

Research Article

Digital Governance, Cybersecurity Risks, and Public Administration in Africa: Emerging Challenges, Institutional Responses, and Policy Implications

Dr. Bakari Muhammadu SUKARE¹, Dr. UMAR Dauda Usman²

^{1 & 2} Department of Public Administration, Faculty of Management Sciences, Taraba State University, Jalingo, Nigeria

***Related declarations are provided in the final section of this article*

ARTICLE INFORMATION

Received: 07 Sep 2026

Revised: 20 Sep 2026

Accepted: 08 Oct 2026

Published: 12 Oct 2026

Correspondence Author:

Dr. Bakari Muhammadu
SUKARE *

Copyright © 2026 The Author(s). The Authors retain copyright. Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Digital governance has transformed public administration by improving service delivery, transparency, accountability, administrative efficiency, and citizen engagement. However, increasing reliance on digital systems has exposed African public institutions to cybersecurity risks, including ransomware, phishing, malware, data breaches, identity theft, cyber espionage, and disruption of critical services. This study examines the relationship between digital governance, cybersecurity risks, and public administration in Africa, with emphasis on institutional challenges and policy responses. Guided by the Technology–Organization–Environment (TOE) Framework and Institutional Theory, the study adopts a qualitative documentary research design. Data were drawn from peer-reviewed journal articles, government publications, policy documents, reports of international organizations, and other credible secondary sources, and were analysed thematically. The study finds that digital governance has improved administrative efficiency, financial management, transparency, accountability, and access to public services across several African countries. However, these gains remain vulnerable to inadequate cybersecurity infrastructure, weak regulatory enforcement, limited technical expertise, insufficient funding, fragmented institutional coordination, outdated technological systems, and low cybersecurity awareness. The study further finds that stronger cybersecurity strategies, effective regulatory institutions, institutional coordination, and sustained investment in digital capacity enhance governmental resilience and public sector performance. It concludes that sustainable digital governance requires cybersecurity risk management to be integrated into public administration reforms. The study recommends

strengthening cybersecurity policies and legal frameworks, investing in secure digital infrastructure and human capacity, institutionalizing enterprise risk management, improving incident response mechanisms, promoting regional cooperation, and enhancing continuous cybersecurity monitoring and public awareness.

Keywords: Digital Governance; Cybersecurity; Public Administration; Africa; Cyber Resilience

INTRODUCTION

The twenty-first century has witnessed an unprecedented digital transformation in public administration, fundamentally altering the manner in which governments design policies, deliver public services, interact with citizens, and manage public resources. Digital governance, broadly understood as the application of information and communication technologies (ICTs) to government processes and public service delivery, has become a strategic instrument for improving administrative efficiency, transparency, accountability, citizen participation, and institutional effectiveness (United Nations, 2024). Governments across the globe are increasingly leveraging digital technologies to modernize public administration, streamline bureaucratic procedures, reduce operational costs, enhance service accessibility, and promote evidence-based decision-making. Consequently, digital governance has evolved from a technological innovation into a critical pillar of sustainable governance and national development.

In Africa, the adoption of digital governance has accelerated significantly over the past decade, driven by increasing internet penetration, mobile technology expansion, digital identity initiatives, electronic payment systems, cloud computing, artificial intelligence, big data analytics, and the growing demand for efficient public service delivery. Numerous African governments have implemented digital reforms aimed at strengthening governance through electronic tax administration, online procurement systems, digital health services, electronic voting initiatives, integrated financial management information systems, and e-government portals (African Union, 2020). Countries such as Rwanda, Kenya, South Africa, Ghana, Nigeria, and Mauritius have made notable progress in integrating digital technologies into aspects of public administration, although the level and scope of digital-government development vary across countries as part of broader national development and digital transformation strategies (Liu & Qiang, 2023).

The emergence of digital governance has created opportunities for improvements in public administration. Digital technologies can help reduce administrative bottlenecks, improve financial accountability, enhance transparency in procurement processes, facilitate communication between governments and citizens, and expand access to public services, although the extent and sustainability of these outcomes vary according to institutional capacity, infrastructure, regulatory conditions, and implementation context (Organisation for Economic

Co-operation and Development [OECD], 2023). Furthermore, digital governance can support institutional coordination, data-informed policy formulation, government responsiveness during emergencies, and citizen engagement through digital participation platforms (United Nations, 2024). The COVID-19 pandemic further accelerated digital transformation across governments worldwide by demonstrating the importance of resilient digital systems for maintaining continuity in governance, healthcare, education, and public service delivery during crises (Liu & Qiang, 2023).

Despite these remarkable achievements, digital transformation has simultaneously exposed governments to an expanding range of cybersecurity risks. As governments increasingly rely on interconnected digital platforms, cloud-based services, electronic databases, and online communication systems, public institutions have become attractive targets for cybercriminals, hackers, terrorists, and state-sponsored cyber actors. Cybersecurity threats such as ransomware attacks, phishing schemes, malware infections, data breaches, cyber espionage, identity theft, denial-of-service attacks, and unauthorized access to government databases now constitute significant threats to national security, institutional integrity, economic stability, and public trust (International Telecommunication Union [ITU], 2024).

Cybersecurity risks within public administration extend beyond technological vulnerabilities to encompass organizational, legal, financial, and human dimensions. Weak institutional capacity, inadequate cybersecurity awareness among public servants, outdated technological infrastructure, fragmented governance frameworks, insufficient funding, and poor enforcement of cybersecurity regulations significantly increase governments' exposure to cyber threats (World Economic Forum, 2024). The increasing sophistication of cyberattacks has demonstrated that digital transformation without corresponding investments in cybersecurity creates substantial governance risks capable of disrupting essential government functions and undermining public confidence in state institutions.

The African continent faces particularly complex cybersecurity challenges due to varying levels of digital maturity, infrastructural limitations, resource constraints, and institutional weaknesses. Although digital government initiatives continue to expand rapidly across African countries, cybersecurity preparedness has not progressed at an equivalent pace. Although digital government initiatives continue to expand across African countries, the level of cybersecurity preparedness varies considerably. Some countries have strengthened national cybersecurity strategies, regulatory frameworks, institutional arrangements, and technical capabilities, while others continue to face significant challenges relating to infrastructure, funding, skilled personnel, incident response, data protection, and regulatory enforcement (African Union, 2020). These differences reflect variations in national resources, institutional capacity, technological development, policy priorities, and implementation conditions.

Nigeria provides an important illustration of the opportunities and challenges associated with digital governance in Africa. Initiatives such as the Treasury Single Account (TSA), Integrated Personnel and Payroll Information System (IPPIS), Government Integrated Financial Management Information System (GIFMIS), National Identification Number (NIN) system, electronic tax platforms, and other digital government services demonstrate the increasing use of

digital technologies in public administration. These initiatives have expanded the use of digital systems for financial management, personnel administration, identification, taxation, and public service delivery.

However, the implementation of digital-government initiatives should be distinguished from evidence of improved cybersecurity outcomes. The existence or expansion of digital platforms does not, by itself, demonstrate that government systems are adequately protected against cyberattacks, data breaches, identity theft, fraud, or other cybersecurity threats. Digitalization can simultaneously improve administrative processes while increasing the volume and importance of data and systems that require protection. Consequently, the cybersecurity implications of Nigeria's digital-government initiatives need to be assessed in relation to institutional capacity, regulatory enforcement, technical safeguards, data protection, incident-response mechanisms, skilled personnel, and inter-agency coordination.

