Journal of Governance and Public Administration (JoGaPA)
Volume 3, No 1 – Desember 2025
e-ISSN : 3031-7584

THE PRACTICAL ROLE OF ARTIFICIAL INTELLIGENCE IN STRENGTHENING DIGITAL GOVERNANCE AND NETWORK SECURITY IN POST-CONFLICT AFGHANISTAN

Mir Mohammad Naim Sadat[1], Shahabuddin Esmati[2], Mustafa Tokhi[3], Muhammad Ajmal Azizi[4]
[13,4]Salam University Kabul, Afghanistan
[2]Universitas Hasanuddin, Indonesia
muhammadajmalazizi@gmail.com[1], esmatis24e@ms.unhas.ac.id[2],
mustafatokhi47@gmail.com[3] , muhammadajmalazizi@gmail.com[4]
Corresponding author email: muhammadajmalazizi@gmail.com

Received: 24-09-2025	Revised: 10-10-2025	Approved: 09-11-2025

ABSTRACT

This study examines the practical role of artificial intelligence (AI) in strengthening digital governance and network security in post-conflict Afghanistan. Drawing on a qualitative approach, data were collected through semi-structured interviews with 20 key informants, including government officials, ICT and cybersecurity experts, academics, and representatives from international organizations, complemented by document analysis of policy reports and strategic frameworks. The findings reveal that AI is perceived as a critical enabler of governance reform, with the potential to enhance transparency, reduce corruption, and improve efficiency in service delivery, contributing to institutional legitimacy. At the same time, participants emphasized the importance of AI-driven cybersecurity tools, such as predictive analytics and anomaly detection, in mitigating rising digital threats from both state and non-state actors. However, the study also highlights significant barriers, including weak infrastructure, limited technical capacity, and reliance on external actors, which constrain effective adoption. These dual dynamics underscore that while AI offers opportunities for resilience and modernization, its success in fragile context depends on context-sensitive, ethically grounded, and inclusive deployment. The research contributes to ongoing debates on technology-enabled governance in fragile states and provides practical insights for policymakers, practitioners, and international partners engaged in Afghanistan's digital transformation.
Keywords: *AI, Digital, Governance, Network, Afghanistan*

INTRODUCTION

The accelerating integration of artificial intelligence (AI) into governance and security infrastructures has become one of the defining features of contemporary statecraft. Around the world, governments are increasingly embracing AI-driven technologies to optimize decision-making, enhance service delivery, and secure critical digital networks against growing cyber threats (Dunleavy & Margetts, 2025; Emynorane et al., 2025). These developments occur at a moment of profound geopolitical and societal transformation, where fragile and post-conflict states such as Afghanistan face urgent challenges in rebuilding governance capacity and restoring public trust. In contexts characterized by institutional fragility, widespread insecurity, and weak infrastructure, the adoption of AI is not a mere technological choice but a strategic imperative (Esmati et al., 2024). It carries the potential to foster resilience, strengthen digital governance, and mitigate network vulnerabilities that have historically undermined stability in such environments (Ahn & Chen, 2022).

The concept of digital governance broadly refers to the use of information and communication technologies (ICTs) in administrative processes to improve efficiency, transparency, and accountability. As digitalization advances, governance is increasingly

intertwined with networked systems that must remain secure in the face of escalating cyber risks. The rapid spread of disinformation, ransomware attacks, and state-sponsored cyber intrusions illustrates that digital systems are not merely administrative tools but potential battlegrounds of strategic contestation (Calderaro & Blumfelde, 2022). For countries like Afghanistan, which remain vulnerable to both physical and digital forms of insecurity, network security emerges as a vital domain for safeguarding sovereignty and protecting fragile state institutions. AI-driven cybersecurity mechanisms such as predictive analytics, anomaly detection, and intelligent intrusion-prevention systems have shown promise in countering sophisticated threats that often overwhelm traditional security infrastructures (Schmitt, 2023). Thus, the intersection of AI, governance, and digital security represents a critical area of inquiry with profound implications for post-conflict recovery.

