Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 10, No. 3, August, Pp. 319-328

Cybersecurity management strategies for smart cities in Indonesia: cultural factors and implementation challenges

RG Guntur Alam*[1], Amrul Faruq[2], Machmud Effendy[2]
Universitas Muhammadiyah Bengkulu, Bengkulu, Indonesia[1]
Universitas Muhammadiyah Malang, Indonesia[2]

Article Info

Keywords:
Cybersecurity Management, Smart City, Cultural Context, Implementation Challenges, Actor-Network Theory

Article history:
Received: January 15, 2025
Accepted: April 20, 2025
Published: August 31, 2025

Cite:
R. G. Alam, A. Faruq, and M. Effendy, "Cybersecurity Management Strategies for Smart Cities in Indonesia: Cultural Factors and Implementation Challenges", *KINETIK*, vol. 10, no. 3, Aug. 2025. https://doi.org/10.22219/kinetik.v10i3.2226

*Corresponding author.
RG Guntur Alam
E-mail address:
rgguntural am@umb.ac.id

Abstract

The implementation of smart cities in Indonesia presents significant cybersecurity challenges, particularly amid bureaucratic complexity, low digital literacy, and limited institutional capacity. This study explores cybersecurity management strategies in the context of Jakarta Smart City (JSC), emphasizing sociotechnical dynamics and embedded cultural-institutional factors. Employing a qualitative approach and the Actor-Network Theory (ANT) framework, this research examines four key moments in the stabilization of cybersecurity networks: problematization, interessement, enrollment, and mobilization. Empirical findings reveal that challenges such as fragmented governance, security awareness gaps, and limitations in technological adaptation are addressed through context-specific strategies. These include regulatory reforms, multi-stakeholder collaboration, hybrid governance models, and the localization of international standards, particularly ISO/IEC 27001. The study also incorporates Indonesia's Personal Data Protection Law (Law No. 27/2022) as a foundational legal framework that supports the integration of regional cybersecurity policies. Rather than focusing solely on technical solutions, this research emphasizes the importance of aligning cybersecurity strategies with local norms, leadership structures, and user practices. The proposed strategic model contributes to the cybersecurity governance literature by integrating ANT perspectives with empirical insights from a developing country. It offers a locally adapted and scalable framework to guide policymakers and smart city administrators in building resilient and culturally sensitive cybersecurity systems.

1. Introduction

Smart cities integrate advanced technologies, including Information and Communication Technology (ICT) and the Internet of Things (IoT), to optimize urban resources, improve public services, and enhance citizens' quality of life. These initiatives aim to address the challenges of rapid urbanization, resource efficiency, and environmental sustainability [1]. The role of ICT in driving innovation across government, civil society, and the private sector is widely recognized. However, as cities become more connected, cybersecurity risks have become a critical concern due to increased vulnerabilities within digital infrastructures, IoT networks, and essential services [2].

International experiences, such as those in Dubai, Barcelona, Shanghai, and Como, have shown the importance of integrating cybersecurity strategies into smart city development frameworks [3][4]. These cities have adopted clear security protocols to protect urban data systems. In contrast, Indonesia's smart city initiatives have yet to fully incorporate cybersecurity as a core element of urban digital transformation [5].

Despite the growing adoption of smart city technologies in Indonesia, cybersecurity readiness remains insufficient. Government awareness of cyber threats is low, and legal instruments, such as the 2008 Electronic Information and Transactions (ITE) Law, are outdated and poorly enforced. A recent regulatory development, the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP), aims to strengthen Indonesia's cybersecurity posture. However, its implementation still faces structural and institutional challenges, especially at the regional level [6].

Furthermore, technical and operational gaps persist. Threat detection systems are reactive, stakeholder coordination is fragmented, and cybersecurity budgeting is often not prioritized [7]. Regulatory inconsistencies and a lack of proactive monitoring mechanisms exacerbate the risk of attacks. Cultural barriers, such as bureaucratic fragmentation, low digital literacy, and hierarchical decision-making patterns, compound these issues and hinder the adoption of standardized cybersecurity protocols [8][9].

Although various cybersecurity management standards exist globally, this study chooses ISO/IEC 27001 due to its wide international adoption, alignment with national technical guidelines by BSSN, and adaptability to local governance contexts. ISO/IEC 27001 provides a flexible yet structured framework for auditing, risk assessment, and policy development in public sector environments [10].

To address these multilayered challenges, this study adopts the Actor-Network Theory (ANT) as an analytical lens to explore the socio-technical dynamics that shape cybersecurity governance in Jakarta Smart City, a representative case study of smart city development in Indonesia. ANT enables a nuanced understanding of how human and non-human actors (institutions, technologies, and policies) interact, negotiate, and stabilize within cybersecurity networks [11].

This research divides the analytical process into four moments: Problematization, Interessement, Enrollment, and Mobilization—to explain how cybersecurity strategies evolve in practice. Unlike previous studies, this research emphasizes not only technical and regulatory dimensions but also cultural and organizational realities that influence policy effectiveness.

