

Beyond firewalls: public integrity and cyber resilience in European smart city governance

Marianna dr. Szabóné dr. Gál,

*Ludovika University of Public Service, Doctoral School of Public Administration, Budapest, Hungary
doktorgalmarianna@gmail.com*

Abstract

This study examines how the level of public sector integrity influences cyber resilience and the security of digital governance in smart city environments across Europe. The research aims to move beyond a purely technological understanding of cybersecurity by demonstrating that smart city resilience also depends on transparent public procurement, accountable institutional oversight, reliable data governance, and the public sector's capacity to govern complex digital infrastructures. The study builds on existing concepts of public sector integrity, cyber resilience, digital governance, and smart city governance, with particular attention to the relationship between corruption risks, supplier dependency, vendor lock-in, and the institutional conditions required for secure digital transformation. The research employs a comparative, indicator-based approach. It examines six European countries—Denmark, Finland, Estonia, Hungary, Romania, and Bulgaria—using public sector integrity indicators, cyber resilience indices, digital governance indicators, and public procurement risk proxies. As complementary explanatory dimensions, the analysis also considers supplier concentration, public procurement competition, and institutional control mechanisms. The findings suggest that, in the cases of Denmark, Finland, and Estonia, relatively high levels of public sector integrity are associated with strong cyber resilience and advanced digital governance capacity. Hungary and Romania display mixed profiles: both countries possess relatively strong formal cybersecurity capacities, while their integrity and public procurement indicators point to institutional vulnerabilities. Bulgaria emerges as the most vulnerable case among the countries examined, combining weaker integrity, lower cyber resilience, and more limited institutional control. The conclusions are relevant for researchers, policymakers, and practitioners alike, as they highlight that smart city cybersecurity cannot be ensured solely through firewalls and technical solutions. The study's main contribution lies in integrating public sector integrity, public procurement governance, and cyber resilience within a common analytical framework for assessing the security of smart city governance in Europe.

Keywords: public integrity, cyber resilience, smart city governance, digital governance, cybersecurity,

1. Introduction

Smart city governance is becoming increasingly dependent on interconnected digital infrastructures. Urban sensor networks, intelligent transportation systems, digital identification services, e-government portals, smart utilities, public safety platforms, and data-driven urban management tools all expand the operational capacity of public administration.

According to the smart governance literature, digital technologies can enhance the efficiency of public services, transparency, citizen participation, and data-driven decision-making. At the same time, however, smart city systems also increase technological dependency and institutional exposure [1], [2], [3]. In parallel, the attack surface of the public sector continues to expand. Consequently, smart city cybersecurity cannot be reduced to firewalls, endpoint protection, or incident response centers. It is equally a governance issue: who designs, procures, operates, audits, and oversees the digital systems upon which public services depend?

The central argument of this study is that public sector integrity constitutes one of the institutional preconditions for effective cyber resilience in smart city governance. Where public procurement is transparent, institutional oversight is accountable, and supplier relationships are auditable, digital transformation is more likely to result in secure and resilient public services.

Conversely, where public sector integrity is weaker, smart city systems may become vulnerable not only because of technical deficiencies but also due to overpriced procurement, supplier concentration, vendor lock-in, weak contract management, formalistic compliance, and inadequate independent auditing. This logic is reinforced by the institutional approach to smart governance, which treats e-government, data analytics, citizen participation, transparency, interoperability, resilience, and public sector capacity-building as interconnected conditions [1].

This study investigates these relationships through a comparative analysis of six European countries: Denmark, Finland, Estonia, Hungary, Romania, and Bulgaria.

The case selection is not random but based on theoretical sampling, as the six countries represent three distinct institutional–digital profiles. Denmark, Finland, and Estonia form the first group because international indicators consistently show high levels of public sector integrity, advanced digital governance, and strong cybersecurity capacity.

According to the Corruption Perceptions Index (CPI) and the Worldwide Governance Indicators (WGI) Control of Corruption measure, Denmark and Finland rank among Europe’s top performers, while Estonia demonstrates the strongest integrity profile in the Baltic region [4], [5]. At the same time, Denmark, Estonia, and Finland are among the global leaders in the United Nations E-Government Development Index (EGDI), while both the National Cyber Security Index (NCSI) and the ITU Global Cybersecurity Index (GCI) indicate strong cybersecurity capabilities in all three countries [6], [7], [8].

Hungary and Romania represent a distinct mixed-profile category. Although both countries exhibit relatively strong formal cybersecurity capacities, their public sector integrity and public procurement indicators suggest more vulnerable institutional environments. According to the NCSI, both countries achieve high scores; however, the CPI, the WGI Control of Corruption indicator, and EU public procurement competition proxies point to more significant integrity and supplier-related risks than those observed in the Nordic–Baltic group [4], [5], [6], [9].

