

Formation of a conceptual model for cyber-physical monitoring of critical infrastructure environmental objects^{*}

Vadym Chytulian^{1,†}, Andrii Kolodiuk^{1,†}, Ivan Oleinikov^{1,†}, Viktoriia Zhebka^{1,*,†},
and Valeriia Balatska^{2,†}

¹ State University of Information and Communication Technologies, 7 Solomenskaya str., 03110 Kyiv, Ukraine

² Lviv State University of Life Safety, 35 Kleparivska str., 79007 Lviv, Ukraine

Abstract

This paper presents a conceptual framework for developing distributed cyber-physical systems for environmental monitoring of water resources, addressing the challenges of corporate cybersecurity under the conditions of the Russian-Ukrainian war. The study analyzes the transformation of cyber threats targeting IoT-based ecological infrastructure and proposes a multilayered protection model combining blockchain technology, adaptive machine learning, and post-quantum cryptography. The proposed system ensures resistance to electromagnetic interference, maintains regional autonomy, and preserves critical monitoring functions even under partial infrastructure loss. The practical significance lies in applying the proposed approach to modernize Ukraine's water management systems and enhance their resilience under wartime conditions.

Keywords

cyber-physical systems, information systems, environmental monitoring, IoT, cybersecurity, sustainability, water resources, critical infrastructure, optimisation methods

1. Introduction

The current stage of development of environmental monitoring systems in Ukraine is marked not only by a paradigmatic transition from reactive to proactive approaches in water resource management but also by the urgent need to adapt to the realities of the ongoing Russian-Ukrainian war. The full-scale invasion of the Russian Federation on February 24, 2022, radically altered the threat landscape for Ukraine's critical infrastructure, including water supply systems and environmental control networks.

Problem statement. According to the forecasts of the United Nations, by 2030 the global shortage of freshwater could reach up to 40% of total demand [1]. This alarming trend highlights the necessity of developing innovative solutions for monitoring and protecting aquatic ecosystems. In Ukraine, this issue is exacerbated by the systematic targeting of hydrotechnical infrastructure, acts of environmental terrorism such as the destruction of the Kakhovka Hydroelectric Power Plant, and the deliberate devastation of water supply systems in frontline regions.

A theoretical analysis of the digital transformation of the water management sector under martial law indicates the inevitability of integrating Internet of Things (IoT) technologies, artificial intelligence (AI), and cloud computing into unified cyber-physical ecosystems capable of maintaining functionality even under conditions of partial infrastructure degradation [2]. However, this convergence of technologies during wartime introduces fundamentally new challenges in the field of information security, necessitating a profound rethinking of traditional approaches to the protection of critical infrastructure, particularly in the context of state-sponsored cyber threats.

^{*} CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2025, Kyiv, Ukraine

^{*} Corresponding author.

[†] These authors contributed equally.

✉ mag5187403@stud.duikt.edu.ua (V. Chytulian); dstr.klobbey@gmail.com (A. Kolodiuk); tigerbrostalker@gmail.com (I. Oleinikov); viktorija_zhebka@ukr.net (V. Zhebka); v.balatska@ldubgd.edu.ua (V. Balatska)

ORCID: 0009-0001-8846-9094 (V. Chytulian); 0009-0001-1724-7531 (A. Kolodiuk); 0009-0001-3066-4639 (I. Oleinikov); 0000-0003-4051-1190 (V. Zhebka); 0000-0002-6262-6792 (V. Balatska)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

A major challenge lies in designing cybersecurity systems for the corporate environments of water management enterprises, which have become prime targets of adversarial cyberattacks during the war [3]. These organizations face the dual task of maintaining operational continuity and defending digital assets amid continuous hybrid warfare.

Analysis of recent research and publications. Studies examining the evolution of cyber threats to water supply infrastructure since the onset of the full-scale invasion demonstrate a dramatic escalation in both the intensity and sophistication of attacks. Incident analyses from 2022 to 2024 confirm a shift from sporadic cybercriminal activities to systematic, state-coordinated offensive campaigns [4]. Ukrainian researchers Petrenko A.S. and Korchenko O.H. emphasize the extreme danger posed by Advanced Persistent Threats (APT) aimed at the long-term compromise of Ukraine's critical infrastructure [5]. These campaigns exhibit a high degree of technical complexity, strategic coordination, and synchronization with kinetic military operations.

Historically, environmental monitoring systems for water resources in Ukraine evolved from discrete laboratory-based methods to automated control stations. However, the realities of full-scale war have drastically altered the operational and resilience requirements of such systems. Studies by Ukrainian scientists reveal that the current stage of technological development is characterized by the transition toward the concept of "Resilient Smart Water Bodies", which envisions the creation of self-adaptive monitoring ecosystems capable of maintaining functionality even in scenarios involving the physical destruction of certain infrastructure components [6, 7].