The result is a localized cybersecurity management model that identifies seven core challenges, such as fragmented governance, digital illiteracy, and lack of stakeholder collaboration, and provides targeted strategies, including cross-sectoral regulatory reform, culture-based digital training, hybrid governance through BLUD (local public service agency) status, and contextualized implementation of ISO/IEC 27001. While grounded in Jakarta's experience, this model offers practical insight for other developing nations facing similar issues in smart city cybersecurity governance.

2. Research Method

The philosophical framework guiding this research is critical realism. This approach seeks to uncover and explain the reasons behind occurrences and explores the structures and mechanisms that underpin observable social events [12]. The study revisits social phenomena, questions their nature, and seeks new insights. Specifically, the research aims to understand the context, obstacles, challenges, and key elements related to cybersecurity in Jakarta Smart City (JSC). Various factors or actors are considered, including those originating from human resources, technology, processes, policies, financial aspects, and other domains. A case study methodology was employed to gather data, utilizing informal and semi-structured interviews [13]. This flexible approach enables the researcher to pose follow-up questions during and after the interviews [8] [9].

The primary purpose of these interviews is to identify human and non-human factors influencing the implementation of cybersecurity within Indonesia's smart cities. The unit of analysis in this study is the network of actors involved in implementing cybersecurity in JSC.

To analyze the data, the study adopts template analysis, a method that involves creating a list of codes (template) to represent themes derived from the textual data [14].

This study employs an interpretative case study approach guided by Actor-Network Theory (ANT), as shown in Figure 1, to investigate the cybersecurity challenges in Jakarta Smart City [15]. Semi-structured interviews were conducted with key stakeholders; a total of 7 respondents participated in this study, comprising the Director of Jakarta Smart City, the Head of Cyber and Code Control Section, the Head of JSC Operational Unit, and 4 operational staff members. Each interview lasted between 45 and 90 minutes and was recorded with participant consent. The transcripts were then analyzed using template analysis, a structured coding technique that categorizes themes derived from the textual data [14].

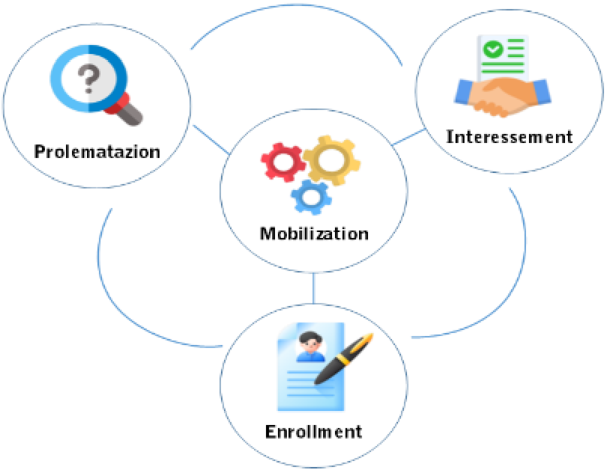

Figure 1. Actor-Network Theory (ANT) Workflow

Actor networks are established by implementing four stages of translation conducted by key actors [16] [17]. These stages aim to identify diverse actors within the network, which, in this study, include individuals, technologies, and processes [18]. The roles of these actors are defined, and strategies for aligning their interests with those of the key actors are employed to encourage them to progress through the OPP (Obligatory Passage Point) [19] [20]. Details of the research guide based on Actor-Network Theory are shown in Figure 2.

