Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 8
August 2025

AI and Cybersecurity in the Lagos State Public Sector: Opportunities and Risks

Gbemisola Kayode-Bolarinwa [1]

[1] ICT Training & Service Management, Lagos State Ministry of Innovation, Science and Technology, UCAM, Spain

Abstract

Artificial Intelligence (AI) is rapidly transforming the global cybersecurity landscape, offering advanced capabilities in threat detection, incident response, and operational automation (Buczak & Guven, 2016; Khan et al., 2021). In subnational contexts such as Lagos State, Nigeria's economic and digital innovation hub, AI adoption within the public sector presents both strategic opportunities and significant challenges (Adekunle & Akinyemi, 2022; Lagos State Government, 2023). As Lagos State intensifies its digital transformation efforts through initiatives like the Smart City Project and Digital Lagos, the integration of AI into cybersecurity systems promises to improve the resilience of government institutions against increasingly sophisticated cyber threats (Olaniyi et al., 2023; Kayode-Bolarinwa, 2025).

AI technologies can empower public agencies by enabling real-time network monitoring, predictive analytics for risk prevention, and automated responses to cyber incidents (Adeniran & Ojo, 2023). These capabilities are particularly important for protecting sensitive datasets such as biometric records, tax information, and healthcare data. However, AI deployment also raises concerns about algorithmic bias, adversarial attacks, increased attack surfaces, and the erosion of public trust due to opaque decision-making (Eze & Olatunde, 2022; Adetunji & Sanyaolu, 2021). Additionally, Lagos State faces challenges including limited regulatory clarity, infrastructure gaps, and insufficient technical capacity for secure AI implementation (Ogunleye & Adeoye, 2023).

This article examines both the transformative potential and the emerging risks of using AI in the cybersecurity architecture of Lagos State's public sector. Drawing from contemporary literature, government policy documents, and empirical case examples, the paper presents evidence-based recommendations. These include establishing AI-specific cybersecurity governance frameworks, building digital literacy among public servants, developing ethical standards for AI and data use, and fostering inter-agency and public-private collaboration. Together, these strategies aim to ensure a secure, transparent, and citizen-centric application of AI in public administration.

Keywords: AI, Cybersecurity, Public Sector, Lagos State, Risks, Threats.

1. Introduction

Lagos State, the commercial and technological heartbeat of Nigeria, is home to over 20 million residents and accounts for nearly one-third of the nation's GDP (National Bureau of Statistics [NBS], 2022). In recent years, Lagos has embarked on an ambitious digital transformation agenda aimed at modernizing governance, improving public service delivery, and positioning the state as Africa's foremost smart city (Lagos State Government, 2023). Initiatives such as the Digital Lagos project and the implementation of e-governance platforms in ministries, departments, and agencies (MDAs) have significantly increased the use of digital infrastructure across the public sector.

However, this rapid digitization has also led to an expanded cybersecurity threat surface. Public institutions now manage vast amounts of sensitive data, including citizens' biometrics, financial transactions, health records, and geographic information, which makes them attractive targets for cybercriminals (Oyedele & Adebayo, 2021). In 2021 alone, Nigeria witnessed a 50% increase in cyber incidents, many of which targeted state-level institutions with weak defenses (Cybersecurity Nigeria, 2022).

In response to these growing threats, Artificial Intelligence (AI) technologies have emerged as a promising solution to bolster cybersecurity defenses. AI offers transformative capabilities such as real-time anomaly detection, automated incident response, and predictive analytics that can forecast and prevent cyberattacks (Buczak & Guven, 2016; Adeniran & Ojo, 2023). When integrated into public sector cybersecurity frameworks, AI can help Lagos State monitor complex systems, detect suspicious behaviors,

and respond swiftly to intrusions, especially as the volume and complexity of attacks continue to rise (Kayode-Bolarinwa, 2025).

Yet, the application of AI in cybersecurity is not without significant risks. For one, adversarial AI techniques allow attackers to manipulate algorithms, bypass detection systems, and exploit machine learning vulnerabilities (Eze & Olatunde, 2022). Moreover, the deployment of AI models trained on biased or incomplete datasets can lead to discriminatory outcomes, undermining citizen trust in digital public services (Adetunji & Sanyaolu, 2021). Privacy concerns also arise, as AI systems often require the processing of large volumes of personal data, which can conflict with legal protections such as the Nigerian Data Protection Act (NDPA) of 2023.