Bulgaria constitutes the third category because its lower public sector integrity profile is accompanied by weaker cyber resilience and institutional control indicators, making it the most vulnerable configuration among the countries examined [4], [5], [7], [9]. The six-country sample therefore enables the study to examine not only linear relationships but also distinct institutional profiles, including high-integrity digital states, cases characterized by

mixed formal cyber capacities, and more vulnerable integrity–cybersecurity configurations.

Research Question

How does the level of public sector integrity influence cyber resilience and the security of digital governance in smart city environments across Europe?

Main Hypothesis

European countries with higher levels of public sector integrity are more likely to demonstrate stronger cyber resilience and more advanced digital governance capacities.

The study does not claim that public sector integrity alone determines cyber resilience. Cyber resilience is also shaped by economic capacity, digital infrastructure, national cybersecurity strategies, technical expertise, and geopolitical exposure. Rather, the study argues that public sector integrity influences whether investments in digitalization and cybersecurity are transformed into genuine resilience or merely create formal capacities without robust implementation.

2. Previous Research and Conceptual Background

The smart governance literature emphasizes the role of digital technologies in improving the efficiency, transparency, inclusiveness, and responsiveness of public administration.

The smart governance literature associated with Smart Cities and Regional Development (SCRD) is particularly relevant because it conceptualizes smart cities not merely as technological systems but as institutional and participatory governance arrangements. Pau's smart governance framework identifies e-government, data analytics, citizen participation, transparency and accountability, digital services, interoperability, sustainability/resilience, and capacity building as key components of smart governance [1]. This is directly relevant to the present study because these elements also constitute the institutional environment within which cybersecurity decisions are made.

Previous SCRD literature further emphasizes that smart governance depends on municipalities' ability to use technology to improve public policymaking and citizen-centered service delivery. Langa and Thakhathi examine the role of municipalities in smart governance within smart cities [10]. Kumar analyzes actual practices of citizen participation in smart cities, highlighting how participatory and transparent governance can strengthen trust and accountability in digital environments [11]. Carboni compares leading smart cities and provides valuable insights into how digital performance varies across different urban contexts [12]. Radchenko's work on the economic and social impacts of smart cities is also relevant because it demonstrates that smart city initiatives may generate unintended consequences when stakeholder perceptions, institutional contexts, and implementation capacities are not adequately considered [13].

The broader smart governance literature similarly argues that smart cities should be understood as governance systems rather than merely technical platforms. Bolívar and

Meijer define smart urban governance as a domain in which digital technologies intersect with decision-making, collaboration, and institutional arrangements [2].

Tomor and colleagues argue that smart governance for sustainable cities produces mixed outcomes and therefore requires empirical investigation into how digital collaboration functions in practice [3]. Barns' concept of platform urbanism is particularly important because smart city services are increasingly organized through digital platforms and supplier ecosystems [14]. Such platform-based environments create specific risks, including data dependency, closed architectures, unequal bargaining power, and vendor lock-in.

From a cybersecurity perspective, the key issue is that smart city governance connects public administration with private suppliers, cloud services, Internet of Things (IoT) devices, surveillance systems, transportation networks, and critical urban infrastructure. This makes supplier governance and public procurement integrity central elements of cyber resilience. Even a technologically advanced system may remain vulnerable if it is procured under weak competitive conditions, inadequately audited, dependent on a single supplier, or implemented without sufficient public sector expertise.

3. Analytical Framework

The study employs an analytical framework consisting of five dimensions:

1. Public Sector Integrity: the perceived and institutional quality of corruption control and public sector integrity.
2. Supplier Risk: the extent to which procurement and vendor structures may create dependency, concentration, weak competition, or vendor lock-in.
3. Cyber Resilience: national cybersecurity capacity and the preparedness of public systems.
4. Digital Governance: the level of development of digital government services and the infrastructures that enable them.
5. Institutional Control: the rule-of-law, auditing, procurement, and accountability environment that determines how effectively digital capacities are governed.

Public sector integrity serves as the primary independent variable. Cyber resilience and digital governance capacity constitute the principal outcome dimensions. Supplier risk and institutional control are treated as mediating variables. The proposed causal mechanism is as follows:

The analytical framework assumes that higher levels of public sector integrity contribute to more transparent public procurement processes and stronger institutional control mechanisms. These conditions reduce supplier concentration and the risk of vendor lock-in, thereby supporting more reliable digital governance and stronger cyber resilience. Conversely, lower levels of public sector integrity are often associated with weaker procurement competition and less effective contractual oversight. As a result, supplier concentration and vendor dependency may increase, creating situations in which formal digital or cybersecurity capacities do not necessarily translate into genuine operational resilience.

