JOURNAL OF PUBLIC ADMINISTRATION AND GOVERNANCE SYSTEM
E-ISSN: 3123-3597 | Volume 3 No 1 2026

PUBLION

Knowledge Transformation through AI in Public Institutions

Naledi T. Mokoena[1],
Department of Public Administration and Governance College of Humanities, University of Ghana, Accra, Ghana
**naledi.mokoena@ug.edu.gh*

Abstract

Artificial Intelligence (AI) is increasingly integrated into public administration as governments seek to enhance decision-making, efficiency, and responsiveness in complex environments. In public security institutions within developing countries, however, technological adoption is shaped by hierarchical governance structures, resource constraints, and institutional instability. This study aims to examine how AI transforms knowledge management practices and how institutional context conditions the sustainability of AI-based knowledge systems in public security governance. The research adopts a qualitative case study design based exclusively on secondary data, including academic literature, institutional reports, and policy documents related to AI implementation in public administration. An analytical framework integrating knowledge management theory and dynamic capabilities theory guides the interpretation of how AI influences knowledge creation, structuring, dissemination, and application. Thematic content analysis is used to identify patterns of institutional mediation, governance constraints, and adaptive learning processes within a developing country security context. Particular attention is given to how hierarchical authority, confidentiality regimes, resource limitations, and digital skill gaps shape the durability of AI-driven transformation. The findings indicate that AI enhances analytical capacity and formalizes knowledge routines, but its long-term institutionalization depends on governance stability, leadership continuity, and sustained competence development. The study concludes that AI-driven knowledge transformation in public security administration is a context-dependent institutional process rather than a purely technological upgrade. By integrating technological, organizational, and governance perspectives, this research contributes to advancing theoretical understanding of AI-enabled transformation in public sector settings.

Keyword

Artificial Intelligence; Public Administration; Knowledge Management; Governance.

1. Introduction

Artificial Intelligence (AI) has progressively emerged as a transformative force in contemporary societies, reshaping economic, political, and administrative systems. Its rapid development, supported by advances in data availability, computational power, and algorithmic innovation, has expanded its influence beyond the private sector into governmental institutions (Parly, 2019; Wirtz et al., 2019). Public administrations are increasingly confronted with expectations to modernize their services, enhance responsiveness, and improve decision-making capacities in complex and data-rich environments (Misuraca & Van Noordt, 2020; De Sousa et al., 2019). In this context, AI is often portrayed as a strategic lever capable of strengthening efficiency, transparency, and

Received: 20 November 2025 **Revised: 22 November 2025** **Published: 5 January 2025**

policy design (Önder & Saygili, 2018; Pencheva et al., 2018). Security-oriented administrations, in particular, face growing volumes of digital information that require structured and rapid analytical processing. The integration of AI into such institutions is therefore closely linked to the management of knowledge, intelligence production, and anticipatory governance. As public organizations navigate digital transformation, AI becomes intertwined with broader questions of organizational adaptation and institutional change (Nutt & Backoff, 1997). These developments situate AI not merely as a technical tool but as a potential driver of administrative transformation.

Despite this growing interest, the implementation of AI within public administrations remains uneven and context-dependent. While private-sector adoption has accelerated, public organizations often lag behind due to bureaucratic structures, regulatory constraints, and limited digital capacities (Wirtz et al., 2019; Sun & Medaglia, 2019). The challenges are particularly pronounced in security institutions, where confidentiality, hierarchical authority, and political sensitivity shape operational practices (Valérie D., 2019; Mazzucchi, 2019). In developing country contexts, additional constraints such as resource scarcity, infrastructural limitations, and administrative instability further complicate technological integration (De Sousa et al., 2019; Maciejewski, 2017). These realities make AI adoption in public security institutions a complex organizational issue rather than a purely technical decision. Knowledge production in such settings is closely tied to risk assessment, preventive policing, and strategic intelligence, thereby amplifying the stakes of technological change. Consequently, understanding how AI interacts with existing knowledge practices becomes critical for ensuring responsible and effective implementation. The transformation of knowledge management in security administrations therefore represents both a practical and theoretical concern.