Compounding these risks is the limited capacity within Lagos State's public sector in terms of AI governance, regulatory frameworks, and digital skills among civil servants (Ogunleye & Adeoye, 2023). While efforts are underway to build digital resilience, a comprehensive strategy is still needed to guide the ethical and secure use of AI in government cybersecurity operations.

Therefore, this paper explores the role of AI in enhancing cybersecurity within the Lagos State public sector. It analyzes the current opportunities AI presents for threat detection, response, and operational efficiency, while also highlighting key vulnerabilities and ethical challenges. The study concludes with practical recommendations for policymakers aimed at ensuring the safe, inclusive, and effective adoption of AI technologies in Lagos State's cybersecurity ecosystem.

2. Opportunities of AI in Lagos State Public Sector Cybersecurity

Artificial Intelligence (AI) presents immense opportunities to improve the cybersecurity posture of Lagos State's public sector. With increasing digital infrastructure across ministries, departments, and agencies (MDAs), government institutions are under pressure to protect sensitive data and ensure continuity of service. AI technologies offer solutions that can transform how public sector systems detect, respond to, and anticipate cyber threats.

2.1. Advanced Threat Detection and Real-Time Monitoring

As Lagos State continues its ambitious digital transformation across sectors, including e-governance, healthcare, and internal revenue administration, its public institutions have become increasingly vulnerable to a wide spectrum of cyber threats. These threats include but are not limited to ransomware, phishing, insider data breaches, and distributed denial-of-service (DDoS) attacks (Oyedele & Adebayo, 2021). Traditional cybersecurity approaches, primarily rule-based firewalls, antivirus software, and static threat databases, often lack the sophistication and agility needed to detect and respond to these dynamic, evolving threats.

Artificial Intelligence (AI), particularly through the application of Machine Learning (ML) and Deep Learning (DL) algorithms, offers a powerful alternative. AI-powered cybersecurity systems can analyze terabytes of network traffic, authentication logs, endpoint activity, and application behaviors in real time. These systems detect patterns that deviate from historical norms, helping to identify potential breaches even before they fully materialize (Afolabi & Ibrahim, 2022; Kayode-Bolarinwa, 2025). AI models not only flag suspicious activities but also continuously refine their accuracy by learning from past incidents, false positives, and evolving threat signatures.

For instance, the Lagos State Health Management Agency (LASHMA) has started integrating AI-powered monitoring systems capable of detecting unusual access patterns in sensitive healthcare databases. These tools help secure electronic medical records (EMRs) by flagging unauthorized login attempts, large data exports, or anomalies in patient data access times, thereby reducing the likelihood of data theft and privacy violations (Afolabi & Ibrahim, 2022).

In addition, the Lagos State Ministry of Innovation, Science and Technology has begun evaluating AI-enhanced Security Information and Event Management (SIEM) platforms. These platforms utilize AI to aggregate and analyze data from disparate sources such as cloud services, mobile endpoints, and IoT sensors across the state's digital infrastructure. The application of AI in SIEM enhances visibility, prioritizes alerts based on threat severity, and reduces incident response time, ensuring a more resilient cybersecurity posture across Ministries, Departments, and Agencies (MDAs) (Lagos State Government, 2023).

Such proactive threat detection mechanisms are particularly critical in departments like the Lagos State Internal Revenue Service (LIRS) and the Ministry of Finance, where any disruption could have major financial and reputational consequences. AI systems help protect not just against external attacks but also monitor for insider threats from employees who might misuse their access privileges intentionally or inadvertently (Oyedele & Adebayo, 2021).

In sum, AI-powered threat detection systems enable Lagos State to shift from a reactive to a predictive and preventive cybersecurity strategy, strengthening digital trust in public services while safeguarding sensitive citizen data.

2.2. Automation of Cybersecurity Operations

One of the key challenges faced by public sector IT departments in Lagos is a shortage of skilled cybersecurity personnel and the burden of managing routine security tasks with limited resources (Ayoade & Oladejo, 2020). AI presents a viable solution through the automation of repetitive, time-consuming tasks such as log monitoring, malware analysis, vulnerability scanning, and software patch deployment.