Nigeria provides an important illustration of the opportunities and challenges associated with digital governance in Africa. Initiatives such as the Treasury Single Account (TSA), Integrated Personnel and Payroll Information System (IPPIS), Government Integrated Financial Management Information System (GIFMIS), National Identification Number (NIN) system, electronic tax platforms, and other digital government services demonstrate the increasing use of digital technologies in public administration. These initiatives have expanded the use of digital systems for financial management, personnel administration, identification, taxation, and public service delivery.

However, the implementation of digital-government initiatives should be distinguished from evidence of improved cybersecurity outcomes. The existence or expansion of digital platforms does not, by itself, demonstrate that government systems are adequately protected against cyberattacks, data breaches, identity theft, fraud, or other cybersecurity threats. Digitalization can simultaneously improve administrative processes while increasing the volume and importance of data and systems that require protection. Consequently, the cybersecurity implications of Nigeria's digital-government initiatives need to be assessed in relation to institutional capacity, regulatory enforcement, technical safeguards, data protection, incident-response mechanisms, skilled personnel, and inter-agency coordination.

The Nigerian experience therefore illustrates the importance of integrating cybersecurity risk management into digital-government development rather than treating cybersecurity as a separate technical concern. Digital-government implementation provides the technological foundation for modern public administration, while effective cybersecurity governance is necessary to protect the systems, information, institutions, and public trust upon which these digital services depend.

The Nigerian experience therefore illustrates the importance of integrating cybersecurity risk management into digital-government development rather than treating cybersecurity as a separate technical concern. Digital-government implementation provides the technological foundation for modern public administration, while effective cybersecurity governance is

necessary to protect the systems, information, institutions, and public trust upon which these digital services depend.

Beyond Nigeria, several African countries have experienced major cybersecurity incidents affecting critical government infrastructure, financial systems, healthcare institutions, electoral management bodies, and public utilities. Such attacks have demonstrated that cybersecurity has become an essential component of public administration rather than merely a technical concern. Effective governance in the digital age increasingly depends on governments' ability to anticipate, prevent, detect, respond to, and recover from cyber threats while maintaining uninterrupted public service delivery and safeguarding citizens' personal information (ITU, 2024).

Risk management has therefore become indispensable within contemporary public administration. Modern governments are expected not only to implement digital technologies but also to establish comprehensive enterprise risk management systems capable of identifying, assessing, mitigating, and continuously monitoring cybersecurity risks. Integrating cybersecurity risk management into public sector governance strengthens institutional resilience, enhances accountability, protects national information assets, and supports sustainable digital transformation (ISO, 2018). This requires coordinated efforts involving policymakers, public administrators, cybersecurity professionals, legislators, private-sector stakeholders, and international partners.

Although existing literature has extensively examined digital governance, cybersecurity, and e-government independently, relatively fewer studies have comprehensively explored their intersection within the broader context of African public administration. Much of the available research concentrates on technological innovations while paying comparatively limited attention to institutional governance, administrative capacity, policy implementation, organizational resilience, and strategic risk management within public institutions. This gap necessitates further scholarly inquiry into how cybersecurity considerations can be systematically integrated into public administration reforms to enhance governance outcomes across Africa.

Against this background, this study examines the relationship between digital governance, cybersecurity risks, and public administration in Africa. It explores the opportunities presented by digital transformation, identifies the principal cybersecurity risks confronting public institutions, evaluates existing institutional responses, and proposes policy measures for strengthening cyber resilience and improving public sector performance. By situating cybersecurity within the broader discourse of governance and administrative reform, the study contributes to emerging scholarship on digital public administration and provides practical recommendations for policymakers, public administrators, development partners, and researchers seeking to promote secure, transparent, accountable, and resilient governance systems across Africa.

The cybersecurity environment in Africa is diverse, and African countries should not be treated as having identical levels of cybersecurity preparedness or institutional capacity. Some countries have developed national cybersecurity strategies, established dedicated cybersecurity

institutions, strengthened legal and regulatory frameworks, and invested in digital infrastructure and technical capacity. At the same time, other countries continue to face significant constraints relating to funding, cybersecurity infrastructure, skilled personnel, regulatory enforcement, institutional coordination, and public awareness. Even among countries that have made considerable progress, the rapid expansion of digital government systems continues to create new cybersecurity and data-protection challenges. These differences reflect variations in national resources, institutional arrangements, technological development, policy priorities, and implementation capacity. Accordingly, this study approaches cybersecurity in Africa as a diverse and evolving governance challenge rather than as a uniform continental weakness.

Objectives of the Study

The broad objective of this study is to examine the relationship between digital governance, cybersecurity risks, and public administration in Africa, with particular emphasis on the implications for effective governance, institutional resilience, and sustainable public service delivery.

The specific objectives are to:

1. Examine the concept and evolution of digital governance within the context of public administration in Africa.
2. Identify the major cybersecurity risks confronting public institutions in African countries.
3. Assess the effects of cybersecurity threats on public administration, service delivery, transparency, accountability, and citizens' trust in government.
4. Evaluate the institutional, legal, and policy responses adopted by African governments to strengthen cybersecurity and digital governance.
5. Examine the role of risk management in enhancing cybersecurity resilience and protecting critical public sector digital infrastructure.
6. Identify the major challenges limiting the effective integration of cybersecurity risk management into public administration in Africa.
7. Propose policy recommendations for strengthening digital governance, cybersecurity resilience, and public sector performance across African countries.

Significance of the Study

The significance of this study lies in its contribution to the growing body of knowledge on digital governance, cybersecurity, and public administration within the African context. As governments increasingly rely on digital technologies to improve governance and service delivery, cybersecurity has become a strategic governance issue rather than merely a technological

concern. This study therefore provides timely insights into the opportunities and risks associated with digital transformation in public administration.

Academically, the study contributes to existing literature by integrating the concepts of digital governance, cybersecurity risk management, and public administration into a single analytical framework. While previous studies have often examined these concepts separately, this study demonstrates their interdependence and highlights the importance of incorporating cybersecurity considerations into governance reforms. Consequently, the study enriches scholarly discourse on public sector modernization, digital transformation, and institutional resilience.

The study is equally significant to policymakers at national, regional, and continental levels. Its findings provide evidence-based recommendations that can guide governments in developing stronger cybersecurity policies, improving digital governance frameworks, strengthening institutional coordination, and enhancing national cyber resilience. The recommendations will also assist governments in designing comprehensive strategies capable of protecting critical public infrastructure, government information systems, and citizens' digital identities.

Public administrators and civil servants will benefit from the study through a better understanding of the risks associated with digital government operations and the importance of embedding cybersecurity risk management into administrative processes. The study emphasizes that effective public administration requires not only technological innovation but also strong institutional governance, continuous risk assessment, staff capacity development, and organizational preparedness against cyber threats.

The research is also significant to cybersecurity professionals, information technology managers, and public sector risk managers. It identifies major institutional vulnerabilities affecting government digital systems and highlights practical approaches for improving cybersecurity governance, enterprise risk management, incident response mechanisms, and organizational resilience. These insights can support the development of more secure and reliable digital public services.