Previous study on AI in public administration highlights its transformative role in reshaping bureaucratic practices and fostering innovation within government services. Studies suggest that AI can improve responsiveness, automate routine administrative tasks, and support evidence-based decision-making by analyzing complex datasets with unprecedented accuracy (Neumann et al., 2024). Moreover, AI applications in governance are not limited to operational efficiency but extend to strengthening citizen trust, particularly when deployed transparently and responsibly (Gesk & Leyer, 2022). In fragile states, where administrative inefficiencies and corruption often undermine public confidence, AI offers an opportunity to improve transparency and accountability through algorithmic processes less susceptible to discretionary manipulation. This promise, however, is contingent on robust ethical frameworks, local adaptability, and the alignment of technological tools with broader governance objectives (Kim et al., 2022).

Despite such global advances, scholarships on the role of AI in post-conflict settings remains limited. Much of the existing literature examines AI adoption in stable democracies or technologically advanced economies, where the infrastructure and regulatory foundations for digital transformation are relatively mature (Neumann et al., 2024). By contrast, countries like Afghanistan present a distinct context where chronic insecurity, political instability, and resource scarcity intersect with digital vulnerabilities. While studies on Afghanistan have examined challenges related to education, infrastructure, and women's rights under conflict (Utsumi & Muradi, 2024; Ma et al., 2025; Ahmadzai & Ye, 2024), the application of AI in the domain of digital governance and network security remains largely unexplored. This represents a critical gap in literature: the absence of a systematic understanding of how AI can be practically applied to address governance deficits and cybersecurity challenges in fragile, post-conflict environments.

The Afghan context magnifies the stakes of this inquiry. Following decades of war and political instability, Afghanistan's governance systems are characterized by weak institutions, limited digital infrastructure, and persistent threats from both domestic and external actors. Cybersecurity risks are heightened by the proliferation of non-state groups that exploit digital platforms for propaganda, recruitment, and financial operations. Moreover, the country's transition to digitalized public services has been uneven, leaving critical vulnerabilities in data protection, identity management, and network resilience. Without robust security mechanisms, digital initiatives intended to modernize governance risk being compromised, thereby exacerbating rather than mitigating fragility (Eom & Lee, 2022). AI's potential to enhance predictive capacity,

detect anomalies in real-time, and adaptively respond to evolving cyber threats makes it an indispensable tool for countries in such precarious conditions.

Beyond security, AI also holds promise for strengthening Afghanistan's broader digital governance agenda. Research underscores that AI can facilitate integrated platforms for e-services, improve inter-agency coordination, and streamline bureaucratic processes that are often marred by inefficiency and corruption (Bokhari & Myeong, 2022). In environments where public resources are scarce and institutional trust is fragile, the efficient use of AI can help governments prioritize critical service delivery functions while reducing administrative burdens. For example, algorithmic tools can assist in identity verification, streamline digital registries, and ensure fair distribution of public resources. These functions are particularly crucial in post-conflict contexts where equitable service delivery plays a vital role in fostering social cohesion and rebuilding public legitimacy (Ahmadzai & Ye, 2025; Abdelfattah et al., 2025).

Nevertheless, adopting AI in post-conflict states is fraught with challenges. Scholars caution that the deployment of AI without careful consideration of local socio-political contexts risks reinforcing existing inequalities and creating new vulnerabilities (Osonuga et al., 2025). Algorithmic bias, lack of digital literacy, and inadequate regulatory oversight can undermine the inclusivity and effectiveness of AI systems, particularly in fragile states where marginalized groups often lack access to digital tools (Loisel et al., 2025; González-Díaz et al., 2025; Eric et al., 2025). Furthermore, external dependencies on international actors for technological infrastructure may expose countries like Afghanistan to geopolitical vulnerabilities, complicating sovereignty and data protection concerns (Calderaro & Blumfelde, 2022). These challenges underscore the necessity of developing a contextualized framework for AI adoption that is sensitive to Afghanistan's unique governance and security realities.

