Editorial: Building Cyber-Resilient Intelligent Cities

The 7th International Conference on Machine Intelligence & Security for Smart Cities (TRUST 2026)

Catalin VRABIE, Conference Chair

National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania

Jacek MAŚLANKOWSKI, Guest Editor

University of Gdańsk, Poland

Attila BARTA, Guest Editor

University of Debrecen, Hungary

The seventh edition of the International Conference on Machine Intelligence & Security for Smart Cities (TRUST 2026), organized in Bucharest on 15–16 June 2026 under the theme "Building Cyber-Resilient Intelligent Cities," brought together an interdisciplinary community concerned with the opportunities and risks created by artificial intelligence, connected infrastructures, data-intensive governance, and rapidly evolving cyber threats. This editorial introduces the intellectual architecture of the proceedings and situates the included contributions within five mutually reinforcing domains: AI-enabled cybersecurity and critical-infrastructure resilience; trustworthy, explainable, and socially legitimate AI; secure interoperability and data governance; intelligent public services and sectoral applications; and human, institutional, and educational capacity. Taken together, the papers demonstrate that cyber-resilience cannot be reduced to defensive technology. It is a governance capability that must combine technical robustness, institutional accountability, human oversight, legal compliance, social inclusion, and the capacity to recover and learn. The volume therefore reflects the central premise of TRUST: intelligent cities become sustainable only when trust is deliberately designed, continuously tested, and institutionally defended.

1. From Smartness to Trustworthiness

The seventh edition of TRUST was convened at a moment when the language of the smart city is undergoing an important correction. For more than two decades, urban intelligence was frequently presented through the vocabulary of connectivity, optimization, automation, and data abundance. These remain important ambitions, but – in these times of multiple crisis – they are no longer sufficient. A city may be highly connected and still be fragile; it may automate services while obscuring accountability; it may accumulate data while weakening privacy; and it may deploy artificial intelligence without securing the legitimacy of the decisions that follow. The defining question is therefore no longer simply whether cities can become smarter, but whether their intelligence can remain interoperable [1], secure, explainable, equitable, governable, and worthy of public confidence.

This concern shaped the conference theme, "Building Cyber-Resilient Intelligent Cities." TRUST 2026 approached cyber-resilience as a mandate shared by engineers, public administrators, policy makers, researchers, educators, and practitioners. The event brought together approximately 94 participants from 17 countries and 63 institutions, reflecting a genuinely international conversation. Its hybrid format connected the SNSPA campus in Bucharest with contributors from Europe, Asia, and Africa, while the

Doctoral Workshop created a dedicated space for emerging scholars to test research questions, methods, and policy relevance before an interdisciplinary audience.

The conference title itself expresses the normative proposition of the series. Trust does not arise automatically from technological sophistication. It must be earned through reliable systems, transparent institutions, comprehensible rules, professional competence, and credible remedies when failures occur. In smart-city settings, this means designing not only for efficiency, but also for security, contestability, continuity, and public value. The papers collected in this volume illuminate these requirements from multiple disciplinary and sectoral perspectives. This framing also extends prior work by the editors on AI-enabled public organizations and e-government [2], [3], data-intensive urban knowledge and data-quality management [4], [5], and the legal safeguards and territorial organization of contemporary public administration [6], [7].

2. AI, Cyber Threats, and Critical-Infrastructure Resilience

A first group of contributions addresses the dual-use nature of artificial intelligence. Khuduyev examines how AI strengthens defensive capabilities while simultaneously enabling hyper-personalized phishing, adaptive malware, deepfake social engineering, and automated exploit chains, thereby connecting technical threats with regulatory and organizational responsibilities [8], while extending earlier TRUST discussions of AI's double-edged role in cybersecurity [9]. Rosca and Ciobanu provide a concrete Moldovan case in which claims of AI-powered investment intelligence became an instrument of persuasion in a large-scale fraudulent scheme, showing that contemporary cybercrime often targets human trust as much as technical infrastructure [10]. Their analysis also resonates with research on how public cybercrime-prevention communication must address the social channels through which digital deception spreads [11]. Drobot extends the problem into the democratic sphere by analysing how AI-generated disinformation can sabotage the public image of European institutions, erode legitimacy, and intensify political polarization [12], within a broader smart-city cybercrime ecosystem [13]. Nistor adds a linguistic dimension: uneven large-language-model performance across languages may create a structural information-security disadvantage for non-Anglophone media ecosystems and minority-language publics [14], a concern reinforced by TRUST research on social engineering and phishing as communicative practices [15].