Development partners, international organizations, and regional institutions such as the African Union will equally find the study valuable. The findings provide useful evidence for supporting continental initiatives aimed at strengthening digital transformation, promoting cyber resilience, harmonizing cybersecurity regulations, and encouraging cross-border cooperation against cybercrime within Africa.

Furthermore, the study contributes to the achievement of the United Nations Sustainable Development Goals (SDGs), particularly Goal 9 (Industry, Innovation and Infrastructure), Goal 16 (Peace, Justice and Strong Institutions), and Goal 17 (Partnerships for the Goals). Secure and resilient digital governance systems are essential for building transparent, accountable, and effective public institutions capable of promoting sustainable socio-economic development.

Finally, this study serves as a valuable reference for researchers, postgraduate students, lecturers, and practitioners interested in digital governance, cybersecurity, public administration, public policy, and risk management. It also identifies important knowledge gaps that can stimulate

further empirical research on cybersecurity governance, digital public administration, and institutional resilience within Africa and other developing regions.

LITERATURE REVIEW

The growing importance of digital governance and cybersecurity has generated extensive scholarly interest in public administration, information systems, governance studies, and public policy. Researchers have examined the opportunities presented by digital transformation as well as the challenges associated with cybersecurity, institutional capacity, public sector reforms, and service delivery. Although the literature consistently recognizes the transformative potential of digital technologies, there remains considerable debate regarding the readiness of African public institutions to manage cybersecurity risks while sustaining effective digital governance.

Cybersecurity as an Institutional and Governance Issue

Cybersecurity in public administration extends beyond the deployment of technical security tools and should be understood as an institutional and governance responsibility. Effective protection of digital government systems depends on the capacity of public institutions to establish clear responsibilities, provide effective leadership, implement appropriate policies and regulations, coordinate across agencies, and integrate cybersecurity risks into broader institutional risk-management processes. Weak organizational capacity, fragmented responsibilities, inadequate coordination, limited technical expertise, and insufficient resources can reduce the ability of public institutions to prevent, detect, respond to, and recover from cyber incidents. Regulatory frameworks are similarly important, but their effectiveness depends on consistent implementation, institutional enforcement, and the capacity of relevant agencies. Cyber resilience therefore requires an integrated approach in which technology, institutional capacity, leadership, governance structures, risk management, and organizational preparedness operate together. From a public-administration perspective, cybersecurity should consequently be treated as a core component of institutional effectiveness, service continuity, public accountability, and resilience in the digital era.

Digital Governance and Public Administration

Digital governance has fundamentally reshaped the theory and practice of public administration by introducing innovative approaches to policy implementation, service delivery, citizen engagement, and institutional accountability. According to the United Nations (2024), digital governance enhances government effectiveness by facilitating data-driven decision-making, improving transparency, reducing administrative costs, and promoting inclusive participation in governance processes. The United Nations further argues that governments embracing digital transformation are better positioned to deliver quality public services and achieve sustainable development.

Similarly, the OECD (2023) maintains that digital governance strengthens institutional coordination and promotes evidence-based policymaking by integrating digital technologies into administrative systems. The organization emphasizes that governments should adopt a citizen-centered approach to digital transformation, ensuring that technological innovations improve accessibility, efficiency, and responsiveness while maintaining public trust.

Liu and Qiang (2023) studies further demonstrate that digital governance contributes significantly to economic development by reducing transaction costs, improving revenue generation, facilitating business registration, strengthening financial accountability, and supporting efficient public expenditure management. The World Bank, however, cautions that these benefits depend largely on institutional capacity, political commitment, digital infrastructure, and regulatory effectiveness.

Within Africa, scholars have increasingly documented the progress made by countries such as Rwanda, Kenya, Mauritius, Ghana, Botswana, and South Africa in implementing digital government initiatives. These countries have successfully deployed integrated digital platforms for tax administration, digital identity management, electronic procurement, health information systems, and business registration, thereby improving administrative efficiency and citizen satisfaction (African Union, 2020). Nevertheless, considerable disparities remain across African countries due to differences in institutional capacity, financial resources, digital infrastructure, and political commitment.

Conceptual Clarification: Digital Governance, E-Government, Digital Government, and Digital Transformation

Although the concepts of digital governance, e-government, digital government, and digital transformation are closely related, they are not synonymous. E-government generally refers to the use of information and communication technologies (ICTs) by government institutions to provide information and deliver public services electronically. Digital government represents a broader approach in which digital technologies are integrated into government operations, service delivery, policymaking, and institutional processes to improve how government functions and interacts with citizens and other stakeholders. Digital transformation goes beyond the adoption of digital tools by involving fundamental changes in organizational processes, institutional capabilities, administrative practices, and service models through the strategic use of digital technologies. Digital governance is broader still, encompassing the institutional arrangements, rules, policies, processes, relationships, and accountability mechanisms through which digital technologies are governed and used in the public sector. In this study, digital governance therefore provides the broader governance context within which e-government initiatives, digital government practices, and digital transformation processes occur. Maintaining these distinctions is important because the adoption of digital technologies or electronic services does not, by itself, demonstrate successful digital transformation or effective digital governance.

Cybersecurity and Digital Government

The expansion of digital government has simultaneously increased governments' exposure to cybersecurity threats. NIST (2024) argues that cybersecurity should no longer be regarded solely as an information technology issue but rather as a strategic governance function requiring organizational leadership, risk management, regulatory oversight, and continuous institutional learning.

According to the ITU (2024), cyber threats have become increasingly sophisticated due to advances in artificial intelligence, cloud computing, digital financial systems, and interconnected government databases. Public institutions worldwide have experienced increasing incidents of ransomware attacks, phishing campaigns, identity theft, malware infections, insider threats, cyber espionage, and attacks on critical infrastructure.

The World Economic Forum (2024) similarly notes that governments have become attractive targets for cybercriminals because they manage sensitive national information and provide essential public services. The report emphasizes that successful cyberattacks may disrupt healthcare systems, financial management, transportation, energy infrastructure, and electoral processes while undermining citizens' confidence in government institutions.

Within Africa, cybersecurity preparedness remains uneven despite growing digital transformation. The African Union (2020) observes that although many governments have adopted national cybersecurity strategies and cybercrime legislation, implementation remains constrained by inadequate funding, limited technical expertise, weak institutional coordination, shortage of cybersecurity professionals, and insufficient public awareness.

Risk Management in Public Administration

Risk management has become increasingly recognized as a strategic component of effective public administration. ISO (2018) emphasizes that public organizations should integrate risk management into governance, organizational planning, policy implementation, financial management, and operational decision-making. The objective is not merely to respond to crises but to anticipate uncertainties and improve organizational resilience.

COSO (2017) similarly advocates Enterprise Risk Management (ERM) as a comprehensive governance framework integrating strategic planning, organizational performance, internal control, and risk governance. ERM recognizes that organizations operate within environments characterized by interconnected strategic, operational, financial, technological, legal, environmental, and reputational risks.

Recent studies indicate that public institutions adopting enterprise risk management demonstrate greater resilience during crises because they systematically identify organizational vulnerabilities, prioritize high-impact risks, allocate resources efficiently, and strengthen institutional preparedness (OECD, 2023). However, many public institutions in developing countries continue to rely on reactive rather than preventive approaches to risk management.

Cybersecurity risk management has emerged as one of the fastest-growing areas within enterprise risk management. NIST (2024) argues that governments should adopt continuous risk assessment, vulnerability management, incident response planning, security awareness training, and business continuity planning to minimize cyber risks. These recommendations have become increasingly relevant as governments expand digital public services.