The significance of this study lies in its attempt to bridge the gap between global discourses on AI in governance and the specific needs of post-conflict Afghanistan. By focusing on the practical role of AI in strengthening digital governance and network security, the research aims to generate insights that are both contextually relevant and theoretically valuable. It contributes to ongoing debates about how fragile states can leverage emerging technologies not simply as tools of modernization but as instruments of resilience. Moreover, it emphasizes the dual potential of AI as both a technological enabler and a governance innovation that can address Afghanistan's urgent needs for security, efficiency, and legitimacy. While the risks of technological dependency and exclusion cannot be overlooked, the strategic deployment of AI offers Afghanistan a pathway toward rebuilding institutions and securing its digital future.

RESEARCH METHODS

This study uses a qualitative research design to gain a deeper, contextually grounded understanding of how artificial intelligence can strengthen digital governance and network security in post-conflict Afghanistan. A qualitative approach is particularly suitable for this study because it prioritizes depth over breadth, allowing the researcher to capture the complex, nuanced realities of governance, technology adoption, and security within a fragile state context. Rather than relying on numerical data, this approach emphasizes the meanings, perceptions, and experiences of individuals directly involved in shaping or implementing digital strategies. The study involved 20 key informants selected through purposive sampling, each chosen for their specific expertise and strategic roles in Afghanistan's digital transformation landscape. These

participants included senior government officials from ministries responsible for digital governance, cybersecurity experts from national and international NGOs, technology consultants, academic researchers in AI and public policy, and representatives from international organizations supporting post-conflict state-building. Their involvement was crucial because they possess firsthand knowledge of both the structural challenges and emerging opportunities surrounding AI deployment in governance and security systems.

Data were collected through semi-structured interviews conducted in person and via secure online platforms, complemented by a review of relevant policy documents, government strategies, and international reports. Semi-structured interviews were chosen to balance consistency in guiding questions with flexibility, enabling participants to share detailed insights while allowing the researcher to probe emerging themes during the conversation. Each interview lasted approximately 45–60 minutes and was audio-recorded with the participants' consent. Thematic analysis was applied to interpret the data, following an iterative coding process to identify key patterns, categories, and conceptual linkages aligned with the study's objectives. NVivo software was used to organize, code, and analyze the data regularly, enhancing transparency and rigor. To ensure credibility and trustworthiness, multiple verification strategies were employed, including triangulation of interview data with documentary sources, member checking by sharing preliminary findings with a subset of five participants for validation, and maintaining a detailed audit trail throughout the study process. The overall research process is summarized in the methodological flow presented in Figure 1.