Several papers move from diagnosis to the design of resilient technical architectures. Bratcovici proposes an AI-driven framework combining IoT sensing, predictive analytics, federated learning, and digital-twin governance for critical urban infrastructure [16], in dialogue with SCRD research on the technological and legal dimensions of collective intelligence, security, and surveillance [17]. Stanescu, Niculae, Suciu, and Sachian argue that explainability is essential for both "AI for cybersecurity" and "cybersecurity for AI," presenting XAI as a means to improve analyst understanding, accountability, and adversarial robustness [18]. Their proof-of-concept use of Grad-CAM connects the smart-city argument to an established method for interpretable deep learning [19]. Sachian and colleagues compare Shodan and Censys as instruments for mapping exposed IoT infrastructures, demonstrating that visibility, freshness, and metadata richness differ significantly across platforms and that no single reconnaissance source should be treated as complete [20]. These findings complement SCIC research on IoT-based cultural-heritage monitoring [21] and defensive honeypots for smart-city infrastructures [22].

The infrastructure perspective is further developed in the work of Babin, Tutunaru, and Covalenco on cyber-resilient water management in the Dniester Basin [23], supported by governance research on city-level smart coordination [24], and by Babin, Serdyuk, and Ciloci on secure cross-border mobility between Moldova, Ukraine, and Romania [25], which also builds on prior work on AI prospects for public

organizations and smart cities [2]. Both studies show that resilience depends on interoperable data, transboundary coordination, common standards, and governance arrangements capable of operating across institutional and national boundaries. These contributions are especially valuable because they reject the fiction that urban systems can be secured one device or one agency at a time. Critical infrastructures are interdependent, and their failures may cascade across sectors, jurisdictions, and communities.

3. Secure Interoperability, Edge Systems, and Data Governance

A second major theme concerns the architecture of data exchange. Pintilie, Borbak, and Suciu use the Arrowhead fPVN project as a reference case for structured interoperability, showing how microservices, semantic translation, and controlled service interaction can inform secure smart-city integration [26]. Their institutional reading of interoperability is consistent with SCRD research on the factors shaping the content of smart-city initiatives [27]. Sachian and colleagues demonstrate the value of edge computing through the integration of OpenEMS Edge into residential energy systems, combining local processing, encryption, MQTT communication, and an open-source energy-management platform [28]. Their work highlights a broader principle: resilience improves when critical functions can continue locally, rather than depending exclusively on distant cloud services, and it extends SCIC work on fine-grained household-level IoT monitoring [29].

Mălureanu, Pânișoară, and Lazar examine an apparently modest artefact: the QR code printed on a fiscal receipt and reveal its potential as a post-purchase digital infrastructure [30]. Their analysis is important because it illustrates how legal identifiers, interoperability, consumer services, privacy obligations, and commercial integration can converge around a small but scalable public-facing interface. The broader public-administration agenda is articulated in SCRD research on smart cities and digitalization [31] and in TRUST work on compliance-oriented digitalization [32]. The contribution reminds us that trustworthy digital infrastructure often develops incrementally, through standards and identifiers that become valuable only when institutions and firms agree on governance and implementation.

Iatco's physics-informed digital twin for regional sugar-beet supply chains offers a sophisticated example of data governance linked to physical processes, optimization, and stakeholder fairness [33]. By combining biochemical modelling, delayed-observation reconciliation, logistics optimization, RFID-enabled transparency, and growers' equity, the study shows how technical accuracy and institutional justice can be treated within one decision-support architecture. Its approach is situated within a wider SCRD discussion of digital twins and management-information-system integration for urban resilience [34]. This is a significant conceptual advance: cyber-physical intelligence should not merely optimize throughput; it should also expose information asymmetries and protect stakeholders from systematic disadvantage.