Digital Public Service Delivery

Digital public service delivery represents one of the most visible outcomes of digital governance. The United Nations (2024) argues that governments utilizing digital platforms improve accessibility, efficiency, transparency, and responsiveness while reducing administrative burdens on citizens and businesses.

Research indicates that digital public services significantly improve tax administration, healthcare delivery, social welfare programmes, education management, public procurement, licensing, and judicial administration (Liu & Qiang, 2023). Electronic government services reduce waiting times, minimize corruption opportunities, improve financial accountability, and expand access to services in geographically remote areas.

Despite these advantages, scholars caution that digital service delivery remains vulnerable to technological failures, cybersecurity threats, digital exclusion, and institutional weaknesses. OECD (2023) emphasizes that digital transformation must be accompanied by robust cybersecurity governance, effective regulatory frameworks, continuous technological innovation, and comprehensive organizational capacity building.

Institutional Capacity and Cyber Resilience

Institutional capacity remains one of the most significant determinants of successful digital governance. According to the African Union (2020), many African public institutions continue to experience shortages of qualified cybersecurity professionals, inadequate technological infrastructure, fragmented organizational responsibilities, and weak enforcement of cybersecurity regulations.

The United Nations (2024) similarly emphasizes that digital transformation requires more than technological investment. Sustainable digital governance depends on competent leadership, institutional coordination, organizational learning, skilled personnel, adequate funding, supportive legislation, and strong political commitment.

Researchers also emphasize the importance of cyber resilience rather than cybersecurity alone. Cyber resilience refers to the capacity of organizations to anticipate, withstand, respond to, recover from, and adapt to cyber incidents while maintaining essential public services (World Economic Forum, 2024). Public institutions capable of rapid recovery from cyber disruptions are better positioned to maintain public trust and ensure continuity of governance.

Critical Review of Existing Literature

The reviewed literature demonstrates broad agreement that digital governance has significantly transformed contemporary public administration by improving efficiency, transparency, accountability, and citizen participation. There is also substantial consensus that cybersecurity has become indispensable for protecting government information systems and sustaining digital public service delivery.

However, important differences exist regarding implementation priorities. While technology-oriented scholars emphasize digital infrastructure and technological innovation, governance scholars argue that institutional capacity, organizational leadership, legal frameworks, and risk

management are equally important determinants of successful digital transformation. These differing perspectives suggest that technological advancement alone cannot guarantee secure and effective digital governance.

Furthermore, much of the existing literature focuses on developed countries where institutional capacity, technological infrastructure, and cybersecurity governance are relatively mature. Comparatively fewer studies provide comprehensive analyses of the unique governance, institutional, financial, and cybersecurity challenges confronting African public administrations. Even fewer studies integrate digital governance, cybersecurity risk management, and public administration into a unified analytical framework.

This study addresses these limitations by examining the intersection of digital governance, cybersecurity risks, and public administration within the African context. It integrates technological, organizational, governance, and risk management perspectives to provide a holistic understanding of how African governments can strengthen institutional resilience, improve public service delivery, and sustain digital transformation in an increasingly complex cybersecurity environment.

EMPIRICAL REVIEW

Empirical studies on digital governance, cybersecurity, and public administration have expanded considerably over the past decade as governments increasingly adopt digital technologies to improve governance and public service delivery. Existing studies have examined issues relating to digital transformation, cybersecurity preparedness, institutional capacity, electronic government implementation, enterprise risk management, and organizational resilience. However, the findings remain diverse, reflecting variations in research contexts, methodologies, institutional environments, and levels of digital development.

A study by the United Nations (2024), based on the United Nations E-Government Survey, examined the progress of digital government across member states using comparative cross-country analysis. The study found that countries with well-developed digital infrastructure, strong institutions, and supportive public policies achieved significantly higher levels of public service efficiency, transparency, and citizen participation. It further revealed that effective digital governance requires substantial investment in institutional capacity, digital literacy, cybersecurity governance, and inclusive digital infrastructure. The report concluded that cybersecurity has become an essential determinant of sustainable digital government and recommended that governments integrate cybersecurity into national digital transformation strategies.

Similarly, the Liu and Qiang (2023) conducted a comparative assessment of digital public sector reforms in developing countries using documentary analysis and institutional performance indicators. The findings indicated that digital governance significantly improved tax administration, financial management, public procurement, business registration, and service accessibility. Nevertheless, the study identified inadequate institutional capacity, limited financial resources, weak legal frameworks, and cybersecurity vulnerabilities as major constraints to successful implementation. The report recommended stronger institutional

reforms, improved cybersecurity investment, and enhanced organizational capacity to sustain digital transformation.

The Organisation for Economic Co-operation and Development (OECD, 2023) investigated digital government maturity among member and partner countries through policy analysis and comparative institutional evaluation. The study concluded that governments adopting integrated digital governance frameworks demonstrated greater administrative efficiency, accountability, and responsiveness than governments relying on fragmented digital initiatives. However, it emphasized that organizational leadership, inter-agency coordination, enterprise risk management, and cybersecurity governance remain indispensable for maintaining public trust and ensuring uninterrupted digital public services.

Using global cybersecurity performance indicators, the International Telecommunication Union (ITU, 2024) assessed national cybersecurity readiness across countries through its Global Cybersecurity Index. The findings revealed significant disparities in cybersecurity preparedness between developed and developing countries. While several African countries had made progress in developing national cybersecurity strategies and legal frameworks, many continued to experience shortages of cybersecurity professionals, weak institutional coordination, inadequate funding, and limited incident response capacity. The study recommended strengthening national cybersecurity governance, regional cooperation, and continuous capacity development.

The African Union (2020) evaluated the implementation of digital transformation and cybersecurity initiatives across African member states using policy reviews and institutional assessments. The study found that countries such as Rwanda, Kenya, Mauritius, Ghana, and South Africa had achieved notable progress in digital government implementation through investments in digital identity systems, electronic public services, digital payment platforms, and cybersecurity governance. However, numerous African countries continued to face challenges associated with inadequate ICT infrastructure, weak cybersecurity legislation, low digital literacy, financial constraints, and fragmented institutional responsibilities. The report emphasized the importance of harmonizing cybersecurity policies across the continent and strengthening regional cooperation against cybercrime.

Bada and Nurse (2019) examined cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Their study highlighted the importance of context-sensitive cybersecurity education and awareness, noting that SMEs face significant challenges associated with limited resources, cybersecurity knowledge, and organisational capacity. These findings reinforce the broader importance of sustained cybersecurity awareness and organisational preparedness, while recognising that the study focused on SMEs rather than public-sector employees.

Using case study analysis, Von Solms and Van Niekerk (2013) examined cybersecurity governance within public organizations. Their study concluded that cybersecurity should be regarded as an organizational governance issue rather than merely a technical responsibility of information technology departments. Effective cybersecurity, according to the study, depends on institutional leadership, organizational culture, regulatory compliance, enterprise risk management, and continuous monitoring of emerging threats.

Research on enterprise risk management has also provided important insights for public administration. COSO (2017) emphasized that organizations integrating enterprise risk management into strategic planning demonstrated stronger organizational resilience, improved governance, and better decision-making than institutions adopting fragmented approaches to risk management. Similarly, ISO (2018) argued that systematic risk management enables organizations to anticipate uncertainties, reduce vulnerabilities, improve resource allocation, and strengthen institutional sustainability.