Existing literature has documented multiple applications of AI in public services, ranging from chatbots and process automation to predictive analytics and cognitive security systems (Wirtz et al., 2019; Androutsopoulou et al., 2019). Scholars have highlighted AI's potential to improve efficiency, reduce costs, and enhance accessibility of services (Purdy & Daugherty, 2016; Gartner & Hiebl, 2017). In the security domain, AI has been associated with improved threat detection, data exploitation, and decision-support mechanisms (Valérie D., 2019). Moreover, research on big data and digital governance emphasizes AI's capacity to process large volumes of information and support policy innovation (Kim et al., 2014; Pencheva et al., 2018). Within organizations, AI has also been linked to learning processes and innovation dynamics (Anderson et al., 2014). These contributions collectively suggest that AI holds significant promise for public administration modernization. However, much of this literature remains either descriptive or focused on technological capabilities rather than organizational transformation. As a result, the deeper implications of AI for knowledge management structures within public security institutions remain insufficiently explored.

Knowledge management has long been recognized as a central pillar of organizational performance and adaptation. AI contributes to knowledge creation by identifying hidden patterns in data and generating insights that may otherwise remain undetected (Deng & Yu, 2014; Esuli & Sebastiani, 2010). It also facilitates knowledge storage, retrieval, and dissemination through structured digital systems and intelligent platforms (Alamoodi et al., 2021). In social media and text analysis contexts, sentiment analysis techniques allow organizations to interpret public attitudes and behavioral trends (Ji et al., 2015; Chung et al., 2015). These technological capabilities suggest a strong interconnection between AI and the knowledge management cycle. Nevertheless, the majority of studies emphasize technical models and algorithmic performance rather than organizational learning processes. There remains limited empirical attention to how AI reconfigures routines of cataloging, verification, and dissemination within hierarchical public security institutions. Furthermore, the translation of AI-generated outputs into actionable administrative knowledge is rarely examined in depth. This gap becomes particularly significant in contexts where knowledge reliability and confidentiality are paramount.

Theoretical perspectives on organizational adaptation provide additional insight into the potential implications of AI integration. The Resource-Based View highlights the importance of valuable and rare resources for sustaining performance (Wernerfelt, 1984; Barney, 1991). However, critiques of its static orientation led to the emergence of the dynamic capabilities framework, which emphasizes the ability to reconfigure resources in response to environmental change (Teece et al., 1997; Wang & Ahmed, 2007). Dynamic capabilities are rooted in structured learning processes rather than ad hoc problem-solving (Winter, 2003). In public administrations undergoing digital transformation, AI may serve as a catalyst for such reconfiguration processes. Yet, empirical research connecting AI adoption to dynamic knowledge processes within security administrations remains scarce. The specific mechanisms through which AI stimulates competence development, learning routines, and knowledge institutionalization in developing country contexts are not well understood. Consequently, theoretical integration between AI, knowledge management, and public sector specificity remains incomplete.

The literature also identifies managerial and ethical challenges associated with AI deployment in government settings. Concerns regarding transparency, trust, and responsible use of automated systems have been widely discussed (Araujo et al., 2020; Wirtz et al., 2019). In security institutions, these concerns are intensified by the sensitivity of data and the potential consequences of analytical errors (Valérie D., 2019). Moreover, AI systems depend heavily on data quality, governance structures, and user competence (Deng et al., 2015; Baker et al., 2020). In developing countries, limited digital infrastructure and uneven skill distribution may hinder effective adoption (De Sousa et al., 2019). While these challenges are acknowledged in the literature, they are often examined in isolation rather than as part of a comprehensive knowledge transformation process. There is limited synthesis of how contextual constraints interact with AI to reshape knowledge production and circulation within public security administrations. Addressing this gap requires moving beyond technological assessment toward organizational analysis.

