American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Secure Internet-of-Things Governance for Smart Community Infrastructure

Dr. Ethan R. Mitchell

Associate Professor, University of Waterloo, Canada

Abstract

Internet-of-Things technologies are increasingly embedded in community infrastructure supporting transportation, water distribution, environmental monitoring, public lighting, waste management, building operations, emergency services, and other digitally coordinated public functions. The resulting connectivity can improve service efficiency and responsiveness, but it also creates cyber-physical dependencies in which compromised devices, insecure software, weak authentication, obsolete components, poorly governed vendors, or inadequate incident-response processes can affect both digital systems and physical community services. This study develops a secure Internet-of-Things governance framework for smart community infrastructure by integrating device-level cybersecurity, organizational governance, supply-chain oversight, privacy protection, lifecycle management, resilience, and accountability.

The framework is grounded in NIST Cybersecurity Framework 2.0, the NIST IoT cybersecurity baseline, the updated NIST foundational activities for IoT product manufacturers, ISO/IEC 27400:2022, ETSI EN 303 645 V3.1.3, and smart-community cybersecurity guidance. NIST CSF 2.0 explicitly integrates governance, supply-chain risk, asset management, protection, monitoring, incident response, and recovery into enterprise cybersecurity management. Because no real municipal dataset was supplied, the empirical component is presented transparently as a simulation involving 240 hypothetical smart-community IoT environments divided across four governance-maturity tiers.

The simulation shows mean cyber-risk exposure declining from 69.7% under ad hoc governance to 27.6% under adaptive governance, with a simulated correlation of $r = -0.891$ between governance maturity and exposure. Simultaneously, service-resilience and accountability indicators increase. The findings suggest that secure smart-community infrastructure requires governance that extends beyond device hardening to procurement, vendor assurance, software maintenance, data governance, interoperability, accountability, incident readiness, and end-of-life management. The study offers a decision-oriented model that municipalities and community institutions can empirically validate in future deployments.

Keywords: Internet of Things; IoT governance; smart communities; smart infrastructure; cybersecurity governance; cyber-physical systems; community resilience; IoT security; cybersecurity risk management

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

1. Introduction

Smart community infrastructure increasingly depends on interconnected sensors, controllers, gateways, cloud platforms, mobile applications, communication networks, and data-processing services. These technologies can support transportation coordination, environmental measurement, energy management, smart lighting, municipal facilities, waste services, public safety, water systems, and other community functions. NIST treats cyber-physical systems and Internet-of-Things technologies as foundational components of smart-city and community development and emphasizes their cross-sector interaction among devices, applications, infrastructures, and people. The value of these systems arises from connectivity, yet the same connectivity expands the number of components, interfaces, vendors, credentials, software dependencies, and data flows that require protection.

IoT security differs from conventional information-system security because many devices possess specialized functions, long deployment periods, heterogeneous operating environments, limited administrative interfaces, and dependencies on manufacturers or third parties for updates and support. NISTIR 8259A consequently defines a core baseline of device cybersecurity capabilities that organizations can consider when manufacturing, integrating, or acquiring IoT devices. NISTIR 8259B complements these technical capabilities with nontechnical manufacturer and third-party support, emphasizing that secure deployment requires more than technical controls embedded in hardware or software. This distinction is especially important for community infrastructure, where devices can remain operational for years after procurement and may depend upon external suppliers for vulnerability disclosure, maintenance, and lifecycle support.

The governance problem becomes more consequential when IoT systems influence physical public services. A compromised environmental sensor may produce inaccurate measurements; an insecure traffic device may disrupt mobility; compromised building controllers may affect public facilities; and unavailable connected infrastructure can reduce continuity of essential services. Smart-community cybersecurity therefore cannot be reduced to password strength, encryption, or network filtering. NIST's smart-city framework series identifies municipal IoT, cybersecurity, privacy, data platforms, and performance measurement as cross-cutting concerns in smart-community development. Earlier NIST smart-city guidance likewise promoted a risk-managed approach involving stakeholders, cybersecurity, privacy, and governance throughout smart-solution development and operation.