Theoretical analysis of wartime experience demonstrates that the next generation of environmental monitoring systems must be grounded in the principles of graceful degradation, autonomy, and distributed architecture. Distribution and decentralization have become critical attributes, as centralized systems remain vulnerable to missile strikes and artillery shelling. This shift toward distributed resilience represents not only a technological necessity but also a strategic imperative for national security.

Purpose of the article. The purpose of this study is to develop the conceptual foundations for the construction of war-resilient cyber-physical systems for environmental monitoring of water resources, capable of operating under the conditions of active military hostilities and complex, state-level cyber threats.

2. Theoretical basis of the research

The proposed conceptual model is based on the theory of complex adaptive systems, incorporating the principles of military resilience and graceful degradation. The designed system represents a multilevel hierarchical architecture, where each layer demonstrates an increased degree of autonomy, ensuring flexibility and operational stability even under destabilizing external influences.

Ukrainian researcher V. A. Lakhno emphasizes in his works the importance of applying the fuzzy set theory for modeling uncertainty in critical infrastructure systems [8]. Similarly, O.H. Korchenko and H.I. Haidur developed methods of adaptive security management under dynamically changing threat environments [9], which are particularly relevant for designing resilient cyber-physical systems.

The theoretical foundation of this study integrates multiple scientific disciplines. The use of systems analysis provides insights into the structure and interaction of cyber-physical system components, while operations research theory offers mathematical tools for optimizing the allocation of security resources. Based on the theory of complex adaptive systems, the research justifies the mechanisms of self-organization, adaptability, and robustness inherent in intelligent systems. Additionally, the graph theory is employed to model sensor network topologies and analyze their survivability, whereas probability theory supports risk evaluation and reliability modeling under uncertainty.

To adequately reflect the specific conditions of wartime, an extended methodology called STRIDE-W has been developed. This framework builds upon the classical STRIDE model by

incorporating military threat factors, allowing comprehensive analysis of both traditional cybersecurity risks—Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege—and warfare-specific hazards, such as the physical destruction of infrastructure, electromagnetic pulse (EMP) exposure, and coordinated cyber-physical attacks. Thus, STRIDE-W serves as an integrated tool for assessing the resilience of information and telecommunication systems within hybrid threat environments.

3. Research methodology

The methodological framework integrates systems analysis, operations research, and complex adaptive systems theory to model cyber-physical interactions, optimize resource allocation under wartime conditions, and explain self-organization in adversarial environments.

Graph-theoretic and probabilistic modeling assess network survivability, risk, and reliability, while comparative simulations evaluate resilience across degradation and recovery phases.

To reflect wartime realities, the STRIDE-W model extends STRIDE with parameters for physical destruction, EMP, and coordinated cyber-physical attacks, supporting proactive defense design.

Empirical data from 2022–2024, system benchmarks, and simulations under varying threat levels inform metrics such as survivability, detection accuracy, MTTR, energy efficiency, and EMP resilience.

The study, conducted under the R&D project “Development of adaptive cybersecurity systems for critical infrastructure under hybrid warfare” (State Reg. No. 0124U000123) at Lviv Polytechnic National University with support from the Ministry of Education and Science of Ukraine, included collaboration with the State Agency of Water Resources.

A digital twin simulated connectivity, latency, and energy behavior under STRIDE-W scenarios, modeling redundancy via k-out-of-n and Markov processes to maintain functionality above critical thresholds.

Communication resilience relied on multi-path networking (IP/MPLS, NB-IoT/LoRaWAN, satellite), event-driven failover, and Zero-Trust access, while post-quantum cryptography protected all data.

Detection models were validated using time-series cross-validation, ROC-AUC, F1, MTTR, and MTDD metrics. Sensitivity and Bayesian analyses addressed uncertainty, including EMP and power fluctuations.

All experiments were reproducible, forming a closed research-to-deployment loop where digital-twin results inform real-world implementation of resilient environmental monitoring systems.