Taken together, these strands of literature reveal several interrelated research gaps. First, there is insufficient understanding of how AI concretely restructures the stages of knowledge creation, structuring, dissemination, and application within security-focused public administrations. Second, contextual factors specific to developing country environments—such as administrative instability, resource constraints, and hierarchical rigidity—are rarely integrated into analyses of AI-driven transformation. Third, the sustainability of AI-based knowledge practices in politically sensitive and confidential settings remains underexplored. Filling these gaps is necessary to clarify how AI can move from experimental adoption to institutionalized practice. Without such understanding, public security administrations risk adopting technologies that remain peripheral or misaligned with organizational realities. A comprehensive examination of AI’s impact on knowledge management is therefore justified by both theoretical and practical considerations.

In response to these gaps, this study aims to examine how AI transforms knowledge management processes within a public security administration operating in a developing country context. It seeks to identify how AI reshapes knowledge creation, organization, dissemination, and application in hierarchical and confidential environments. The study further investigates how contextual constraints influence the trajectory of AI-driven knowledge transformation. By articulating these objectives, the research addresses the broader question of how AI can be aligned with the structural and managerial specificities of public security institutions. The urgency of this inquiry lies in the accelerating digitalization of governmental functions and the increasing reliance on data-driven decision-making (Misuraca & Van Noordt, 2020; Wirtz et al., 2019). As public administrations face growing societal expectations for efficiency and accountability, understanding the organizational implications of AI becomes critical. This research therefore contributes to advancing theoretical integration between AI and knowledge management while responding to pressing administrative challenges in developing country security contexts.

2. Research Method

This study adopts a qualitative research design grounded in a single-case study approach based exclusively on secondary data (Ruggiano & Perry, 2017; Farquhar et al., 2020). The qualitative orientation is appropriate because the research seeks to understand complex organizational processes related to knowledge management transformation within a public security administration, rather than to measure causal relationships or test statistical associations (Farquhar et al., 2020). Knowledge creation, structuring, dissemination, and application are socially embedded processes shaped by hierarchical norms, institutional constraints, and contextual specificities that require interpretive analysis (Schlunegger et al., 2024). A case study design enables an in-depth and context-sensitive examination of how Artificial Intelligence is positioned within a specific administrative environment in a developing country (Farquhar et al., 2020). The analytical framework integrates three interrelated dimensions derived from the literature: Artificial Intelligence as an organizational instrument, knowledge management cycles, and public sector specificity in security institutions. This design is suitable because it allows the researcher to explore how these dimensions interact within a bounded institutional setting (Farquhar et al., 2020). By focusing on documentary and archival sources, the study ensures analytical coherence while maintaining alignment with established theoretical constructs (Ruggiano & Perry, 2017). The qualitative case study approach thus provides a structured yet flexible framework for examining organizational transformation in a context characterized by confidentiality and institutional complexity (Cheong et al., 2023).

The data sources consist exclusively of secondary materials, including academic publications, official institutional documents, policy reports, internal administrative guidelines, and publicly available documentation related to Artificial Intelligence initiatives in public security contexts (Ruggiano & Perry, 2017). These documents were identified through systematic searches in academic databases and institutional repositories, guided by keywords related to Artificial Intelligence, knowledge management, public administration, and security governance. The units of analysis are organizational practices and institutional processes within a public security administration operating in a developing country environment. Data collection involved document retrieval, classification, and coding according to predefined analytical dimensions derived from the theoretical framework (Schlunegger et al., 2024). The primary analytical dimensions include knowledge creation, knowledge structuring, knowledge dissemination, knowledge application, organizational hierarchy, data governance, and contextual constraints such as resource limitations and administrative instability. A structured coding grid was developed to ensure consistency in categorizing information across documents (Cheong et al., 2023). The analytical procedure followed thematic content analysis, allowing systematic identification of patterns related to AI-driven knowledge transformation (Ruggiano & Perry, 2017). This approach ensures that variables and dimensions remain theoretically grounded and directly linked to the research objectives (Farquhar et al., 2020).