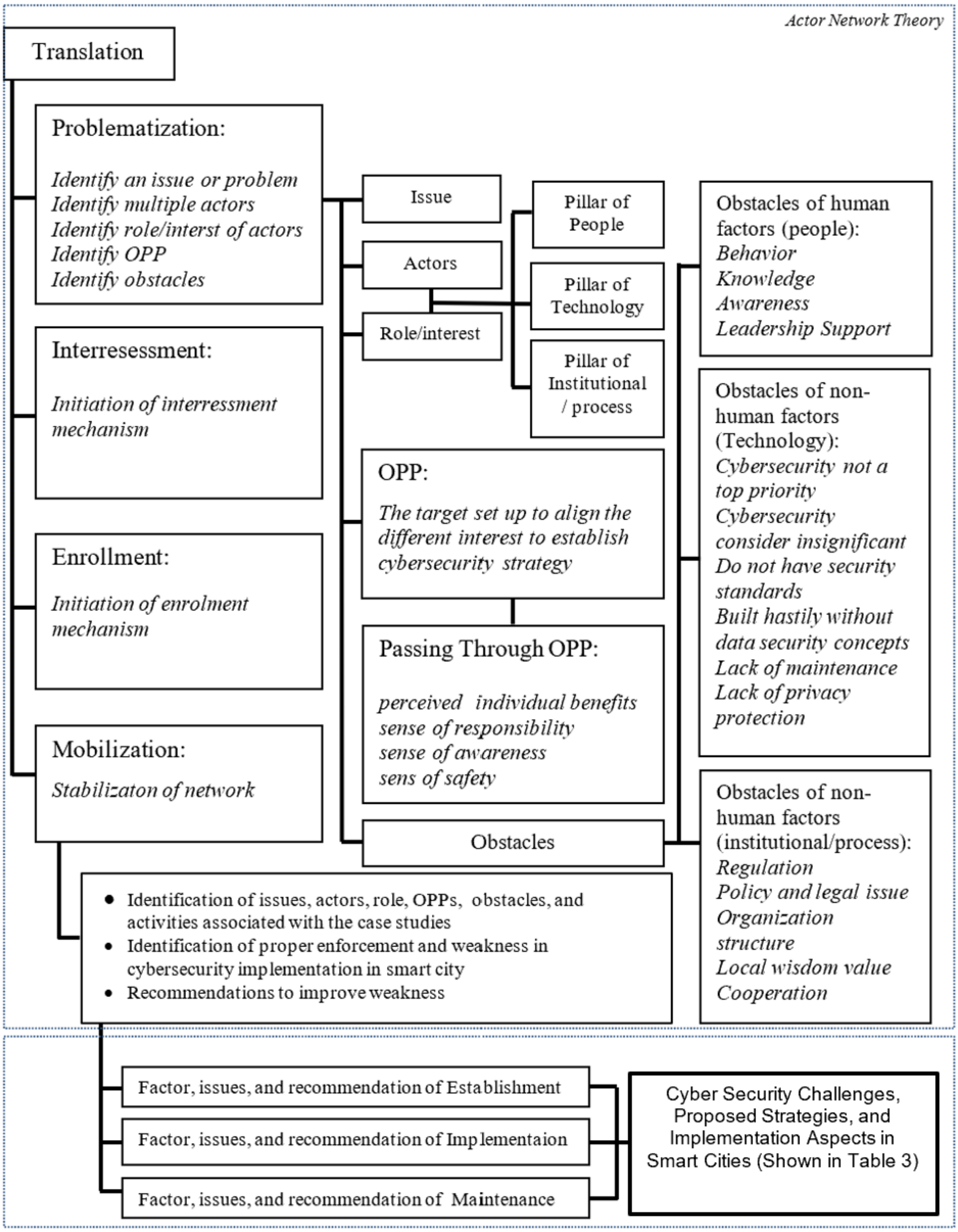
Actor Network Theory
Translation
Problematization:
Identify an issue or problem
Identify multiple actors
Identify role/interst of actors
Identify OPP
Identify obstacles
Interresessment:
Initiation of interressment mechanism
Enrollment:
Initiation of enrolment mechanism
Mobilization:
Stabilizaton of network
Issue
Actors
Role/interest
Pillar of People
Pillar of Technology
Pillar of Institutional / process
OPP:
The target set up to align the different interest to establish cybersecurity strategy
Passing Through OPP:
perceived individual benefits
sense of responsibility
sense of awareness
sens of safety
Obstacles
Obstacles of human factors (people):
Behavior
Knowledge
Awareness
Leadership Support
Obstacles of non-human factors (Technology):
Cybersecurity not a top priority
Cybersecurity consider insignificant
Do not have security standards
Built hastily without data security concepts
Lack of maintenance
Lack of privacy protection
Obstacles of non-human factors (institutional/process):
Regulation
Policy and legal issue
Organization structure
Local wisdom value
Cooperation
Identification of issues, actors, role, OPPs, obstacles, and activities associated with the case studies
Identification of proper enforcement and weakness in cybersecurity implementation in smart city
Recommendations to improve weakness
Factor, issues, and recommendation of Establishment
Factor, issues, and recommendation of Implementaion
Factor, issues, and recommendation of Maintenance
Cyber Security Challenges, Proposed Strategies, and Implementation Aspects in Smart Cities (Shown in Table 3)

Figure 2. Detail of Actor-Network Theory (ANT) Workflow

Cite: R. G. Alam, A. Faruq, and M. Effendy, "Cybersecurity Management Strategies for Smart Cities in Indonesia: Cultural Factors and Implementation Challenges", KINETIK, vol. 10, no. 3, Aug. 2025. https://doi.org/10.22219/kinetik.v10i3.2226

The translation process consists of the following steps:

1) Problematization Stage
   a) Identifying an Issue
   This step involves identifying issues related to cybersecurity implementation in smart cities. For instance, one issue could be the need to protect Indonesian smart cities from cyber threats. This issue helps guide the primary and secondary actors in framing the problem in relation to the research questions.
   b) Identifying Multiple Actors
   Potential actors in this network may include stakeholders such as the head of Jakarta's Information and Communication Office (policy-makers), the director of Jakarta Smart City, technical staff (employees), cybersecurity regulations, legal frameworks, and cooperation agreements on cybersecurity.
   c) Identifying Actors' Roles and Interests
   Examples of actor interests include: policymakers aiming for smart city success to enhance their leadership reputation, technical staff requiring safe and efficient working environments, and users ensuring data security for online transactions.
   d) Identifying the OPP
   The OPP represents a shared objective that aligns the varied interests of the actors to create a cybersecurity strategy. For instance, a collective effort to integrate cybersecurity into the smart city framework could serve as the OPP.
   e) Identifying Obstacles
   Common challenges might include low awareness, limited knowledge, and inadequate privacy safeguards.
2) Interessment Stage
   The interessment stage involves actions and initiatives aimed at supporting cybersecurity development. An example could be engaging all stakeholders in evaluating cybersecurity measures.
3) Enrollment Stage
   Enrollment focuses on planning, programming, and documenting steps to advance cybersecurity. For example, regularly documenting cyber incidents can help prioritize their resolution effectively.
4) Mobilization Stage
   During mobilization, the key actor ensures that all other actors act in accordance with their agreements and remain committed to the shared objectives.