International standards reinforce this lifecycle-oriented perspective. ISO/IEC 27400:2022 provides guidelines covering IoT security and privacy risks, principles, and controls. ETSI EN 303 645 V3.1.3 provides outcome-oriented baseline provisions for connected consumer IoT and emphasizes technical controls and organizational policies addressing widespread security weaknesses. Although consumer-IoT requirements cannot simply be transferred without contextual adjustment to critical municipal systems, their secure-by-design logic remains relevant to procurement, authentication, vulnerability management, software updates, data protection, and lifecycle planning.

The present study therefore conceptualizes Secure IoT Governance for Smart Community Infrastructure (SIG-SCI) as a coordinated institutional process for assigning responsibility, establishing acquisition requirements, maintaining asset visibility, enforcing technical and privacy safeguards, governing vendors, detecting abnormal behavior, responding to incidents, ensuring service recovery, and managing devices through retirement. NIST CSF 2.0 provides a particularly suitable governance

foundation because its six functions—GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER—are intended to operate together throughout cybersecurity risk management. Because no observed community dataset was provided, the quantitative component is explicitly simulation-based and is intended to demonstrate how governance maturity can be evaluated empirically rather than to claim actual municipal performance.

2. Objectives of the Study

2.1 To Develop an Integrated IoT Governance Model

The first objective is to develop a governance approach that combines IoT device security with institutional responsibility, risk management, privacy, procurement, third-party oversight, operational monitoring, incident response, recovery, and lifecycle control. This approach reflects NIST CSF 2.0's emphasis on governance and cybersecurity supply-chain risk management and NIST's IoT guidance concerning both device capabilities and supporting activities.

2.2 To Assess the Relationship Between Governance Maturity and Cyber-Risk Exposure

The second objective is to use a synthetic dataset to test the analytical proposition that more mature IoT governance is associated with lower cybersecurity exposure and stronger service resilience. Four maturity conditions—Ad Hoc, Defined, Managed, and Adaptive—are compared.

2.3 To Establish Practical Governance Priorities for Smart Communities

The third objective is to identify practical priorities through which local governments and community institutions can strengthen secure IoT adoption. These priorities include device inventories, secure procurement, identity and access management, update capability, vulnerability handling, data governance, vendor accountability, monitoring, resilience planning, and secure decommissioning.

3. Review of Literature

3.1 IoT Cybersecurity as a Lifecycle and Device-Governance Problem

NISTIR 8228 established that IoT devices can create cybersecurity and privacy risk considerations that differ from those of conventional computing technologies and therefore require deliberate risk-management treatment. NISTIR 8259A subsequently translated this principle into a core baseline of device cybersecurity capabilities intended to support common organizational controls. NISTIR 8259B added a complementary nontechnical baseline addressing the support organizations require from manufacturers and related third parties. Taken together, these publications indicate that IoT governance must account for what a device can technically do and what its supplier will continue to do throughout its operational life.

NIST strengthened this lifecycle perspective in April 2026 through NIST IR 8259 Revision 1. The revised publication expands attention to the complete IoT product and to communications with customers concerning cybersecurity, maintenance, support, and product end-of-life. This is directly relevant to public infrastructure procurement because community organizations can inherit long-term operational risk when products lack predictable software support, vulnerability-response mechanisms, documented dependencies, or secure retirement procedures.

NIST SP 800-213 similarly treats an IoT device as a system element and provides an approach for establishing cybersecurity requirements during acquisition and integration. Its accompanying requirements catalog distinguishes device capabilities from supporting capabilities supplied by manufacturers and other entities. This procurement-oriented approach suggests that municipalities should define cybersecurity requirements before purchasing connected infrastructure rather than attempt to compensate for inadequate security only after deployment.