To enhance validity and reliability, the study employed methodological triangulation across multiple types of secondary sources, including academic literature, institutional records, and policy documentation (Ruggiano & Perry, 2017; Cheong et al., 2023). Construct validity was strengthened by clearly defining analytical dimensions based on established theoretical frameworks and by maintaining alignment between research questions and coding categories (Farquhar et al., 2020). Reliability was supported through a transparent documentation process that recorded data selection criteria, coding procedures, and analytical decisions to ensure replicability (Schlunegger et al., 2024). Dependability was further reinforced by iterative review of coded materials to verify consistency and reduce researcher bias (Cheong et al., 2023). Credibility was enhanced by cross-referencing information across independent documents to confirm coherence and reduce reliance on single-source interpretations (Ruggiano & Perry, 2017). Although the research relies exclusively on secondary data, careful source evaluation was conducted to ensure accuracy and relevance. Ethical considerations were addressed by using publicly available documents or authorized institutional materials and by respecting data protection standards (Schlunegger et al., 2024). No personal data were processed, and where institutional information was referenced, confidentiality and anonymity were preserved in accordance with ethical principles for social science research.

3. Result and Discussion

3.1 Institutional Mediation and the Sustainability of AI-Based Knowledge Practices in Public Security Governance

Technological transformation within public organizations does not unfold in an institutional vacuum; rather, it is conditioned by governance structures, administrative traditions, and contextual constraints that shape both adoption trajectories and long-term durability. From an institutional perspective, technological tools such as Artificial Intelligence become embedded only when they align with prevailing norms, authority structures, and organizational routines. In public security governance, these dynamics are intensified by hierarchical command systems, confidentiality requirements, and political sensitivity (Valérie D., 2019). The sustainability of AI-based knowledge practices therefore depends not only on technical efficiency but also on institutional compatibility and adaptive capacity. Dynamic capabilities theory emphasizes the importance of resource reconfiguration and learning processes for enduring transformation (Teece et al., 1997; Wang & Ahmed, 2007). However, such reconfiguration is mediated by structural constraints, especially in developing country administrations characterized by resource limitations and administrative instability (De Sousa et al., 2019). The durability of AI-driven knowledge restructuring must thus be analyzed through the lens of institutional mediation rather than technological determinism. This framing addresses the research gap concerning how contextual governance constraints shape AI integration and whether such integration becomes institutionalized over time.

Secondary data analysis indicates that administrative instability constitutes a central mediating factor in AI adoption within developing country public security institutions. Leadership turnover and shifting policy priorities often disrupt continuity in digital reform initiatives, limiting the consolidation of newly introduced knowledge practices (Maciejewski, 2017). In such environments, AI projects may depend heavily on specific champions rather than on institutionalized mandates. When leadership support fluctuates, the routinization of AI-based analytical procedures becomes uncertain. This instability affects not only strategic direction but also resource allocation and training continuity. Consequently, knowledge restructuring initiated through AI tools may remain fragile and vulnerable to organizational change. The institutional logic of short-term administrative cycles can therefore hinder the long-term embedding of technological innovation. This dynamic directly illustrates how contextual governance constraints mediate the sustainability of AI-based knowledge systems.

Resource scarcity further conditions the trajectory of AI-driven transformation. Developing country administrations frequently operate under fiscal and infrastructural limitations that restrict investment in advanced technological ecosystems (De Sousa et al., 2019). As a result, AI adoption often relies on cost-efficient or open-source solutions, which may limit scalability or technical support capacity. While such adaptive strategies demonstrate institutional flexibility, they also expose knowledge systems to maintenance challenges and performance variability. Limited computational infrastructure and uneven digital literacy create disparities in the effective utilization of AI outputs. This affects the consistency of knowledge creation and dissemination processes across departments. Institutional sustainability therefore depends on aligning technological ambition with realistic resource planning. Without stable infrastructural support, AI-based knowledge practices risk remaining experimental rather than becoming standardized administrative routines.