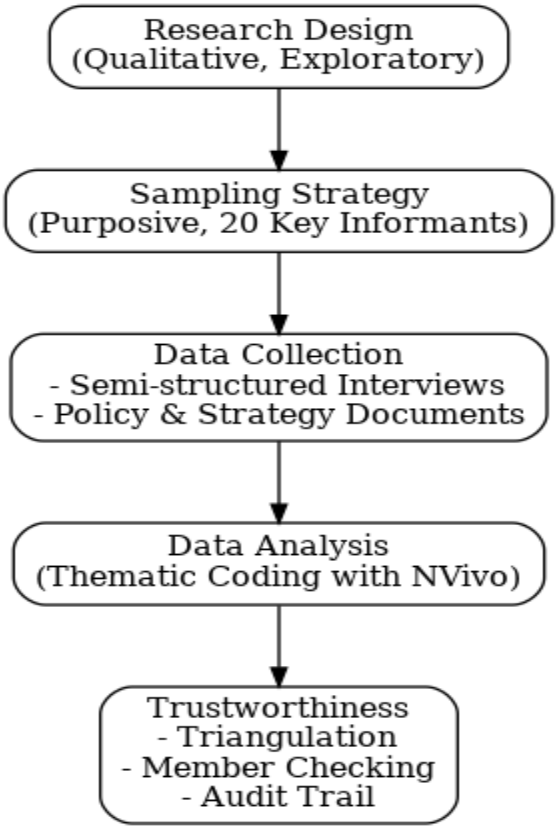

Figure 1. Research flow diagram of the study process

RESULTS AND DISCUSSION

Results

The findings of this study reveal that informants consistently stressed the dual potential of artificial intelligence in Afghanistan's post-conflict recovery: as both a tool to strengthen digital governance and as a protective mechanism for securing fragile networks. Government officials and ICT practitioners noted that AI-driven tools, such as automated data management systems and intelligent identity verification platforms, could help reduce bureaucratic inefficiencies and limit corruption by minimizing human discretion in service delivery. Participants also highlighted AI's ability to improve transparency through real-time monitoring and analytics, which could strengthen public trust in government institutions that have long been marred by weak accountability. Several respondents from international organizations stressed that AI, when integrated into digital service platforms, could enable resource optimization and fair distribution of public goods, particularly in rural and marginalized communities where governance gaps are most severe. This indicates that stakeholders see AI not only as a technological upgrade but as a strategic enabler of institutional legitimacy and citizen confidence.

In terms of network security, cybersecurity experts and technical specialists interviewed identified AI-powered predictive analytics, anomaly detection, and intelligent firewalls as critical for countering the escalating cyber threats facing Afghanistan. Participants explained that malicious digital actors, including extremist groups, increasingly exploit vulnerabilities in communication systems for propaganda, recruitment, and financial activities, making robust digital defenses essential. Informants also stressed that traditional manual monitoring systems are insufficient for handling the volume and complexity of modern cyberattacks, whereas AI can provide adaptive and real-time responses. However, participants also cautioned that Afghanistan's weak infrastructure, limited digital literacy, and dependency on external actors for technological expertise could constrain AI's effectiveness if not carefully managed. Despite these challenges, most informants agreed that the adoption of AI-based cybersecurity measures is indispensable for safeguarding Afghanistan's digital sovereignty and ensuring the resilience of emerging e-governance systems.

Discussion

The results of this study point toward the growing relevance of artificial intelligence (AI) as a transformative enabler of both digital governance and network security in post-conflict Afghanistan. Informants consistently emphasized AI's potential to strengthen institutional legitimacy through more transparent and efficient service delivery, while simultaneously enhancing digital resilience against the evolving cyber threats that jeopardize fragile governance infrastructures. These findings resonate strongly with the broader body of scholarship on AI in governance, which underscores the dual role of emerging technologies in advancing bureaucratic performance and securing digital environments. Yet, the Afghan context introduces unique complexities, shaped by historical fragility, security deficits, and dependency on external actors, which both expand and constrain AI's practical role.

From a governance perspective, the evidence from this study aligns with Dunleavy and Margetts' (2025) notion of the “third wave of digital era governance,” in which data science and AI fundamentally reshape the state's capacity to deliver services. Participants described AI-enabled platforms for identity verification, real-time

monitoring, and data management as mechanisms for reducing corruption and increasing transparency issues that have long plagued Afghanistan's governance system. This finding echoes Esmati et al. (2024), who argues that digital technologies and AI can contribute to bureaucratic transformation by minimizing discretionary human decision-making and enhancing accountability. In a fragile state setting, where inefficiencies and corruption undermine legitimacy, such tools are not simply technical solutions but potentially pivotal reforms in the state–citizen relationship.

The study's results also confirm the relevance of literature that positions AI as a driver of trust in government institutions. Informants repeatedly highlighted the idea that algorithmic governance could help overcome public skepticism by ensuring fairer and more consistent service delivery. This perspective finds support in Gesk and Leyer's (2022) study, which demonstrated that citizen acceptance of AI in public services is largely contingent on perceptions of fairness, transparency, and accountability. In Afghanistan, where the erosion of trust has been both deep and persistent, AI has the potential to rebuild legitimacy although this will require careful design to avoid reinforcing inequalities or inadvertently excluding vulnerable populations.