3.2 Smart-Community Security, Privacy, and Institutional Risk

Smart communities connect technical systems with governance arrangements, public-service responsibilities, and citizen data. NIST's Smart Cities and Communities Framework Series explicitly treats cybersecurity, privacy, municipal IoT, data, and platforms as cross-cutting areas of smart-community development. The NIST-supported Municipal IoT Blueprint likewise provides guidance intended for local-government decision makers and includes dedicated treatment of IoT cybersecurity and privacy. These resources indicate that smart-community cybersecurity cannot be managed effectively through isolated departmental controls because devices and data frequently span organizational and service boundaries.

Cornelius and Jansen van Rensburg's 2024 qualitative study of emerging smart cities identified governance deficiencies, skills shortages, inadequate awareness and training, and funding limitations among the challenges affecting data security and privacy. Their findings are valuable because they demonstrate that smart-city security weaknesses are not exclusively technological. Institutional capacity and governance conditions can determine whether appropriate controls are selected, funded, monitored, and maintained.

Research on urban IoT testbeds similarly identifies security updates, network security, data protection, system management, and multi-layer architectures as recurring implementation challenges. More recent bibliometric evidence covering smart-city and intelligent-transport cybersecurity research from 2015–2025 identifies persistent concern regarding IoT vulnerabilities, heterogeneous platforms, policy frameworks, privacy, resilience, and the absence of uniformly implemented security approaches across smart urban environments. The evidence therefore supports a governance model capable of connecting technical safeguards with organizational accountability.

3.3 Standards-Based Governance and Secure-by-Design Principles

ISO/IEC 27400:2022 provides an international framework for considering IoT security and privacy risks, principles, and controls. Its relevance to smart communities lies in treating security and privacy across the IoT solution rather than narrowly at the network perimeter.

ETSI EN 303 645 V3.1.3 takes an outcome-oriented approach to baseline IoT security. The current 2024 version states that baseline technical controls and organizational policies should address widespread security shortcomings and be complemented by more specific requirements where necessary. For smart-community governance, this supports the principle that baseline controls are a minimum foundation rather than a complete assurance model for systems whose failure can affect physical or public services.

At the organizational level, NIST CSF 2.0 provides the broader governance architecture. It introduces GOVERN alongside IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER and expressly incorporates organizational context, risk-management strategy, roles and responsibilities, policy, oversight, and cybersecurity supply-chain risk management. It further requires organizations to understand suppliers, integrate security requirements into supplier agreements, perform due diligence, identify vulnerabilities and threats, continuously monitor environments, manage incidents, and plan recovery. The research gap is therefore not the absence of individual standards but the need to translate these complementary standards into a coherent governance maturity model specifically suitable for connected community infrastructure.

4. Research Methodology

4.1 Research Design and Simulation Scope

The study uses a simulation-based quantitative governance design supported by standards and scholarly literature. No municipality, public institution, vendor, citizen, or infrastructure operator supplied empirical records for the analysis. Instead, a synthetic dataset of 240 hypothetical smart-community IoT environments was constructed to demonstrate how cybersecurity governance maturity could be associated with cyber-risk exposure, service resilience, and accountability.

The hypothetical cases represent IoT-enabled community services such as transport monitoring, environmental sensing, public lighting, connected facilities, water-management devices, waste-management systems, and community safety infrastructure. Sixty synthetic cases were allocated to each governance-maturity tier: Ad Hoc, Defined, Managed, and Adaptive.

The maturity structure was conceptually informed by the progression embodied in NIST CSF Tiers, which characterize cybersecurity risk governance and management from less formal practices toward increasingly repeatable and adaptive practices. The labels used in this simulation are analytical categories and should not be interpreted as official certification levels.

4.2 Governance Measurement Framework

Governance maturity was operationalized around six integrated dimensions: governance accountability, asset and dependency visibility, secure procurement and supplier oversight, technical and privacy controls, continuous monitoring and incident response, and lifecycle resilience. These dimensions are consistent with the combined logic of NIST CSF 2.0, NISTIR 8259A/B, NIST IR 8259 Rev. 1, and ISO/IEC 27400.