Automating these functions allows human analysts to concentrate on more complex threat investigations, policy formulation, and strategic planning. AI-enabled endpoint detection and response (EDR) systems can isolate compromised devices within milliseconds, helping prevent lateral movement of malware within government networks.

A notable local example is the pilot initiative by the Lagos State Traffic Management Authority (LASTMA), which incorporated AI-based firewalls and automated threat response tools to secure its connected infrastructure, including smart traffic control systems and data communication devices (Eze & Olatunde, 2022). This move has reportedly reduced downtime and improved system resilience against external attacks.

2.3. Predictive Analytics for Risk Management

AI systems excel in predictive analytics by leveraging historical data to forecast future trends and threats. This capability is particularly critical in cybersecurity, where anticipating attacks before they occur can make a significant difference in response readiness and resource allocation (Adeniran & Ojo, 2023).

By analyzing patterns in past incidents such as unauthorized login attempts, phishing reports, and patching delays, AI can generate risk scores for various departments and recommend targeted interventions. Lagos State's Ministry of Economic Planning and Budget, for instance, can benefit from such tools by integrating them into digital budget monitoring platforms to predict and pre-empt attempts to compromise sensitive financial records.

Additionally, predictive AI models can aid in disaster recovery planning by simulating various attack scenarios and evaluating the effectiveness of existing response protocols. This is essential in a dynamic threat environment, especially as Lagos State continues to adopt cloud-based services and smart city technologies, which increase the complexity of its digital footprint.

3. Risks and Challenges of AI in Lagos State Public Sector Cybersecurity

While AI technologies offer transformative benefits to cybersecurity systems in Lagos State, they also introduce several critical risks that could undermine public trust, institutional integrity, and data security. The successful and ethical deployment of AI in government settings requires careful evaluation and mitigation of these risks.

3.1. Adversarial AI and Sophisticated Cyber Attacks

While Artificial Intelligence (AI) is a powerful tool for enhancing cybersecurity, it also introduces new and complex risks, particularly in the form of adversarial AI attacks. These are intentional manipulations of AI systems by cybercriminals who leverage the very same technologies to design intelligent, adaptive, and evasive cyber threats. Such attacks exploit vulnerabilities in AI algorithms, data pipelines, and training models, making them significantly more difficult to detect and neutralize using conventional methods (Brundage et al., 2018; Kayode-Bolarinwa, 2025).

Two major adversarial techniques present growing threats to Lagos State's digital infrastructure:

1. **Data Poisoning** – This occurs when attackers insert misleading or malicious data into the training datasets of machine learning (ML) models. In public institutions, this could result in models that fail to detect real threats or worse, misclassify legitimate government operations as

attacks, leading to operational disruptions (Eze & Olatunde, 2022).

2. **Evasion Attacks** – These involve crafting malicious inputs that are subtly modified to evade AI-based threat detection. For example, malware can be encoded in such a way that AI-powered firewalls or antivirus programs do not recognize it, allowing attackers to bypass security protocols unnoticed (Brundage et al., 2018).

AI also enables automated spear-phishing, where personalized and context-aware emails are generated using natural language processing (NLP) algorithms to trick public employees into revealing credentials or downloading malicious attachments. The scale and precision of these attacks drastically increase when driven by AI, especially in high-target environments like revenue collection, healthcare, and digital identity systems (Kayode-Bolarinwa, 2025).

Lagos State public institutions are particularly susceptible to these threats due to several compounding factors:

- Limited internal expertise in adversarial machine learning and AI security.
- Underfunded and outdated cybersecurity infrastructure, especially in local government councils and smaller MDAs.
- Dependency on legacy systems that lack the resilience to detect or respond to new AI-powered exploits (Eze & Olatunde, 2022).

Moreover, the lack of formal testing and validation protocols for AI tools within Lagos State's cybersecurity architecture compounds these risks. Unlike traditional software, AI models must be regularly retrained, validated, and stress-tested against simulated adversarial inputs to remain secure and reliable (Kayode-Bolarinwa, 2025). Without a strong institutional framework to oversee this process, public systems remain vulnerable to sophisticated attacks with potentially severe consequences, including data breaches, service outages, and erosion of public trust.

To safeguard AI systems in this context, Lagos must invest in AI security research, red teaming exercises, and threat modelling specific to adversarial AI scenarios. Collaboration with academic institutions and global cybersecurity organizations can further enhance the State's resilience to these emerging threats.