This framework is particularly relevant in smart city environments because local and national digital systems are often procured, integrated, and operated by external suppliers. In such settings, resilience depends not only on technical architecture but also on the integrity of procurement and governance processes.

4. Methodology

This study employs a comparative, indicator-based research design. It compares six European countries across five dimensions: public sector integrity, supplier risk, cyber resilience, digital governance, and institutional control. The analysis relies on internationally comparable indicators, which are interpreted as diagnostic signals rather than direct causal evidence. The methodological premise is that smart city cyber resilience cannot be captured by a single metric; rather, it depends simultaneously on public sector integrity, the quality of the procurement and supplier environment, formal cybersecurity capacities, digital governance maturity, and the effectiveness of institutional controls.

To measure public sector integrity, the study uses two composite indicators: Transparency International's Corruption Perceptions Index (CPI) and the World Bank's Worldwide Governance Indicators (WGI) Control of Corruption measure. The CPI assesses the perceived level of corruption in the public sector on a scale from 0 to 100, where 0 represents a highly corrupt public sector and 100 represents a very clean one. The CPI is constructed from multiple independent data sources and is based on assessments by experts and business actors; therefore, it should be interpreted not as a direct measure of corruption but as a perception-based risk indicator [9]. The WGI Control of Corruption indicator captures the extent to which public power is exercised for private gain, including both petty and grand corruption, as well as state capture. The WGI scale typically ranges from -2.5 to +2.5, with higher values indicating better governance quality [10]. The combined use of these two indicators is justified because both approximate the integrity environment, although they rely on different data sources and aggregation methodologies.

To assess cyber resilience, the study employs the National Cyber Security Index (NCSI) and the ITU Global Cybersecurity Index (GCI). The NCSI focuses on measurable cybersecurity capacity elements implemented by central governments, including legislation, dedicated organizational structures, cooperation mechanisms, strategic documents, exercises, technologies, and publicly verifiable outputs [6]. The GCI evaluates national cybersecurity commitment and capacity across five pillars: legal, technical,

organizational, capacity-building, and cooperative measures [7]. Both indices are suitable for comparing countries' formal cybersecurity preparedness. However, their methodological limitation is that they primarily measure existing regulatory, institutional, and capacity-related elements. Consequently, a high score does not necessarily indicate actual resistance to cyberattacks but rather reflects the level of formal cybersecurity maturity.

Digital governance capacity is assessed through the United Nations E-Government Development Index (EGDI). The EGDI is a composite indicator that measures e-government development across three principal dimensions: the quality and availability of online services, the development of telecommunications infrastructure, and the level of human capital [8]. The index is particularly useful for comparing state digital service capacity and digital administrative maturity. However, it does not comprehensively measure the security, integrity, procurement background, or auditability of digital public services. Therefore, the study treats the EGDI not as an independent security indicator but as a proxy for the level of digital governance development.

Supplier risk is approximated through public procurement competition proxies, primarily based on the European Commission's Single Market Scoreboard public procurement indicators. A key measure is the proportion of single-bid tenders, which indicates the share of contracts awarded through procedures involving only one bidder. The proportion of direct awards and non-competitive procedures is also relevant, as these may limit market competition [9]. These indicators do not prove corruption, but they can be interpreted as procurement-related red flags. High values may indicate weaker competition intensity, potential supplier concentration, or vendor dependency. A methodological limitation of the Scoreboard is that it provides only a partial picture of procurement performance and addresses corruption, administrative burdens, and procurement professionalism only indirectly [9]. Consequently, supplier risk is treated not as evidence of misconduct but as an institutional risk dimension that may influence the effectiveness of cybersecurity procurement.

To interpret institutional control, the study considers the WGI Rule of Law indicator, the public procurement control environment, and aspects of independent auditability. The Rule of Law indicator approximates the quality of legal institutions, contractual security, property rights, courts, and the enforcement of rules [5]. From the perspective of smart city cyber resilience, this is important because the security of digital systems depends not only on technical protection but also on the enforceability of contractual obligations, independent oversight, compliance with data governance rules, and institutional accountability. Institutional control therefore functions as a mediating dimension, influencing whether formal digital and cybersecurity capacities are transformed into secure, auditable, and resilient public services.