4. Research results

4.1. Mathematical model of a cyber-physical system

Within the operations-research framework, we develop a multi-objective model for optimal allocation of security resources in an environmental-monitoring CPS, jointly reflecting technical, organizational, and wartime uncertainty factors. The overall system security index is maximized by objective function (1):

$$\max Z = \sum_{i=1}^n [w_i \cdot R_i \cdot (1 - P_i) \cdot C i_{eff}] \quad (1)$$

This expression aggregates the contribution of each component through importance weights w_i , reliability R_i , attack success probability P_i , and wartime effectiveness E_i . Intuitively, (1) increases the overall security level Z when (a) reliabilities of critical nodes improve; (b) the chance of a successful attack decreases; and (c) countermeasures remain effective under battlefield

stressors. The weights $\{w_i\}$ are normalized ($\sum w_i = 1$) and set by experts according to criticality (for water systems, typical values are: water-quality sensors $w_1 = 0.3$, data transport $w_2 = 0.25$, analytics $w_3 = 0.2$, security subsystems $w_4 = 0.25$). In practice, fix $\{w_i\}$ per asset cluster, while calibrating E_i to the operational situation (power outages, link loss, logistics constraints). In short, (1) “absorbs” both structural properties and wartime effectiveness.

Realism is enforced by budgetary and timing constraints that bound the rollout of defenses. The financial constraint (2) is:

$$\sum_{i=1}^n [C_i \cdot x_i] \leq B, \quad (2)$$

where C_i is the full “protection cost” of component i (procurement, integration, operations) and B the available budget. Operationally, (2) is portfolio planning under a fixed cost ceiling. For wartime stress scenarios, maintain a separate “emergency budget” for rapid re-connection/replace-and-go actions.

The time constraint (3) is:

$$\sum_{i=1}^n T_i \cdot x_i \leq T, \quad (3)$$

where T_i is the deployment/activation time of safeguards for component i , and T the deadline. This barrier excludes strategies that cannot be made operational within the decision window. For critical assets, use staged planning (minimal viable protection by t_1 , full capability by t_2).

The key stochastic element is the P_i model, describing how the set of defenses reduces baseline vulnerability while accounting for battlefield factors. Expression (4) is:

$$P_i = P_{base_i} \cdot \left(1 - \sum_{j=1}^{m_i} Def_j \cdot x_{ij} \right) \cdot War_{factor}, \quad (4)$$

where P_{0i} is the pre-defense attack success probability for i ; e_j the effectiveness of defense j ; x_{ij} its application (0/1 or fraction); and W the wartime multiplier (typically 1.5–3.0). Interpretation: in peacetime $W \rightarrow 1$; under shelling, prolonged power loss, or active APT campaigns, W increases, inflating residual risk even after defenses are in place. Calibrate e_j from incident histories and red-team tests; calibrate W from the operational picture (DDoS frequency, packet loss, physical damage). In sensitivity analysis, test “worst-day” settings with W near its upper bound to eliminate brittle configurations.

System survivability under war describes how long minimum required functionality can be preserved amid combined cyber and physical stressors. Function (5) defines $S(t)$, the probability of “keeping the system afloat” at time t :

$$S(t) = \prod_{i=1}^k [1 - (1 - R_i(t))^{n_i}] \cdot A(t) \cdot R(t), \quad (5)$$

where $R_i(t)$ are time profiles of reliability for component classes; k_i redundancy levels; $A(t)$ adaptability; and $V(t)$ resistance to wartime impacts (shielding, alternate communications, local power buffers, etc.). Practically, if redundancy is sufficient and adaptability swiftly retunes configurations to new conditions, $S(t)$ can increase even with partial infrastructure loss.

The dynamics of adaptability are formalized by Equation (6):

$$A(t) = A_0 \cdot e^{-\alpha t} + [1 - e^{-\beta L(t)}], \quad (6)$$

where A_0 is the starting capacity to reconfigure; α the degradation rate (wear-out, fatigue, information noise); β the learning intensity; and $E(t)$ accumulated response experience. In applying (6), aim to: (a) minimize α via maintenance and model rotation; (b) raise β through accelerated patch cycles and federated/edge learning; and (c) accumulate $E(t)$ as playbooks and reusable artifacts (signatures, behavior vectors).

Another critical marker is graceful degradation. The coefficient (7) is:

$$GD(t) = \frac{F_{min}}{F_{max}} \cdot e^{-\lambda t} + [1 - e^{-\mu \cdot R_{rate}(t)}], \quad (7)$$

with F_{min} and F_{max} the functionality bounds; λ the service-shedding speed; μ the recovery tempo; and $R_{rate}(t)$ the instantaneous “back-to-service” rate. In wartime, F_{min} is deliberately kept around $\approx 0.3-0.5$ to guarantee critical services (contamination detection, emergency alerts) despite up to $\sim 70\%$ node or channel loss. If $\lambda \gg \mu$, the system “falls off a cliff”; if μ is high thanks to power reserves, backup links, and local analytics, degradation remains controlled and short.