To enhance the credibility of findings, data triangulation was applied by cross-referencing interview responses with government policy documents, industry reports, and expert opinions [21]. Preliminary findings were shared with selected experts to ensure accuracy and contextual relevance of interpretations.

From this perspective, cybersecurity implementation in smart cities is viewed as a network of human and non-human elements (referred to as actors in ANT terminology). It involves various interactions among these actors. Consequently, the interactions and actors shaping cybersecurity networks can be analyzed through the lens of ANT. By examining, analyzing, and interpreting data from this framework, researchers can validate or challenge factors influencing cybersecurity in smart cities and identify new elements. This process ultimately enhances the original conceptual framework tailored to cybersecurity within the context of smart cities.

3. Results and Discussion

Jakarta's cybersecurity risks align with those faced by other smart cities worldwide. For instance, Singapore's Smart Nation initiative experienced a major data breach in 2018 [22], affecting 1.5 million citizens, including medical records [23]. Similarly, Barcelona's smart city infrastructure was compromised when cybercriminals exploited IoT vulnerabilities to disrupt municipal services [2]. Meanwhile, Los Angeles' smart traffic management system was targeted by ransomware attacks, that sought to disable real-time traffic control systems [24]. Table 1 presents a comparative analysis of Jakarta's cybersecurity measures against those of other developed smart cities.

Table 1. Comparative Analysis of Cybersecurity Frameworks in Smart Cities

Strategy	Jakarta Smart City	Singapore	Barcelona	Los Angeles
ISO/IEC 27001 Adoption	Partial	Yes	Yes	Yes
AI-driven Threat Detection	Limited	Advanced	Moderate	Advanced
Smart City-Specific Cyber Law	No	Yes	Yes	Yes
Multi-Stakeholder Collaboration	Weak	Strong	Strong	Moderate
Budget Allocation for Cybersecurity	Limited	High	High	High

These comparisons indicate that Jakarta Smart City must enhance its cybersecurity regulations, invest in AI-driven security systems, and promote stakeholder collaboration to match the cybersecurity maturity of Singapore, Barcelona, and Los Angeles.

This study uses the Actor-Network Theory (ANT) approach to analyze the dynamics of cybersecurity implementation in the Jakarta Smart City (JSC) ecosystem. ANT views technology not as a passive entity but as the result of the construction of a complex and continuously negotiated socio-technical network. In this context, the results and discussion are divided based on four main moments of ANT, namely: (1) Problematization, (2) Interessement, (3) Enrollment, and (4) Mobilization. The Problematization stage is explained through two analytical focuses: Punctualization, which maps actors and network relations, and Obligatory Passage Point (OPP), which identifies mandatory passage points toward common goals. The discussion then continues with an analysis of the negotiation of interests and the formation of strategic coalitions through Interessement and Enrollment to see how the cybersecurity system is consolidated and mobilized in the real practice of Jakarta Smart City.

3.1 Punctualization: Identifying Key Actors in JSC Cyber Security

At this stage, ANT is used to “open the black box” of the JSC cybersecurity system. The study found that there are three key actors that form the network configuration in cybersecurity management, namely: the JSC Director, the DKI Jakarta Communication, Informatics, and Statistics Agency (*Diskominfotik*), and the Operational Implementation Unit. Each actor has an interdependent role in realizing a reliable information security system.

The JSC Director acts as a focal actor who coordinates policy-making, internal regulation development, and the strategic direction of cybersecurity. The Communication and Informatics Agency functions as a policy-directing actor at the local government level, while the UPO carries out daily technical operations and implements established policies.

The relationship and dynamics among the actors are visualized with descriptive information in the following Table 2:

Table 2. Dynamics of the Relationship Between Actors in the Implementation of Cybersecurity in JSC

Puctualized Actor	Member	Task	Obstacle/Support	Goal
Director of JSC	Process, People, Technology	Aims to negotiate, motivate, coordinate, and then work with other towardalized actors	Must have flexibility in planning programs and budgets	Initiation, implementation, monitoring and evaluation of cybersecurity
The DKI Jakarta Province Communication, Informatic, and Statistic Agency	Process (regulations, standards and laws)	Prepare rules, regulations, and standards for the successful implementation of cybersecurity	Must be assisted by other units to carry out the functions assigned by the governor	Leadership in cybersecurity implementation
The Operational Executing Unit	People, Technology	Implement cyber security for public services in Jakarta Smart City	Work according to the rules, regulations, and direction of the leadership	Improve cybersecurity in public services

3.2 Obligatory Passage Point (OPP)

The next stage in the punctualization moment is to examine the Obligatory Passage Point (OPP). All actors must pass the OPP to achieve the common goal of implementing an integrated and effective cybersecurity system in Jakarta. In the context of JSC, this OPP includes elements such as agreement on security standards (ISO/IEC 27001), the need for regional regulations (Governor Regulations), and synergy between institutions.

