platforms are recognized as a central instrument for implementing the Detect and Respond functions at scale (SIEM Correlation Rules, 2025). However, the governance literature has paid relatively less attention to how SIEM programs are resourced, staffed, and adapted under adverse human-capital conditions – such as those created by partial staff mobilization and air-raid disruptions.

This study contributes to the intersection of these literatures by providing a governance-level case study of a real municipal IT enterprise operating under active hostilities. Unlike laboratory or simulation studies, it documents actual administrative decisions and their outcomes, including constraints that theoretical models rarely capture: budget freezes, staff attrition through military mobilization, physical damage to facilities, and the psychological demands of sustained crisis leadership.

Research problem. The central question addressed by this paper is: what governance principles enable a public-sector IT enterprise designated as a critically important enterprise to maintain acceptable service continuity and security posture when operating under simultaneous kinetic and cyber threats, with constrained resources and an unstable human-capital base?

This question has both descriptive and normative dimensions. Descriptively, it asks what actually happened – which decisions were made, in what sequence, under what constraints. Normatively, it asks which of those decisions proved effective and why, so that lessons can be extracted for other organizations.

Methodology. The study follows a practitioner case-study approach (Yin, 2018). Occupying the decision-making role under study enables rich, first-hand reconstruction of governance choices, but also introduces potential for self-serving interpretation. This limitation is acknowledged and partially mitigated by grounding observations in verifiable outcomes (service availability metrics, incident counts, infrastructure milestones) and by triangulating with the governance literature. To reduce this limitation further, the analysis focuses on governance mechanisms, documented operational constraints, and observable organizational outcomes rather than on personal leadership evaluation.

Data sources include: (a) administrative records generated during the period under study, internal operational notes, personal professional archives, and contemporaneous management documentation, supplemented by first-hand reconstruction of decision-making processes; (b) technical documentation and monitoring data from the SOC and network-management systems; (c) post-incident reports and inter-agency communications; and (d) public reporting on the broader context of cyber and physical threats. To protect operational security and avoid disclosure of sensitive deployment parameters, specific technical configurations, exact incident timelines, and identifying details about partner organizations are presented in generalized or anonymized form.

The analytical framework organizes findings around governance principles inductively derived from the case material and then mapped onto existing theoretical constructs. This approach is appropriate when the phenomenon is empirically underexplored, as is the case for municipal IT governance under active hostilities.

Institutional profile. The enterprise was officially recognized as a critically important enterprise under Ukrainian wartime regulations. In this article, this designation is treated as evidence of the enterprise's public-service importance and operational responsibility, rather than as a direct equivalent of European Union critical-infrastructure classifications. At the same time, the continuity expectations, incident-reporting responsibilities, and cooperation with relevant public authorities associated with this status are conceptually comparable to the resilience and cybersecurity obligations reflected in the EU NIS2 Directive and the Critical Entities Resilience (CER) Directive.

The enterprise's operational perimeter encompassed: (i) fiber-optic network operations serving over 1,800 municipal institutions; (ii) management of a large-scale CCTV system integrated with emergency-services dispatch; (iii) IoT sensor infrastructure supporting city monitoring applications; (iv) hosting and security operations for digital-government platforms serving millions of residents; and (v) a SOC responsible for 24/7 monitoring, threat detection, and incident coordination across all of the above.

Phase structure. For analytical purposes, the 2021–2024 period divides into three governance phases, summarized in Table 1 and elaborated below.

Table 1

Governance phases, 2021–2024

Phase	Period	Main threat environment	Governance focus
Phase 1	Feb 2021 – Feb 2022	Normal public-sector constraints	SOC build-up, SIEM, LoRaWAN, monitoring
Phase 2	Feb 2022 – Dec 2022	Full-scale invasion; cyber and kinetic threats	Continuity, emergency response, prioritization
Phase 3	2023 – Mar 2024	Prolonged wartime operations	Stabilization, redundancy, institutional learning

Phase 1 (February 2021 – February 2022): Organizational build-up. The enterprise underwent significant restructuring, including the establishment of the SOC, deployment of a SIEM platform, buildout of the LoRaWAN sensor network, and expansion of network monitoring capabilities. The primary governance challenge was accelerating institutional development while managing the normal constraints of public-sector procurement and staffing.