A limitation of the methodological approach is that some of the indicators employed are perception-based or composite in nature and are therefore not suitable for establishing

causality on their own. The CPI and WGI rely on perceptions and expert/business assessments; the NCSI and GCI primarily measure formal capacity elements; the EGDI captures digital governance development but is not specifically a security index; and the procurement indicators serve only as proxies for supplier risk. For this reason, the study adopts a triangulation logic, interpreting indicators in relation to one another rather than in isolation. The purpose of the analysis is not to demonstrate that integrity alone causes cyber resilience, but rather to identify the patterns associated with higher or lower integrity environments in the areas of cybersecurity capacity, digital governance, and supplier risk.

The analysis is exploratory and comparative in nature. Its objective is to identify patterns and develop a theoretically grounded explanation of how integrity may influence smart city cyber resilience and the security of digital governance. The selection of six countries enables the comparison of three distinct configurations: high-integrity countries with strong digital and cybersecurity profiles, mixed-profile cases, and more vulnerable integrity–cybersecurity configurations. This approach is particularly well suited to examining smart city cybersecurity not merely as a technological issue, but as an institutional and public policy challenge.

5. Results

The results are presented across five dimensions: public sector integrity, supplier risk, cyber resilience, digital governance, and institutional control. Following the individual tables for each dimension, an integrated comparative matrix summarizes the overall profiles of the six countries. The purpose of these tables is not to establish causality but to illustrate the country profiles that emerge from different indicators in relation to smart city cyber resilience and the security of digital governance.

5.1. Public Sector Integrity

The public sector integrity dimension is interpreted through the Corruption Perceptions Index (CPI) and the WGI Control of Corruption indicator. Higher values on both indicators suggest a more favorable integrity environment.

The CPI ranges from 0 to 100, where higher scores indicate a cleaner perceived public sector. The WGI Control of Corruption indicator ranges approximately from –2.5 to +2.5, where higher values represent stronger control of corruption [4], [5].

Table 1. Public Sector Integrity in the Countries Examined

Country	CPI 2025	WGI Control of Corruption 2024	Interpretation
Denmark	89	2.29	Very strong integrity profile
Finland	88	2.19	Very strong integrity profile
Estonia	76	1.67	Strong integrity profile
Romania	45	0.03	Weak-to-moderate integrity profile
Hungary	40	0.04	Weak integrity profile
Bulgaria	40	-0.24	Weak integrity profile

Source: Author’s compilation based on Transparency International CPI and World Bank WGI data [4], [5].

The integrity indicators reveal a clear Nordic–Baltic advantage. Denmark and Finland demonstrate exceptionally strong corruption control and public sector integrity, while Estonia also exhibits a stable and high-integrity profile. Hungary, Romania, and Bulgaria perform significantly less favorably.

According to the CPI, Romania presents a somewhat more favorable picture than Hungary and Bulgaria, while under the WGI Control of Corruption indicator Hungary and Romania show nearly identical results, with Bulgaria recording the weakest score. This dimension establishes the institutional baseline of the study, as the observed differences in integrity provide a basis for examining whether they are associated with different cyber resilience and digital governance profiles.

5.2. Supplier Risk

Supplier risk is approximated through public procurement competition proxies. The proportion of single-bid tenders indicates the share of procurement procedures in which only one bidder participated. The proportion of direct awards and non-competitive procedures is also relevant from the perspectives of competition intensity and transparency. Although these indicators do not prove corruption, they may serve as red flags for supplier concentration, weak competition, and vendor lock-in risks [9].

Table 2. Supplier Risk Based on Public Procurement Competition Proxies

Country	Single-Bid Procurement Rate (2024)	Direct Awards / No Calls (2024)	Supplier Risk Assessment
Finland	15%	5%	Low-to-moderate risk
Denmark	23%	10%	Moderate risk
Estonia	28%	13%	Moderate-to-high risk
Hungary	34%	4%	High risk due to single-bid procedures
Bulgaria	36%	20%	Very high risk
Romania	44%	1%	High risk due to single-bid procedures

Source: Author’s compilation based on European Commission Single Market Scoreboard public procurement indicators [9].

The supplier risk indicators provide a more nuanced picture of integrity. Finland performs favorably in this dimension as well. Denmark and Estonia display relatively high shares of single-bid tenders, suggesting that procurement competition deserves separate attention even in countries with strong integrity profiles.

In Hungary, Romania, and Bulgaria, higher rates of single-bid procedures raise concerns regarding supplier concentration and competition intensity. Bulgaria appears particularly vulnerable because it combines a high share of single-bid procedures with a high rate of direct awards.