The findings of this stage indicate sectoral egos, reliance on a top-down approach, and low digital literacy. These are the main obstacles to achieving the OPP. A statement from one informant illustrates the resistance between government units to accepting new security protocols:

"*When implementing a new system, we often face resistance from other departments who view cybersecurity protocols as disrupting their workflow*."

On the other hand, low digital literacy makes operational staff the weakest link in the system. Gamified training and culture-based socialization have been carried out, but behavioral change requires a more sustainable strategy. The OPP structure in this context can be visually depicted in Figure 3 below:

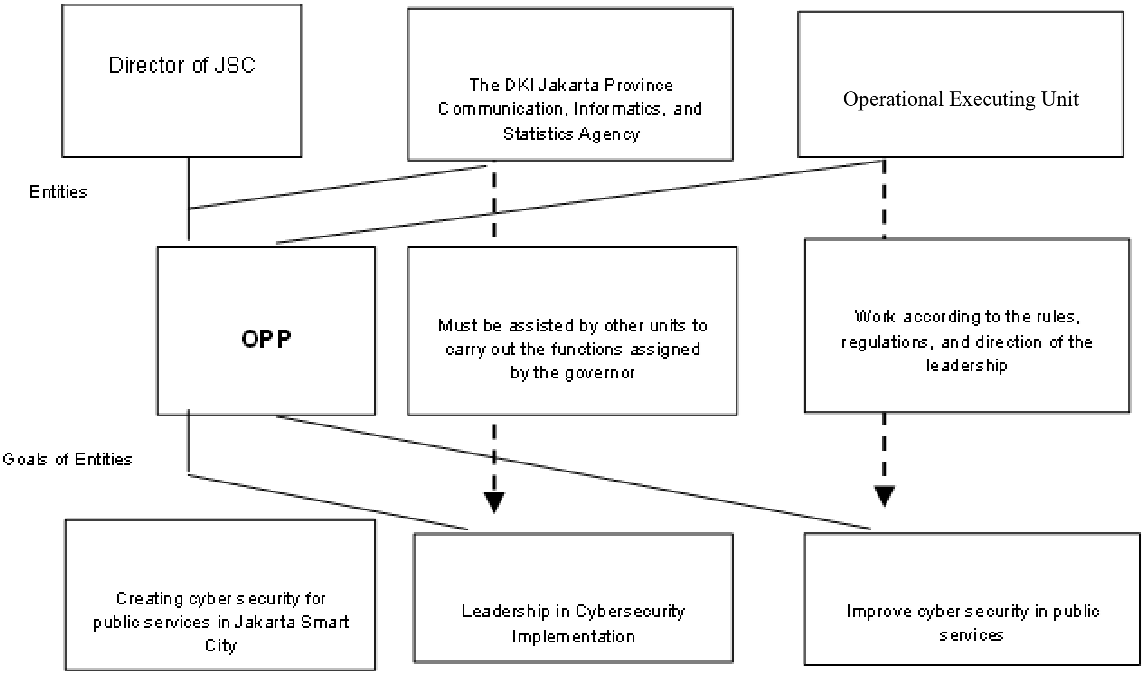
Director of JSC
The DKI Jakarta Province Communication, Informatics, and Statistics Agency
Operational Executing Unit
Entities
OPP
Must be assisted by other units to carry out the functions assigned by the governor
Work according to the rules, regulations, and direction of the leadership
Goals of Entities
Creating cyber security for public services in Jakarta Smart City
Leadership in Cybersecurity Implementation
Improve cyber security in public services

Figure 2. Obligatory Passage Point on JSC Cybersecurity Actor Network

After the Problematization moment, the following three ANT moments (interessement, enrollment, and mobilization) were conducted. Through these three moments, implementing cybersecurity in Jakarta Smart City reveals the complex interaction between technological needs and deep-rooted cultural-institutional factors. This study identifies three dominant cultural dimensions that shape cybersecurity practices: (1) bureaucratic fragmentation, (2) low digital literacy, and (3) leadership-dependent decision-making. These factors interact with implementation challenges to create a unique governance landscape that requires context-specific strategies.