Phase 2 (February 2022 – December 2022): Acute crisis response. The onset of full-scale armed conflict on February 24, 2022 fundamentally altered the operating environment. Physical attacks on energy infrastructure created recurring power outages affecting both the enterprise's facilities and those of client institutions. Cyberattack volume and sophistication increased markedly, consistent with the national-level escalation later documented in SSSCIP and CERT-UA reporting (Analytics, 2025). Staff availability became unpredictable due to military mobilization, shelter requirements during air raids, and displacement. The primary governance challenge was maintaining operational continuity under conditions that had not been fully anticipated.

Phase 3 (2023 – March 2024): Adaptive stabilization. Having absorbed the initial shock of full-scale hostilities, the enterprise entered a phase of deliberate adaptation: hardening infrastructure against recurring attack patterns, developing redundant communication pathways, implementing remote-work capabilities for security staff, and building institutional practices for long-term operation in a persistently degraded environment.

The principles below are derived from the Kyiv case but are formulated at a level of generality intended for application by other European municipal IT organizations exposed to hybrid or wartime disruption. They are derived inductively from the case material and represent the governance logic that proved most consequential for service continuity and security outcomes during the study period; their integrated relationship is summarized in Figure 1.

Principle 1: Situational prioritization over procedural uniformity.

Pre-crisis governance typically applies uniform procedures to all services and institutions. Under active hostilities, this approach becomes unsustainable – resources are insufficient to maintain all functions simultaneously at normal standards, and attempting to do so produces failure across the board.

Effective crisis governance requires explicit, defensible prioritization of services by criticality. In the enterprise studied here, this was operationalized as a three-tier hierarchy: (i) life-safety systems (emergency dispatch integration, critical public-safety CCTV coverage, first-responder communications); (ii) continuity-enabling systems (authentication infrastructure, core network routing, SOC operations); and (iii) standard municipal services (citizen-facing digital platforms, administrative workflows). Resources – both human and technical – were allocated starting from Tier 1, with Tier 3 systems explicitly placed in maintenance-only or degraded mode during capacity-constrained periods.

This tiering was not static. As the threat environment evolved, certain services migrated between tiers – for example, the enterprise's own backup infrastructure was elevated to Tier 1 status once it became clear that power-grid attacks would be recurrent. The administrative discipline of revisiting the priority structure quarterly proved more valuable than any fixed classification scheme.

Principle 2: Layered redundancy as a governance commitment, not a technical detail.

Redundancy is frequently discussed in technical terms – backup power, diverse routing, replicated data. What is less often recognized is that redundancy must be governed: it requires budget allocation decisions, procurement lead-time management, and maintenance discipline, all of which involve leadership choices rather than engineering choices alone.

Several specific redundancy investments made prior to and during the conflict proved decisive for service continuity. First, the deployment of uninterruptible power supply (UPS) systems and generator backup at key network nodes was a governance decision that required budget prioritization over competing uses of public funds. Second, the buildout of alternative wireless communication pathways – including LoRaWAN for IoT telemetry and TETRA radio for emergency services – provided resilience when fiber routes were disrupted. Third, the migration of certain critical workloads to geographically distributed private cloud infrastructure reduced exposure to physical attacks on any single facility.

The governance lesson is that redundancy investments are most valuable when made before they are needed and become nearly impossible to implement adequately after a crisis begins. Leaders responsible for critical IT infrastructure must continuously advocate for redundancy funding as a cost of operational security rather than as optional enhancement.

Principle 3: Human capital continuity requires proactive architecture.

Wartime conditions create human-capital shocks that are qualitatively different from normal turnover. Military mobilization removes personnel with little notice and often with no replacement. Sustained psychological stress produces burnout and attrition among those who remain. Air-raid requirements interrupt workflows unpredictably. Physical displacement of staff due to security conditions affects availability and concentration.

The enterprise responded to these pressures through three governance interventions. First, cross-training across critical roles – ensuring that no single person was the unique holder of operational knowledge for a Tier 1 or Tier 2 function. This required deliberate organizational effort because specialists tend to work in depth rather than breadth. Second, a structured remote-operations capability for SOC personnel, developed during Phase 3, allowed security monitoring to continue during air raids and reduced the vulnerability of having the entire security team co-located in a single facility. Third, a deliberate shift toward written runbooks and documented procedures reduced dependence on tacit knowledge held by individuals, enabling faster onboarding of replacement staff.