Recent studies focusing on cyber resilience have further emphasized organizational preparedness rather than mere technological protection. The World Economic Forum (2024) found that governments investing in cyber resilience—including incident response planning, business continuity management, cybersecurity workforce development, and inter-agency collaboration—were more capable of maintaining essential public services during cyber incidents. The report concluded that resilience requires continuous adaptation to evolving cyber threats rather than reliance on static security controls.

Overall, the empirical evidence consistently demonstrates that digital governance contributes positively to administrative efficiency, transparency, accountability, and public service delivery. Likewise, the studies agree that cybersecurity governance and enterprise risk management significantly enhance institutional resilience and protect government information assets. However, the literature also reveals persistent challenges associated with inadequate institutional capacity, limited funding, weak cybersecurity governance, fragmented policy implementation, and shortages of skilled personnel, particularly across many African public institutions.

Although previous empirical studies have generated valuable knowledge on digital governance, cybersecurity, and public administration, most have concentrated on individual aspects of these issues. Many studies focus exclusively on e-government adoption, cybersecurity awareness, information systems, or technological innovation without examining how these dimensions interact within broader public administration and governance reforms. Furthermore, a substantial proportion of the available literature originates from developed countries whose institutional environments differ significantly from those of many African states.

Consequently, there remains a need for comprehensive studies that integrate digital governance, cybersecurity risk management, enterprise risk management, and public administration within the African context. This study seeks to address that need by providing a holistic analysis of emerging cybersecurity risks, institutional responses, governance challenges, and policy options for strengthening resilient digital governance and effective public administration across Africa.

GAP IN THE LITERATURE

The existing literature provides substantial discussion of digital governance, e-government, cybersecurity, digital public service delivery, and institutional capacity, but these areas are often examined separately. Studies of digital government have generally emphasized the adoption of ICTs, electronic service delivery, administrative modernization, and citizen engagement, while cybersecurity literature has focused more strongly on technical threats, information security, cybercrime, and the protection of digital systems. Other studies have examined institutional

capacity, regulatory frameworks, or public-sector digital transformation without sufficiently connecting these dimensions to cybersecurity risk management within public administration.

A further gap concerns the limited integration of technological, organizational, environmental, and institutional factors in explaining cybersecurity challenges associated with digital governance in the African public sector. The literature also provides insufficient attention to how cybersecurity risks affect administrative continuity, public trust, institutional resilience, and the sustainability of digital public services. In addition, differences in institutional capacity and cybersecurity preparedness across African countries require a more context-sensitive analysis rather than a uniform continental assessment.

This study addresses these gaps by examining digital governance and cybersecurity as interconnected public-administration and governance issues. It combines the Technology–Organization–Environment (TOE) Framework with Institutional Theory to analyse how technological conditions, organizational capacity, environmental pressures, institutional arrangements, regulatory structures, and inter-agency relationships shape cybersecurity preparedness and resilience. The study therefore contributes an integrated analytical perspective that connects digital governance, cybersecurity risk management, and institutional effectiveness within the African public-sector context.

Integrating Technological, Organizational, Environmental, and Institutional Dimensions

The literature reviewed indicates that cybersecurity in digital public administration cannot be explained by technological factors alone. The adoption and effective management of digital government systems are influenced by the characteristics of the technologies being adopted, the organizational capacity of public institutions, the wider policy and regulatory environment, and the institutional structures within which digital initiatives operate. Technological factors include the availability, security, compatibility, and reliability of digital infrastructure and systems. Organizational factors include leadership, human resources, financial capacity, institutional structures, risk-management practices, and inter-agency coordination. Environmental factors include government policies, regulatory requirements, external stakeholders, cybersecurity threats, and broader national and international conditions. Institutional factors further include formal rules, regulatory expectations, professional norms, established administrative practices, and pressures for institutional conformity.

These dimensions provide a useful basis for understanding why countries and public institutions may experience different levels of digital governance and cybersecurity preparedness. The Technology–Organization–Environment (TOE) Framework provides a structured basis for examining how technological, organizational, and environmental conditions influence the adoption and implementation of technological innovations. However, because public institutions operate within formal regulatory and institutional environments, the analysis also requires attention to the institutional pressures and structures that shape organizational behaviour. Institutional Theory therefore complements the TOE Framework by explaining how coercive, normative, and mimetic pressures influence institutional practices and responses. The integration

of these perspectives provides a more comprehensive analytical foundation for examining cybersecurity and digital governance within African public administration.

Nigeria-Specific Digital Governance and Cybersecurity Context

Integrating Technological, Organizational, Environmental, and Institutional Dimensions

The literature reviewed indicates that cybersecurity in digital public administration cannot be explained by technological factors alone. The adoption and effective management of digital government systems are influenced by the characteristics of the technologies being adopted, the organizational capacity of public institutions, the wider policy and regulatory environment, and the institutional structures within which digital initiatives operate. Technological factors include the availability, security, compatibility, and reliability of digital infrastructure and systems. Organizational factors include leadership, human resources, financial capacity, institutional structures, risk-management practices, and inter-agency coordination. Environmental factors include government policies, regulatory requirements, external stakeholders, cybersecurity threats, and broader national and international conditions. Institutional factors further include formal rules, regulatory expectations, professional norms, established administrative practices, and pressures for institutional conformity.

These dimensions provide a useful basis for understanding why countries and public institutions may experience different levels of digital governance and cybersecurity preparedness. The Technology–Organization–Environment (TOE) Framework provides a structured basis for examining how technological, organizational, and environmental conditions influence the adoption and implementation of technological innovations. However, because public institutions operate within formal regulatory and institutional environments, the analysis also requires attention to the institutional pressures and structures that shape organizational behaviour. Institutional Theory therefore complements the TOE Framework by explaining how coercive, normative, and mimetic pressures influence institutional practices and responses. The integration of these perspectives provides a more comprehensive analytical foundation for examining cybersecurity and digital governance within African public administration.

THEORETICAL FRAMEWORK

This study is anchored on the Technology–Organization–Environment (TOE) Framework, complemented by Institutional Theory. These theories provide a comprehensive analytical lens for understanding how public institutions adopt digital governance technologies, manage cybersecurity risks, and respond to institutional pressures in the pursuit of effective public administration. While the TOE Framework explains the factors influencing the adoption and implementation of digital technologies, Institutional Theory highlights the influence of legal, political, cultural, and organizational environments on government behaviour and policy implementation.

Technology–Organization–Environment (TOE) Framework

The Technology–Organization–Environment (TOE) Framework was developed by Tornatzky and Fleischer (1990) to explain the factors influencing the adoption and implementation of technological innovations within organizations. Since its introduction, the framework has become one of the most widely applied theoretical models in studies of information systems, digital transformation, electronic government, innovation management, and organizational change.

The TOE Framework posits that the adoption and successful implementation of technological innovations are influenced by three interrelated contexts: the technological context, the organizational context, and the environmental context.

The technological context refers to the technologies available to an organization, including both existing and emerging innovations. It considers factors such as technological compatibility, complexity, reliability, security, cost, scalability, and perceived usefulness. Within public administration, the technological context includes digital infrastructure, internet connectivity, cloud computing, artificial intelligence, integrated government information systems, cybersecurity technologies, and digital communication platforms. Governments are more likely to adopt digital governance initiatives when technological infrastructure is reliable, secure, and capable of supporting efficient service delivery (Tornatzky & Fleischer, 1990).

