AI-driven cyber-resilience framework for smart city infrastructure: integrating IoT, predictive analytics and digital twin governance

Ing. Bratcovici Maria Niamh
Technical University of Civil Engineering Bucharest, Romania
maria.bratcovici@sustainstruct.com

Abstract

The rapid digitalization of urban infrastructure has transformed smart cities into complex cyber-physical ecosystems where Internet of Things (IoT) devices, cloud platforms, and artificial intelligence (AI) systems operate as critical enablers of public services. However, this interconnected architecture expands the attack surface of essential assets such as bridges, transport networks, energy grids, and water systems. Cyber incidents targeting sensor networks or data management platforms can cascade into physical disruptions, undermining public safety and trust. This paper proposes an AI-driven cyber-resilience framework designed specifically for smart city critical infrastructure. Methodologically, the paper develops a layered architecture model and evaluates its resilience capacity against representative threat scenarios, including data spoofing, denial-of-service attacks, and sensor manipulation. The analysis demonstrates that integrating predictive analytics within a digital twin governance structure significantly improves early detection rates while reducing false positives and response latency. Beyond technical contributions, the study outlines policy implications for municipal administrations, emphasizing interoperability, data protection compliance, and cross-sector coordination. The proposed framework advances the transition from reactive cybersecurity strategies to anticipatory cyber-resilience in intelligent urban systems.

Keywords: *smart city security; federated learning IoT threat detection*; critical infrastructure protection; urban resilience; connected public services

1. Cybersecurity Challenges in Smart City Environments

The proliferation of smart city technologies represents one of the most consequential transitions in contemporary urban governance. Municipalities across Europe and beyond are investing heavily in intelligent infrastructure, sensor-laden roadways, automated water management systems, AI-optimised energy grids, and data-driven public safety platforms, with the aim of improving service delivery, sustainability, and citizen quality of life. Yet this digital transformation simultaneously expands the attack surface available to malicious actors, creating systemic vulnerabilities that can cascade across interconnected urban subsystems with devastating effect.

This paper addresses this critical gap by proposing ARCIS (Adaptive Resilience for Critical Infrastructure in Smart cities), an AI-driven cyber-resilience framework that synthesises three convergent technological domains: IoT-based real-time threat sensing and edge intelligence; federated machine learning for predictive cross-domain threat analytics; and Digital Twin (DT) governance for simulation-based decision support and automated response orchestration. Together, these components form a unified, proactive, and self-adapting security fabric capable of anticipating, detecting, containing, and recovering from cyber incidents at city scale.

1.1. Vulnerabilities and Cyber Risks in Smart City Critical Infrastructure

The rapid digitalisation of urban infrastructure has fundamentally transformed the architecture of modern cities. Smart city ecosystems increasingly rely on interconnected digital technologies such as Internet of Things (IoT) devices, cloud platforms, edge computing nodes, and advanced data analytics to manage critical services including transportation systems, energy distribution networks, water management, emergency services, and public safety infrastructures. While these technologies significantly improve operational efficiency, sustainability, and service responsiveness, they simultaneously introduce complex cybersecurity vulnerabilities that challenge traditional approaches to infrastructure protection. [1]

Unlike conventional infrastructure systems, smart city architectures operate through highly distributed cyber-physical networks in which digital control systems interact continuously with physical assets. Sensors, actuators, and communication interfaces embedded within infrastructure components generate vast streams of real-time data that enable dynamic monitoring and automation. However, this interconnectedness also expands the potential attack surface available to malicious actors. Compromised IoT devices, insecure communication protocols, or [2] vulnerabilities in data management platforms may enable adversaries to infiltrate critical infrastructure systems and disrupt essential services.

One of the primary cybersecurity challenges associated with smart city infrastructures is the heterogeneity of technological components. Urban digital ecosystems typically incorporate devices produced by multiple vendors, operating under different communication standards and security protocols. [3]This fragmentation complicates the implementation of uniform security policies and often results in inconsistent levels of protection across infrastructure systems. Many IoT devices deployed in urban environments possess limited computational capacity and therefore lack robust built-in security mechanisms, making them particularly vulnerable to exploitation.