4. Trustworthy AI in Public Services, Organizations, and Society

The proceedings also show that trustworthy AI is not confined to cybersecurity operations. Spatariu analyses the transformation of auditing through automation, anomaly detection, data analytics, and predictive modelling, while preserving the centrality of professional judgement and ethical standards [35], a position consistent with field evidence on the opportunities and challenges of AI in auditing [36]. Dogeanu considers the relationship between compliance and corporate lobbying in the banking sector, arguing for a unified code of conduct that aligns representation of interests with integrity, transparency, and reputational-risk control [37], against the background of earlier SCIC work on sustainable corporate governance [38]. Leovaridis and Grafu bring cybersecurity into AI-assisted recruitment, proposing a security-by-design framework in which data integrity and technical controls become conditions for procedural fairness and the

mitigation of algorithmic bias [39]. Their argument is strengthened by SCRD research on human-centric digital leadership [40] and SCIC work on training a workforce capable of multi-source, AI-enhanced analysis [41].

Frangulea and Lincă examine the influence of generative AI on architecture and design, connecting changing aesthetic production with copyright, cybersecurity, and the risk of manipulative or unsafe design processes [42]. The contribution follows an established SCIC concern with the transformation and reuse of the built environment [43]. Schachtner and Braun contribute a systemic perspective through a pattern language for innovation diffusion in urban systems, offering a technology-independent vocabulary for communicating, adapting, and scaling urban transformation [44]. Their argument builds on prior SCRD work on wise municipal governance [45] and on the social-change dimension of smart-city strategy development [46]. Together, these papers challenge a narrow interpretation of trustworthiness. Trust is not achieved solely by preventing unauthorized access; it also requires integrity in professional practice, explainability in organizational decisions, transparency in public-private interaction, and the capacity to debate the social meanings of technological change.

5. Smart Health, Medical AI, and Citizen-Centred Prevention

Healthcare is represented as both a high-value application domain and a demanding test of responsible AI. Aber and Singh present a convolutional-neural-network approach for automatic brain-tumour detection in MRI images, demonstrating the potential of comparatively compact architectures to support medical image classification [47], consistent with recent work on lightweight CNNs under limited-data conditions [48]. Yet performance metrics alone cannot ensure successful adoption. Alexandru, Suciu, and Niculae therefore focus on stakeholder engagement and societal impact in the ONCOSCREEN project, emphasizing communication, co-design, training, user acceptance, and the integration of AI-supported colorectal-cancer screening into real clinical and policy environments [49]. Their stakeholder-centred perspective is reinforced by SCRD research on ICT-enabled hospital logistics [50] and digital inclusion for older and potentially vulnerable users [51].

The same authors examine the ONCODIR ecosystem as an integrated architecture connecting citizen engagement, clinical decision support, and policy analytics [52]. Their contribution is particularly aligned with the conference theme because it treats digital health as a multi-level public infrastructure rather than as an isolated medical application, extending SCRD work on IoT-enabled healthcare [53] and information-security management in healthcare [54]. Niculae and colleagues extend preventive public health into environmental surveillance through an AI- and IoT-enabled mosquito-detection system designed to support earlier and more targeted interventions against vector-borne disease [55]. That architecture advances sensor-rich and digital-twin approaches previously demonstrated in SCIC research [21], [56]. Across these studies, trustworthy smart healthcare emerges as a combination of technical validation, secure data flows, professional responsibility, inclusion, and sustained stakeholder participation.

6. Education and the Human Foundations of Cyber-Resilience

No cyber-resilient city can be built without people capable of understanding and governing complex systems. Turcan and Gujuman address this requirement directly through a cybernetic model for training information-security specialists [57]. Their framework integrates technical, analytical, decision-making, and ethical competences, and it argues against the artificial separation between operational security skills and strategic thinking. This argument is consistent with SCRD work on the hybrid nature of contemporary cyber and information-security threats [58] and with earlier contributions on AI in education and the digital

transformation of university learning [59], [60]. It also extends a longer research trajectory on the collaborative, technology-mediated learning practices of the NET Generation [61] and on living labs as mechanisms through which ICT, co-creation, and social innovation can strengthen capacity in rural communities [62]. The contribution also resonates with the role of the TRUST Doctoral Workshop, which was designed not merely as a presentation venue, but as an academic environment for methodological scrutiny, feedback, communication training, and the development of policy-relevant research.

The human factor appears throughout the volume: citizens who must recognize synthetic manipulation; journalists working in under-resourced languages; auditors and recruiters responsible for algorithmically assisted decisions; public officials coordinating cross-border infrastructure; clinicians interpreting AI-supported recommendations; and security professionals operating under uncertainty. These examples confirm a basic but sometimes neglected truth: cyber-resilience is a socio-technical achievement. Technology can amplify institutional capability, but it cannot substitute for judgement, responsibility, professional standards, or public education.

