

Digital Trust and Cyber Resilience: From Technical Protection to Institutional Responsibility

Catalin VRABIE | Editor-in-Chief | SNSPA, Bucharest, Romania

Patrycja KRAUZE-MAŚLANKOWSKA | Guest Editor | University of Gdańsk, Poland

The promise of a smart city is often expressed through speed, integration and prediction: services that respond faster, infrastructures that exchange information, and algorithms that anticipate disruption. Yet increasing connectivity also multiplies dependencies. A vulnerability in a public-facing application, a compromised information environment, a poorly governed automated decision or a disruption in a supply chain can extend well beyond its original technical setting. The decisive question is therefore not simply how intelligent a system becomes, but whether its institutions can understand its risks, sustain essential functions, explain decisions and preserve public confidence when conditions deteriorate. This is the central concern of Digital Trust and Cyber Resilience, the Special Issue of Volume 10 of the Smart Cities and Regional Development (SCRD) Journal.

The seven contributions assembled here approach that concern from distinct methodological and geographical perspectives: application security, disinformation and crisis governance, Industry 4.0, Ukrainian cybersecurity policy, multimodal urban mobility, public-sector integrity, and agro-industrial logistics. Their diversity is instructive. Cyber resilience is not one product or one policy domain. It emerges when technical controls, organizational preparedness, institutional accountability and adaptive operational decisions reinforce one another. The papers also reveal an important limit of the smart-city vocabulary: efficiency may be observable under routine conditions while resilience remains untested until systems experience strain.

Securing services and preserving trust

The issue opens with Dolantina Hyka, Festim Kodra and Daniel Çika, whose study of advanced penetration testing treats web application security as a continuing cycle of reconnaissance, verification, impact assessment, remediation and retesting [1]. Its key editorial contribution is the insistence that an automated alert is not yet evidence of an exploitable vulnerability: technical claims require validation and must be translated into priorities that service owners can act upon. The authors present a qualitative testing framework, rather than a reproducible quantitative benchmark, a distinction worth retaining when assessing the scope of their conclusions. This argument extends Christian Schachtner's discussion of Business Continuity Management in public institutions [2] and complements Pooya Teimoory's examination of threats and protective strategies in smart-payment infrastructures [3]. Together, these studies suggest that secure coding and testing matter most when connected to continuity planning, operational responsibility and citizen-facing service reliability.

Security also depends on the integrity of the information through which public institutions explain what is happening. Agnieszka Rogozińska's analysis of cyber governance, disinformation and digital trust in the context of Ukraine in 2022 shifts attention from systems to the relationship between institutions and society [4]. Based on a qualitative examination of published sources, the article argues that cyber incidents and information manipulation can reinforce one another, making institutional coordination and credible strategic communication essential to crisis response. Its concerns resonate with Svitlana Bulbeniuk's work on resilience, citizenship skills and smart education in Ukrainian universities [5]. They also intersect with research on smart borders and digital corridors in the Romania–Moldova–Ukraine area, where interoperable information systems are presented as important to security and cross-border coordination [6]. Read together, these

contributions underline that trust is not an accessory to cybersecurity; it shapes whether people can interpret, use and rely on information during disruption.

Governing automation and crisis capacity

The connection between resilience and responsibility becomes particularly visible in Sonia García-Moreno's examination of cyber-resilient Industry 4.0 [7]. Connected industrial and urban infrastructures may improve monitoring and productivity, but their reliance on networked components also creates new failure pathways. The paper adds an algorithmic dimension: decisions can be fast and consistent while remaining opaque, biased or difficult to contest. This brings industrial systems into the wider debate over governance of artificial intelligence. Guy Waizel's agentic-AI security adoption matrix [8] shows why adoption readiness cannot be separated from oversight requirements and domain-specific risks, while Raed Mohammed Benshams emphasizes organizational culture as a precondition for responsible AI integration [9]. The shared lesson is that technical sophistication neither guarantees institutional readiness nor substitutes for human accountability.

Vira Haponenko's contribution on cybersecurity public policy in Ukraine [10] offers a related but institutionally focused argument. Examining wartime policy responses and cooperation among governmental, private and civic actors, the article identifies partnerships and cybersecurity networks as mechanisms through which expertise and resources may be mobilized under pressure. This perspective connects with Nataliia Fedirko's analysis of smart governance and Ukraine's macroeconomic recovery, which highlights both the promise of digital public systems and problems of inter-system integration [11]. It also complements Haponenko's earlier SCRD study of civil institutions and sustainable development in Ukraine [12]. These papers should not be read as proof that digital instruments alone produce national resilience. Rather, they invite investigation of the conditions under which institutional coordination, civic participation and technological capacity become mutually supportive.