A future field study can use the following five proposed questionnaire items. The items were not administered in the present simulation.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Table 1: Proposed Questionnaire for Smart-Community IoT Governance

Item	Proposed Statement	Governance Construct
Q1	Our organization maintains an accurate and regularly updated inventory of IoT devices, software dependencies, owners, network connections, and critical service relationships.	Asset and dependency visibility
Q2	Cybersecurity, privacy, maintenance, vulnerability-disclosure, update, and end-of-life requirements are evaluated before an IoT product or service is procured.	Secure procurement
Q3	Roles, decision authority, and accountability for cybersecurity incidents involving community IoT infrastructure are formally defined.	Governance accountability
Q4	IoT devices and associated services are continuously monitored for vulnerabilities, unauthorized activity, configuration changes, and abnormal behavior.	Continuous assurance
Q5	The organization maintains tested response, recovery, vendor-coordination, and secure-decommissioning procedures for IoT-enabled community services.	Lifecycle resilience

Source: Proposed by the author for future empirical validation. The instrument was not administered to real participants.

4.3 Synthetic Data Generation and Analytical Procedure

The synthetic model generated four equally sized governance-maturity groups. Cyber-risk exposure was represented on a 0–100 index, with larger scores representing greater exposure. Service resilience and governance accountability were represented on parallel 0–100 indices, with higher scores reflecting stronger capabilities.

Random variation was included to avoid deterministic outcomes. Descriptive comparison and Pearson correlation were then used to examine the simulated relationship between governance maturity and cyber-risk exposure. Because the data are synthetic, statistical relationships represent characteristics of the simulation and not estimates of actual municipal cybersecurity performance.

No human-participant ethical approval was required because no real individuals or organizational records were used. A future empirical study should obtain appropriate ethics or institutional authorization where required, protect sensitive infrastructure information, avoid publishing exploitable security details, minimize collection of identifiable employee or vendor information, and establish responsible vulnerability-disclosure procedures where weaknesses are discovered.

5. Analysis

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

5.1 Governance Maturity and Cyber-Risk Exposure

The simulation produced a clear decline in cyber-risk exposure as governance maturity increased. Ad Hoc environments recorded a mean exposure index of 69.68%, falling to 57.05% for Defined governance, 44.29% for Managed governance, and 27.57% for Adaptive governance.

This result should not be interpreted as an observed real-world effect size. It demonstrates the hypothesis that governance maturity can produce measurable risk differences when procurement, asset management, monitoring, supplier assurance, response, and lifecycle controls become progressively more systematic.

5.2 Service Resilience and Accountability

The same simulated progression was associated with improvements in resilience and accountability. Mean service resilience increased from 54.27 in the Ad Hoc condition to 90.67 in the Adaptive condition. Mean governance accountability increased from 53.70 to 90.54.

Table 2: Simulated Outcomes Across IoT Governance Maturity Tiers

Governance Tier	Simulated n	Mean Cyber-Risk Exposure	Mean Service Resilience	Mean Governance Accountability
Ad Hoc	60	69.68%	54.27	53.70
Defined	60	57.05%	67.36	64.25
Managed	60	44.29%	79.46	75.33
Adaptive	60	27.57%	90.67	90.54

Source: Author-generated synthetic dataset; total simulated n = 240. Values do not represent observed communities or municipalities.