3.3 Cultural Barriers to Cybersecurity Adoption

The study revealed how Indonesia's bureaucratic culture significantly hampers cybersecurity integration. Sectoral ego—a reluctance to collaborate across government units—emerged as a persistent barrier. As one operational unit informant explained:

"*When implementing a new system, we often face resistance from other departments who view cybersecurity protocols as disrupting their workflow. To overcome this, we have to issue a Governor Regulation to enforce compliance.*"

This finding is consistent with [25], Indonesia's bureaucracy, where vertical silos and territorialism often undermine horizontal coordination. The reliance on regulatory coercion (e.g., the Governor's Decree) to overcome resistance suggests that voluntary cooperation remains elusive in this cultural context. Digital literacy gaps compound these institutional challenges. The JSC Director stated emphatically:

"No matter how smart our security technology is, human operators remain the weakest link. Many employees still write passwords on sticky notes attached to their monitors."

This statement reflects a broader social issue—Indonesia's digital literacy index was only 3.49 out of 5 in 2022 [26]. JSC's response through gamified training (e.g., WhatsApp cloning simulation) demonstrates an attempt to bridge this gap using a culturally familiar medium. However, the persistence of this fundamental security omission suggests that behavioral change requires sustained intervention beyond a one-off training program.

3.4 Implementation Challenges in a Resource-Constrained Environment

The study revealed how budget constraints force pragmatic—and potentially risky—tradeoffs between functionality and security. A Director's admission that "*We postpone advanced security features for low-interaction applications due to cost constraints*" illustrates a common dilemma in smart cities in developing countries [27]. This "security-as-a-second-thought" approach leaves systems vulnerable during the initial deployment phase. Technology adaptation is another hurdle. Although JSC has upgraded its firewall from Layer 3 to Layer 7, the Cyber Section Chief admitted:

"*Security is a never-ending race. Every time we patch one vulnerability, a new threat emerges that requires a different solution*."

This technology treadmill strains limited human and financial resources. A Proof of Concept (POC) approach—testing technologies such as F5 network security before full deployment—emerged as a risk mitigation strategy. However, informants noted that the POC process often delays the implementation timeline, creating tension between security teams and departments that push for rapid digital service rollouts.

3.5 Hybrid Governance as a Strategic Response

Facing these challenges, JSC developed a hybrid governance model that blends bureaucratic hierarchy with network collaboration. Three key strategies emerged:

First, leveraging its BLUD (Regional Public Service Agency) status to navigate regulatory constraints. As the Director explained:

"*Our BLUD status allows for service monetization, funding cybersecurity innovation while maintaining SNI 27001 compliance.*"

This flexible autonomy differs from conventional bureaucratic units, suggesting that a semi-independent governance structure may be better suited to the dynamic needs of cybersecurity.

Second, multi-stakeholder partnerships address capability gaps. Collaboration with the Swiss-German University provides technical skills enhancement, while BSSN (National Cyber and Crypto Agency) manages certification. An operational staff member described this symbiosis:

"*We cannot work alone. When faced with advanced persistent threats, we directly contact the network at BSSN and university partners.*"

Third, cultural adaptation to security protocols. Rather than simply adopting international standards, JSC modifies implementations to suit local contexts. The Clean Desk policy—adapted from ISO but delivered through JSC's internal socialization program—exemplifies this glocalization. As the Head of the Cyber Section noted:

"We repackaged security concepts in familiar formats such as infographics and announcements on mosque pulpits to increase staff acceptance."

The empirical findings discussed in this section highlight that cybersecurity implementation in Jakarta Smart City is shaped by complex socio-cultural and institutional dynamics. Table 3 illustrates the interrelationships between these challenges, proposed strategies, and key aspects of implementation within the smart city cybersecurity framework.

Table 3. Cybersecurity Challenges, Proposed Strategies, and Implementation Aspects in Smart Cities

Challenges	Proposed Strategies	Aspects	Strategy Details
Fragmented bureaucracy in governance	Institutional reform and strengthening of regulatory leadership	Regulations and Organizational Structure	Issuance of Governor Regulations to enforce cross-sector compliance; strengthening Jakarta Smart City's coordinating role.
Low digital literacy among personnel	Culturally-based digital education	Human Resource Capacity	Cybersecurity training using gamification and culturally relevant simulations; awareness campaigns through local media and places of worship.
Security as a secondary priority in budget allocation	Reprioritizing cybersecurity budget during early implementation	Risk and Budget Management	Setting minimum cybersecurity features at the planning stage of each application development.
Technology adaptation burdens in limited-resource environments	Phased approach using Proof of Concept (POC)	Technology and Implementation	Testing systems, such as F5, before full implementation; developing realistic technology roadmaps.
Reliance on traditional bureaucratic hierarchy	Implementation of hybrid governance model	Organizational Model	Utilization of BLUD status for flexible funding and management of cybersecurity innovation.
Technical capability gaps within internal staff	Multi-stakeholder partnerships	Collaboration and Capacity Building	Collaboration with universities and BSSN for technical training and certification; engagement with tech industry players.
Mismatch between global standards and local practices	Localization of international standards	Policy Glocalization	ISO 27001 implementation adjusted through internal outreach and use of culturally familiar formats (infographics, mosque announcements).