Intelligent infrastructures beyond the city centre

Two papers widen the scope from cybersecurity governance to the operational intelligence of interconnected systems. Boban Davidovic and Slobodan Djordjevic examine AI-based anomaly detection across multimodal mobility streams, drawing on publicly available Norwegian transport data [13]. By integrating different transport sources and applying unsupervised methods, their study explores how unusual patterns and disruptions may be identified for operational monitoring. Such signals, however, are not self-explanatory: anomalies require contextual interpretation before they justify intervention. Mahdi Ghandehari's framework for smart transportation in Mashhad [14] and Tibor László Buskó's analysis of smart, sustainable mobility in Hungarian urban policy [15] provide useful complements. They remind us that mobility intelligence becomes public value only when analytics meet coherent planning, organizational coordination and locally defensible objectives.

Marianna Szabóné Gál's comparative analysis of public integrity and cyber resilience across Denmark, Finland, Estonia, Hungary, Romania and Bulgaria brings institutional variation into sharper focus [16]. The paper considers cybersecurity readiness alongside procurement risk, transparency and governance indicators, arguing that formal cyber capacity may coexist with vulnerabilities in supplier oversight and public accountability. These are comparative associations and risk signals, not in themselves causal proof of the effect of corruption or procurement arrangements on cyber incidents. The contribution is nonetheless important: trust requires that digital infrastructures be governed through transparent decisions, credible audit trails and responsibilities that survive procurement cycles. Dali Sologashvili and Tatia Udesiani's earlier SCRD work on digital accounting and financial audit [17], together with Monika Namysłowska and Aleksandra Olbryk's study of algorithmic smart

governance in Łódź [18], offer complementary perspectives on the legal, financial and administrative instruments needed to make technological systems accountable.

The final paper, by Corneliu Iațco, takes the discussion into regional agro-industrial logistics [19]. Its proposed architecture combines Drum-Buffer-Rope logic, rolling-horizon optimization and mixed-integer linear programming to synchronize the uncertainties of harvesting and transportation with continuous processing demand. The manuscript reports analysis of an eleven-year industrial dataset and rapid computational performance in the tested scenarios, illustrating a potential route from digital-twin concepts to operational decision support. The comparison with Frida Zisko and Besjana Mema's MIS-Digital Twin framework for urban resilience [20] is especially productive: both treat simulation as useful when connected to managerial choices rather than isolated dashboards. Nissrine Khouna, Kaoutar Hablatou and Mostapha Amri's research on ICT-enabled hospital logistics [21] shows a parallel concern with coordination and resource flows in a different service domain. The sectors differ, but the governing problem recurs: how to adapt decisions to changing constraints without sacrificing continuity, traceability or the quality of outcomes.

A research and policy agenda

Across the contributions, three requirements recur. First, resilience must be observable through service continuity, recovery, verified security findings and operational performance, rather than inferred from the purchase of technologies. Second, trust must be institutionally earned through transparent procedures, communicable evidence, meaningful oversight and the ability to challenge automated or administrative decisions. Third, digital intelligence must remain adaptive: mobility anomalies, cyber alerts and shifting logistical bottlenecks are inputs to judgment, not substitutes for it. These principles join otherwise different research designs into a shared agenda for smart cities and regions.

Several questions remain open. How can studies of cyber governance move from plausible associations to evidence about mechanisms and outcomes? What common indicators would make resilience comparable across municipalities without overlooking their very different capacities? How should public organizations evaluate the trade-offs among automation, cost, fairness and the human ability to contest a decision? And how can algorithmic tools be assessed after deployment, when institutional routines and citizen behaviour begin to change in response to the technology itself? Addressing these questions will require reproducible technical evidence, careful comparative research, longitudinal assessment and genuine dialogue among engineers, administrators, citizens and policymakers.

The articles in this Special Issue do not offer a single model of the secure or resilient smart city, nor should they. They instead help redefine the standard against which digital transformation should be judged. A system is not resilient merely because it is connected, nor trustworthy merely because it is automated. It becomes worthy of public reliance when vulnerabilities are identified, responsibilities are clear, disruptions are managed, and institutional decisions remain open to scrutiny. We hope that this collection contributes to a more demanding understanding of smart development—one in which innovation strengthens the capacity of cities and regions to serve people reliably, fairly and under conditions of uncertainty.