3.2. Data Privacy and Protection Concerns

AI systems rely heavily on large datasets to function effectively. In the Lagos State context, this often means processing personally identifiable information (PII), including health records, tax histories, education data, and social services access. If not properly managed, this could result in severe data privacy violations, exposing citizens to identity theft, surveillance abuse, or unauthorized data sharing (Kayode-Bolarinwa, 2025).

Compliance with Nigeria's Data Protection Act (NDPR 2023) is legally required, but enforcement and awareness remain weak in many MDAs (NDPC, 2023). Furthermore, the "black box" nature of many AI models, especially those built using deep learning, makes it difficult to explain how decisions are made, complicating accountability and redress mechanisms in the event of data misuse or algorithmic harm (Crawford, 2021).

Without clear policies around data minimization, informed consent, and algorithmic transparency, the deployment of AI in public services risks violating fundamental rights and eroding public trust in digital governance.

3.3. Algorithmic Bias and Inequality

Another critical risk is the reproduction of social bias through AI systems. Machine learning algorithms can amplify existing inequalities if they are trained on datasets that reflect historical discrimination, underrepresentation, or geographic bias. In Lagos State, where ethnic, gender, and socioeconomic diversity is pronounced, biased AI models could lead to disproportionate impacts on marginalized communities (Adetunji & Sanyaolu, 2021).

For example, AI-based fraud detection tools used by welfare or healthcare programs may inadvertently deny services to individuals from disadvantaged areas if the training data underrepresents these populations. Such outcomes not only reduce the fairness of service delivery but may also result in legal challenges, protests, and public backlash against the government's digital initiatives.

A lack of rigorous impact assessments or equity audits in AI deployment strategies exacerbates this challenge, as public institutions often lack the technical know-how to detect or correct bias (Kayode-Bolarinwa, 2025).

3.4. Regulatory and Capacity Limitations

Despite growing interest in digital governance, Lagos State lacks a comprehensive regulatory framework for the ethical and secure deployment of AI technologies. Existing data protection and IT guidelines do not adequately address issues such as AI model auditing, risk classification, or standards for public procurement of AI systems (Ogunleye & Adeoye, 2023).

Moreover, there is a significant capacity gap among civil servants. Many public sector personnel do not possess the technical skills required to understand, deploy, or monitor AI applications effectively. This shortage of skilled professionals limits the government's ability to evaluate vendor solutions, enforce compliance, or respond to emerging threats.

These regulatory and human capacity challenges must be urgently addressed if Lagos State is to sustainably integrate AI into its cybersecurity architecture without compromising public accountability or operational safety.

4. Case Example: Lagos State Digital Innovation and AI in Cybersecurity

The Lagos State Government, in pursuit of its ambition to become a smart, technology-driven subnational economy, introduced the Digital Lagos Initiative in 2020. This initiative is aimed at transforming public service delivery through digital infrastructure, data-driven governance, and the integration of emerging technologies, particularly Artificial Intelligence (AI) (Lagos State Government, 2023). A core component of this digital transformation strategy is the enhancement of cybersecurity capabilities across Ministries, Departments, and Agencies (MDAs).

4.1. AI Integration in Cybersecurity Operations

Under the Digital Lagos Initiative, the Ministry of Innovation, Science and Technology (MIST) spearheaded pilot projects to deploy AI-driven cybersecurity tools. These tools include intelligent firewalls, real-time anomaly detection systems, and automated threat response platforms. These AI systems were implemented to monitor network traffic, flag suspicious activities, and support incident response teams through predictive analytics and automated decision-making (Afolabi & Ibrahim, 2022).

Initial deployments focused on high-risk agencies, including Ministry of Finance**,** Ministry of Health**,** and Lagos State Internal Revenue Service (LIRS)**.** These institutions were chosen due to their role in managing sensitive data such as financial records, health information, and citizen identification systems. AI-based systems helped reduce false positives in threat alerts and allowed for faster triaging of incidents, thus improving operational efficiency (Eze & Olatunde, 2022).

4.2. Observed Benefits and Challenges

Preliminary outcomes from these pilots were promising. According to internal reports from MIST, the AI systems recorded a 34% improvement in cyber threat detection accuracy and a reduction in average response time by 41% over six months in 2023 (Lagos State Government, 2023). The integration of AI also helped streamline manual processes such as log analysis and malware classification, tasks that previously took days to complete.