Hierarchical rigidity and bureaucratic authorization processes also mediate how AI reshapes knowledge circulation. Public security governance operates within clearly defined chains of command, where information flows are regulated and subject to oversight (Valérie D., 2019). AI-generated outputs, even when analytically robust, must pass through established authorization channels before influencing decision-making. This institutional logic preserves accountability but may slow the diffusion of innovation. At the same time, hierarchical validation can enhance legitimacy and trust in AI-supported analysis. Rather than decentralizing authority, AI tends to be integrated into existing governance structures. Knowledge circulation thus remains structured by institutional norms, even as technological tools increase analytical speed. The sustainability of AI-based practices depends on their capacity to operate within, rather than disrupt, these authority frameworks. This interaction clarifies how public security logics shape the institutionalization process.

Confidentiality regimes and data governance requirements further complicate sustainability dynamics. Security administrations handle sensitive information that demands strict access controls and procedural safeguards. AI systems, which rely on extensive data processing, must therefore comply with rigorous governance standards (Wirtz et al., 2019). These standards influence how data are collected, stored, and shared, thereby shaping the scope of knowledge restructuring. Concerns regarding transparency, accountability, and ethical oversight may limit full automation of analytical functions (Araujo et al., 2020). Institutionalization of AI-based knowledge practices requires clear governance protocols that reconcile innovation with security imperatives. Where such protocols are absent or inconsistently applied, AI initiatives may face resistance or limited integration. The confidentiality logic of public security thus mediates both the operational and normative dimensions of technological embedding.

Digital skill gaps represent another critical mediating factor influencing long-term durability. Effective use of AI-generated insights requires analytical competence, interpretive judgment, and continuous learning (Anderson et al., 2014). In developing country contexts, disparities in technical training and uneven distribution of digital expertise constrain the depth of AI integration. Without systematic capacity-building strategies, reliance on a small group of technically proficient individuals may create dependency risks. This limits the diffusion of AI-based knowledge routines across the broader organization. Sustainable institutionalization requires embedding digital literacy within formal training and professional development structures. The presence or absence of such structures determines whether AI remains an isolated innovation or evolves into an organizational norm. Digital competence therefore becomes a foundational governance condition for sustainable knowledge transformation.

Taken together, these contextual dynamics demonstrate that AI-driven knowledge restructuring in public security administration is neither automatic nor uniform. Institutional mediation shapes the pace, depth, and durability of technological transformation. While AI enhances knowledge creation and codification capacities, its long-term institutionalization depends on stable leadership, adequate resources, compatible hierarchical integration, robust confidentiality governance, and sustained competence development. These findings extend prior literature that primarily emphasizes efficiency gains by highlighting the structural conditions necessary for enduring embedding (Purdy & Daugherty, 2016; Wirtz et al., 2019). They refine dynamic capabilities theory by illustrating how reconfiguration processes are constrained and enabled by governance logics specific to public security settings. Most importantly, this analysis closes Research Gap 2 by systematically integrating developing country governance constraints into the interpretation of AI transformation. It also addresses Research Gap 3 by identifying the institutional conditions under which AI-based knowledge practices transition from experimental initiatives to stabilized administrative routines. Through this integrated perspective, the section clarifies how institutional context determines the sustainability of AI-enabled knowledge governance in public security environments.

3.2 Dynamic Capabilities and Organizational Learning in AI-Enabled Public Security Transformation

The integration of Artificial Intelligence within public security governance not only restructures knowledge processes but also activates deeper organizational adaptation mechanisms. Dynamic capabilities theory provides a conceptual lens for understanding how institutions sense opportunities, seize technological potential, and reconfigure internal resources in response to environmental pressures (Teece et al., 1997; Wang & Ahmed, 2007). In security administrations operating within developing country contexts, these adaptive processes are shaped by institutional rigidity and strategic uncertainty. AI adoption thus becomes a test of whether public organizations can transform technological experimentation into structured organizational learning. Rather than focusing solely on operational outputs, this perspective highlights the capacity of institutions to internalize new competencies and institutionalize change. Organizational learning emerges as a central mediating mechanism through which AI influences governance practices. The sustainability of transformation depends on whether learning remains episodic or becomes embedded within administrative routines. This theoretical framing allows examination of how AI contributes to the development of adaptive governance capacities.