References

- [1] D. Hyka, F. Kodra, and D. Çika, "Enhanced web application security through advanced penetration testing techniques," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, Special Issue, 2026.
- [2] C. Schachtner, "On the way to resilient information security management: Business Continuity Management (BCM) for public institutions," *Smart Cities and Regional Development (SCRD) Journal*, vol. 9, no. 1, pp. 7–15, 2025, doi: 10.25019/dq18x683.

- [3] P. Teimoory, "Towards robust security in smart payment systems: challenges and solutions," *Smart Cities and Regional Development (SCRD) Journal*, vol. 9, no. 3, pp. 29–38, 2025, doi: 10.25019/zp8nva19.
- [4] A. Rogozińska, "Cyber governance, disinformation and digital trust: lessons from the 2022 Ukraine case study," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, Special Issue, 2026.
- [5] S. Bulbeniuk, "Formal and informal smart education in the university space through the prism of developing resilience and citizenship skills," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, no. 2, pp. 85–90, 2026, doi: 10.25019/kqwbb994.
- [6] C. Vrabie, S. Serdyuk, A. Babin, and H. Bulgar, "Smart borders and digital corridors for ensuring security in NATO-oriented border areas: the Romania–Moldova–Ukraine case," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, no. 3, pp. 87–105, 2026, doi: 10.25019/nj61kj27.
- [7] S. García-Moreno, "Cyber-resilient Industry 4.0: digital system failures, algorithmic bias and governance challenges for sustainable smart cities," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, Special Issue, 2026.
- [8] G. Waizel, "The agentic AI security adoption matrix: Understanding readiness and resistance across domains," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, no. 2, pp. 75–84, 2026, doi: 10.25019/hccxvf87.
- [9] R. M. Benshams, "Cultivating organizational culture for AI integration: A framework for Smart Cities and Regional Development," *Smart Cities and Regional Development (SCRD) Journal*, vol. 9, no. 4, pp. 125–137, 2025, doi: 10.25019/cmstt369.
- [10] V. Haponenko, "Public policy of cybersecurity in Ukraine," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, Special Issue, 2026.
- [11] N. Fedirko, "Leveraging smart governance for Ukraine's macroeconomic recovery and stabilisation," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, no. 1, pp. 109–128, 2026, doi: 10.25019/hpnjsx94.
- [12] V. Haponenko, "Capacity of civil institutions of sustainable development in Ukraine," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, no. 3, pp. 107–118, 2026, doi: 10.25019/x2yjxv52.
- [13] B. Davidovic and S. Djordjevic, "AI-based anomaly detection in multimodal urban mobility data streams," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, Special Issue, 2026.
- [14] M. Ghandehari, "Driven urban development in Mashhad: A strategic framework for smart transportation systems," *Smart Cities and Regional Development (SCRD) Journal*, vol. 9, no. 4, pp. 65–76, 2025, doi: 10.25019/e93th449.
- [15] T. L. Buskó, "Smart, sustainable mobility in the Hungarian urban development discourse," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, no. 1, pp. 87–107, 2026, doi: 10.25019/qre5x555.
- [16] M. Szabóné Gál, "Beyond firewalls: public integrity and cyber resilience in European smart city governance," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, Special Issue, 2026.
- [17] D. Sologashvili and T. Udesiani, "Digital accounting and financial audit as the foundation of smart governance," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, no. 3, pp. 67–73, 2026, doi: 10.25019/cqh8hn11.
- [18] M. Namysłowska and A. Olbryk, "Smart governance in Poland: The case study of the city of Łódź," *Smart Cities and Regional Development (SCRD) Journal*, vol. 9, no. 3, pp. 81–97, 2025, doi: 10.25019/y3xw2e27.
- [19] C. Iațco, "Drum-Buffer-Rope and rolling horizon MILP for shifting bottleneck synchronization in sugar beet logistics," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, Special Issue, 2026.
- [20] F. Zisko and B. Mema, "Digital twins and MIS integration for urban resilience: A strategic approach to smart city evolution," *Smart Cities and Regional Development (SCRD) Journal*, vol. 10, no. 2, pp. 35–50, 2026, doi: 10.25019/6df15r93.
- [21] N. Khouna, K. Hablatou, and M. Amri, "The role of ICT in Moroccan smart cities: towards innovative hospital logistics," *Smart Cities and Regional Development (SCRD) Journal*, vol. 9, no. 3, pp. 7–17, 2025, doi: 10.25019/549yh549.