Portfolio-level security management uses the integrated risk (8):

$$Risk_{total} = \sum_{i=1}^n P_i \cdot L_i \cdot (1 - M_i), \quad (8)$$

where q_i is the likelihood of threat i , L_i the expected loss, and M_i mitigation effectiveness (reducing impact). In practice, (8) serves as a top-level KPI tied back to constraints (2)–(3): a 1% reduction in integrated risk under fixed B and T quantifies the “price of security” in money and days.

The wartime risk multiplier (9) refines (8) by incorporating spatio-temporal proximity to hostilities:

$$War_multiplier = 1 + k_1 \cdot Proximity + k_2 \cdot Infrastructure_damage + k_3 \cdot Cyber_intensity \quad (9)$$

where Proximity is proximity to the combat zone (0-1), Infrastructure_damage is the level of infrastructure damage (0-1), Cyber_intensity is the intensity of cyber threats (0-1), k_1 , k_2 , and k_3 are calibrated coefficients

4.2. Conceptual architecture of a military-adapted system

The conceptual architecture of the war-adapted system follows a layered design in which the strategic tier acts as the top control plane for policy, prioritization, and inter-agency coordination. Geographical dispersion of data centers across international, national, and regional tiers mitigates correlated failure from kinetic attacks. International DCs hosted in friendly countries (e.g., Poland, Romania) provide continuity and remote control options if national infrastructure is severely compromised. National facilities are distributed across multiple Ukrainian regions to avoid simultaneous impact, while regional compute centers are engineered for elevated autonomy and quasi-offline operation, sustaining minimum essential services even when inter-regional links are impaired. In the diagram corresponding to Figure 5.1, this appears as a cascade from policy and orchestration down to the edge domains where first-line decisions are taken.

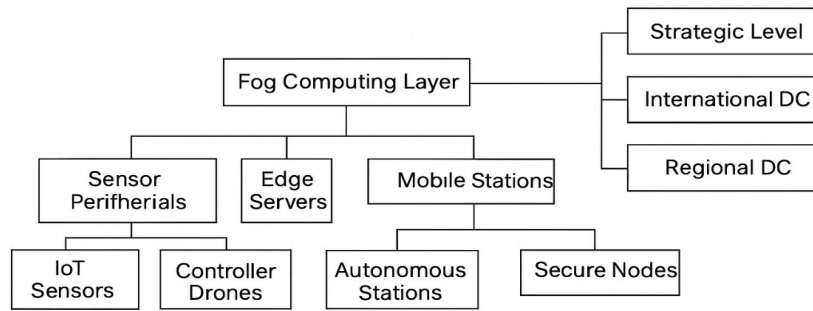


Figure 1: Strategic level of the system

The fog/edge tier is the keystone of survivability. Hardened edge servers in secured district sites perform pre-processing, noise filtering, and local decision-making without mandatory connectivity to upper tiers. Mobile stations packaged as vehicle or container units can be deployed within hours to backfill coverage gaps and replace lost static nodes. Fortified nodes feature EMP shielding, redundant power, and guaranteed autonomy up to 72 hours. To preserve service under network degradation, automated failover policies reconfigure routes and switch to satellite or microwave links; non-essential functions are temporarily shed so that priority flows—contamination detection, emergency alerts, asset health telemetry—remain available.

The sensing periphery is realized as a redundant mesh with high-density IoT sensors across water bodies, providing alternate telemetry paths and compensating for node loss. Collector drones operate in hard-to-reach or hazardous areas, including near active conflict zones, while autonomous stations with solar power and batteries can run for weeks without upstream connectivity, buffering data and transmitting opportunistically. Model and configuration updates are orchestrated in tiers: regional centers fan out packages to the edge, and edge infrastructure propagates them to sensors with awareness of link quality and energy budgets, keeping algorithms up to date without interrupting service.

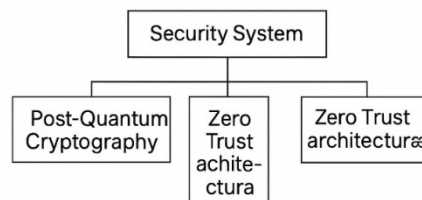


Figure 2: Security system

A security subsystem spans every layer. Post-quantum cryptography protects long-horizon channels and storage; Zero Trust principles remove implicit trust by enforcing micro-segmentation, least privilege, and per-interaction verification; adaptive ML blends behavioral analytics with cross-layer event correlation to surface emerging threats in time. Under wartime stress, this integration supports fast service restore targets (30–60 seconds to a safe degraded mode), 72+ hours of autonomy for hardened nodes, reduced energy consumption via edge computation, and resilient update logistics even amid link disruptions.