The organizational context encompasses the internal characteristics of public institutions that influence technology adoption. These include organizational size, leadership commitment, financial capacity, human resource competence, institutional culture, organizational structure, administrative capability, strategic vision, and availability of technical expertise. Successful implementation of digital governance depends significantly on the willingness of public institutions to invest in skilled personnel, organizational learning, cybersecurity governance, and effective change management. Strong institutional leadership promotes innovation, mobilizes resources, and facilitates the integration of digital technologies into routine administrative processes.

The environmental context refers to external factors affecting organizational decision-making. These include government regulations, political stability, legal frameworks, public expectations, technological competition, international standards, donor support, economic conditions, and inter-organizational collaboration. In African public administration, environmental factors such as national digital transformation strategies, cybersecurity legislation, regional cooperation, international development assistance, and the regulatory environment significantly influence governments' ability to implement secure digital governance systems.

The TOE Framework is highly relevant to this study because it explains why some African governments have achieved greater success in digital governance than others. Countries possessing stronger technological infrastructure, competent public institutions, supportive legal frameworks, and effective cybersecurity policies are generally better positioned to implement resilient digital public services than countries facing infrastructural deficiencies, institutional weaknesses, and inadequate regulatory support.

Furthermore, the framework provides a useful basis for understanding cybersecurity governance within public administration. Cybersecurity effectiveness depends not only on technological solutions but also on organizational readiness, leadership commitment, institutional coordination, financial investment, regulatory compliance, and external collaboration. Consequently, cybersecurity should be viewed as an organizational governance issue rather than merely an information technology function.

Institutional Theory

Institutional Theory provides an additional perspective for understanding how public institutions respond to external pressures while implementing digital governance and cybersecurity reforms. The theory was advanced by Meyer and Rowan (1977) and later expanded by DiMaggio and Powell (1983), who argued that organizations often adopt structures, policies, and practices to achieve legitimacy, credibility, and social acceptance rather than solely to improve efficiency.

According to Institutional Theory, organizational behaviour is influenced by three forms of institutional pressure: coercive, normative, and mimetic pressures.

Coercive pressures arise from laws, regulations, government directives, and formal policy requirements. In the context of digital governance, governments establish cybersecurity legislation, data protection laws, electronic transaction regulations, and digital governance policies that compel public institutions to strengthen information security and adopt internationally recognized cybersecurity standards.

Normative pressures originate from professional standards, educational institutions, expert networks, and professional associations. Public administrators, cybersecurity professionals, auditors, and information technology specialists influence organizational practices by promoting internationally accepted principles of digital governance, information security, enterprise risk management, and ethical administration.

Mimetic pressures occur when organizations imitate successful institutions, particularly during periods of uncertainty. African governments frequently adopt digital governance models, cybersecurity frameworks, and e-government strategies that have proven successful in countries such as Estonia, Singapore, Rwanda, Kenya, and Mauritius. Such policy learning accelerates innovation and strengthens institutional modernization.

Institutional Theory explains why many African governments have introduced cybersecurity agencies, national digital transformation strategies, Computer Emergency Response Teams (CERTs), data protection authorities, and cybercrime legislation in response to increasing international expectations and global technological developments. It also explains why governments participate actively in regional and international initiatives led by the African Union, the United Nations, the International Telecommunication Union (ITU), and other organizations promoting secure digital governance.

Nevertheless, Institutional Theory recognizes that formal adoption of policies does not necessarily guarantee effective implementation. Many public institutions may establish cybersecurity policies or digital governance frameworks to satisfy legal or international

expectations without possessing the financial resources, technical expertise, organizational capacity, or institutional commitment required for effective implementation. This observation is particularly relevant in many developing countries where implementation gaps remain a major governance challenge.

Relevance of the Theories to the Study

The combination of the TOE Framework and Institutional Theory provides a comprehensive theoretical foundation for this study. The TOE Framework explains the technological, organizational, and environmental factors influencing the adoption of digital governance and cybersecurity practices within public administration. Institutional Theory complements this perspective by explaining how legal frameworks, political environments, professional norms, and international pressures shape government responses to cybersecurity risks.

Together, the two theories demonstrate that successful digital governance is not determined solely by technological investment. Rather, it depends on the interaction between technological readiness, institutional capacity, organizational leadership, regulatory effectiveness, professional competence, stakeholder collaboration, and comprehensive risk management.

This integrated theoretical perspective aligns closely with the objectives of the present study, which seeks to examine digital governance, cybersecurity risks, and public administration in Africa. It provides an appropriate framework for analysing institutional responses to cyber threats, evaluating governance challenges, and proposing practical policy recommendations capable of strengthening cyber resilience, improving public service delivery, and promoting sustainable digital governance across African countries.

RESEARCH METHODOLOGY

This study adopts a qualitative research methodology based on documentary analysis to examine the relationship between digital governance, cybersecurity risks, and public administration in Africa. A qualitative approach is considered appropriate because the study seeks to develop an in-depth understanding of the concepts, institutional dynamics, policy frameworks, governance challenges, and risk management strategies associated with digital transformation in the public sector. Unlike quantitative studies that emphasize numerical measurement and statistical analysis, qualitative research enables a comprehensive examination of complex governance issues through the systematic interpretation of documentary evidence and scholarly literature (Creswell & Creswell, 2023).

The documentary research approach provides an opportunity to synthesize evidence from multiple authoritative sources, identify recurring patterns, compare institutional experiences across countries, and generate evidence-based policy recommendations. Given the evolving nature of digital governance and cybersecurity, documentary analysis offers a reliable means of integrating contemporary knowledge from academic publications, government reports, international organizations, policy documents, and professional standards.

The study is descriptive and analytical in nature. It not only describes the concepts of digital governance, cybersecurity, risk management, and public administration but also critically

evaluates their interrelationships within the African context. Through thematic analysis, the study identifies the major opportunities presented by digital governance, examines emerging cybersecurity risks confronting public institutions, evaluates institutional responses adopted by African governments, and proposes strategies for strengthening cyber resilience and sustainable public administration.

The qualitative methodology adopted in this study is consistent with previous research in governance, public administration, public policy, and information systems, where documentary analysis has been widely employed to examine institutional reforms, administrative innovations, policy implementation, and governance challenges (Creswell & Creswell, 2023; Yin, 2023). Consequently, the chosen methodology provides an appropriate framework for achieving the objectives of the study while ensuring analytical depth, credibility, and scholarly rigour.

Research Design

The study adopts a descriptive documentary research design. Documentary research design involves the systematic collection, examination, interpretation, and synthesis of information contained in published and unpublished documentary sources relevant to the research problem. This design is particularly suitable because the study focuses on analysing existing knowledge relating to digital governance, cybersecurity, risk management, and public administration rather than collecting primary data from respondents.

The descriptive design enables the researcher to present a comprehensive account of contemporary developments in digital governance while critically examining institutional responses to cybersecurity challenges within African public administration. It also facilitates comparative analysis of policy initiatives, governance frameworks, and digital transformation strategies implemented across different African countries.