5.3. Cyber Resilience

The cyber resilience dimension is interpreted using the National Cyber Security Index (NCSI) and the ITU Global Cybersecurity Index (GCI). The NCSI provides a numerical assessment of national cybersecurity capacity, while the 2024 GCI categorizes countries into performance tiers. Tier 1 (T1) represents the most advanced, role-model level; Tier 2 (T2) indicates advanced capacity; and Tier 3 (T3) reflects emerging capacity [6], [7].

Table 3. Cyber Resilience in the Countries Examined

Country	NCSI Score	ITU GCI 2024 Category	Interpretation
Estonia	96.67	T1	Outstanding formal cyber capacity
Finland	95.83	T1	Outstanding formal cyber capacity
Hungary	93.33	T2	High formal cyber capacity
Romania	92.50	T2	High formal cyber capacity
Denmark	89.17	T1	Strong cyber capacity
Bulgaria	80.83	T3	Moderate and more vulnerable cyber capacity

Source: Author’s compilation based on National Cyber Security Index and ITU Global Cybersecurity Index data [6], [7].

An important methodological insight emerging from the cyber resilience indicators is that formal cyber capacity does not always follow the integrity ranking. Estonia and Finland clearly stand out, consistent with their integrity and digital governance profiles. Hungary and Romania, however, achieve high NCSI scores despite weaker integrity indicators. This mixed profile constitutes one of the study’s central observations: formal cybersecurity institutions and the actual integrity-based implementation environment may diverge significantly.

5.4. Digital Governance

The digital governance dimension is assessed using the United Nations E-Government Development Index (EGDI). The EGDI is a composite indicator measuring e-government development based on online services, telecommunications infrastructure, and human capital [8].

Table 4. Digital Governance According to the UN EGDI

Country	EGDI 2024 Score	Global Rank	Interpretation
Denmark	0.98474	1st	World-leading digital governance
Estonia	0.97274	2nd	Globally leading digital stat
Finland	0.95746	9th	Highly advanced digital governance
Bulgaria	0.81453	55th	Moderately high digital governance development
Hungary	0.80430	59th	Moderately high digital governance development
Romania	0.76364	72nd	Lowest level of digital governance development in the sample

Source: Author’s compilation based on the United Nations E-Government Development Index 2024 [8].

According to the EGDI, Denmark, Estonia, and Finland clearly belong to the leading group of digitally governed states. Bulgaria, Hungary, and Romania also demonstrate high or moderately high levels of digital development, but they lag considerably behind the Nordic–Baltic group.

Bulgaria presents an interesting deviation: it ranks ahead of Hungary in the EGDI despite weaker integrity and cyber resilience indicators. This finding reinforces the methodological conclusion that digital governance development alone does not guarantee secure and integrity-based digital government operations.

5.5. Institutional Control

The institutional control dimension is assessed through the WGI Rule of Law indicator and the interpretation of the public procurement control environment. The Rule of Law indicator measures the extent to which individuals and organizations have confidence in and abide by the rules of society, with particular emphasis on contract enforcement, property rights, the police, the courts, and the likelihood of crime and violence. The scale ranges approximately from –2.5 to +2.5, where higher values indicate stronger institutional control [5].

Table 5. Institutional Control Based on the WGI Rule of Law Indicator

Country	WGI Rule of Law 2024	Institutional Control Assessment
Finland	2.02	Very strong institutional control
Denmark	2.00	Very strong institutional control
Estonia	1.49	Strong institutional control
Hungary	~0.40	Moderate/weaker institutional control
Romania	0.37	Moderate/weaker institutional control
Bulgaria	-0.03	Weak institutional control

Source: Author’s compilation based on World Bank WGI Rule of Law data [5].

The institutional control indicator closely follows the integrity pattern identified earlier. Finland and Denmark demonstrate very strong rule-of-law environments and institutional control systems, while Estonia also exhibits a favorable profile. Hungary and Romania occupy an intermediate and more vulnerable position, whereas Bulgaria records the weakest score. This is particularly relevant from the perspective of smart city cyber resilience because the security of digital systems depends not only on technical safeguards but also on the enforceability of contractual obligations, procurement oversight, auditability, and institutional accountability.

5.6. Integrated Comparative Matrix

The country profiles emerging from the individual dimensions are summarized in the integrated comparative matrix below. The purpose of the matrix is to make integrity, supplier risk, cyber resilience, digital governance, and institutional control patterns directly comparable within a single framework.