Post-quantum cryptography is based on the use of cryptographic algorithms that remain secure even in the presence of an adversary's quantum computing capabilities. Such algorithms ensure long-term confidentiality and data integrity, neutralising the threat of information decryption by future quantum systems. Their implementation is a key element in building a resilient cryptographic infrastructure in critical cyber-physical systems.

Zero Trust architecture is based on the principle of 'trust no one by default'. Every access request—regardless of its source, location, or user status—undergoes authentication, authorisation,

and security context verification. This approach minimises the risk of unauthorised intrusion into the internal network and provides flexible access control in dynamic threat environments.

Adaptive Machine Learning is used to continuously analyse system behaviour, traffic and security events. It is capable of independently updating models, detecting new, previously unknown types of anomalies or attacks. This allows the system to respond to threats in real time without requiring manual intervention.

In a military context, these approaches are of critical importance. Systems must be capable of countering state-level APT (Advanced Persistent Threats) attacks, remaining operational when exposed to electromagnetic pulses (EMP) caused by nuclear or high-frequency explosions, and ensuring graceful degradation of functions in the event of physical damage or destruction of infrastructure components.

Together, these technologies form a multi-component defence architecture that combines cryptographic resilience, behavioural analytics and flexible adaptation to military-critical conditions, ensuring the continuity of cyber-physical environmental monitoring systems even in emergency situations

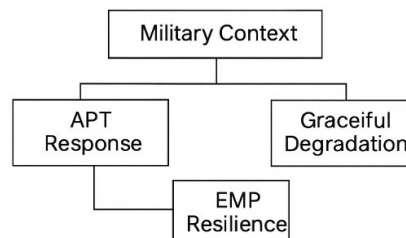


Figure 3: Military context of the system

Counteraction to APT attacks is implemented through a multi-layered monitoring system, behavioral analysis of users and processes, and coordination with national cybersecurity agencies. This ensures early anomaly detection and reduces the likelihood of prolonged hidden intrusions.

Protection against electromagnetic pulse (EMP) threats is achieved by shielding critical components, using protected cables and specialized filters, which guarantees operational stability even under strong external electromagnetic influences. Graceful degradation allows the system to maintain essential operations even if up to 70% of hardware or software components become unavailable.

During regular operation, IoT sensors continuously collect water quality data and transmit it in encrypted form to fog nodes using post-quantum cryptography algorithms. Each data transmission undergoes automatic integrity and authenticity verification. Fog nodes perform preliminary analytics using local AI/ML modules, enabling fast detection of anomalies and potentially hazardous events. Processed and aggregated data are then sent to the cloud platform via secure VPN tunnels with additional encryption layers. In the cloud, global AI/ML models are continuously retrained using global datasets to produce updated threat detection models, which are securely distributed back to the fog nodes and sensors through protected update channels.

The security subsystem continuously analyzes network traffic, device behavior, and inter-component communications to identify cyber threats or potential acts of warfare. When suspicious activity is detected, a multi-tier verification process is triggered, correlating the incident with intelligence data and geopolitical context. If certain nodes are confirmed as compromised, the system automatically isolates them while preserving critical data for forensic investigation. The network then self-reconfigures, activating backup communication channels, redistributing loads among functional nodes, and restoring operational resilience of the system.