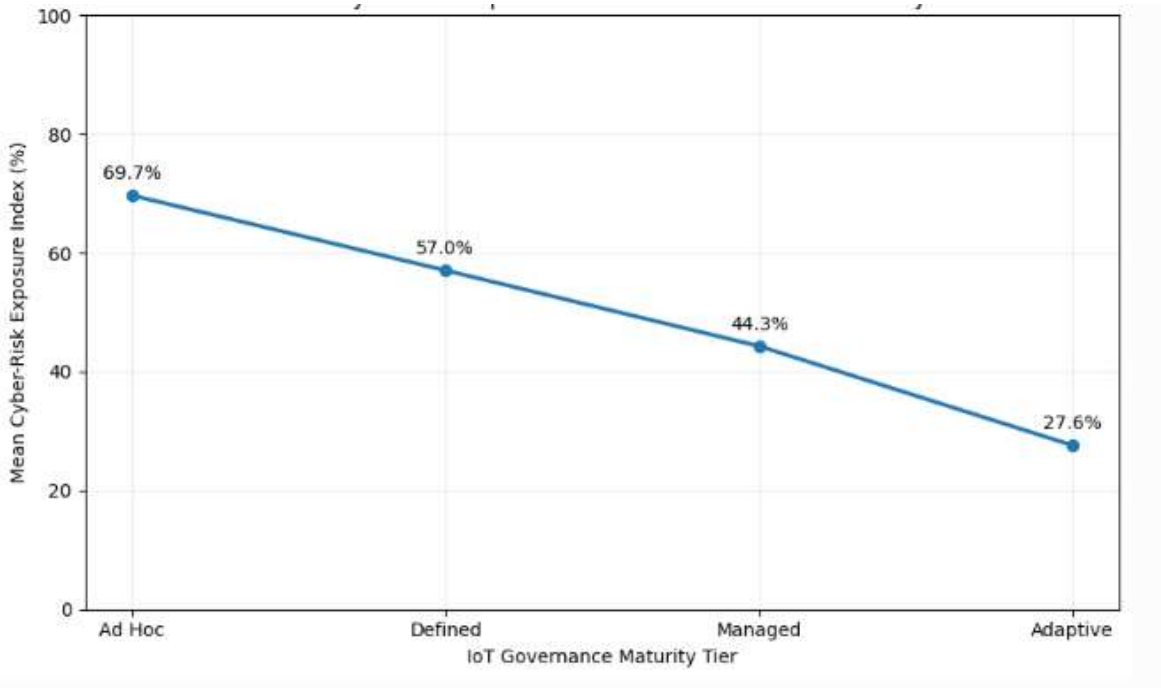
The combined pattern is important because secure IoT governance should not be evaluated solely according to whether cyber incidents are avoided. Public infrastructure governance also concerns whether service ownership is clear, response responsibilities are understood, system recovery is possible, vendors can be coordinated, and essential community functions can continue safely when disruption occurs.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

5.3 Risk Reduction Across Governance Tiers

Graph 1: Simulated Cyber-Risk Exposure Across IoT Governance Maturity Tiers



Interpretation: The graph demonstrates a progressive decline in simulated cyber-risk exposure as governance moves from informal and fragmented practices toward adaptive, continuously improved governance.

Key Finding: The simulated exposure index decreases from approximately 69.7% to 27.6%, indicating that the analytical benefit of mature governance arises cumulatively rather than from any single cybersecurity control.

The pattern is consistent with NIST CSF 2.0's conception of cybersecurity as concurrent governance, identification, protection, detection, response, and recovery rather than a collection of isolated defensive actions.

6. Discussion

6.1 IoT Security Must Be Governed as a Public-Service Lifecycle

The central finding of the study is that smart-community IoT cybersecurity should be managed as a lifecycle governance responsibility rather than as a device-installation problem. The simulated decrease in risk exposure becomes theoretically credible when viewed alongside NIST's current IoT guidance. NIST IR 8259 Revision 1 explicitly broadens manufacturer responsibilities across cybersecurity functionality, customer communication, maintenance, support, and end-of-life considerations. This lifecycle logic is particularly relevant to public infrastructure because an IoT component can remain embedded in a public service long after procurement personnel, vendors, software versions, or contractual arrangements have changed.