Another critical vulnerability arises from the integration of operational technology (OT) systems with information technology (IT) networks. Historically, industrial control systems managing infrastructure operations were isolated from external digital networks, limiting their exposure to cyber threats. Smart city architectures, however, increasingly require these systems to be connected to centralised data platforms in order to enable predictive maintenance, remote monitoring, and automated control. While this integration improves operational efficiency, it also exposes operational systems to cyber intrusions that may originate from conventional IT environments. [4] [5]

Cybersecurity threats targeting smart city infrastructures can manifest in multiple forms, including distributed denial-of-service attacks, data manipulation, ransomware campaigns, and targeted sabotage of cyber-physical control systems. In extreme scenarios, cyber attacks against infrastructure control systems could disrupt electricity distribution, paralyse transportation networks, or compromise water supply systems. The consequences of such disruptions extend beyond economic losses, potentially affecting public safety and social stability.

Moreover, the increasing reliance on data-driven decision-making introduces additional vulnerabilities related to data integrity and trust. Smart city management platforms rely on continuous streams of sensor data to optimise infrastructure operations. If adversaries manipulate these data flows, they may induce incorrect system responses or conceal infrastructure failures. Such attacks are particularly difficult to detect because they exploit legitimate data channels rather than directly compromising physical assets.

The challenge of securing smart city infrastructures is further complicated by the interdependence of urban systems. Energy grids, transportation networks, communication systems, and emergency services operate within tightly interconnected ecosystems in which disruptions within one sector may propagate rapidly across others. Cyber incidents affecting one infrastructure domain can therefore trigger cascading effects that amplify operational disruptions at the city level. [6]

In response to these emerging risks, cybersecurity strategies must evolve beyond traditional perimeter defence models toward more adaptive and intelligence-driven approaches. Conventional security frameworks that rely primarily on static firewalls and reactive incident response mechanisms are insufficient for protecting complex cyber-physical infrastructures. Instead, smart city environments require integrated cyber-resilience architectures capable of continuously monitoring infrastructure behaviour, detecting anomalies in real time, and anticipating potential system failures before they escalate into critical disruptions. [7]

Artificial intelligence and advanced analytics offer promising capabilities for addressing these challenges. Machine learning algorithms can analyse large volumes of infrastructure data to identify abnormal operational patterns that may indicate cyber intrusions or system malfunctions. When combined with digital twin models and predictive monitoring technologies, AI-driven security systems enable proactive risk management strategies that enhance the resilience of critical urban infrastructures. [8]

Consequently, the protection of smart city ecosystems increasingly depends on the development of integrated cyber-resilience frameworks that combine advanced analytics, real-time monitoring, and adaptive governance mechanisms. [9]Such frameworks must operate across both digital and physical layers of infrastructure systems, ensuring that technological innovation does not compromise the security and reliability of essential urban services.

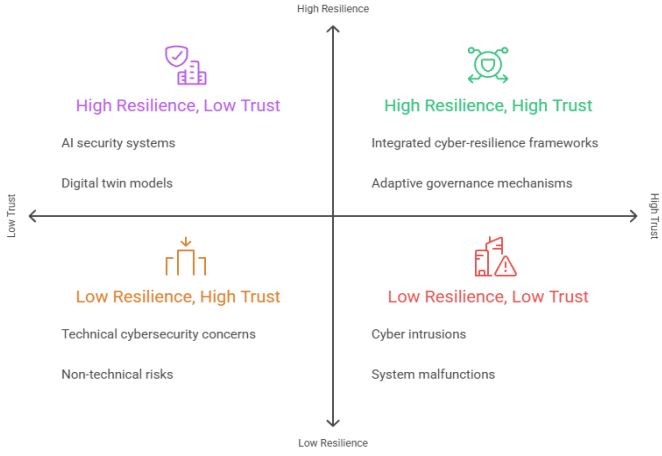


Fig. 1. Smart City Matrix
Source: author's own source

2. AI-Driven Cyber-Resilience Framework for Smart City Critical Infrastructure

Addressing the cybersecurity challenges inherent in smart city environments requires the development of integrated resilience architectures capable of combining real-time monitoring, predictive analytics, and adaptive governance mechanisms. [10]Artificial intelligence technologies provide the analytical capacity necessary to process the vast volumes of data generated by urban infrastructure systems and transform them into actionable insights for infrastructure protection.