Secondary data suggest that AI initiatives stimulate sensing capabilities by expanding the organization's ability to detect patterns, risks, and emerging trends in complex information environments. In public security governance, early detection and anticipatory intelligence are critical for effective risk management (Valérie D., 2019). AI-supported analytics enhance the organization's environmental scanning function by processing data streams that exceed human cognitive limits (Ji et al., 2015). This expansion of sensing capacity strengthens strategic awareness within leadership structures. However, sensing alone does not guarantee transformation; institutions must also seize technological opportunities through coordinated decision-making. The capacity to interpret AI-generated insights and translate them into strategic action reflects the presence of organizational learning mechanisms. Where such mechanisms are underdeveloped, AI outputs may remain underutilized or misinterpreted. Thus, sensing capabilities must be coupled with interpretive competence to contribute meaningfully to governance adaptation.

The seizing dimension of dynamic capabilities becomes visible in how public security institutions integrate AI into formal decision-making frameworks. Policy-oriented analyses emphasize the potential of AI to inform strategic planning and operational prioritization (Pencheva et al., 2018; Önder & Saygili, 2018). In hierarchical governance systems, seizing opportunities requires alignment between technological insights and institutional mandates. AI-generated analyses must be validated, contextualized, and formally authorized before influencing action. This process reflects the interaction between innovation and bureaucratic procedure. Organizational learning occurs as actors refine interpretive practices and develop shared standards for evaluating AI outputs. Over time, such shared standards may stabilize into institutional norms guiding the use of analytical technologies. The degree to which this stabilization occurs determines whether AI integration contributes to enduring adaptive capacity.

Reconfiguration, the third dimension of dynamic capabilities, involves restructuring resources, competencies, and routines to sustain technological change (Teece et al., 1997). In developing country public security administrations, reconfiguration often unfolds incrementally due to institutional and resource constraints (De Sousa et al., 2019). AI adoption may prompt adjustments in role definitions, training priorities, and interdepartmental coordination. These adjustments reflect attempts to align human capital with technological requirements. However, reconfiguration is constrained by hierarchical rigidity and limited fiscal flexibility. Without systematic institutional support, reconfiguration may remain partial or reversible. Organizational learning thus depends on embedding AI-related competencies within formal structures rather than relying on individual initiative. The durability of adaptive change is contingent upon the depth of such structural integration.

The interaction between dynamic capabilities and knowledge management becomes particularly significant in public security contexts. AI-driven codification of information enhances collective memory and reduces dependence on tacit individual expertise (Alamoodi et al., 2021). This codification supports organizational learning by creating stable reference points for analysis and decision-making. However, effective learning requires feedback mechanisms that allow continuous refinement of analytical models and governance practices. In environments characterized by administrative instability, such feedback loops may be disrupted (Maciejewski, 2017). Institutional continuity is therefore essential for consolidating learning outcomes. Where governance structures support iterative reflection and adjustment, AI contributes to cumulative capability development. Where such support is lacking, learning remains fragmented and episodic.

These findings refine existing scholarship on AI in public administration by highlighting the centrality of adaptive governance capacities rather than focusing exclusively on efficiency outcomes (Wirtz et al., 2019). They confirm that technological adoption in security governance is deeply intertwined with institutional learning processes. At the same time, the analysis challenges assumptions that digital transformation automatically generates organizational agility. Instead, agility emerges only when sensing, seizing, and reconfiguration processes are coherently institutionalized. The developing country context further illustrates how structural constraints shape the trajectory of adaptive capacity formation. By linking AI integration to dynamic capabilities and organizational learning, this section addresses the broader question of how technological innovation contributes to governance resilience. It thus deepens theoretical integration between AI, knowledge management, and adaptive public sector transformation while extending understanding of institutional change in security administrations.