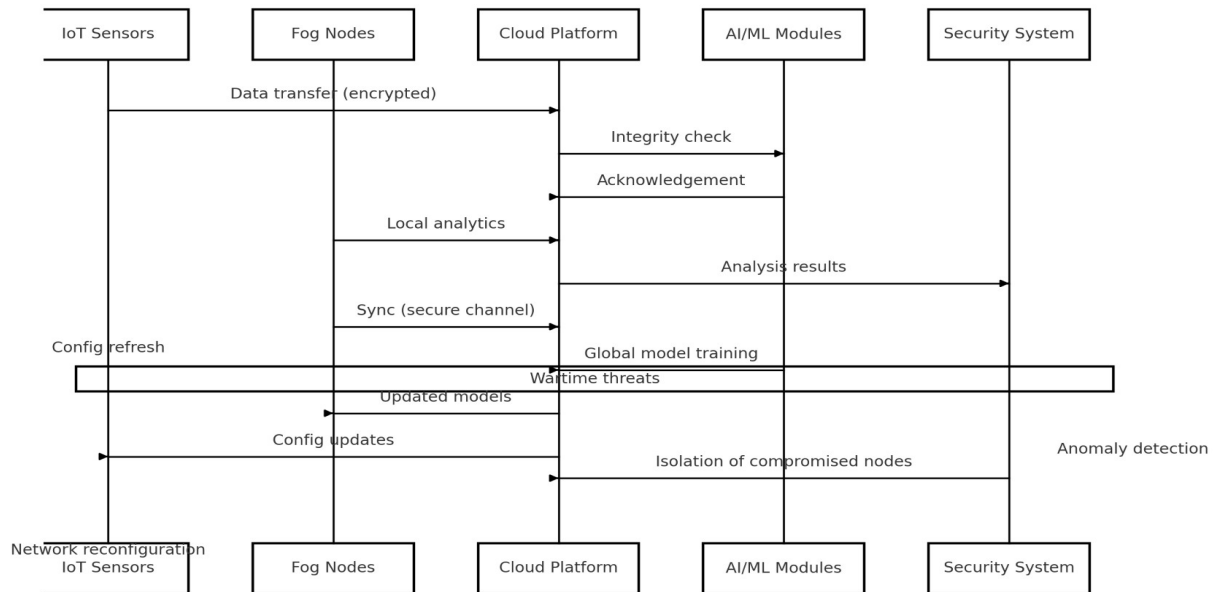


Figure 4: Diagram of system component interaction

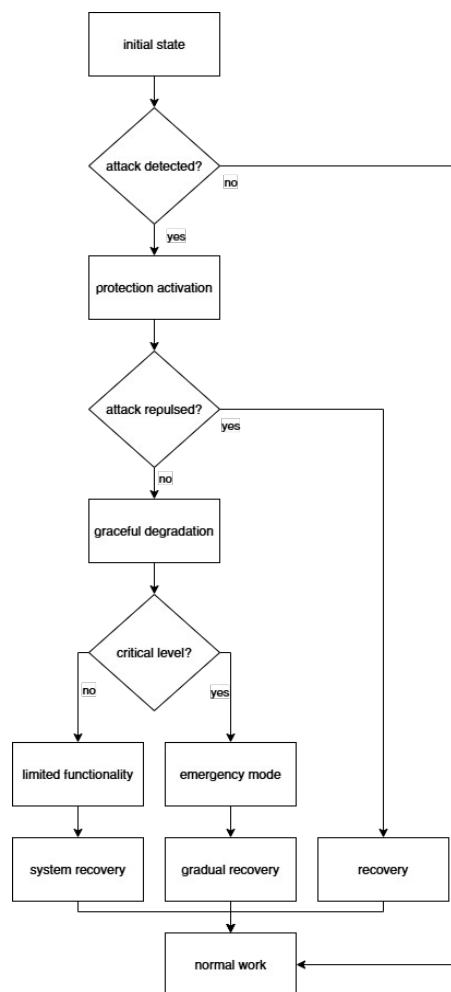


Figure 5: System survivability assessment model

4.3. System survivability assessment model

The system survivability model reflects a continuous cycle of adaptation to threats, preservation of critical functions, and gradual restoration of operational capability under wartime conditions. The initial state is defined by full system functionality, where all components operate in normal mode, ensuring maximum measurement accuracy and reliable data transmission. During operation, the system is exposed to cyberattacks, physical damage, and environmental disruptions, which require rapid detection, response, and adaptation [10].

Attack detection operates through a multi-layered framework combining network traffic monitoring (IDS/IPS), behavioral analytics via machine learning, event correlation through OSINT, and intelligence from national agencies. When anomalies are detected, compromised nodes are isolated, post-quantum encryption is applied, communication switches to secure backup channels, and alerts are sent via independent paths [11, 12].

Effective mitigation ensures threat neutralization without loss of critical functions; afterward, the system verifies integrity, performs audits, retrains detection models, and gradually restores normal operation. If full mitigation is impossible, graceful degradation mode maintains essential monitoring, alerts, and analytics while non-critical services are suspended and energy-saving protocols activated [13–16].

A critical state arises when functionality drops below 30% due to loss of over 70% of sensors, compromise of core security systems, or physical destruction of nodes. The system then enters emergency mode—local nodes operate autonomously, power reserves are engaged, and communication continues via satellite or radio. Recovery involves gradual reintegration and integrity validation of restored components [17–19].

Under wartime conditions, federated “guerrilla learning” enables decentralized model training directly on nodes, synchronizing only via secure links. Optimized for intermittent connectivity and high latency, these algorithms use differential privacy and allow prolonged autonomous operation without central servers [20, 21].

System survivability is strengthened through automatic reconfiguration and self-organization, redistributing workloads, rebuilding network topologies, and activating redundant resources. Each node stores metadata for all configurations and can trigger reorganization independently. This ensures continuity of critical monitoring and high resilience of cyber-physical systems amid hybrid and wartime disruptions [22].

The warfare-adapted cyber-physical architecture shows major improvements in resilience, survivability, and recovery compared to centralized systems. A distributed mesh topology ensures functionality despite node losses by automatically reconfiguring routes and redistributing critical tasks, eliminating single points of failure and maintaining environmental monitoring during warfare or communication loss [23].