The broader governance insight is that human resilience, like technical resilience, requires proactive architecture. Organizations that assume their staff will simply adapt organically to crisis conditions regularly underestimate the resulting performance degradation.

Principle 4: Adaptive command structure with clear authority.

Crisis environments generate a pressure toward centralization – the instinct to have all decisions flow through a single authority. In practice, this creates bottlenecks and cognitive overload at the top, slowing response times precisely when speed matters most. Conversely, excessive decentralization in a crisis produces incoherence and duplication.

The enterprise evolved toward what may be described as structured decentralization: a clear articulation of which decisions required senior approval, which could be taken at the team-lead level, and which were delegated entirely to technical staff. This mapping was explicit and documented, and it was revised as the operating environment changed. For example, certain network-routing changes that required managerial approval under normal conditions were pre-authorized for rapid implementation by on-call engineers during active attack windows, subject to post-hoc review.

This approach was informed in part by the incident-command structure concepts present in emergency-management doctrine, adapted to an IT operations context. The critical governance contribution was institutionalizing the authority map – making it a documented, shared organizational artifact rather than a set of informal understandings that could become confused under stress.

Principle 5: Stakeholder communication as a continuous governance function.

A municipal IT enterprise exists in a web of dependencies: client institutions depend on it for connectivity and security; emergency services depend on it for communication infrastructure; city leadership depends on it for digital service availability; residents depend on the downstream services it enables; and partner agencies including national security bodies depend on its cooperation for threat intelligence. Managing these relationships draws on the logic of collaborative governance, in which outcomes depend on sustained interaction among interdependent actors rather than unilateral control (Ansell, Gash, 2008), and it requires continuous, proactive communication – not only when incidents occur but as a regular governance function.

During the acute crisis phase, the enterprise established a structured reporting cadence to city leadership covering service availability, current threats, and resource constraints. This reporting served two functions: it enabled informed resource-allocation decisions by city leadership; and it created a shared record of the constraints under which the enterprise was operating, which proved important when decisions about resource allocation were later reviewed. Separately, the enterprise maintained liaison relationships with national-level security bodies, ensuring that threat intelligence was exchanged in a timely manner and that enterprise-level observations about the local threat environment were incorporated into broader situational awareness.

The governance insight here is that communication, in a crisis, is not simply an ancillary activity but a core management function that requires dedicated time, structured processes, and deliberate attention from senior leadership.

Principle 6: Post-incident learning as institutional discipline.

High-tempo operations under persistent threat pressure create a risk that organizations become entirely reactive – moving from incident to incident without time for systematic reflection. This pattern produces local fixes that do not address root causes and prevents the accumulation of institutional knowledge that would reduce the cost of future incidents.

The enterprise worked against this tendency by maintaining a structured post-incident review process for significant events, producing written summaries that were archived and reviewed periodically by senior staff. These reviews fed into three types of improvement: SIEM rule refinements (adjusting detection logic based on observed attack patterns); infrastructure hardening priorities (directing investment toward vulnerabilities exposed by actual incidents); and procedural updates (modifying runbooks based on the real performance of response procedures under operational conditions).

An important dimension of this process was the explicit treatment of near-misses alongside actual incidents. Near-misses – situations in which a threat was detected and mitigated before causing impact – contain as much governance information as successful attacks, but are easily overlooked when the team is focused on damage repair. The enterprise's practice of reviewing near-misses alongside incidents was a deliberate adaptation to the high volume of attempted attacks, which would have produced review fatigue if only successful attacks had been analyzed.

The governance principles described above were not adopted as a theoretical framework but emerged from operational experience. Their effectiveness can be assessed against several observable outcomes.

The quantitative indicators reported in this section are based on internal operational monitoring, incident-management records, and management reporting. They should be interpreted as approximate operational indicators rather than independently audited performance metrics.

Service availability: Across the 2021–2024 period, including the periods of most intense kinetic and cyber pressure, the enterprise maintained availability of key city-government digital services at approximately 99.9%. This figure encompasses both the core network infrastructure and the primary digital-government platforms. It was achieved despite multiple physical attacks on energy infrastructure that caused multi-hour power outages at various network nodes, and despite a significant increase in cyberattack volume following the onset of full-scale hostilities.