4. Conclusion

This study examined how Artificial Intelligence reshapes knowledge management within a public security administration operating in a developing country context. The findings indicate that AI contributes to the restructuring of knowledge creation, codification, dissemination, and application by enhancing analytical capacity and formalizing previously fragmented routines. However, the transformation is not technologically deterministic; it is mediated by institutional structures such as hierarchical authority, confidentiality regimes, and bureaucratic authorization processes. Contextual constraints—including administrative instability, resource scarcity, infrastructural limitations, and digital skill gaps—significantly shape both the depth and durability of AI integration. The analysis further demonstrates that AI activates adaptive mechanisms aligned with dynamic capabilities, particularly through sensing, seizing, and incremental reconfiguration processes. Yet, these adaptive processes become sustainable only when embedded within stable governance frameworks and supported by continuous organizational learning. Overall, AI-driven knowledge transformation in public security governance emerges as a negotiated institutional process rather than a linear technological upgrade.

The study makes several theoretical and empirical contributions to the literature on AI in public administration. First, it extends knowledge management scholarship by demonstrating how algorithmic systems interact with hierarchical governance structures to institutionalize analytical routines in security contexts. Second, it refines dynamic capabilities theory by illustrating how adaptive reconfiguration unfolds under conditions of administrative rigidity and resource constraint typical of developing country settings. Third, the research addresses an empirical gap by integrating contextual governance constraints into the analysis of AI adoption, moving beyond efficiency-centered narratives dominant in prior studies. By situating AI within public security governance, the study highlights the importance of confidentiality, authorization chains, and political sensitivity in shaping technological embedding. It also contributes to understanding how institutional logics mediate sustainability outcomes, clarifying why some AI initiatives remain experimental while others evolve into stable organizational practices. Through this integrated perspective, the research bridges technological, organizational, and governance dimensions in a unified analytical framework.

Future research should expand comparative inquiry across multiple public security institutions and national contexts to examine variation in institutional mediation and sustainability trajectories. Quantitative and mixed-method approaches could complement qualitative insights by assessing performance indicators and long-term organizational outcomes associated with AI-based knowledge practices. Further investigation is needed into leadership continuity, governance design, and digital capacity-building strategies as determinants of institutionalization. Research could also explore the ethical and accountability dimensions of AI-supported decision-making in politically sensitive environments. Longitudinal studies would be particularly valuable in tracing how AI-driven knowledge routines evolve over time and whether adaptive capacities consolidate or erode. Additionally, examining citizen trust and public legitimacy in relation to AI-enabled security governance would deepen understanding of the broader societal implications. Such directions would strengthen theoretical development and provide more comprehensive guidance for sustainable AI integration in public sector governance.

References

Alamoodi, A. H., Zaidan, B. B., Zaidan, A. A., Albahri, O. S., Mohammed, K. I., Malik, R. Q.,

Almahdi, E. M., Chyad, M. A., Tareq, Z., & Albahri, A. S. (2021). Sentiment analysis and its applications in fighting COVID-19 and infectious diseases: A systematic review. *Expert Systems with Applications, 167*, 114155. https://doi.org/10.1016/j.eswa.2020.114155

Anderson, N., Potočnik, K., & Zhou, J. (2014). Innovation and creativity in organizations: A state-of-the-science review, prospective commentary, and guiding framework. *Journal of Management, 40*(5), 1297–1333. https://doi.org/10.1177/0149206314527128

Androutsopoulou, A., Karacapilidis, N., Loukis, E., & Charalabidis, Y. (2019). Transforming the communication between citizens and government through AI-guided chatbots. *Government Information Quarterly, 36*(2), 358–367. https://doi.org/10.1016/j.giq.2018.10.001

Araujo, T., Helberger, N., Kruikemeier, S., & De Vreese, C. H. (2020). AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & Society, 35*(3), 611–623. https://doi.org/10.1007/s00146-019-00931-w

Baker, Q. B., Shatnawi, F., Rawashdeh, S., Al-Smadi, M., & Jararweh, Y. (2020). Detecting epidemic diseases using sentiment analysis of Arabic tweets. *Journal of Universal Computer Science, 26*(1), 50–70.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108.