However, the deployment also surfaced critical challenges:

- Capacity Gaps: Many government ICT personnel lacked the technical expertise to interpret AI-generated insights or manage AI-powered systems effectively. This highlighted the urgent need for workforce upskilling in AI and cybersecurity fundamentals (Ayoade & Oladejo, 2020).
- Data Governance Issues: The success of AI depends heavily on high-quality, secure, and ethically managed data. It was found that some departments did not follow standardized data management protocols, posing risks to both AI model performance and compliance with the Nigeria Data Protection Act (NDPA) (NDPC, 2023).
- Algorithmic Transparency: Stakeholders expressed concerns about the "black box" nature of AI models, especially when automated decisions impacted service delivery. For example, flagged access to systems could inadvertently affect operational continuity in key departments without clear recourse or human oversight (Crawford, 2021).

4.3. Lessons and Policy Implications

The experience of Lagos State in deploying Artificial Intelligence (AI) within its public sector cybersecurity infrastructure provides valuable insights for other subnational governments navigating similar digital transitions. The phased adoption of AI in Lagos, particularly through initiatives such as the Digital Lagos

Project and pilot programs in ministries like Innovation, Science and Technology, highlights both the transformative potential of AI and the structural gaps that must be addressed for responsible implementation (Lagos State Government, 2023).

Key Lessons

i. The Necessity of Clear AI Governance Frameworks

One of the most critical lessons is the need for well-defined and enforceable AI governance frameworks. These frameworks must address issues of transparency, accountability, ethical standards, model auditability, and human oversight. Without them, AI systems, especially those involved in cybersecurity and public decision-making, could introduce risks such as data misuse, discrimination, and administrative opacity (Eubanks, 2018; OECD, 2021). Lagos must therefore prioritize the continuous development of legal and ethical standards tailored to local contexts while aligning with global principles.

ii. Importance of Capacity Building and Human Capital Development

Effective AI integration in the public sector depends not only on technology but also on the preparedness of the workforce. The Lagos State government must institutionalize ongoing training programs that cover data ethics**,** machine learning fundamentals**,** cybersecurity practices, and AI governance protocols (Ayoade & Oladejo, 2020). These programs should target civil servants across all levels, policy designers, IT professionals, and end users, ensuring a multidisciplinary understanding of AI's implications.

iii. Public-Private Collaboration is Crucial for Scalable AI Innovation

Lagos State's success also hinges on its ability to forge strong partnerships with private tech firms, academic researchers, and innovation hubs. Such collaboration fosters the co-creation of secure, inclusive, and context-sensitive AI tools tailored to the state's socio-economic realities (Adetunji & Sanyaolu, 2021). Institutions such as LASRIC (Lagos State Science, Research and Innovation Council) and the Lagos State Cybersecurity Advisory Council can serve as coordination platforms for multi-stakeholder engagement in AI development and deployment.

Policy Implications

As Lagos continues to expand AI use across sectors ranging from health and traffic management to internal revenue generation, the State must ensure that technological growth is matched by institutional reform**.** This includes developing new regulatory units, enhancing data governance**,** and fostering greater citizen participation in AI policy formulation. Furthermore, sustained compliance with national data protection frameworks such as the Nigeria Data Protection Act (NDPA) is non-negotiable to ensure citizen rights are upheld (NDPC, 2023).

By integrating these lessons into future policy planning, Lagos State can serve as a model for responsible AI governance at the subnational level—not only within Nigeria but across other developing regions navigating similar digital transitions.

5. Recommendations

To ensure the secure, ethical, and effective deployment of Artificial Intelligence (AI) for cybersecurity in the Lagos State public sector, the following strategic recommendations are proposed:

5.1. Establish AI Cybersecurity Governance Frameworks

As Lagos State accelerates its digital transformation agenda, the deployment of Artificial Intelligence (AI) in cybersecurity must be accompanied by a robust, context-specific governance framework. Without clear governance, the use of AI in sensitive public sector operations could lead to ethical breaches, legal infractions, and loss of public trust. A proactive governance approach will ensure that AI systems deployed across Ministries, Departments, and Agencies (MDAs) operate safely, transparently, and in line with constitutional rights.