Table 6. Five-Dimensional Comparative Matrix of Public Sector Integrity, Supplier Risk, Cyber Resilience, Digital Governance, and Institutional Control

Country	Public Sector Integrity	Supplier Risk	Cyber Resilience	Digital Governance	Institutional Control	Overall Profile
 Denmark	Very strong 	Low-to-moderate 	Strong 	Very strong 	Very strong 	High-integrity digital state with strong governance capacity
 Finland	Very strong 	Low 	Very strong 	Very strong 	Very strong 	The most balanced and lowest-risk profile
 Estonia	Strong 	Moderate 	Outstanding 	Outstanding 	Strong 	Digital and cybersecurity leader with a strong, though not risk-free, procurement environment
 Hungary	Weak 	High 	High formal capacity 	Moderately high 	Moderate/weak 	Mixed profile: strong formal cyber capacity, weaker integrity background
 Romania	Weak-to-moderate 	High 	High formal capacity 	Lower within the sample 	Moderate/weak 	Mixed profile: strong cyber indicators but weaker digital governance and procurement competition
 Bulgaria	Weak 	Very high 	Moderate/weaker 	Moderately high 	Weak 	The most vulnerable configuration within the sample
 Very strong / Outstanding Top performance		 Strong / High Good performance		 Moderate / Moderate-to-high Room for improvement		 Weak / Very high High risk / Vulnerable
				 Supplier Risk legend Low High		

Source: Author's compilation based on CPI, WGI, NCSI, ITU GCI, UN EGDI, and EU public procurement proxy indicators [4]–[9].

The integrated matrix identifies three principal profiles. In Denmark, Finland, and Estonia, high levels of public sector integrity are associated with advanced digital governance and strong cybersecurity capacities. Hungary and Romania display mixed profiles: formal cybersecurity capacity is relatively strong, but integrity, procurement, and institutional control indicators point to a more vulnerable implementation environment. Bulgaria represents the most vulnerable configuration among the countries examined, as weaker integrity and institutional control indicators are accompanied by a lower cyber resilience profile.

The findings therefore provide qualified support for the hypothesis. Higher levels of public sector integrity are generally associated with stronger digital governance and cybersecurity profiles; however, this relationship is mediated by supplier risk, procurement competition, and institutional control.

6. Country-Level Interpretation

6.1. Denmark

Denmark represents a model characterized by high integrity and advanced digital governance. Its public sector is consistently ranked among the least corrupt in Europe, while its digital government performance is globally outstanding.

In the context of smart city governance, this combination is important because digital infrastructure can develop within an environment where public procurement, institutional accountability, and public trust are relatively strong. The principal challenge is not a lack

of capacity, but rather maintaining transparency and cybersecurity standards amid increasing platformization and supplier dependency in urban systems.

6.2. Finland

Finland demonstrates the most balanced profile within the sample. Its indicators of public sector integrity, institutional control, cyber resilience, and digital governance are all consistently strong. This suggests that Finnish smart city governance benefits from a coherent institutional environment in which public trust, rule-of-law capacity, a highly professional public administration, and robust cybersecurity preparedness reinforce one another. Finland therefore provides the strongest support for the study's hypothesis.

6.3. Estonia

Estonia is a leading example of digital governance and cybersecurity. Its e-government model, digital identity infrastructure, and cybersecurity policy environment make it a particularly important case for understanding smart city governance. Estonia's profile demonstrates that strong cyber resilience can be achieved through strategic digital state-building. At the same time, the analytical framework highlights that even successful digital states must continuously address procurement and supplier risks, especially as smart city systems become increasingly dependent on complex digital platforms and external service providers.

6.4. Hungary

Hungary represents a mixed profile. Its formal cybersecurity capacity appears relatively strong; however, public sector integrity indicators and procurement-related risks suggest that careful attention should be paid to whether cybersecurity expenditures are translated into genuine resilience.

This does not imply that Hungarian cybersecurity procurements are inherently ineffective or that domestic suppliers necessarily represent a problem. On the contrary, domestic suppliers may strengthen digital sovereignty by developing local engineering, Security Operations Center (SOC), auditing, and operational capacities. The key issue is whether procurement processes are competitive, auditable, and performance-based. Without strong integrity safeguards, high volumes of cybersecurity procurement may result in supplier concentration, vendor lock-in, or formal compliance rather than measurable resilience.

6.5. Romania

Romania also exhibits a mixed profile. While it performs relatively well in formal cyber capacity indices, its digital governance performance remains below that of the Nordic and Baltic countries. Procurement competition and institutional control continue to serve as important explanatory dimensions. Romania illustrates the distinction between possessing national cybersecurity capacity and achieving the practical implementation of secure, citizen-centered, and resilient digital governance.

6.6. Bulgaria

Bulgaria emerges as the most vulnerable case within the selected sample. Its weaker public sector integrity profile, higher supplier risk, and lower cyber resilience indicators point to a more fragile environment for smart city governance. In such a context, digital transformation may be affected by procurement inefficiencies, limited institutional control, and weaker cybersecurity implementation. Bulgaria therefore exemplifies the risk that, under conditions of lower integrity and weaker institutional oversight, digital governance capacity may remain unevenly developed or insufficiently protected.