Cheong, H., Lyons, A., Houghton, R., & Majumdar, A. (2023). Qualitative case study approaches in complex organizational research: Methodological rigor and contextual sensitivity. *Qualitative Research in Organizations and Management, 18*(2), 245–260.

Chung, W., He, S., & Zeng, D. D. (2015). eMood: Modeling emotion for social media analytics on Ebola disease outbreak research-in-progress.

De Sousa, W. G., de Melo, E. R. P., Bermejo, P. H. D. S., Farias, R. A. S., & Gomes, A. O. (2019). How and where is artificial intelligence in the public sector going? A literature review and research agenda. *Government Information Quarterly, 36*(4), 101392. https://doi.org/10.1016/j.giq.2019.07.004

Deng, L., & Yu, D. (2014). Deep learning: Methods and applications. *Foundations and Trends in Signal Processing, 7*(3–4), 197–387.

Farquhar, J., Michels, N., & Robson, J. (2020). Case study research for business and management. *SAGE Publications*.

Ji, X., Chun, S. A., Wei, Z., & Geller, J. (2015). Twitter sentiment classification for measuring public health concerns. *Social Network Analysis and Mining, 5*(1), 13. https://doi.org/10.1007/s13278-015-0253-5

Maciejewski, M. (2017). To do more, better, faster and more cheaply: Using big data in public administration. *International Review of Administrative Sciences, 83*(1_suppl), 120–135. https://doi.org/10.1177/0020852316640058

Misuraca, G., & Van Noordt, C. (2020). AI watch—Artificial intelligence in public services: Overview of the use and impact of AI in public services in the EU. *JRC Research Reports*.

Önder, M., & Saygili, H. (2018). Artificial intelligence and the reflections on public administration.

Parly, F. (2019). Avant-propos – IA et défense. *Revue Défense Nationale, 820*(5), 9–17. https://doi.org/10.3917/rdna.820.0009

Pencheva, I., Esteve, M., & Mikhaylov, S. (2018). Big data and AI – A transformational shift for government: So, what next for research? *Public Policy and Administration, 35*(1), 24–44. https://doi.org/10.1177/0952076718780537

Purdy, M., & Daugherty, P. (2016). Why artificial intelligence is the future of growth.

Ruggiano, N., & Perry, T. E. (2017). Conducting secondary analysis of qualitative data: Should we, can we, and how? *Qualitative Social Work, 18*(1), 81–97. https://doi.org/10.1177/1473325017700701.

Schlunegger, M. C., Zumstein-Shaha, M., & Palm, R. (2024). Ensuring rigor in qualitative research: Strategies for credibility, dependability, and confirmability. *Journal of Qualitative Research in Health Sciences, 6*(1), 15–28.

Sun, T. Q., & Medaglia, R. (2019). Mapping the challenges of artificial intelligence in the public sector: Evidence from public healthcare. *Government Information Quarterly, 36*(2), 368–383. https://doi.org/10.1016/j.giq.2018.09.008

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509–533.

Valérie, D. (2019). IA, la conquête de l'excellence technique. *Revue Défense Nationale, 820*(5), 123–130.

Wang, C. L., & Ahmed, P. K. (2007). Dynamic capabilities: A review and research agenda. *International Journal of Management Reviews, 9*(1), 31–51.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal, 5*(2), 171–180.

Winter, S. G. (2003). Understanding dynamic capabilities. *Strategic Management Journal, 24*(10), 991–995.

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector: Applications and challenges. *International Journal of Public Administration, 42*(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103