7. An Integrated Research Agenda

Although the papers differ in method, scale, and sector, they converge around several principles. First, resilience must be anticipatory rather than merely reactive. Predictive analytics, digital twins, anomaly detection, and continuous monitoring are valuable because they allow institutions to identify weak signals before disruption becomes systemic. Second, interoperability is inseparable from security. Data exchange that lacks semantic clarity, access control, auditability, or common governance may increase vulnerability even when it improves connectivity. Today, this is far from being merely a technological issue, as the creation of an appropriate legal framework is essential. Third, explainability and human oversight are operational requirements, not decorative ethical additions. They enable validation, contestation, incident response, and institutional accountability.

Fourth, regulation should be approached as a component of system design. GDPR, NIS2, the Cyber Resilience Act, the AI Act, sectoral rules, and professional standards shape architectures, responsibilities, and incentives. Compliance is most effective when embedded early, rather than applied after deployment. Fifth, inclusion matters. A system that performs well only for dominant languages, digitally confident citizens, large organizations, or technologically advanced jurisdictions cannot be considered fully trustworthy. Finally, resilience requires learning. Many examples clearly confirm that prevention and education are extremely important in terms of resilience. Institutions must be able to detect failure, communicate it honestly, recover essential services, and incorporate lessons into future design.

These principles suggest a research agenda extending beyond the present volume. Future work should combine technical evaluation with institutional and societal indicators; test proposed frameworks in longitudinal, real-world settings; examine cascading failures across urban sectors; develop multilingual and culturally grounded benchmarks; and assess how public administrations can procure, audit, and govern AI systems without becoming dependent on opaque vendors. More comparative work is also needed on the capacity of local and regional authorities to implement European cybersecurity and AI obligations under uneven financial and administrative conditions. Such research can be framed through a layered understanding of the smart community, in which sustainable infrastructure, digital integration, governance, and economic development are treated as mutually dependent strategic domains rather than as isolated technology projects [63].

8. Conclusion

TRUST 2026 demonstrates that the future of intelligent cities will not be decided by technological capability alone. The decisive issue is whether capability can be converted into durable public value without compromising security, rights, democratic legitimacy, or institutional responsibility. The contributions gathered here offer no simplistic solution, and that is one of their strengths. An intelligent city is not the end in itself, but rather a way of raising the standard of public administration and public services! They show cyber-resilience as a layered undertaking that spans devices and infrastructures, algorithms and data, law and policy, organizations and professions, citizens and communities.

The conference was founded on the conviction that research should travel beyond the conference room. By bringing together academics, practitioners, public administrators, engineers, and emerging scholars without participation or publication fees, TRUST seeks to keep knowledge open and internationally connected. The present proceedings continue that mission. They document not only what intelligent systems can do, but also what societies must demand from them.

Trust, in this context, is neither optimism nor blind confidence. It is the justified expectation that systems will perform reliably, institutions will act accountably, and failures will be detected, explained, corrected, and learned from. Building cyber-resilient intelligent cities therefore means building the technical and institutional conditions under which such expectations can reasonably be sustained.

Acknowledgment

The Conference Chair gratefully acknowledges the institutional support of the National University of Political Studies and Public Administration (SNSPA), the Faculty of Public Administration, and Smart-EDU Hub; the contributions of the scientific and organizing committees; the participation of invited guests, panel chairs, reviewers, authors, doctoral candidates, and attendees; and the work of all colleagues who made the seventh edition of TRUST possible.

References

[1] M. Suksi, “Interoperability between information systems in automated decision-making in Finland and in the European Union—Blurring oversight by unrestricted access to public registers?,” European Review of Digital Administration & Law, vol. 6, no. 2, pp. 115–140, 2025.

[2] C. Vrabie, “Artificial intelligence promises to public organizations and smart cities,” in Digital Transformation, Lecture Notes in Business Information Processing, vol. 465, Cham, Switzerland: Springer, 2022, pp. 3–14, doi: 10.1007/978-3-031-23012-7_1.

[3] C. Vrabie, “E-Government 3.0: An AI model to use for enhanced local democracies,” Sustainability, vol. 15, no. 12, Art. no. 9572, 2023, doi: 10.3390/su15129572.

[4] J. Maślankowski, “Using sentiment analysis with Big Data tools to enrich knowledge on society in the city,” Smart Cities and Regional Development (SCRD) Journal, vol. 1, no. 2, pp. 37–46, 2017, doi: 10.25019/scrd.v1i2.16.