The AI governance framework should be grounded in international best practices while being tailored to Nigeria's regulatory and socio-political environment. Global standards such as the OECD Principles on Artificial Intelligence, which advocate for inclusive growth, human-centered values, transparency, robustness, and accountability, provide a solid foundation (OECD, 2021). Similarly, the European Commission's AI Act, though still evolving, offers a tiered risk-based model that Lagos State could adapt to classify and manage AI systems based on their impact on public services (European Commission, 2021).

The proposed framework in Lagos State should include the following core components:

- Ethical Principles for AI Deployment in Public Services: These should cover fairness, non-discrimination, data minimization, informed consent, and inclusivity. AI tools used in service eligibility checks, surveillance, or cybersecurity monitoring must not violate citizens' rights or disproportionately affect vulnerable groups (Eubanks, 2018).
- Risk Management Protocols for AI-Driven Cybersecurity Systems: This includes mandatory AI risk assessments, continuous performance evaluations, and real-time auditing mechanisms for AI security tools such as threat detection platforms and biometric authentication systems (Gbenro & Akinyemi, 2023). AI systems should be regularly tested for accuracy, robustness against adversarial inputs, and operational reliability.
- Guidelines for Algorithmic Transparency and Accountability: All public sector AI deployments should be subject to documentation standards that clarify data sources, model logic, decision parameters, and update frequencies. This enhances explainability and supports internal audits and external reviews (Crawford, 2021). Public grievance redress mechanisms must also be embedded to ensure individuals can contest adverse AI-driven decisions.

Crucially, a localized AI regulatory structure will assist Lagos State MDAs in aligning their practices with the Nigeria Data Protection Act (NDPA) and emerging guidelines from the Nigeria Data Protection Commission (NDPC, 2023)**.** The Lagos State Ministry of Innovation, Science and Technology, in collaboration with the Ministry of Justice, could serve as the lead agency in drafting and enforcing such frameworks, working alongside stakeholders from academia, civil society, and the private sector.

By institutionalizing a formal AI governance architecture, Lagos State will be better positioned to unlock the benefits of AI in public cybersecurity while mitigating associated risks, thus ensuring ethical, lawful, and inclusive technology use.

5.2. Invest in Capacity Building

The successful deployment and governance of Artificial Intelligence (AI) in cybersecurity within Lagos State's public sector is fundamentally dependent on the strength of its human capital. As AI systems become integral to securing government digital assets, a competent and continuously trained workforce is essential to ensure effective use, maintenance, and oversight.

Lagos State should roll out structured and tiered capacity-building programs aimed at civil servants, cybersecurity professionals, policy administrators, and IT personnel across Ministries, Departments, and Agencies (MDAs). These programs should be designed to address three critical competency areas:

- Technical Proficiency in AI and Machine Learning (ML): Personnel must be equipped with foundational and advanced knowledge of AI models, how they are trained, deployed, and optimized for tasks such as intrusion detection, anomaly detection, and automated responses. This includes practical exposure to AI development tools, cloud-based security platforms, and algorithmic management systems (Ayoade & Oladejo, 2020; Gbenro & Akinyemi, 2023).
- Cyber Risk Literacy and Interpretive Skills: Staff need to understand the outputs generated by AI systems. This involves interpreting risk scores, understanding false positive and false negative metrics, and making informed decisions based on AI analysis. Without this capacity, the risk of over-reliance on AI or misjudgement of critical alerts increases significantly (Adetunji & Sanyaolu, 2021).
- Ethical and Legal Understanding of AI and Data Protection: Public sector employees must be familiar with Nigeria's Data Protection Act (NDPA) and emerging Lagos State data protection guidelines. Training must cover responsible data handling, ethical concerns in automated decision-making, and how to manage AI biases and discrimination risks (Olaniyi et al., 2023).

To facilitate delivery, Lagos State can partner with academic institutions such as the University of Lagos (UNILAG), Lagos State University (LASU), and technical education providers like NIIT Nigeria**,** Andela**,** or the Lagos State Public Service Staff Development Centre (PSSDC)**.** Additionally, Lagos State Ministry of Innovation, Science and Technology and the Lagos State Residents Registration Agency (LASRRA) can play

coordinating roles in organizing certifications, workshops, and AI training bootcamps.

By investing in this human-centered approach to cybersecurity, Lagos State will not only reduce the risks associated with AI misuse and system misconfiguration but will also cultivate a generation of public servants capable of managing and innovating within a secure digital governance ecosystem.