Incident response efficiency: Following the implementation of a restructured SIEM correlation framework aligned with the NIST CSF functions, the mean time to respond (MTTR) for high-severity incidents decreased by approximately 30% – from roughly 45 minutes to roughly 30 minutes for known attack patterns. Simultaneously, the false-positive alert rate decreased by approximately 90%, primarily by correlating firewall logs with identity-management data to suppress noise generated by the large increase in remote-worker VPN activity. These SIEM-related findings are consistent with earlier work on event-correlation scaling in municipal digital systems under wartime conditions (Chernikov, 2025).

Human capital retention: Despite the challenging operating environment, the core SOC team remained intact throughout the study period. No Tier 1 or Tier 2 function experienced an unrecoverable personnel gap. This outcome is attributed primarily to the cross-training and documentation investments described under Principle 3.

Infrastructure hardening: By the end of the study period, the enterprise had completed a significant expansion of backup power coverage at critical nodes, deployed a TETRA-based emergency radio network covering key city-government facilities, established an alternative IoT communication layer through the LoRaWAN network, and migrated critical workloads to geographically distributed infrastructure. Each of these investments had been identified through the post-incident review process as a gap exposed by actual incidents.

Table 2 summarizes how each governance principle maps to its primary mechanism and associated outcome, while Table 3 traces the path from specific threats and constraints through governance responses to their observed effects.

Table 2

Summary of Governance Principles and Associated Outcomes

No.	Governance Principle	Primary Mechanism	Key Outcome
1	Situational prioritization	Three-tier service hierarchy, quarterly revision	Resources concentrated on life-safety functions; Tier 3 degradation managed explicitly
2	Layered redundancy	Pre-crisis investment in backup power, diverse routing, cloud distribution	Service continuity despite repeated power and physical-network disruptions
3	Human capital continuity	Cross-training, runbook documentation, remote SOC capability	Core team integrity maintained; no unrecoverable staffing gap
4	Adaptive command structure	Documented authority map; pre-authorized rapid response for defined scenarios	Faster incident response; reduced decision bottlenecks under load
5	Stakeholder communication	Structured reporting cadence; liaison with national security bodies	Informed resource decisions; shared situational awareness across agencies
6	Post-incident learning	Structured review of incidents and near-misses; written archive	SIEM improvements; targeted infrastructure hardening; procedural updates

Table 3

Mapping of Threats and Constraints to Governance Responses and Observed Effects

Threat / constraint	Governance response	Observed effect
Cyberattacks and alert overload	SIEM contextual correlation and enrichment	Lower false-positive burden; preserved analyst capacity
Power instability	Redundant infrastructure and backup operations	Improved service continuity during outages
Staff mobilization and attrition	Human-capital continuity planning	Critical functions preserved without unrecoverable gaps
Physical threat to facilities	Distributed operational posture	Reduced single-point dependency
Inter-agency coordination pressure	Adaptive command structure	Faster decisions; shared situational awareness

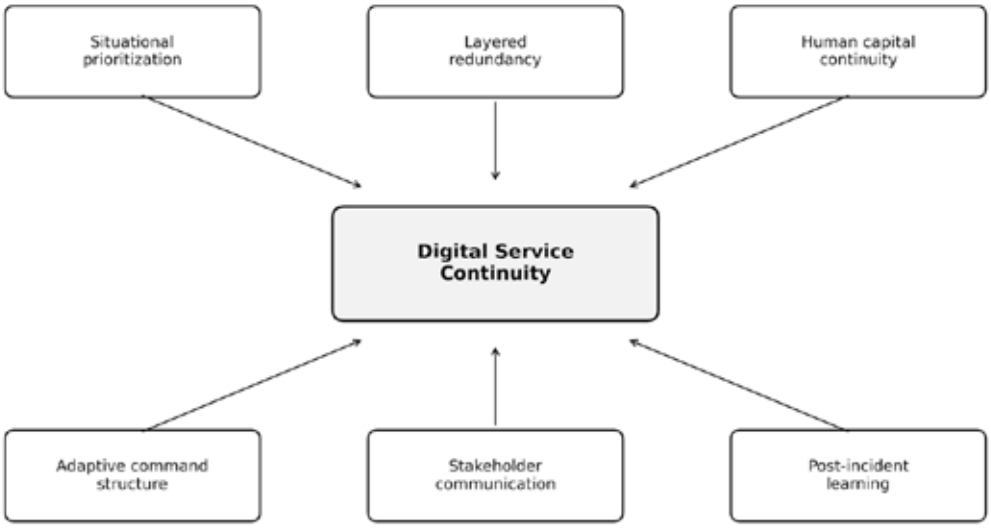

Fig. 1. Municipal IT Resilience Governance Framework

The six governance principles operate concurrently and reinforce one another; together they sustain the central objective of digital service continuity.