[5] J. Maślankowski, “Towards de-duplication framework in Big Data analysis: A case study,” in Information Systems: Development, Research, Applications, Education, Lecture Notes in Business Information Processing, vol. 264, Cham, Switzerland: Springer, 2016, pp. 104–113, doi: 10.1007/978-3-319-46642-2_7.

[6] N. Mäntylä, A. Barta, and V. Karjalainen, “ADM in public administration in Finland and Hungary: Does the legal culture matter?,” European Public Law, vol. 31, no. 4, pp. 511–532, 2025, doi: 10.54648/EURO2025032.

[7] A. Barta and Z. Hegyesi, “Variations on the same theme? The structure of territorial state administration in selected transition countries of the European Union,” Croatian and Comparative Public Administration, vol. 26, no. 1, pp. 65–86, 2026, doi: 10.31297/hkju.26.1.4.

[8] S. Khuduyev, “AI-driven cyber threats and information sabotage: Navigating data security and regulatory challenges,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 128–138.

[9] I. Virtosu, “Guardians or threats? The double-edged role of artificial intelligence in cyber security,” in Proc. Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), vol. 2, Bucharest, Romania: Pro Universitaria, 2025, pp. 61–73. [Online]. Available: https://www.scrd.eu/index.php/trust/article/view/744

[10] M. Rosca and R. Ciobanu, “The interplay between artificial intelligence and cyber security: A Moldovan real-file example of how AI can lead to massive fraud,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 211–226.
[11] A. F. Rahmat, C. Vrabie, and G. B. Soesilo, “Exploring the cybercrime prevention campaign on Twitter: Evidence from the Indonesian government,” Smart Cities and Regional Development (SCRD) Journal, vol. 7, no. 2, pp. 9–24, 2023, doi: 10.25019/by45bd69.
[12] I.-A. Drobot, “Artificial intelligence sabotaging the public image of EU institutions,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 227–242.
[13] C.-A. Gabrian, “The cyber crime ecosystem: Challenges and solutions for smart technology,” in Proc. Smart Cities Int. Conf. (SCIC), vol. 12, 2025, pp. 585–594. [Online]. Available: https://www.scrd.eu/index.php/scic/article/view/716
[14] A. Nistor, “The LLM language divide: A critical examination of generative AI performance disparities in non-Anglophone journalism and the democratic and security implications for public information ecosystems,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 69–88.
[15] N. Vangelov, “Social engineering and phishing: A semiotic perspective,” in Proc. Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), vol. 2, Bucharest, Romania: Pro Universitaria, 2025, pp. 109–118. [Online]. Available: https://www.scrd.eu/index.php/trust/article/view/747
[16] M. N. Bratcovici, “AI-driven cyber-resilience framework for smart city infrastructure: Integrating IoT, predictive analytics and digital twin governance,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 95–106.
[17] D. M. Popa, “A technological and legal investigation into how smart states deploy collective intelligence for security and surveillance purposes,” Smart Cities and Regional Development (SCRD) Journal, vol. 9, no. 2, pp. 77–86, 2025, doi: 10.25019/5n39gz26.
[18] V. Stanescu, M. Niculae, G. Suciu, and M.-A. Sachian, “Explainable artificial intelligence for cyber-resilient smart cities: Enhancing trust, transparency, and adversarial robustness,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 251–264.
[19] R. R. Selvaraju et al., “Grad-CAM: Visual explanations from deep networks via gradient-based localization,” International Journal of Computer Vision, vol. 128, no. 2, pp. 336–359, 2020, doi: 10.1007/s11263-019-01228-7.
[20] M.-A. Sachian, M. Niculae, G. Suciu, V.-A. Ionescu, and M.-S. Lazăr, “Comparative analysis of Shodan and Censys platforms for assessing IoT exposure,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 19–30.
[21] A. Danila et al., “IoT systems for efficient preservation of cultural heritage,” in Proc. Smart Cities Int. Conf. (SCIC), vol. 11, 2024, pp. 515–526. [Online]. Available: https://www.scrd.eu/index.php/scic/article/view/515
[22] G. Waizel, “Using a modern honeypot model to defend smart cities and provide early detection to APT and ransomware attacks,” in Proc. Smart Cities Int. Conf. (SCIC), vol. 10, 2023, pp. 33–46. [Online]. Available: https://www.scrd.eu/index.php/scic/article/view/423
[23] A. Babin, S. Tutunaru, and I. Covalenco, “Cyber-resilient smart water management in the Dniester Basin: Integrating AI and transboundary infrastructure within EU climate missions,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 193–210.
[24] 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.
[25] A. Babin, S. Serdyuk, and R. Ciloci, “Cyber-resilient cross-border smart mobility between Moldova, Ukraine, and Romania: Integrating AI and digital platforms for secure data management,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 175–192.
[26] T. Pintilie, A. Borbak, and G. Suciu, “Secure data exchange in smart cities: Lessons from Arrowhead fPVN,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 243–250.
[27] K. Radchenko, “Factors influencing the content of smart city initiatives (particularly based on institutional theories of organization),” Smart Cities and Regional Development (SCRD) Journal, vol. 8, no. 3, pp. 55–64, 2024, doi: 10.25019/yxf9wh55.
[28] M.-A. Sachian, R. Florescu, M. Niculae, G. Suciu, V.-A. Ionescu, and T.-M. Rasu, “Integrating OpenEMS Edge into smart home energy systems,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 31–44.
[29] I. F. Voicu, D. C. Diaconu, and D. C. Diaconu, “Precision long-term monitoring of local weather at household level,” in Proc. Smart Cities Int. Conf. (SCIC), vol. 12, 2025, pp. 325–334. [Online]. Available: https://www.scrd.eu/index.php/scic/article/view/701
[30] A. Mălureanu, G. Pânișoară, and G. Lazar, “QR codes on fiscal receipts as post-purchase digital infrastructure: The Romanian legal context, comparative practice, and service design opportunities,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 353–369.
[31] L.-S. Beh, M. J. Lee, N. H. Abd Rahman, and S.-L. Lai, “Smart cities and digitalisation: A research agenda of public administration,” Smart Cities and Regional Development (SCRD) Journal, vol. 6, no. 3, pp. 41–58, 2022, doi: 10.25019/scrd.v6i3.135.
[32] E.-M. Andrieș and A.-M. Bercu, “Regulatory compliance policies-digitalization of the public administration,” in Proc. Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), vol. 2, 2025, pp. 133–141.