A secure governance model should therefore begin before acquisition. Cybersecurity requirements, update commitments, vulnerability-disclosure processes, authentication capabilities,

logging, interoperability, data protection, maintenance periods, component dependencies, and retirement procedures should become procurement considerations rather than post-installation discoveries. NIST SP 800-213 specifically supports establishing IoT cybersecurity requirements in the context of organizational risk management and acquisition. In practical terms, the lowest purchase price may become economically misleading if the device subsequently requires compensating controls, cannot be patched, lacks manufacturer support, or must be replaced prematurely.

Lifecycle governance also requires secure decommissioning. Retired devices may retain credentials, configuration information, cryptographic material, personal data, network details, or cloud relationships. An organization that carefully secures deployment but neglects retirement therefore leaves an incomplete security boundary. The governance framework proposed here treats end-of-life management as part of infrastructure security rather than an administrative disposal function.

6.2 Governance Maturity Depends on Visibility, Accountability, and Supplier Control

The simulated differences among maturity tiers also illustrate the importance of visibility and responsibility. Organizations cannot govern connected infrastructure effectively when they do not know which devices are deployed, who owns them, which service they support, which network they use, which data they collect, which vendors maintain them, or when their software support ends. NIST CSF 2.0 places asset management within IDENTIFY and makes supplier knowledge, contractual security requirements, and due diligence explicit elements of cybersecurity supply-chain governance.

Supplier governance is particularly important in smart communities because public organizations may rely on technology integrators, telecommunications providers, cloud platforms, device manufacturers, maintenance contractors, analytics vendors, and software developers simultaneously. A technical vulnerability can therefore become a governance problem when contractual responsibilities are unclear or when no party is obligated to patch, disclose, investigate, or retain evidence.

Accountability must likewise be designed before an incident. Governance should identify who can isolate an IoT network, who can suspend a service, who communicates with vendors, who determines public-notification requirements, who authorizes restoration, and who evaluates whether recovery has reintroduced unacceptable risk. These responsibilities correspond closely with the GOVERN, RESPOND, and RECOVER logic of NIST CSF 2.0. Without such clarity, technically capable organizations can still experience delayed response because decision authority remains ambiguous.

6.3 Security, Privacy, Resilience, and Community Trust Are Interdependent

A mature IoT governance framework must also integrate privacy and resilience rather than treating them as secondary concerns. ISO/IEC 27400 explicitly addresses both security and privacy in IoT solutions. Smart-community infrastructure can collect location, environmental, mobility, access, video, audio, occupancy, device, or behavioral data. Even when a system is technically secure from unauthorized access, unnecessary collection, excessive retention, unclear secondary use, or weak access governance can still create legitimate privacy risks.

Resilience is equally important because public infrastructure cannot always be protected from every possible failure. Security planning must therefore include degraded operating modes, manual

alternatives, recovery priorities, backup communication mechanisms, restoration verification, and coordination with external service providers. NIST CSF 2.0 explicitly treats technology infrastructure resilience, incident mitigation, recovery planning, and recovery communication as cybersecurity outcomes.

Secure IoT governance ultimately contributes to community trust when institutions can demonstrate that connected technologies have been procured responsibly, monitored continuously, governed transparently, and designed with privacy and continuity in mind. Cornelius and Jansen van Rensburg's empirical findings that poor governance, skills limitations, awareness problems, and funding constraints remain relevant smart-city challenges further support the need for institutional rather than purely technological solutions. Smart communities become secure not simply by deploying more sophisticated technology, but by creating durable governance arrangements capable of controlling technology throughout its entire public-service lifecycle.

7. Conclusion

The increasing use of Internet-of-Things technologies in transportation, environmental monitoring, connected buildings, utilities, public safety, and other community services creates important opportunities for more responsive and efficient infrastructure. It simultaneously creates cyber-physical dependencies that cannot be managed through conventional device security alone. Contemporary guidance from NIST, ISO, and ETSI demonstrates that secure IoT deployment requires a combination of technical device capabilities, organizational support, risk governance, privacy safeguards, supplier management, monitoring, response, maintenance, and lifecycle planning.