An AI-driven cyber-resilience framework for smart city critical infrastructure operates through the integration of three core technological layers: IoT sensing networks, predictive analytics systems, and digital twin governance platforms.

At the foundational level, IoT sensor networks provide continuous situational awareness of infrastructure conditions. Sensors embedded in transportation systems, energy grids, bridges, water networks, and environmental monitoring stations collect real-time operational data including structural vibrations, energy consumption patterns, traffic flows, environmental conditions, and system performance indicators. These data streams serve as the primary information source for detecting anomalies and evaluating infrastructure health. [11]

The second layer of the framework consists of predictive analytics systems powered by artificial intelligence algorithms. Machine learning models analyse historical and real-time data to identify patterns associated with normal infrastructure behaviour. Deviations from these patterns may indicate equipment degradation, operational anomalies, or potential cyber intrusions. Predictive models therefore enable early detection of risks before they escalate into infrastructure failures or service disruptions.

Digital twin technologies form the third and most advanced component of the cyber-resilience architecture. A digital twin represents a dynamic virtual replica of physical

infrastructure systems that continuously updates its state based on real-time data inputs. By simulating the operational behaviour of infrastructure assets under various scenarios, digital twins allow decision-makers to evaluate potential system responses to cyber incidents or operational disruptions.

When integrated within a unified governance framework, these technologies enable a shift from reactive cybersecurity approaches toward proactive resilience management. Instead of responding to incidents only after they occur, infrastructure operators can monitor system behaviour continuously, identify vulnerabilities in advance, and implement mitigation measures before disruptions affect service delivery.AI-driven resilience frameworks also enhance cross-sector coordination within smart city environments. Because urban infrastructure systems are highly interconnected, security monitoring platforms must operate across multiple domains simultaneously. [12] Integrated analytics platforms allow city authorities to correlate data from transportation networks, energy systems, telecommunications infrastructures, and emergency response services in order to detect cascading risks that may propagate across sectors.Equally important is the governance dimension of cyber-resilience. Effective implementation of AI-driven security architectures requires clearly defined institutional responsibilities, regulatory standards, and data governance policies. Public authorities, infrastructure operators, and technology providers must collaborate to ensure that cybersecurity strategies align with operational requirements while preserving transparency, accountability, and privacy protections.

Ultimately, AI-enabled cyber-resilience frameworks transform the management of urban infrastructure systems by embedding intelligence within the operational architecture of cities. Through continuous monitoring, predictive risk assessment, and adaptive decision-making capabilities, such frameworks strengthen the capacity of smart cities to withstand cyber threats and maintain the reliable delivery of essential services.

2.1. Governance and Operational Integration of AI-Driven Cyber-Resilience Systems

While advanced technologies such as IoT sensing networks, predictive analytics, and digital twin models constitute the technical foundation of cyber-resilience architectures, their effectiveness ultimately depends on the governance structures through which they are implemented and managed. Smart city infrastructures operate within complex institutional ecosystems involving municipal authorities, infrastructure operators, private technology providers, cybersecurity agencies, and national regulatory bodies. Ensuring that AI-driven resilience systems function effectively therefore requires coordinated governance mechanisms capable of aligning technological capabilities with institutional responsibilities and regulatory frameworks. [13]

One of the primary governance challenges associated with smart city cybersecurity lies in the fragmentation of infrastructure management. Critical urban systems,including transportation networks, energy grids, telecommunications infrastructures, water management facilities, and emergency response services,are often managed by different organisations operating under distinct regulatory regimes. Without integrated governance structures, cybersecurity initiatives risk becoming fragmented, with individual sectors

implementing isolated protection mechanisms that fail to address cross-sector vulnerabilities.

To mitigate these risks, many cities are increasingly adopting centralised cyber-resilience coordination models. These models establish dedicated urban resilience units or digital security centres responsible for monitoring infrastructure systems across multiple sectors. By aggregating operational data from various infrastructure operators, such coordination centres can detect anomalies that might otherwise remain invisible within isolated systems. The integration of AI-driven analytics platforms further enhances this capability by enabling automated detection of abnormal behavioural patterns across interconnected infrastructure networks.