[33] C. Iatco, “Physics-informed digital twin for sucrose loss prevention and transparent governance in regional sugar beet supply chains,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 329–352.
[34] 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.
[35] A. A. Spatariu, “The use of artificial intelligence in the field of auditing—a mini-study,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 7–18.
[36] J. Kokina, S. Blanchette, T. H. Davenport, and D. Pachamanova, “Challenges and opportunities for artificial intelligence in auditing: Evidence from the field,” International Journal of Accounting Information Systems, vol. 56, Art. no. 100734, 2025.
[37] I.-A. Dogeanu, “Integrarea conformității în arta lobby-ului corporativ din sectorul bancar. Reguli de conduită,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 119–127.
[38] D. G. Moșneanu, “Sustainable solutions for corporate governance,” in Proc. Smart Cities Int. Conf. (SCIC), vol. 9, 2021, pp. 27–40.
[39] C. Leovaridis and F.-D. Grafu, “Errors in AI-assisted recruitment and the role of cybersecurity in mitigating risks,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 139–152.
[40] O. Kravchuk, “Human-centric digital leadership for HRM 5.0 ecosystem readiness,” Smart Cities and Regional Development (SCRD) Journal, vol. 10, no. 1, pp. 55–85, 2026, doi: 10.25019/5ykgm661.
[41] A.-C. Alexandru, “Building a smart economy: Training the workforce in multi-source data and AI-enhanced economic analysis,” in Proc. Smart Cities Int. Conf. (SCIC), vol. 12, 2025, pp. 265–283. [Online]. Available: https://www.scrd.eu/index.php/scic/article/view/696
[42] M.-M. Frangulea and A. Lincă, “THE SHIFT: The evolution of design & architecture under the generative AI influence. Safety and implications,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 153–174.
[43] M.-M. Frangulea and I. Toader, “Industrial afterlife: A tale of three cities,” in Proc. Smart Cities Int. Conf. (SCIC), vol. 11, 2024, pp. 87–104.
[44] C. Schachtner and S. Braun, “Review of the pattern language for innovation diffusion in urban systems: The city as a living code,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 89–94.
[45] C. Schachtner, “Wise governance-elements of the digital strategies of municipalities,” Smart Cities and Regional Development (SCRD) Journal, vol. 6, no. 2, pp. 23–29, 2022, doi: 10.25019/scrd.v6i2.126.
[46] C. Schachtner and N. Baumann, “Accompanying study of the development process towards a smart city strategy-with a particular focus on social change,” Smart Cities and Regional Development (SCRD) Journal, vol. 8, no. 2, pp. 63–72, 2024.
[47] A. M. Aber and M. Singh, “Automatic brain tumor detection in MRI images using convolutional neural networks,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 107–118.
[48] A. B. Naeem et al., “Lightweight CNN for accurate brain tumor detection from MRI with limited training data,” Frontiers in Medicine, vol. 12, Art. no. 1636059, 2025, doi: 10.3389/fmed.2025.1636059.