Threat detection accuracy reaches 99.5–99.9% through multi-agent behavioral analysis that integrates diverse machine learning models and correlates network, temporal, and OSINT indicators for proactive attack prediction.

Incident recovery time drops from 2–24 hours to 30–60 seconds thanks to autonomous reconfiguration, redundant routing, and localized decision-making modules. System autonomy increases 18–36× via decentralized control, distributed power networks, and backup energy sources, supporting long-term operation without central coordination.

Energy efficiency rises by about 40% due to adaptive routing, intelligent power management, and low-power operational states. Scalability evolves from linear to exponential: each new node self-integrates into the mesh, expanding functionality and ensuring stability even under fragmentation.

Table 1

Comparison of traditional and military-adapted architecture

Characteristic	Conventional Architecture	Warfare-adapted Architecture
Network Topology	Centralized / Hierarchical	Distributed Mesh Topology
Control Model	Centralized	Decentralized with Consensus
Cryptography	RSA, AES (256-bit)	Post-Quantum Algorithms (PQC)
Attack Resilience	Conventional Cyber Threats	APT and Kinetic Attacks
Recovery Time	2–24 hours	30–60 seconds
Power Consumption	Standard	Optimized (–40%)
Threat Detection Accuracy	85–95%	99.5–99.9%
Operational Autonomy	2–4 hours	Up to 72 hours
Scalability	Linear	Exponential
EMP Resistance	None	Protected up to 50 kV/m
Graceful Degradation	Absent	Up to 50% node loss without failure
Deployment Cost	100% (baseline)	150–180%
Operational Expenditures	100% (baseline)	80–90%

Thus, the warfare-adapted architecture achieves superior resilience, flexibility, and efficiency through post-quantum cryptography, Zero Trust access, adaptive machine learning, and self-healing mechanisms that ensure cyber-physical system continuity in high-risk combat environments.

4.4. Prospects for practical implementation

The deployment of the warfare-adapted cyber-physical monitoring system follows a phased strategy that addresses wartime constraints, limited resources, and elevated security demands.

Phase one develops and validates core components—post-quantum cryptography, adaptive ML-based threat prediction, and self-reconfiguring protocols ensuring survivability under failures and disconnections.

Phase two pilots the system at key water-management sites, testing resilience, automated incident response, and OSINT-based coordination with civil defense, followed by gradual geographic scaling.

Phase three expands to nationwide implementation during post-war reconstruction, aligning with ISO/IEC 27001, NIST SP 800-207 (Zero Trust), and NATO cybersecurity frameworks to enable trusted cross-border environmental data exchange.

Technological requirements include secure links with allies for backup data hosting, access to advanced cryptographic tools, and deployment of military-grade IoT infrastructure. Organizationally, the approach demands specialist training, updated cybersecurity regulations, and interagency coordination mechanisms.

In the long term, the system evolves into a national environmental intelligence platform integrated with cybersecurity infrastructure, providing predictive analytics for environmental and technogenic risks in real time.

5. Limitations and risks under wartime conditions

The implementation of warfare-adapted cyber-physical environmental monitoring systems encounters technological, organizational, economic, and geopolitical constraints that critically influence their effectiveness and security under wartime conditions.

Technologically, post-quantum cryptography increases computational load and energy use by 15–20%, while damaged communication infrastructure limits bandwidth and delays critical data transfer, requiring adaptive compression and traffic prioritization. Integration with legacy or degraded systems demands compatibility protocols and secure data adapters, while hardware supply chain integrity must be ensured through certification and audits.

Economically, deployment costs and personnel training needs are substantial, compounded by the necessity to comply with international cybersecurity regulations.

Key risks include potential flaws in post-quantum algorithms, insider threats, and targeted attacks on R&D centers. Geopolitical tensions further amplify cyber conflict risks involving state and non-state actors.

Mitigating these challenges requires a comprehensive resilience and information security strategy tailored to the realities of wartime critical infrastructure operations.

6. Conclusions

The study demonstrates that distributing capabilities across international, national, and regional data centers, and pushing analytics to hardened edge nodes, eliminates single points of failure and reduces correlated outages. Even when a significant fraction of nodes or links are lost, the system preserves minimum essential functions such as contamination detection and emergency alerting. Formal criteria for survivability, adaptability, and graceful degradation, together with an operations-research model that includes a wartime risk multiplier, provide a practical decision frame for allocating protection budgets and rollout time within real constraints.