The findings presented here have several implications that extend beyond the specific case studied.

First, they challenge the assumption embedded in many continuity-planning frameworks that crises are discrete, bounded events after which normal operations resume. The enterprise studied here operated in a persistently degraded environment for over two years, during which the appropriate governance posture was not emergency response but something closer to sustained adaptive management. Planning frameworks that focus primarily on acute response and short-term recovery are ill-suited to this condition.

Second, the findings highlight the extent to which technical resilience is a downstream product of governance resilience. The infrastructure decisions that proved most consequential – backup power coverage, distributed cloud architecture, LoRaWAN deployment – were governance decisions involving budget competition, procurement management, and political advocacy within the municipal administration, not primarily engineering decisions. This suggests that resilience programs in public-sector IT should give greater attention to the governance conditions that enable or prevent technical investment.

Third, the case illustrates the particular governance challenges created by human-capital disruption in a wartime context. Military mobilization, a phenomenon well understood in other domains of wartime public administration, has not been studied systematically in the context of critical IT operations. The cross-training and documentation practices that proved effective here are not novel in principle – they are standard recommendations in high-reliability organization theory () – but they require deliberate implementation before they are needed, and this requires senior leadership to treat human resilience as a strategic priority rather than an HR function.

Fourth, the study provides empirical support for the value of SIEM contextual enrichment in high-volume, high-stress environments. The reduction of false-positive alerts by nearly 90% through contextual correlation was not merely an operational convenience; it was a precondition for maintaining human analyst effectiveness at a time when staffing was constrained. The governance insight is that alert management is a human-capacity management problem, not only a technical one.

Finally, the study suggests that the governance principles identified here are likely transferable to urban IT organizations outside the specific context of armed conflict – to disaster response, major natural events, or other

scenarios in which multiple simultaneous stressors disrupt normal operations. The principles are stated at a level of generality intended to facilitate this transfer, while the case material provides the grounding needed to evaluate their contextual validity.

Conclusions. This paper has presented a governance case study of a municipal IT enterprise operating under active armed hostilities, documenting the administrative principles and decisions that enabled sustained service continuity and security effectiveness across a three-year period that included the onset of full-scale conflict.

Six governance principles were identified as central to the enterprise's resilience: situational prioritization over procedural uniformity; layered redundancy as a leadership commitment; proactive human capital architecture; adaptive command structure with documented authority; continuous stakeholder communication; and institutionalized post-incident learning. These principles are not individually novel; what the case contributes is evidence of how they interact and reinforce each other in practice under extreme conditions.

The measurable outcomes associated with this governance posture – approximately 99.9% service availability across a period of intense multi-domain threat, a 30% improvement in incident response time, a 90% reduction in false-positive alert volume, and intact human capital throughout – provide a basis for cautious confidence in the framework's effectiveness, while remaining internal operational indicators rather than independently audited metrics.

The study does not claim that the Kyiv model can be directly replicated in all European municipalities. Rather, it identifies governance mechanisms that may inform resilience planning where municipal digital infrastructure is exposed to cyber, physical, and administrative disruption simultaneously.

From a policy perspective, the findings reinforce the importance of treating critical municipal IT infrastructure as a governance challenge first and a technical challenge second. Investment in redundancy, human-capital continuity, and adaptive command structures requires leadership prioritization and budget advocacy that cannot be delegated to technical staff alone. Cities that wish to develop genuine digital resilience must ensure that their IT governance frameworks are designed for adverse conditions, not merely for routine operations.

Future research should examine comparable cases across multiple cities and conflict contexts, develop quantitative models of the governance-resilience relationship, and extend the analysis to the recovery phase – the process by which municipal IT organizations restore full operational capability following protracted crisis periods.