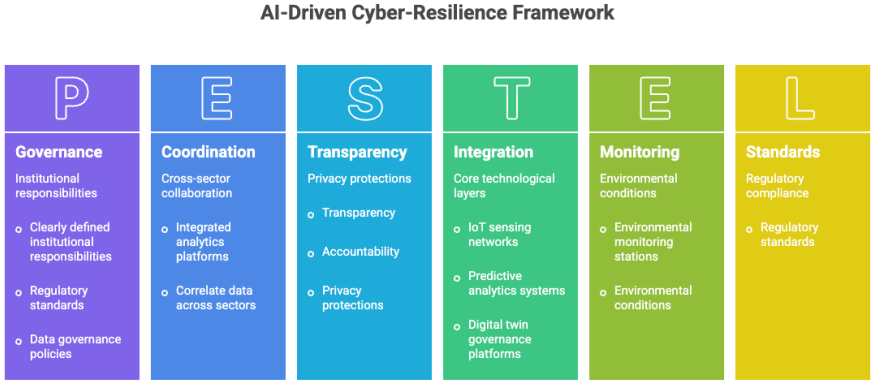


Fig. 2. Political, Economical, Social, Technological, Environmental and Legal Implications
Source: author's own source

Another critical dimension of governance concerns data management and information sharing. AI-based monitoring systems rely on continuous flows of high-resolution infrastructure data collected from sensors, control systems, and operational databases. Effective resilience frameworks therefore require robust data governance policies that define standards for data collection, storage, access control, and privacy protection. These policies must balance the need for real-time operational transparency with the imperative to safeguard sensitive information related to critical infrastructure systems. [14]

Public-private cooperation also plays a central role in the implementation of cyber-resilience architectures. Many smart city infrastructures are owned or operated by private companies, particularly within sectors such as energy distribution, telecommunications, and transportation services. [15] As a result, cybersecurity strategies must be developed through collaborative partnerships that align the objectives of public authorities with the operational realities faced by private infrastructure operators. Joint cybersecurity exercises, shared incident response protocols, and coordinated investment strategies can strengthen collective preparedness against emerging cyber threats.

In addition to institutional coordination, regulatory frameworks must evolve to address the unique challenges posed by AI-enabled infrastructure systems. Traditional cybersecurity

regulations often focus on information systems and data protection rather than on the protection of cyber-physical infrastructures. As digital technologies become increasingly embedded within urban infrastructure networks, regulatory frameworks must expand to encompass the resilience of interconnected systems that combine digital control platforms with physical operational assets.

Training and capacity development constitute another essential component of cyber-resilience governance. The operation of AI-driven monitoring platforms requires specialised expertise in fields such as cybersecurity analytics, infrastructure engineering, and data science. [16] Municipal authorities and infrastructure operators must therefore invest in workforce development programmes capable of equipping personnel with the skills necessary to manage advanced digital infrastructure systems. Continuous training programmes, interdisciplinary education initiatives, and international knowledge-sharing networks can contribute to strengthening the human capital required for resilient smart city governance. [17]

Ultimately, the effectiveness of AI-driven cyber-resilience frameworks depends not solely on technological sophistication but on the institutional capacity to integrate these technologies into coherent governance structures. Smart city resilience emerges from the interaction between advanced digital tools and adaptive organisational systems capable of translating data-driven insights into timely and coordinated operational responses. [18]

By embedding predictive monitoring technologies within transparent governance architectures and collaborative institutional networks, cities can transform cybersecurity from a reactive defensive activity into a proactive strategy for safeguarding the continuity and reliability of critical infrastructure services. [19]In doing so, urban authorities strengthen not only the technological resilience of infrastructure systems but also the broader societal capacity to manage complex risks within increasingly digitalised urban environments. [20]

Table 1. Proposed AI-Driven Cyber-Resilience Framework for Smart City Critical Infrastructure

Framework Layer	**Technology Components**	**Primary Function**	**Strategic Benefit**
IoT Monitoring Layer	Sensors, IoT gateways, edge computing nodes	Collection of real-time infrastructure data	Continuous situational awareness
Predictive Analytics Layer	Machine learning models, anomaly detection algorithms	Identification of abnormal operational patterns	Early detection of cyber threats and system failures
Digital Twin Layer	Virtual infrastructure models, simulation platforms	Real-time system simulation and scenario testing	Anticipatory risk management
Governance Layer	Data governance frameworks, cybersecurity policies	Coordination between institutions and infrastructure operators	Improved strategic resilience