7. Discussion

The comparative findings provide qualified support for the study's hypothesis. Countries with higher levels of public sector integrity—Denmark, Finland, and Estonia—generally exhibit stronger digital governance and cyber resilience profiles. However, the relationship is not deterministic. The cases of Hungary and Romania demonstrate that a country may possess strong formal cybersecurity capacities while simultaneously exhibiting integrity-related vulnerabilities. This suggests that cyber resilience indices should be interpreted alongside public procurement and institutional control indicators.

The primary theoretical conclusion is that smart city cybersecurity should be understood as a governance challenge. Firewalls, software tools, and incident response systems are necessary, but they are not sufficient. Public institutions must be capable of defining cybersecurity requirements, drafting technology-neutral and performance-based procurement specifications, managing conflicts of interest, auditing suppliers, measuring performance, and avoiding long-term vendor lock-in.

The importance of procurement integrity is well illustrated by the Microsoft Hungary case. According to the United States Department of Justice, Microsoft's Hungarian subsidiary paid more than USD 8.7 million in penalties in connection with bid-rigging and bribery allegations related to the sale of software licenses to Hungarian government entities between 2013 and 2015 [15]. Although the case was not a smart city cyber incident, it demonstrates that integrity vulnerabilities in IT procurement linked to public digital infrastructure constitute genuine public policy risks. According to the OECD, public procurement is generally one of the areas of government activity most exposed to corruption and waste, while integrity failures may result in lower-quality outputs, above-market prices, and delays [16], [22]. In cybersecurity procurement, this issue is particularly important because poor quality or merely formal compliance may translate into concrete vulnerabilities.

The SolarWinds Orion compromise illustrates cybersecurity risks within supply chains. The Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive because the compromise of SolarWinds products posed an unacceptable risk to U.S. federal civilian networks [17]. Although this was not a corruption case, it directly demonstrates that supplier oversight, vendor risk management, and software supply-chain security are integral components of public sector cyber resilience. A similar lesson emerges from the ENISA NIS360 report, which identifies complex supplier environments, uneven

levels of maturity, legacy systems, and inadequately protected assets as significant vulnerability factors in sectors covered by NIS2, particularly healthcare and public administration [18].

The importance of institutional capacity and internal controls is illustrated by the Conti ransomware attack against Ireland's Health Service Executive (HSE). An independent post-incident review commissioned by the HSE interpreted the attack not merely as a technical failure but also as an organizational, governance, control, and preparedness problem [19].

This aligns with the argument of the present study: cyber resilience encompasses not only the existence of tools and software but also decision-making responsibility, access management, logging, recovery procedures, auditability, and crisis coordination.

Estonia provides a positive example. The 2007 cyberattack campaign, which lasted for 22 days and affected government, banking, and media services, contributed to Estonia becoming one of Europe's leading examples of a digital state with strong cybersecurity coordination [20]. The Estonian case suggests that digital government development can be transformed into resilience only when it is accompanied by strong institutional coordination, public-private cooperation, auditable systems, and high levels of digital trust. The same logic is reinforced by Ukraine's Prozorro e-procurement system, which is built on the principle that "Everyone can see everything" and institutionalizes transparency, data openness, and procurement monitoring [21].

Vendor lock-in is particularly important in the context of smart city governance. It refers to situations in which a public institution becomes so dependent on a supplier, technology, or platform that switching providers becomes difficult, costly, or operationally risky. In smart cities, this may affect parking systems, surveillance platforms, smart street lighting, traffic management systems, public safety solutions, cloud infrastructures, or e-government portals. Vendor lock-in weakens the bargaining position of public authorities, increases long-term costs, and may create cybersecurity dependencies.

The findings also demonstrate that public sector competence is crucial. Integrity alone does not guarantee resilience if public institutions lack the technical expertise necessary to define their requirements effectively.

In such cases, integrity must operate through procedural safeguards, including independent needs assessments, separation of advisory and implementation roles, functional and technology-neutral tenders, conflict-of-interest controls, independent vulnerability assessments, incident response exercises, service-level monitoring, and clearly defined exit requirements. The overarching practical lesson is that the relationship between public sector integrity and cyber resilience becomes tangible through IT procurement practices, supply-chain oversight, institutional leadership responsibility, internal control mechanisms, and incident reporting cultures.