This study also reflects the theoretical cautions raised by scholars such as Osonuga et al. (2025), who emphasize that AI is not inherently equitable and may perpetuate existing disparities if implemented without sensitivity to context. Participants warned that Afghanistan's limited digital literacy, weak infrastructure, and heavy reliance on external technology providers risk creating new vulnerabilities. This aligns with Calderaro and Blumfelde's (2022) critique of digital sovereignty, which highlights the risks of technological dependency in security-sensitive domains. In Afghanistan, dependence on foreign expertise and infrastructure could compromise the country's digital autonomy, raising concerns about data ownership, external influence, and long-term sustainability. Thus, the application of AI in governance must be framed not only as a technological innovation but also as a political and sovereignty issue.

Turning to network security, the study revealed strong support for AI-powered tools such as predictive analytics, anomaly detection, and adaptive firewalls, which were identified as essential for countering cyber threats in the Afghan context. Cybersecurity experts emphasize that traditional manual systems are insufficient to deal with the scale and sophistication of digital attacks, a finding that echoes Schmitt (2023), who highlights AI's capacity to detect and prevent malware and intrusions in real time. Informants further underscored the specific threat posed by extremist groups leveraging digital networks for propaganda and recruitment, situating Afghanistan within global concerns about non-state actors exploiting cyber vulnerabilities. These insights reinforce the argument of Calderaro and Blumfelde (2022) that AI is becoming central to security strategies, particularly in fragile states where digital infrastructures are highly exposed.

The study's findings also resonate with Bokhari and Myeong's (2022) work on AI-based knowledge management and e-service delivery in smart governance. Informants emphasized that AI could improve coordination across fragmented agencies, optimize resource distribution, and support the fair allocation of limited services in marginalized areas. In a post-conflict environment, such outcomes are not only efficiency gains but also critical contributions to social cohesion and stabilization. By enabling more equitable distribution of resources and reducing the discretionary power of officials, AI tools can help address grievances that often fuel instability. These perspectives are consistent with Ahn and Chen's (2022) findings that government

employees perceive AI as an opportunity to increase efficiency and fairness in public administration.

The Afghan case also provides empirical support for Neumann et al. (2024), who argue that AI adoption in public organizations is deeply shaped by contextual factors such as institutional capacity, political will, and resource availability. While participants acknowledged AI's potential, they also noted that its successful implementation depended on overcoming Afghanistan's infrastructure weaknesses, limited technical expertise, and fragmented regulatory environment. These constraints mirror Eom and Lee's (2022) observation that digital government transformation is particularly challenging in turbulent environments where institutional instability undermines implementation capacity. In Afghanistan, this means that while AI can be a powerful tool for governance and security, its adoption must be carefully calibrated to local realities, avoiding overly ambitious models imported from more stable contexts.

The study underscores the close relationship between governance reform and security imperatives, indicating that AI's effectiveness in Afghanistan relies on addressing both dimensions together. Informants perceive AI not merely as a technical safeguard against cyber threats but also as a source of institutional legitimacy, since citizens are more likely to adopt and trust digital government services when networks are secure. This perspective aligns with Kim et al.'s (2022) notion of "platform government," which stresses that effective governance in the digital era must integrate service delivery and security. In the Afghan context, where persistent insecurity has long weakened state capacity, this dual focus is essential: reliable digital systems form the foundation of functional governance, while effective governance in turn provides the conditions for protecting networks from malicious actors.

The findings also extend the theoretical discourse on resilience in fragile states. Utsumi and Muradi (2024) demonstrate how community social capital can foster educational resilience in conflict settings, suggesting that local agencies are vital in sustaining services under pressure. Similarly, this study's participants highlighted that AI adoption in Afghanistan must be accompanied by capacity building, digital literacy programs, and inclusive design processes that involve local actors. Without such efforts, AI risks becoming a top-down, externally driven project that fails to take root in Afghan society (Zhang & Li, 2025). This observation underscores the need for a resilience-based framework for AI adoption, one that combines technological innovation with social and institutional adaptation.