Source: author's own source

3. Ethical, Regulatory and Strategic Implications of Smart Infrastructure Security

The growing integration of artificial intelligence within critical infrastructure systems raises a range of ethical, regulatory, and strategic considerations that extend beyond purely technical cybersecurity concerns. [1] While AI-driven resilience architectures offer significant advantages in terms of real-time monitoring, predictive risk assessment, and automated response capabilities, their deployment within smart city environments also introduces complex governance challenges related to transparency, accountability, and societal trust. [21]

One of the primary ethical considerations associated with AI-enabled infrastructure security concerns the transparency of algorithmic decision-making. Predictive monitoring systems rely on machine learning models that analyse vast quantities of infrastructure data in order to detect anomalies or forecast potential disruptions. However, many advanced AI models operate as "black-box" systems whose internal decision processes are difficult to interpret. [22]

When such systems are used to guide infrastructure management decisions,such as prioritising maintenance interventions or triggering automated security responses,it becomes essential that decision-makers retain sufficient visibility into the analytical processes underpinning these recommendations. Ensuring algorithmic transparency is therefore a critical requirement for maintaining accountability within public infrastructure governance. [7]

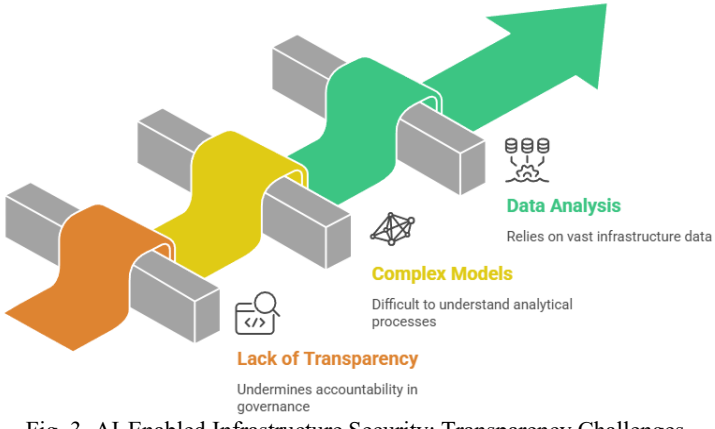


Fig. 3. AI-Enabled Infrastructure Security: Transparency Challenges
Source: author's own source

Closely related to this issue is the question of human oversight. Although AI technologies significantly enhance the analytical capacity of infrastructure management systems, the delegation of operational decisions to automated systems raises concerns regarding control and responsibility. In high-stakes environments such as energy grids, transportation networks, or emergency response systems, automated responses triggered by predictive algorithms may carry significant operational consequences. For this reason, most cyber-resilience frameworks emphasise the importance of maintaining a "human-in-the-loop"

governance model, in which AI systems function as decision-support tools rather than autonomous decision-makers. [23] [24]

Furthermore, international cooperation plays an increasingly important role in strengthening cyber-resilience across interconnected infrastructure systems. Urban infrastructures operate within global technological ecosystems shaped by international standards, software platforms, and supply chains. [25] Cybersecurity threats affecting smart city systems therefore often transcend national borders. Collaborative frameworks involving governments, research institutions, and international organisations can facilitate the exchange of best practices, threat intelligence, and technological innovations that enhance the collective resilience of digital infrastructure systems. [11]

Last but not least, the successful integration of artificial intelligence into smart city infrastructure management requires a balanced approach that combines technological innovation with robust ethical and regulatory safeguards. AI-driven resilience systems offer powerful tools for enhancing infrastructure security, but their long-term effectiveness depends on maintaining public trust, institutional accountability, and transparent governance frameworks. [26]

By addressing the ethical, regulatory, and strategic implications of AI-enabled infrastructure security, policymakers and urban planners can ensure that the digital transformation of cities contributes not only to efficiency and innovation but also to the sustainable protection of critical infrastructure systems upon which modern societies depend. [27]

4. Conclusions

The rapid digital transformation of urban infrastructures has fundamentally reshaped the operational architecture of modern cities. Smart city environments increasingly rely on interconnected cyber-physical systems that integrate sensors, communication networks, data analytics platforms, and automated control technologies in order to optimise the management of essential urban services. While these innovations significantly enhance efficiency, sustainability, and service responsiveness, they also introduce new categories of cybersecurity risks that challenge traditional approaches to critical infrastructure protection.