8. Implications

For researchers, this study offers an integrated analytical framework that connects public sector integrity, public procurement governance, supplier risk, and cyber resilience. This framework can be applied in future research on smart cities, digital governance, and public sector cybersecurity.

For policymakers, the findings suggest that cybersecurity investments should be evaluated not only in terms of expenditure levels or formal compliance but also through measurable resilience outcomes. Relevant indicators may include detection time, response time, remediation speed, backup and recovery testing performance, Security Operations Center (SOC) coverage, vulnerability remediation rates, and the results of independent audits.

For practitioners, the study highlights the importance of procurement design aimed at reducing supplier dependency. Smart city tenders should incorporate open standards, data portability requirements, exit strategies, clearly defined security requirements, audit rights, transparent subcontracting chains, and measurable performance indicators.

9. Conclusion

This study examined how public sector integrity may influence cyber resilience and the security of digital governance in smart city environments across Europe. Based on a comparative analysis of Denmark, Finland, Estonia, Hungary, Romania, and Bulgaria, the findings suggest that higher levels of integrity are generally associated with stronger cyber resilience and more advanced digital governance capacities. However, this relationship is mediated by procurement competition, supplier risk, institutional control, and the professional competence of the public sector.

The central conclusion of the study is that smart city cybersecurity is not merely a technical issue. It is also a matter of public sector integrity. Secure smart city governance requires transparent public procurement, accountable institutions, auditable suppliers, competent public sector purchasers, and measurable security outcomes. The future resilience of European smart cities therefore depends not only on firewalls and digital technologies, but also on the quality of the public governance systems that support them.

References

- [1] C.-L. Pau, „Smart governance: a framework for the future,” Smart Cities International Conference, Resilient Communities Empowered by Collective Intelligence, pp. 243–264, 2024.
- [2] M. Bolívar and A. Meijer, „Governing the smart city: a review of the literature on smart urban governance,” International Review of Administrative Sciences, vol. 82, no. 2, pp. 392–408, 2016.
- [3] Z. Tomor, A. Meijer, A. Michels and S. Geertman, „Smart governance for sustainable cities: findings from a systematic literature review,” Journal of Urban Technology, vol. 26, pp. 27–46, 2019.
- [4] Transparency International, Corruption Perceptions Index 2025, 2026.
- [5] World Bank, Worldwide Governance Indicators: Control of Corruption and Rule of Law, 2024/2025 release.
- [6] E-Governance Academy, National Cyber Security Index, 2026.
- [7] International Telecommunication Union, Global Cybersecurity Index 2024.

- [8] United Nations Department of Economic and Social Affairs, UN E-Government Survey 2024: E-Government Development Index.
- [9] European Commission, Single Market Scoreboard: Public Procurement Indicators, 2024.
- [10] V. G. Langa and R. D. Thakhathi, „The role of smart cities to promote smart governance in municipalities,” *Smart Cities and Regional Development Journal*, vol. 6, no. 2, 2022.
- [11] D. Kumar, „Actual practices of citizen participation in smart cities,” *Smart Cities and Regional Development Journal*, vol. 8, no. 3, 2024.
- [12] S. Carboni, „Smart Cities in comparison: An analysis of the best Smart Cities,” *Smart Cities and Regional Development Journal*, vol. 8, no. 3, 2024.
- [13] K. Radchenko, „The economic and social impacts of smart cities: multi-stakeholder pre-study results,” *Smart Cities and Regional Development Journal*, vol. 7, no. 2, 2023. 2019.
- [14] S. Barns, *Platform Urbanism: Negotiating Platform Ecosystems in Connected Cities*. Palgrave Macmillan, 2020.
- [15] U.S. Department of Justice, “Hungary Subsidiary of Microsoft Corporation Agrees to Pay \$8.7 Million in Criminal Penalties to Resolve Foreign Bribery Case,” 2019.
- [16] Integrity in Public Procurement: Good Practice from A to Z, OECD Publishing, 2007. Paris, <https://doi.org/10.1787/9789264027510-en>.
- [17] Cybersecurity and Infrastructure Security Agency, “Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise,” 2020.
- [18] European Union Agency for Cybersecurity, ENISA NIS360 2024, 2025.
- [19] PricewaterhouseCoopers, *Conti Cyber Attack on the HSE: Independent Post Incident Review*, Health Service Executive, 2021.
- [20] R. Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,” NATO Cooperative Cyber Defence Centre of Excellence, 2008.
- [21] OECD Observatory of Public Sector Innovation, “eProcurement System ProZorro,” 2020.
- [22] OECD Anti-Corruption and Integrity Outlook 2026: Harnessing the Integrity Advantage, OECD Publishing, Paris, <https://doi.org/10.1787/16708b78-en>.