Sources of Data

The study relies exclusively on secondary data obtained from credible documentary sources. These include:

- Peer-reviewed journal articles on digital governance, cybersecurity, public administration, and risk management.
- Books and academic textbooks.
- Government publications and policy documents.
- Reports from international organizations such as the United Nations (UN), World Bank, African Union (AU), International Telecommunication Union (ITU), Organisation for Economic Co-operation and Development (OECD), and the International Organization for Standardization (ISO).
- National cybersecurity strategies and digital transformation policy documents.
- Conference papers and professional reports relevant to digital governance and cybersecurity.

- Official publications from relevant government ministries and regulatory agencies.

These sources were selected because they provide reliable, current, and authoritative information necessary for analysing the subject matter.

Method of Data Collection

Data were collected through a systematic documentary review of relevant literature and official publications. The selection of documents was guided by their relevance to the objectives of the study, credibility of the source, scholarly quality, and currency of publication. Priority was given to publications issued between 2018 and 2026 to ensure that the analysis reflects recent developments in digital governance and cybersecurity. Seminal works published before this period were also included where necessary to provide theoretical and historical foundations.

Relevant information extracted from the selected documents included conceptual definitions, theoretical perspectives, empirical findings, institutional practices, policy initiatives, governance challenges, cybersecurity threats, and recommendations relating to digital governance and public administration in Africa.

Method of Data Analysis

The study employs thematic content analysis to analyse the documentary data collected. Thematic content analysis involves identifying, organizing, interpreting, and synthesizing recurring themes, concepts, and patterns emerging from documentary sources. The method enables the researcher to compare findings from different studies, identify areas of convergence and divergence, evaluate institutional responses, and draw meaningful conclusions.

The analysis was organized around the major themes of the study, including digital governance, cybersecurity risks, public administration, enterprise risk management, institutional capacity, digital public service delivery, cyber resilience, and governance reforms. These themes were interpreted within the context of the Technology–Organization–Environment (TOE) Framework and Institutional Theory to explain how technological, organizational, and environmental factors influence cybersecurity governance in African public administration.

To enhance the credibility and validity of the findings, information was triangulated across multiple authoritative sources. Comparing evidence from academic literature, government reports, and publications of international organizations minimized bias and strengthened the reliability of the study's conclusions and policy recommendations.

Overall, the chosen methodology provides a rigorous and appropriate framework for examining the complex interaction between digital governance, cybersecurity risks, and public administration in Africa. It enables the study to generate comprehensive evidence capable of informing policy decisions, strengthening institutional resilience, and advancing scholarly understanding of secure digital governance in the African public sector.

RESULTS AND DISCUSSION

The findings of this study are organized thematically in line with the objectives of the research. The discussion integrates evidence from the reviewed literature and interprets the implications for digital governance, cybersecurity risk management, and public administration in Africa.

Digital Governance Has Significantly Improved Public Administration

The reviewed evidence suggests that digital governance initiatives can contribute to improved administrative processes, service accessibility, financial management, and interactions between public institutions and citizens. However, these outcomes should not be assumed to occur uniformly across African countries, as implementation capacity and institutional conditions differ considerably. The introduction of electronic government (e-government) platforms has reduced bureaucratic bottlenecks, accelerated decision-making, improved record management, and expanded citizens' access to public services (United Nations, 2024).

Digital initiatives such as electronic tax administration, online business registration, electronic procurement systems, digital identity management, integrated financial management information systems, and online licensing services have significantly improved administrative efficiency. Countries including Rwanda, Kenya, Mauritius, Ghana, South Africa, and Nigeria have demonstrated that digital governance can reduce operational costs, increase government revenue, minimize corruption opportunities, and improve accountability within public institutions (Liu & Qiang, 2023).

The findings further indicate that digital governance has strengthened citizen participation through online complaint mechanisms, digital feedback systems, and electronic consultation platforms. These innovations have enhanced transparency by enabling citizens to access government information and monitor public sector activities more effectively.

However, the level of digital transformation varies considerably across African countries. While some countries have developed relatively advanced digital government ecosystems, others continue to experience significant infrastructural, financial, and institutional constraints that limit the effectiveness of digital public administration.

Cybersecurity Threats Are Increasing Across African Public Institutions

The expansion of digital government systems has increased the exposure of public institutions to cybersecurity risks. The available evidence indicates that these risks can affect service continuity, data protection, institutional trust, and the resilience of public-sector systems, particularly where cybersecurity governance and technical capacity remain limited.

The most common cybersecurity threats identified include ransomware attacks, phishing, malware infections, identity theft, insider threats, cyber espionage, data breaches, and Distributed Denial-of-Service (DDoS) attacks (International Telecommunication Union [ITU], 2024). These threats have disrupted government operations in several countries and exposed weaknesses in cybersecurity governance.

The study further finds that cybercriminals increasingly target public institutions because they maintain extensive databases containing sensitive information relating to citizens, taxation,

healthcare, education, national identity, and public finances. Consequently, cybersecurity has become an essential component of national security and effective governance.

Institutional Capacity Remains a Major Challenge

A major finding of the study is that inadequate institutional capacity continues to undermine effective digital governance and cybersecurity management across many African countries.

Although governments have invested considerably in digital technologies, institutional reforms have often failed to keep pace with technological development. The literature consistently identifies inadequate funding, weak organizational coordination, limited technical expertise, insufficient cybersecurity professionals, poor digital literacy, outdated technological infrastructure, and weak enforcement of cybersecurity regulations as major institutional constraints (African Union, 2020).

The study also reveals that many public institutions continue to rely on fragmented cybersecurity governance structures. Responsibilities for cybersecurity are frequently dispersed among multiple agencies with overlapping mandates, thereby reducing coordination, accountability, and rapid response to cyber incidents.

Risk Management Is Essential for Sustainable Digital Governance

The findings demonstrate that enterprise risk management has become indispensable for modern public administration.

Governments that systematically identify, assess, mitigate, monitor, and review cybersecurity risks demonstrate greater organizational resilience than institutions relying primarily on reactive responses after cyber incidents occur. International frameworks such as ISO 31000 and the NIST Cybersecurity Framework provide practical guidance for integrating cybersecurity into organizational governance and strategic planning (ISO, 2018; Pascoe et al., 2024).

The study further establishes that cybersecurity should no longer be regarded solely as a technical responsibility of information technology departments. Instead, cybersecurity risk management should be integrated into institutional leadership, strategic planning, budgeting, human resource development, organizational culture, and policy implementation.

This finding supports the Technology–Organization–Environment (TOE) Framework, which emphasizes that technological innovation succeeds only when supported by organizational readiness and a conducive external environment.

Public Trust Depends on Secure Digital Government

Another important finding is that citizens' confidence in digital government depends largely on the security and reliability of public information systems.

The literature indicates that repeated cybersecurity incidents reduce citizens' willingness to utilize online government services because of concerns regarding privacy, financial fraud, and unauthorized disclosure of personal information (World Economic Forum, 2024).

Conversely, governments that demonstrate strong cybersecurity governance, effective data protection, transparent communication, and rapid incident response enjoy higher levels of public confidence and increased utilization of digital public services.

Therefore, cybersecurity contributes directly to government legitimacy, accountability, and democratic governance.

Regional Cooperation Strengthens Cyber Resilience

The findings further reveal that cybersecurity is increasingly becoming a transnational governance issue.