All in all, this study has examined the cybersecurity challenges associated with smart city ecosystems and proposed an integrated AI-driven cyber-resilience framework capable of addressing the vulnerabilities inherent in digitally interconnected infrastructure systems. The analysis demonstrates that conventional perimeter-based cybersecurity strategies are insufficient for protecting complex cyber-physical environments in which operational technology, digital platforms, and physical infrastructure assets are deeply interconnected. Instead, the protection of smart city infrastructures requires adaptive resilience architectures capable of continuously monitoring system behaviour, detecting anomalies in real time, and anticipating emerging threats before they disrupt essential services.The proposed framework integrates three key technological components: IoT-based monitoring networks, artificial intelligence–driven predictive analytics, and digital twin governance

platforms. Together, these elements create a multi-layered resilience architecture that transforms infrastructure protection from a reactive process into a proactive and anticipatory strategy. IoT sensor networks enable continuous situational awareness by generating real-time operational data from infrastructure systems. Predictive analytics powered by machine learning algorithms analyse these data streams to identify anomalies and forecast potential system failures. Digital twin technologies extend these capabilities by enabling virtual simulations of infrastructure behaviour, allowing decision-makers to evaluate risk scenarios and implement preventive interventions before disruptions occur.

Beyond technological innovation, the study also highlights the critical importance of governance frameworks capable of integrating these advanced systems into coherent operational strategies. Effective cyber-resilience depends not only on technological capabilities but also on institutional coordination between public authorities, infrastructure operators, and technology providers. Robust data governance policies, regulatory adaptation, and collaborative public–private partnerships are essential for ensuring that digital resilience architectures function effectively while maintaining transparency, accountability, and societal trust.

Furthermore, the research emphasises that the growing reliance on artificial intelligence in infrastructure management raises significant ethical and regulatory considerations. Issues related to algorithmic transparency, human oversight, and the protection of sensitive infrastructure data must be carefully addressed in order to ensure that AI-enabled resilience systems operate in accordance with democratic governance principles and public interest objectives. Maintaining a balance between automation and human decision-making will remain a key challenge as infrastructure systems become increasingly intelligent and autonomous.

At a broader strategic level, the integration of AI-driven resilience architectures has important implications for the security and stability of modern societies. Critical infrastructures form the backbone of economic activity, social wellbeing, and public safety, and their protection has become a central priority in an era characterised by increasing cyber threats and geopolitical uncertainty. The ability to anticipate, detect, and mitigate disruptions within complex cyber-physical systems represents a decisive capability for ensuring the continuity of essential services in digitally interconnected urban environments.

In conclusion, the transition toward AI-enabled infrastructure governance marks a fundamental shift in the way cities manage security and resilience. By embedding predictive intelligence, real-time monitoring, and adaptive decision-support systems within infrastructure management frameworks, smart cities can significantly enhance their capacity to withstand cyber threats and operational disruptions. The development of integrated cyber-resilience architectures therefore represents not only a technological innovation but also a strategic necessity for safeguarding the reliability and sustainability of critical infrastructure systems in the digital age.

References

[1] 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.

[2] 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, p. 35–50, 2026.

[3] R. Alharbey, A. Shafiq, A. Daud and H. Dawood, "Digital Twin Technology for Enhanced Smart Grid Performance: Integrating Sustainability, Security, and Efficiency," *Frontiers in Energy Research,* 2024.

[4] A. M. Mohsen, M. A. Jasim and M. A. Abdulrazzaq, "A ComprehensiReview of Smart Cities Components, Applications, and Technologies Based on Internet of Things," 2020.

[5] International Organization for Standardization, "Information Technology-Security Techniques-Information Security Management Systems," ISO/IEC 27001:2013, Geneva, Switzerland, 2013.

[6] M. Grieves and J. Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems.," *Transdisciplinary Perspectives on Complex Systems,* no. Springer, pp. 85-112, 2017.

[7] Agency, Cybersecurity and Infrastructure Security, "Cybersecurity Best Practices for Smart Cities," U.S. Cybersecurity and Infrastructure Security Agency, 2023.

[8] I. Virtosu, "Guardians or threats? The double-edged role of artificial intelligence in cyber security, Ensuring Trust and Security in Intelligent Urban Ecosystems.," 2025.