REFERENCES

1. Wildavsky, A. (1988). Searching for Safety. Transaction Publishers. DOI : https://doi.org/10.4324/9781351316248 [in English].
2. Boin, A., Hart, P., Stern, E., & Sundelius, B. (2016). The Politics of Crisis Management: Public Leadership Under Pressure (2nd ed.). Cambridge University Press. DOI : https://doi.org/10.1017/9781316339756 [in English].
3. Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Transactions on Power Systems, 32(4), 3317–3318. DOI : https://doi.org/10.1109/TPWRS.2016.2631891 [in English].
4. Kapucu, N., & Hu, Q. (2016). Understanding multiplexity of collaborative emergency management networks. The American Review of Public Administration, 46(4), 399–417. DOI : https://doi.org/10.1177/0275074014555645 [in English].
5. Comfort, L. K., Boin, A., & Demchak, C. C. (Eds.). (2010). Designing Resilience: Preparing for Extreme Events. University of Pittsburgh Press. DOI : 10.1108/ijdrbe.2011.2.2.178.1 [in English].
6. Touhill, G. J., & Touhill, C. J. (2014). Cybersecurity for Executives: A Practical Guide. Wiley. URL : https://www.wiley.com/en-be/shop/general-introductory-electrical-electronics-engineering/cybersecurity-for-executives-a-practical-guide-p-9781118888148 [in English].
7. Federal Emergency Management Agency. (2017). Continuity Guidance Circular (CGC 1). U.S. Department of Homeland Security. URL : https://www.fema.gov/emergency-managers/national-preparedness/continuity/circular [in English].
8. European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union, L 333, 27.12.2022, 80–152. URL : https://eur-lex.europa.eu/eli/dir/2022/2555/oj [in English].
9. European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive). Official Journal of the European Union, L 333, 27.12.2022, 164–198. URL : https://eur-lex.europa.eu/eli/dir/2022/2557/oj [in English].
10. Zubok, V. Yu., Davydiuk, A. V., & Klymenko, T. M. (2023). Cybersecurity of critical infrastructure in Ukrainian legislation and in Directive (EU) 2022/2555. Electronic Modeling, 45(5), 54–66. DOI : https://doi.org/10.15407/emodel.45.05.054 [in English].
11. European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. Publications Office of the European Union. URL : https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 [in English].
12. State Service of Special Communications and Information Protection of Ukraine (SSSCIP) / CERT-UA. (2025). Russian Cyber Operations: Analytics for the H2 2024. State Cyber Protection Centre, Kyiv. URL : https://cip.gov.ua/services/cm/api/attachment/download?id=68768 [in English].
13. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper). U.S. Department of Commerce. URL : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [in English].
14. Cymulate. (2025). SIEM Correlation Rules: Fine-Tune Detection Logic at Scale. Cymulate Glossary. URL : https://cymulate.com/cybersecurity-glossary/siem-correlation-rules/ [in English].

15. Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). Sage Publications. URL : https://ebooks.umu.ac.ug/librarian/books-file/Case%20Study%20Research%20and%20Applications.pdf [in English].
16. Chernikov, P. (2025). Cyber defense of urban digital systems: scaling SIEM correlation to reduce incidents in a wartime city. Cybersecurity: Education, Science, Technique, 3(31), 773–780. DOI : https://doi.org/10.28925/2663-4023.2025.31.1066 [in Ukrainian].
17. Weick, K. E., & Sutcliffe, K. M. (2015). Managing the Unexpected: Sustained Performance in a Complex World (3rd ed.). Wiley. URL : https://www.wiley.com/en-us/shop/general-introductory-business-management/managing-the-unexpected-sustained-performance-in-a-complex-world-3rd-edition-p-9781118862414 [in English].
18. Naserinia, V., Ekstedt, M., & Asplund, M. (2021). Cyber Resilience for Critical Infrastructure: A Systematic Literature Review. KTH Royal Institute of Technology. URL : https://www.diva-portal.org/smash/get/diva2:1576950/FULLTEXT03.pdf [in English].
19. Bellini, E., Marrone, S., & Di Mauro, N. (2025). Situation awareness for cyber resilience: A review. International Journal of Critical Infrastructure Protection, 48, Article 100720. DOI : https://doi.org/10.1016/j.ijcip.2025.100755 [in English].
20. Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. Journal of Public Administration Research and Theory, 18(4), 543–571. https://doi.org/10.1093/jopart/mum032 [in English].