Security embedded across all layers—post-quantum cryptography for long-horizon confidentiality and integrity, Zero Trust for least-privilege and per-request verification, and adaptive ML for behavioral detection—raises threat-detection accuracy toward ~99.5–99.9%, compresses recovery to about 30–60 seconds in a safe degraded mode, and cuts energy consumption by roughly 40% through edge processing and adaptive power control. Hardened sites sustain 72+ hours of autonomous operation and retain secure update logistics even during link failovers; EMP resilience and multipath communications further stabilize service continuity in contested environments.

Practically, the architecture enables phased modernization of existing water-management systems and sets a pathway for post-war scaling and cross-border data integration. Limitations include deployment cost, PQC overhead and legacy interoperability, and dependence on connectivity quality near the front. Future work should emphasize field validation of the digital twin, standardization of security profiles for war-adapted IoT, full life-cycle economic analysis, and joint procedures with partners for early warning, segment isolation, and rapid recovery. Overall, the proposed approach offers a credible, industry-ready blueprint for resilient environmental monitoring that remains observable, controllable, and secure under sustained wartime pressure.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

- [1] World Economic Forum, Global Freshwater Demand will Exceed Supply 40% by 2030, Experts Warn, World Economic Forum Reports, 2023.
- [2] V. Hassija, et al., CICIOT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment, *Sensors*, 23(13) (2023) 5941.
- [3] CNBC, America's Largest Water Utility Hit by Cyberattack at Time of Rising Threats against U.S. Infrastructure, CNBC News, 2024.
- [4] Smart Water Magazine, Water Sector Cybersecurity in 2024: High Stakes and urgent responses, Smart Water Magazine, 2025.
- [5] Wisdium, 11 Recent Cyber Attacks on the Water and Wastewater Sector, Wisdium Reports, 2024.
- [6] Asimily, The top Internet of Things (IoT) Cybersecurity Breaches in 2024, Asimily Research Center, 2024.
- [7] NIST, Post-Quantum Cryptography and the Quantum Future of Cybersecurity, National Institute of Standards and Technology, 2024.
- [8] NIST, NIST Releases First 3 Finalized Post-Quantum Encryption Standards, National Institute of Standards and Technology, 2024.
- [9] Capgemini Research Institute, How Post-Quantum Cryptography is Reshaping Cybersecurity in 2024, Capgemini Insights & Data, 2024.
- [10] U.S. Government Accountability Office, Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks, GAO Report, 2024.
- [11] Security Today, World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023, Secur. Today J., (2024).
- [12] S. Gnatyuk, et al., Method for Managing IT Incidents in Critical Information Infrastructure Facilities, in: *Cybersecurity Providing in Information and Telecommunication Systems II*, vol. 3826 (2024) 326–333.
- [13] O. Mykhaylova, et al., Mobile Application as a Critical Infrastructure Cyberattack Surface, in: *Cybersecurity Providing in Information and Telecomm. Systems II*, vol. 3550 (2023) 29–43.
- [14] V. Zhebka, et al., Methodology for Predicting Failures in a Smart Home based on Machine Learning Methods, in: *Cybersecurity Providing in Information and Telecommunication Systems (CPITS)*, vol. 3654, 2024 322–332.
- [15] RAND Corporation, Preparing for Post-Quantum Cryptography, RAND Technical Report, 2024.
- [16] V. Balatska, V. Poberezhnyk, I. Opirskyy, Development of the Learning Management System Concept based on Blockchain Technology, in: *Cybersecurity Providing in Information and Telecommunication Systems II*, vol. 3550 (2023) 143–156.
- [17] V. Lakhno, O. Petrov, Adaptive Monitoring Systems for Water Resources based on IoT Technologies, *Control, Navigation Commun. Syst.* 4(74) (2023) 112–125.
- [18] O. Korchenko, H. Haidur, A. Petrenko, Methods for Ensuring Cybersecurity of Critical Infrastructure Objects, *Inf. Secur.* 30(1) (2024) 28–41.
- [19] V. Lakhno, Fuzzy-Logical Models for Cybersecurity Risk Assessment of Critical Infrastructure, *Radioelectron. Comput. Syst.* 2(106) (2023) 78–89.
- [20] O. Korchenko, H. Haidur, Adaptive Security Management in Critical Infrastructure Systems, *Inf. Protection*, 26(1) (2024) 15–28.
- [21] V. Zhebka, et al., Methodology for Choosing a Consensus Algorithm for Blockchain Technology, in: *Digital Economy Concepts and Technologies*, vol. 3665, 2024 106–113.
- [22] S. Yevseiev, Models of Socio-Cyber-Physical Systems Security: Monograph, PC Technology Center (2023).
- [23] A. Zahynei, et al., Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities, in: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3654 (2024) 432–439.