5.3. Promote Transparency and Accountability

As Lagos State integrates Artificial Intelligence (AI) into its public sector cybersecurity systems, promoting transparency and accountability is essential to ensure ethical governance and sustained public trust. Given the complexity and opacity often associated with AI especially in high-stakes domains such as government data management and public service delivery specific strategies must be adopted to address potential risks and perceptions of unfairness.

A critical step is the implementation of Explainable AI (XAI) frameworks. Explainable AI refers to systems that make their processes, decisions, and outputs interpretable to human users. In public sector cybersecurity, this means AI tools must clearly show how decisions such as threat detection, system flagging, or access restrictions are made. For example, if an AI system flags a login attempt as malicious and denies access to a public employee, XAI should provide a rationale based on understandable indicators such as IP anomalies or behavioral patterns (Crawford, 2021; Gunning & Aha, 2019). This not only helps government staff trust AI recommendations but also allows users to contest and appeal unjust outcomes.

Transparency is also reinforced through mandatory third-party audits**,** regular algorithmic impact assessments**,** and comprehensive documentation of AI systems. These mechanisms help uncover hidden biases, monitor performance across demographic groups, and ensure that public AI systems adhere to Lagos State's data protection and service delivery principles (Adetunji & Sanyaolu, 2021). Impact assessments, in particular, can identify where automated decisions may negatively impact citizen access to healthcare, housing, education, or welfare benefits, enabling adjustments before harm occurs.

Furthermore, Lagos State should consider publishing AI usage reports that detail where and how AI is used across agencies, what data is collected, what decisions are automated, and the accuracy or fairness metrics associated with each deployment. Such disclosures, coupled with accessible grievance redress systems, ensure that AI does not operate as a "black box" beyond public scrutiny (Olaniyi, Adeyemi & Balogun, 2023).

By embedding these transparency and accountability practices into its AI cybersecurity strategy, Lagos State can enhance trust, prevent systemic discrimination, and uphold citizens' digital rights in an increasingly automated public administration landscape.

5.4. Encourage Public-Private Partnerships

To effectively address evolving cybersecurity threats and accelerate the adoption of Artificial Intelligence (AI) in government operations, Lagos State must promote strategic public-private partnerships (PPPs). These collaborations can serve as a powerful vehicle for advancing cyber resilience, accelerating technological innovation, and bridging the gap between government needs and private sector capabilities (OECD, 2021; Olaniyi, Adeyemi, & Balogun, 2023).

By engaging with private technology startups, established cybersecurity firms, and academic institutions, Lagos State can achieve several key objectives:

- Co-Development of Localized AI Cybersecurity Solutions**:** Local tech startups possess contextual understanding of Nigeria's cyber threat landscape. Partnering with them will enable the design of AI tools customized to the specific vulnerabilities and data environments of Lagos State institutions. This includes tools for anomaly detection, automated incident response, and identity management tailored for public infrastructure (Adetunji & Sanyaolu, 2021).
- Knowledge Transfer and Innovation Incubation: Collaboration with universities and research institutions, such as the University of Lagos (UNILAG) and Lagos State University (LASU), can help build AI expertise within the civil service. Joint research programs and innovation incubators can also encourage student-led AI projects focused on public-sector security challenges (Ogunleye & Adeoye, 2023).
- Real-Time Threat Intelligence Sharing**:** Private cybersecurity firms often detect and analyze threats faster due to their commercial monitoring infrastructure. Through secure partnerships,

government agencies can gain access to real-time threat intelligence, enabling quicker response and pre-emptive risk mitigation across state systems (Eze & Olatunde, 2022).

Institutional platforms such as the Lagos State Cybersecurity Advisory Council and the Lagos State Science, Research, and Innovation Council (LASRIC) should be empowered to facilitate these collaborations. These councils can coordinate grants, pilot programs, hackathons, and joint task forces to accelerate AI integration while ensuring that private innovations are aligned with public values and legal frameworks (Lagos State Government, 2023).

By fostering such synergy, Lagos State can harness the speed and creativity of the private sector while retaining regulatory oversight, promoting innovation in a secure and accountable manner.