Compared to previous studies on smart city cybersecurity in Indonesia (see [7],[23]), this research provides a deeper contextual perspective by integrating socio-cultural dynamics into the analysis. While existing studies often emphasize technical controls and policy recommendations, this study uniquely applies Actor-Network Theory to map negotiation processes, resistance patterns, and actor interactions, which are often overlooked. The triangulation of field interviews, policy documents, and comparative benchmarks validates the robustness of the findings. The resulting framework is not only grounded in empirical evidence but also aligned with practical needs and regulatory landscapes.

This study fills a crucial gap in existing literature by combining technical frameworks with socio-cultural analysis, offering a comprehensive understanding of cybersecurity governance in a smart city context. The proposed strategies are validated through empirical findings and are applicable to urban settings in developing countries with similar institutional challenges. These findings are expected to inform not only academic discourse but also regional and national policy strategies on smart city cybersecurity governance in Indonesia.

4. Conclusion

This study concludes that cybersecurity in the smart city ecosystem is a multidimensional challenge that cannot be solved through a purely technical approach. The implementation of cybersecurity in Jakarta Smart City is heavily influenced by institutional fragmentation, cultural dynamics, and low digital literacy among stakeholders. Through a qualitative approach and the Actor-Network Theory (ANT) framework, this study reveals how bureaucratic structures, leadership-dependent decision-making patterns, and barriers to cross-sector coordination significantly shape cybersecurity practices and policies.

Empirical data from informants show that adaptive strategies, such as hybrid governance models, cultural context-based awareness-raising programs, and the application of proof-of-concept-based technologies, have been effective in reducing institutional and operational risks. Jakarta Smart City's use of flexible institutional structures such as BLUDs, as well as strategic partnerships with BSSN, academics, and the private sector, are pragmatic responses to evolving cybersecurity needs.

The proposed strategies—ranging from regulatory reform and stakeholder collaboration to investment in artificial intelligence-based detection systems—emphasize the importance of aligning global standards with local realities. The process of policy glocalization that has been implemented also shows the potential to increase the acceptance and effectiveness of cybersecurity policies in diverse bureaucratic and cultural environments. This study contributes to the enrichment of smart city cybersecurity literature by offering a context-based framework and empirical findings. These findings not only represent the governance landscape of Jakarta but also serve as a starting point for other developing countries in designing resilient, adaptive, and inclusive cybersecurity policies. Further research is recommended to explore the long-term impact of this strategy, assess its scalability, and examine the role of emerging technologies such as blockchain and artificial intelligence in strengthening urban cybersecurity resilience.

Acknowledgement

The author acknowledges the invaluable contributions of all those who supported this research, particularly Jakarta Smart City and the Informatics Systems Department at Universitas Muhammadiyah Bengkulu.

References

[1] A. M. Toli and N. Murtagh, “The Concept of Sustainability in Smart City Definitions,” *Front. Built Environ.*, vol. 6, no. June, pp. 1–10, 2020. https://doi.org/10.3389/fbuil.2020.00077

[2] M. Kalinin, V. Krundyshev, and P. Zegzhda, “Cybersecurity risk assessment in smart city infrastructures.,” *Machines*, vol. 9., no. 4, p. 78, 2021. https://doi.org/10.3390/machines9040078

[3] M. D. S. Hadi, P. Widodo, and R. W. Putro, “Analysis of the Impact of the Covid 19 Pandemic in Indonesia from a Cybersecurity Point of View,” *Natly. J.*, vol. 1, no. 1, pp. 1–9, 2020.

[4] R. G. G. Alam and H. Ibrahim, “Cybersecurity Strategy for Smart City Implementation,” in *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, 2019. https://doi.org/10.5194/isprs-archives-XLII-4-W17-3-2019

[5] L. Axon *et al.*, “Emerging cybersecurity capability gaps in the industrial internet of things: Overview and research agenda.,” *Digit. Threat. Res. Pract.*, vol. 3, no. 4, pp. 1–27, 2022. https://doi.org/10.1145/3503920

[6] M. R. Syailendra, G. Lie, and A. Sudiro, “Personal Data Protection Law in Indonesia: Challenges and Opportunities,” . *Indon. L. Rev.*, vol. 14, p. 175, 2024. https://doi.org/10.15742/ilrev.v14n2.1

[7] R. G. Alam, H. Ibrahim, and I. R. Karas, “Key Issues in Cybersecurity Implementation in Government Agencies: A Case Study in Jakarta Smart City,” in *In International Conference on Computing and Informatics*, Singapore: Springer Nature Singapore., 2024, pp. 3–16. https://doi.org/10.1007/978-981-99-9589-9_1

[8] R. G. Guntur Alam and H. Ibrahim, “Cybersecurity implementation succes factors in smart city,” *J. Theor. Appl. Inf. Technol.*, vol. 99, no. 13, pp. 3353–3364, 2021.