[9] H. Song, R. Srinivasan, T. Sookoor and S. Jeschke, Smart Cities: Foundations, Principles, and Applications, ISBN: 9781119226390, 2017.

[10] K. Werner, M. Karner, G. Traar, J. Henjes and W. Sihn, "Digital Twin in Manufacturing: A Conceptual Framework," Procedia CIRP 67, 2018, pp. 101-107.

[11] M. El-Hajj, "Leveraging digital twins and intrusion-detection systems for enhanced security in IoT-based smart-city infrastructures," *Electronics,* vol. 13, no. 19, p. Art. no. 3941, 2024.

[12] I.-A. Dobrot, "Attacks against data security in smart cities: hypothetical scenarios or reality?"," in *TRUST Proc*, Bucharest, 2024.

[13] E. Hossain and M. Rahman, "Smart Infrastructure and Predictive Maintenance: A Systemic Review.," *IEEE Access,* 2022.

[14] S. Vempati and N. N, "Securing smart cities: a cybersecurity perspective on integrating IoT, AI, and machine learning for digital-twin creation,," *Journal of Electrical Systems,* vol. 20, no. 20, p. 2024, 2024.

[15] "Technological trends in the 21st-century defense and security sector," 17 03 2025. [Online]. Available: https://www.gmv.com/en-es/media/blog/defense-security/technological-trends-21st-century-defense-security-sector. [Accessed 4 11 2025].

[16] S. Ntalampiras and P. Daponte, "AI-Based Predictive Maintenance for Critical Infrastructure Protection.," *Sensors 23 no.14,* 2023.

[17] J. hen and W. Lu, "What are the driving factors of innovation in Smart City? A systematic review of journal publications from 2014 to 2024," *Smart Cities and Regional Development (SCRD) Journal,* vol. 9, no. 4, pp. 105-123, 2025.

[18] C.-L. Pau, "'Smart governance: a framework for the future',," Smart Cities International Conference., 2024.

[19] G. B. Kanushi, "Integration of AI and IoT for Smart and Secure Mobility," *Smart Cities and Regional Development (SCRD) Preprints,* Vols. vol. 2, nr. 2, dec 2025.

[20] G. Waizel, "The agentic AI security adoption matrix: Understanding readiness and resistance across domains," *Smart Cities and Regional Development (SCRD) Journal,* vol. 2, no. 10, pp. 75-84, 2026.

[21] H. Yeritsyan and L. Sargsyan, "Yerevan's transformation into a smart city: innovating infrastructure and driving sustainable urban development," *Smart Cities and Regional Development (SCRD) Journal,* vol. 9, no. 3, pp. 53-65, 2025.

[22] ABI Research, "Lack of Critical Infrastructure Cybersecurity Investments in Smart Cities Will Seed the Future IoT Vulnerabilities," August 20 2019. [Online]. Available: https://www.abiresearch.com/press/lack-critical-infrastructure-cybersecurity-investments-smart-cities-will-seed-future-iot-vulnerabilities/. [Accessed 16 March 2026].

[23] E. Bolisani and E. Scarso, "The Digital Twin in the Context of Industry 4.0: A Review of Its Role and Future Perspectives.," *Journal of Industrial Information Integration,* 2023.

[24] "Digitalisation of Infrastructure for a Sustainable Future.," European Commission, Brussels, 2022.

[25] O.-A. Sarcea, "AI & Cybersecurity — connection, impacts, way ahead," *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings,* vol. 1, pp. 17-26, 2024.

[26] C. Vrabie, "Improving municipal responsiveness through AI-powered image analysis in E-Government", Public Policy and Administration," 2025.

[27] OECD, "Strengthening Critical Infrastructure Resilience:Policy Tools and Approaches," OECD Publishing, Paris, 2021.

[28] United Nations Economic Commission, "Trans-European Motorway and Trans-European Railway Networks: Road and Rail Infrastructure," UNECE, Geneva, 2020.

[29] K. Mkhitaryan, A. Sanamyan, M. Mnatsakanyan and E. Kirakosyan, "The smart city paradigm in the 21st century: Pathways and pitfalls," *Smart Cities and Regional Development (SCRD) Journal,* vol. 9, no. 4, pp. 77-92, 2025.