The practical role of AI in Afghanistan emerges most clearly when viewed through the simultaneous realities of promise and limitation. On the one hand, AI carries enormous potential to enhance digital governance, curb corruption, and fortify vulnerable networks, thereby contributing directly to the country's post-conflict recovery and stabilization. On the other hand, persistent infrastructure weaknesses, political fragility, and dependence on external actors present serious risks of dependency, social exclusion, and potential misuse. These contrasting dynamics echo wider scholarly debates that caution against technological determinism and highlight the necessity of adopting AI in ways that are context-sensitive and ethically grounded (Osonuga et al., 2025; Neumann et al., 2024).

CONCLUSION

This study demonstrates that artificial intelligence holds significant promise for advancing digital governance and strengthening network security in Afghanistan's post-

conflict context, yet its practical role is shaped by both enabling and constraining factors. While AI can enhance efficiency, transparency, and resilience, its implementation is challenged by weak infrastructure, limited technical expertise, and dependency on external actors. These conditions highlight the need for carefully tailored strategies that prioritize local capacity building, ethical safeguards, and sustainable integration rather than rapid technological adoption. The study's findings are limited by the scope of informants, as it relied on 20 key stakeholders, which may not capture the full diversity of perspectives across Afghan society. To address these limitations, future research should expand participation to include broader segments of the population and adopt longitudinal designs to assess AI's evolving role over time. For policymakers, development agencies, and international partners, the recommendation is to invest in digital literacy programs, strengthen institutional frameworks for cybersecurity, and support inclusive governance models that embed AI responsibly into public administration. Only through such comprehensive and context-sensitive efforts can AI contribute effectively to Afghanistan's stability and digital resilience.

REFERENCES

Abdelfattah, F., Madi, H., Al-Washahi, M., AlAraimi, A., Nagi, S., & Abbas, M. (2025). Harnessing artificial intelligence, business intelligence, and digital technologies for achieving supply chain excellence in Oman: Investigating the mediating role of predictive analytics. *Journal of Open Innovation: Technology, Market, and Complexity*, 11, 100644. https://doi.org/10.1016/j.joitmc.2025.100644

Ahmadzai, M. B., & Ye, K. (2024). Modelling the impacts of security on construction delays: A case of Afghanistan. *Heliyon*, 10, e32662. https://doi.org/10.1016/j.heliyon.2024.e32662

Ahmadzai, M. B., & Ye, K. (2025). A mixed-method investigation of the root causes of construction project delays in Afghanistan. *Heliyon*, 11, e41923. https://doi.org/10.1016/j.heliyon.2025.e41923

Ahn, M. J., & Chen, Y. C. (2022). Digital transformation toward AI-augmented public administration: The perception of government employees and the willingness to use AI in government. *Government Information Quarterly*, 39(2), 101664. https://doi.org/10.1016/j.giq.2022.101664

Bokhari, S. A. A., & Myeong, S. (2022). Artificial intelligence-based technological-oriented knowledge management, innovation, and e-service delivery in smart cities: Moderating role of e-governance. *Applied Sciences*, 12(17), 8732. https://doi.org/10.3390/app12178732

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, 31(3), 415–434. https://doi.org/10.1080/09662839.2022.2065812

Dunleavy, P., & Margetts, H. (2025). Data science, artificial intelligence and the third wave of digital era governance. *Public Policy and Administration*, 40(2), 185–214. https://doi.org/10.1177/09520767221121312

Emynorane, R. H., Ibrahim, M. A., Hasniati, & Yunus, M. (2025). Challenges to the Effectiveness of Higher Education in Madagascar: An Analysis of Key Hindering Factors. *KnE Social Sciences*, 10(18), 579–595. https://doi.org/10.18502/kss.v10i18.19486

Emynorane, R. H., Kazakov, I., & Arrive, J. T. (2025). Obstacles Encountered by the English Department Students in Learning English: Case Study of Universitas

Negeri Malang. *NU Madura: Journal of Islamic Studies, Social, and Humanities*, 3 (2), 92-99.