[9] A. R. Arief, “An analysis of cybersecurity policies and practices in public administration.,” *J. public Represent. Soc. Provis.*, vol. 2, no. 2, pp. 88–100, 2022. https://doi.org/10.55885/jprsp.v2i2.211

[10] A. Salihu and R. Dervishi, “Evaluating the Impact of Risk Management Frameworks on IT Audits: A Comparative Analysis of COSO, COBIT, ISO/IEC 27001, and NIST CSF.,” in *In 2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, IEEE, 2024, pp. 1–8. https://doi.org/10.1109/ICECCE63537.2024.10823548

[11] T. Ryan, N. Ryan, and B. Hynes, “The integration of human and non-human actors to advance healthcare delivery: unpacking the role of actor-network theory, a systematic literature review,” *BMC Health Serv. Res.*, vol. 24, no. 1, pp. 1–33, 2024. https://doi.org/10.1186/s12913-024-

11866-4

[12] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, “Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework.,” *Inf. Syst. Front.*, vol. 1, no. 22, 2022. https://doi.org/10.1007/s10796-020-10044-1

[13] R. G. Alam, D. Abdullah, H. Ibrahim, and I. R. Karas, “Building a Resilient Smart City Ecosystem: A Comprehensive Security and Cybersecurity Management Model.,” in *In The Proceedings of the International Conference on Smart City Applications*, Cham: Springer Nature Switzerland., 2023, pp. 596–607. https://doi.org/10.1007/978-3-031-53824-7_53

[14] M. Tight, *Designing case studies. The sage handbook for qualitative research design, 6th edn.* SAGE Publications Ltd, Thousand Oaks, 2022.

[15] M. Striepe, “Combining concept mapping with semi-structured interviews: adding another dimension to the research process.,” *Int. J. Res. Method Educ.*, vol. 44, no. 5, pp. 519–532, 2021. https://doi.org/10.1080/1743727X.2020.1841746

[16] Y. S. Chen and S. T. Wu, “An exploration of actor-network theory and social affordance for the development of a tourist attraction: A case study of a Jimmy-related theme park, Taiwan.,” *Tour. Manag.*, vol. 82, p. 104206, 2021. https://doi.org/10.1016/j.tourman.2020.104206

[17] R. Cury, M. Kennelly, and M. Howes, “Enacting environmental commitments and initiatives in Australian Olympic sport: an actor-network theory perspective.,” *Manag. Sport Leis.*, no. 1–18, 2024. https://doi.org/10.1080/23750472.2023.2299823

[18] M. A. Sarlak, Y. Salamzadeh, and F. S. Farzad, “Actor-network theory and networked organizations, proposing a conceptual framework.,” *Contemp. Appl. Actor Netw. Theory*, pp. 197–210, 2020. https://doi.org/10.1007/978-981-15-7066-7_11

[19] K. Park, S. Park, and T. J. Lee, “Analysis of a spatial network from the perspective of actor-network theory.,” *Int. J. Tour. Res.*, vol. 22, no. 5, pp. 653–665, 2020. https://doi.org/10.1002/jtr.2363

[20] M. Bolz, S. Mallon, and M. S. Estrada, *Actor-Network Theory (ANT) as a Methodology for Researching Academic Knowledge Circulation.* In Routledge Handbook of Academic Knowledge Circulation, 2023.

[21] I. R. Ticau, M. C. Dan, S. Hadad, and P. Nistoreanu, “Sustainable development in peri-urban regions: A triangulation analysis,” *Sustainability*, vol. 15, no. 20, p. 14837, 2023. https://doi.org/10.3390/su152014837

[22] M. Aslam *et al.*, “Getting Smarter about Smart Cities: Improving Data Security and Privacy through Compliance,” *Sensors*, vol. 22, no. 23, p. 9338, 2022. https://doi.org/10.3390/s22239338

[23] K. Khoirunnisa and D. Jubaidi, “Indonesia’s Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism.,” *Polit. J. Public Adm. Polit. Sci. Int. Relations*, vol. 2, no. 2, pp. 62–82, 2024. https://doi.org/10.61978/politeia.v2i2.211

[24] J. S. Gracias, G. S. Parnell, E. Specking, E. A. Pohl, and R. Buchanan, “Smart cities—a structured literature review.,” *Smart Cities*, vol. 6, no. 4, pp. 1719–1743, 2023. https://doi.org/10.3390/smartcities6040080

[25] M. Sawir, *Birokrasi Pelayanan Publik Konsep, Teori, Dan Aplikasi*. Deepublish, 2020.

[26] M. A. A. Pangestu and M. Christin, “Analisis Strategi Komunikasi Program Indonesia Makin Cakap Digital Kementerian Komunikasi dan Informatika dalam Meningkatkan Literasi Digital,” *JIIP-Jurnal Ilm. Ilmu Pendidik.*, vol. 5, no. 9, pp. 3272–3280, 2022.

[27] D. Kim and S. Kim, “Role and challenge of technology toward a smart sustainable city: Topic modeling, classification, and time series analysis using information and communication technology patent data,” *Sustain. Cities Soc.*, vol. 82, p. 103888, 2022. https://doi.org/10.1016/j.scs.2022.103888