[49] C. Alexandru, G. Suciu, and M. Niculae, “Stakeholder engagement and societal impact of AI-enabled CRC screening tools within the ONCOSCREEN project,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 265–298.
[50] 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.
[51] O. Sula, “Bridging the digital divide for Generation X and Boomers in the Western Balkan region through smart cities,” Smart Cities and Regional Development (SCRD) Journal, vol. 9, no. 3, pp. 19–27, 2025, doi: 10.25019/20stww05.
[52] C. Alexandru, G. Suciu, and M. Niculae, “Digital ecosystems for cancer prevention: Integrating citizen engagement, clinical decision support, and policy analytics,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 299–316.
[53] A. Labus, B. Rodić, M. Radenković, S. Mitrović, and T. Naumović, “An IoT system for healthcare in the smart city,” Smart Cities and Regional Development (SCRD) Journal, vol. 6, no. 2, pp. 77–87, 2022.
[54] V. Bozic, “Managing information security in healthcare,” Smart Cities and Regional Development (SCRD) Journal, vol. 4, no. 2, pp. 63–83, 2020, doi: 10.25019/scrd.v4i2.72.
[55] M. Niculae, C. Stalidi, G. Suciu, and A.-M. Serbanica, “Smart mosquito detection: Leveraging AI and IoT for vector-borne disease prevention,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 45–68.
[56] G. Suciu and C. Stalidi, “Digital twins, the software solution for safer cities,” in Proc. Smart Cities Int. Conf. (SCIC), vol. 10, 2023, pp. 273–282. [Online]. Available: https://www.scrd.eu/index.php/scic/article/view/443
[57] A. Turcan and L. Gujuman, “Information security and the cybernetic approach: A model for training information security specialists in the era of digitalization,” in Proc. 7th Int. Conf. Machine Intelligence & Security for Smart Cities (TRUST), Bucharest, Romania, 2026, pp. 317–328.
[58] O. Tsaruk and M. Korniiets, “Hybrid nature of modern threats for cybersecurity and information security,” Smart Cities and Regional Development (SCRD) Journal, vol. 4, no. 1, pp. 57–78, 2020, doi: 10.25019/scrd.v4i1.63.
[59] C. Vrabie, “Artificial intelligence and education,” All in on Tech (AIoT), vol. 1, 2025. [Online]. Available: https://www.scrd.eu/index.php/aiot/article/view/680

[60] A. Turcan, L. Gujuman, and T. Colesnicov, “Digital transformation in education: ASEM case study and the integration of modern technologies in the learning process,” Smart Cities and Regional Development (SCRD) Journal, vol. 9, no. 3, pp. 67–80, 2025, doi: 10.25019/zkppex15.
[61] A.-M. Tîrziu and C. I. Vrabie, “NET Generation. Thinking outside the box by using online learning methods,” New Trends and Issues Proceedings on Humanities and Social Sciences, vol. 2, no. 7, pp. 41–47, 2016, doi: 10.18844/gjhss.v2i7.1178.
[62] A.-M. Tîrziu and C. Vrabie, “Living labs—Instruments of social innovation in rural areas,” in Proc. Central and Eastern European eDem and eGov Days 2017, vol. 325, Budapest, Hungary, 2017, pp. 511–523, doi: 10.24989/ocg.v325.42.
[63] V. Stoicescu, T. I. Bițoiu, and C. Vrabie, “The smart community: Strategy layers for a new sustainable continental framework,” Smart Cities, vol. 6, no. 1, pp. 410–444, 2023, doi: 10.3390/smartcities6010020.