Eom, S. J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. *Government Information Quarterly*, 39(2), 101690. https://doi.org/10.1016/j.giq.2022.101690

Eric, R. R., Arrive, J. T., Emynorane, R. H., & Bien-Aimé, W. D. (2025). The role of Technology in School Resource Management: A Study on Public Elementary Schools in Madagascar. *Jurnal Ilmiah Widya Pustaka Pendidikan*, 13(1), 72 - 80. https://jiwpp.unram.ac.id/index.php/widya/article/view/305

Esmati, S., Emynorane, R. H., & Arrive, J. T. (2024). The Neoliberal Political Economy of Higher Education: Marketization and its Impact on Access and Quality at Universitas Hasanuddin. *Journal of Governance and Public Administration*, (2)1, 175 – 184. https://doi.org/10.70248/jogapa.v2i1.1688

Esmati, S., Lewa, I., Herawwaty, H., Khaled, A., & Indrawati, I. (2024). Aligning Administrative Law and Public Administration: Key to Effectiveness and Public Trust. *JOELS: Journal of Election and Leadership*, 5(2), 172-182.

Gesk, T. S., & Leyer, M. (2022). Artificial intelligence in public services: When and why citizens accept its usage. *Government Information Quarterly*, 39(3), 101704. https://doi.org/10.1016/j.giq.2022.101704

González-Díaz, S. N., Morais-Almeida, M., Ansotegui, I. J., Macouzet-Sánchez, C., Ordóñez-Azuara, Y. G., Camarena-Galván, J., & Alanís-Alvarez, J. M. (2025). Artificial intelligence in allergy practice: Digital transformation and the future of clinical care. *World Allergy Organization Journal*, 18, 101078. https://doi.org/10.1016/j.waojou.2025.101078

Keshavarzi, S., Becker, J. C., Ruhani, A., & Ebrahimi, F. (2025). Responses to the rapid reactionary social change: A social-psychological investigation of young Afghan women's experiences during the Second-Taliban era. International *Journal of Intercultural Relations*, 108, 102250. https://doi.org/10.1016/j.ijintrel.2025.102250

Kim, S., Andersen, K. N., & Lee, J. (2022). Platform government in the era of smart technology. *Public Administration Review*, 82(2), 362–368. https://doi.org/10.1111/puar.13492

Loisel, Q. E. A., Balaskas, G., Papadopoulos, H., Pappa, D., & Chastin, S. F. M. (2025). Can digital technologies and artificial intelligence enhance co-creation in public health? A Health CASCADE needs assessment study and critical recommendations. *Public Health*, 248, 105921. https://doi.org/10.1016/j.puhe.2025.105921

Ma, Y., Zhang, W., Ma, C., Ai, Y., & Hu, J. (2025). Artificial intelligence, data elements, digital economy, and corporate innovation performance. *International Review of Economics and Finance*, 103, 104560. https://doi.org/10.1016/j.iref.2025.104560

Neumann, O., Guirguis, K., & Steiner, R. (2024). Exploring artificial intelligence adoption in public organizations: A comparative case study. *Public Management Review*, 26(1), 114–141. https://doi.org/10.1080/14719037.2022.2124010

Osonuga, A., Osonuga, A. A., Fidelis, S. C., Osonuga, G. C., Juckes, J., & Olawade, D. B. (2025). Bridging the digital divide: Artificial intelligence as a catalyst for health equity in primary care settings. *International Journal of Medical Informatics*, 204, 106051. https://doi.org/10.1016/j.ijmedinf.2025.106051

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, 36, 100520. https://doi.org/10.1016/j.jii.2023.100520

Utsumi, Y., & Muradi, M. T. (2024). Leveraging social capital for educational resilience in conflict: The impact of community behaviors on educational access in pre-Taliban ruling Afghanistan. *International Journal of Disaster Risk Reduction*, 106, 104428. https://doi.org/10.1016/j.ijdrr.2024.104428

Zhang, Y., & Li, Y. (2025). The impact of artificial intelligence on government digital service capacity. *International Review of Economics and Finance*, 102, 104374. https://doi.org/10.1016/j.iref.2025.104374