Cybercrime frequently transcends national boundaries, making regional and international cooperation indispensable. Institutions such as the African Union, the International Telecommunication Union, the United Nations, and regional economic communities have introduced frameworks encouraging cooperation in cybercrime prevention, information sharing, capacity building, and harmonization of cybersecurity legislation.

Strengthening continental cooperation will improve Africa's collective capacity to combat cybercrime, protect digital infrastructure, and support secure digital transformation.

Discussion of Findings

The findings demonstrate that digital governance has fundamentally transformed public administration in Africa by improving efficiency, transparency, accountability, and accessibility of public services. These findings are consistent with those of the United Nations (2024), the Liu and Qiang (2023), and the OECD (2023), all of which argue that digital transformation enhances government effectiveness when supported by strong institutions and appropriate policy frameworks.

The findings also confirm that cybersecurity has become one of the most significant governance challenges confronting contemporary public administration. Rather than representing merely a technological concern, cybersecurity now influences institutional credibility, economic development, national security, democratic governance, and citizens' trust in government.

Furthermore, the study demonstrates that institutional capacity remains the principal determinant of successful digital governance in Africa. Countries possessing competent leadership, effective legal frameworks, adequate funding, skilled human resources, and integrated cybersecurity governance consistently perform better than countries experiencing institutional weaknesses.

The findings further validate the Technology–Organization–Environment (TOE) Framework by demonstrating that successful digital governance depends upon the interaction of technological readiness, organizational capability, and supportive external environments. Similarly, Institutional Theory explains why governments increasingly adopt cybersecurity legislation, digital governance policies, and international standards in response to legal requirements, professional norms, and international expectations.

Overall, the study concludes that sustainable digital governance cannot be achieved through technological investment alone. Long-term success requires comprehensive cybersecurity governance, enterprise risk management, institutional reforms, continuous capacity development, effective leadership, regional cooperation, and sustained political commitment. These interconnected factors collectively strengthen cyber resilience, improve public service delivery, and promote effective public administration across Africa.

CONCLUSION

Digital governance has become an increasingly important component of public administration in Africa, creating opportunities to improve administrative processes, public service delivery, financial management, transparency, and interactions between governments and citizens. However, the expansion of digital government systems has also increased the exposure of public institutions to cybersecurity risks that can affect data protection, service continuity, institutional resilience, and public trust. The evidence reviewed indicates that these challenges vary across African countries, reflecting differences in technological development, institutional capacity, regulatory environments, financial resources, and human capabilities.

The study further demonstrates that cybersecurity should not be treated solely as a technical concern but as an important institutional and governance responsibility. Effective cybersecurity requires appropriate leadership, clear institutional responsibilities, skilled personnel, secure infrastructure, effective regulatory implementation, inter-agency coordination, and integration of cybersecurity risk management into broader public-administration processes. The TOE Framework and Institutional Theory provide complementary perspectives for understanding how technological, organizational, environmental, and institutional conditions influence digital governance and cybersecurity preparedness.

The study concludes that the sustainability of digital governance depends not only on the adoption of digital technologies but also on the capacity of public institutions to manage associated cybersecurity risks. Strengthening cybersecurity governance, institutional capacity, secure infrastructure, legal and regulatory implementation, workforce development, regional cooperation, and continuous monitoring can contribute to more resilient digital public administration. Future efforts should therefore pursue digital transformation and cybersecurity as interconnected dimensions of effective and sustainable public-sector governance.

RECOMMENDATIONS

Based on the findings of the study, the following broader recommendations are proposed:

1. Strengthen cybersecurity governance, institutional capacity, and risk management.

African governments should strengthen national and institutional cybersecurity governance by developing and effectively implementing comprehensive cybersecurity policies, clear

institutional responsibilities, appropriate legal and regulatory frameworks, and enterprise risk-management systems. Public institutions should integrate cybersecurity risk assessment, monitoring, incident response, and resilience planning into routine administrative and digital-governance processes. Stronger inter-agency coordination and effective cybersecurity institutions, including Computer Emergency Response Teams (CERTs) or equivalent structures, should also be supported.

2. Invest in secure digital infrastructure, human capacity, and public awareness.

Governments should increase investment in secure and resilient digital infrastructure while addressing shortages of skilled cybersecurity professionals. Continuous training and professional development should be provided for public officials responsible for digital systems, cybersecurity, data protection, and risk management. Public awareness programmes should also be strengthened to improve safe digital practices among government employees and citizens. Partnerships with universities, professional institutions, technology organizations, and other relevant stakeholders can support skills development and innovation.

3. Strengthen legal implementation, regional cooperation, and multi-stakeholder collaboration.

African countries should strengthen the implementation and enforcement of cybersecurity, data-protection, privacy, and related digital laws. Regional cooperation should be expanded through information sharing, joint capacity-building initiatives, coordinated responses to cross-border cyber threats, and collaboration among governments and regional institutions. Partnerships with private-sector organizations, development partners, research institutions, and cybersecurity professionals should complement government efforts to strengthen cyber resilience.

4. Promote continuous monitoring, evaluation, and further research.

Public institutions should establish mechanisms for continuously monitoring cybersecurity risks, evaluating the effectiveness of digital-government systems, and documenting incidents and institutional responses. Future research should examine country-specific differences in digital governance and cybersecurity preparedness, assess the effectiveness of cybersecurity policies and institutional arrangements, and generate empirical evidence on the relationship between cybersecurity resilience, digital public services, public trust, and administrative performance.

Article Publication Details

This article is published in the [OpenMind Journal of Multidisciplinary Innovation & Development](#), ISSN: 3108-2920 (Online). In Volume 2 (2026), Issue 5 (Sep - Oct) - 2026
The journal is published and managed by [OMR PUBLICATION](#) .

Acknowledgements

We sincerely thank the editors and the reviewers for their valuable suggestions on this paper.

Authors' contributions

All author(s) read and approved the final manuscript.

Funding

The author(s) declare that no funding was received for this work.

Data availability

No datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate

The author(s) declare that not applicable.

Consent for publication

The author(s) declare that not applicable.

Competing interests

The author(s) declare no competing interests.

REFERENCES

1. African Union. (2020). *The digital transformation strategy for Africa (2020–2030)*. African Union Commission. <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>
2. Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410. <https://doi.org/10.1108/ICS-07-2018-0080>

3. Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*.
4. Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approach* (6th ed.). SAGE Publications.
5. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
6. International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines*.
7. International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.).
8. Liu, Y., & Qiang, Z. (2023). *Digital progress and trends report 2023*. World Bank Group. <https://doi.org/10.1596/978-1-4648-2049-6>
9. Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
10. OECD. (2023). *Digital government review of Türkiye: Towards a digitally-enabled government*. OECD Publishing. <https://doi.org/10.1787/3958d102-en>
11. Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST cybersecurity framework (CSF) 2.0*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.29>
12. Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The processes of technological innovation*. Lexington Books.

13. United Nations. (2024). *United Nations e-government survey 2024: Accelerating digital transformation for sustainable development*. United Nations Department of Economic and Social Affairs.
14. Von Solms, B., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
15. World Economic Forum. (2024). *Global cybersecurity outlook 2024*.
16. Yin, R. K. (2023). *Case study research and applications: Design and methods* (7th ed.). SAGE Publications.

PUBLISHER'S NOTE

OMR PUBLICATION remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of OMR PUBLICATION and/or the editor(s). OMR PUBLICATION disclaims responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.