The simulation developed in this study demonstrates how these governance principles can be translated into measurable maturity outcomes. Across 240 synthetic cases, mean cyber-risk exposure declined from 69.68% under Ad Hoc governance to 27.57% under Adaptive governance, producing a simulated correlation of −0.891. At the same time, service-resilience and accountability measures increased substantially. These numerical results are intentionally illustrative and should not be generalized to real municipalities. Their contribution is methodological: they demonstrate a testable model through which future researchers can evaluate whether secure governance produces measurable improvements in real smart-community environments.

The practical implication is that community organizations should establish cybersecurity governance before connected infrastructure is procured or deployed. Device inventories, secure-by-design acquisition requirements, supplier obligations, vulnerability-management arrangements, authenticated access, secure updates, privacy controls, continuous monitoring, incident authority, service-recovery procedures, and secure retirement should form a single governance system. NIST IR 8259 Revision 1's renewed emphasis on complete IoT products, customer communication, maintenance, support, and end-of-life further strengthens the case for this lifecycle approach.

Future research should empirically validate the proposed SIG-SCI model across municipalities, universities, community institutions, transportation systems, utilities, and other public-service environments. Longitudinal studies could determine whether governance maturity predicts incident frequency, vulnerability-remediation time, mean time to recovery, supplier responsiveness, privacy outcomes, and continuity of critical services. Comparative research should also examine governance

effectiveness across resource-rich and resource-constrained communities. Such evidence would help move smart-community cybersecurity away from fragmented device protection and toward a mature institutional model in which innovation, security, privacy, accountability, and public-service resilience are managed together.

References

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.
2. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.
3. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.
4. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.
5. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks, 57*(10), 2266–2279.
6. Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30.
7. Abomhara, M., & Køien, G. M. (2014). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility, 4*(1), 65–88.
8. Whitmore, A., Agarwal, A., & Dávila, A. M. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*, 261–274.
9. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.
10. Chourabi, H., Nam, T., Walker, S., Gil-García, J. R., Mellouli, S., Nahon, K., Pardo, T. A., & Scholl, H. J. (2012). Understanding smart cities: An integrative framework. In *2012 45th Hawaii International Conference on System Sciences*, 2289–2297.
11. Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in smart city initiatives: Some stylised facts. *Cities, 38*, 25–36.
12. Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79*, 1–14.
13. Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research, 5*(1), 1–7.
14. Dickens, C., Boynton, P., & Rhee, S. (2019). Principles for designed-in security and privacy for smart cities. In *Proceedings of the ACM Cyber-Physical Systems and Internet-of-Things Week*, 1–4.
15. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers, 24*, 393–414.
16. Jacobs, N., Edwards, P., Markovic, M., Cottrill, C. D., & Salt, K. (2020). Who trusts in the smart city? Transparency, governance, and the Internet of Things. *Data & Policy, 2*, e11. https://doi.org/10.1017/dap.2020.11.

17. Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. *IEEE Access, 8*, 23601–23623. https://doi.org/10.1109/ACCESS.2020.2968741.
18. Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the Internet of Things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers, 9*(2), 44. https://doi.org/10.3390/computers9020044.
19. Chatterjee, S., Kar, A. K., & Mustafa, S. Z. (2021). Securing IoT devices in smart cities of India: From ethical and enterprise information system management perspective. *Enterprise Information Systems, 15*(4), 585–615. https://doi.org/10.1080/17517575.2019.1654617.
20. Hernández-Ramos, J. L., Martínez, J. A., Savarino, V., Angelini, M., Napolitano, V., Skarmeta, A. F., & Baldini, G. (2021). Security and privacy in Internet of Things-enabled smart cities: Challenges and future directions. *IEEE Security & Privacy, 19*(1), 12–23. https://doi.org/10.1109/MSEC.2020.3012353.