5.5. Strengthen Data Protection Compliance

Artificial Intelligence (AI) systems depend heavily on access to large volumes of data to train algorithms, enhance accuracy, and generate predictive insights. In the Lagos State public sector, this reliance introduces significant risks to data privacy and protection, particularly when handling sensitive citizen data such as health, financial, or biometric records. Therefore, strict compliance with Nigeria's *Nigeria Data Protection Act* (NDPA) and emerging Lagos State-specific policies is critical (NITDA, 2019; Ogunleye & Adeoye, 2023).

To ensure lawful, fair, and accountable use of AI in government services, the Lagos State Government must prioritize the following measures:

- Data Minimization and Anonymization**:** Agencies must collect only data that is directly relevant and necessary for the intended purpose. Any personal identifiers should be removed or encrypted to prevent individual re-identification during AI processing (Afolabi & Ibrahim, 2022).
- Securing Informed Consent: Before collecting or processing personal data using AI, public institutions must obtain explicit and informed consent from data subjects. This includes providing clear explanations about how data will be used, stored, and safeguarded (Eubanks, 2018).
- Conducting Data Protection Impact Assessments (DPIAs**)**: DPIAs should be a mandatory precondition for all AI-related projects within Lagos public agencies. This structured process helps identify and mitigate potential privacy risks associated with automated decision-making systems (NITDA, 2019).

Furthermore, the State should establish data governance teams within ministries to monitor AI compliance, facilitate secure data sharing between agencies, and ensure alignment with global best practices, such as the OECD AI Principles (OECD, 2021).

Failure to implement these safeguards can lead to serious consequences, including identity theft, algorithmic discrimination, reputational damage to public institutions, and lawsuits stemming from NDPR violations (Adetunji & Sanyaolu, 2021; Olaniyi, Adeyemi & Balogun, 2023). A well-enforced data protection regime will therefore help foster trust in AI systems while safeguarding citizen rights in Lagos State's digital governance journey.

6. Conclusion

Artificial Intelligence (AI) represents a powerful enabler for strengthening cybersecurity across Lagos State's public sector. From real-time anomaly detection and automated threat mitigation to predictive analytics for strategic planning, AI offers the potential to revolutionize how government institutions anticipate, respond to, and recover from cyber threats (Afolabi & Ibrahim, 2022; Adeniran & Ojo, 2023; Kayode-Bolarinwa, 2025). In a rapidly digitizing governance environment like Lagos, where essential services are increasingly delivered through digital platforms, the integration of AI can serve as a foundational pillar for cyber resilience.

However, this transformative potential is not without significant risks. AI systems can also be exploited for malicious purposes, such as adversarial attacks or social engineering, and may introduce challenges related to data privacy, algorithmic bias, and opaque decision-making processes (Eze & Olatunde, 2022; Adetunji & Sanyaolu, 2021). Additionally, the capacity limitations within many public institutions and the underdeveloped nature of AI-specific regulatory frameworks in Nigeria further complicate secure and ethical adoption (Ogunleye & Adeoye, 2023).

Therefore, it is imperative for the Lagos State Government to take a balanced, strategic, and human-centered approach to deploying AI in cybersecurity. This entails:

- Institutionalizing AI governance that aligns with ethical principles and regulatory mandates.
- Investing in workforce development to equip public servants with the necessary technical and ethical competencies.
- Fostering transparency and public trust through explainable AI and independent oversight mechanisms.
- Enhancing data protection protocols to ensure citizens' rights and Nigeria's legal obligations are upheld (NDPC, 2023; Crawford, 2021).

By aligning technological innovation with robust governance, Lagos State can responsibly leverage AI to support its broader digital transformation goals while safeguarding public trust and societal well-being. The lessons from Lagos may also serve as a model for other subnational governments in Africa embarking on similar digital security transitions.

References

[1] Adekunle, O., & Akinyemi, B. (2022). Artificial Intelligence Applications in Nigerian Public Sector Cybersecurity: Opportunities and Challenges. International Journal of Computer Science and Information Security, 20(3), 45–57.

[2] Adeniran, A., & Ojo, T. (2023). Predictive Analytics in Cybersecurity: Emerging Tools for Public Sector Resilience. Journal of Nigerian Cyber Policy Studies, 2(1), 55–70.

[3] Adeniran, O., & Ojo, T. (2023). Predictive Analytics for Cybersecurity in Lagos State: A Case for AI-Driven Risk Management. Lagos State University Journal of ICT, 5(2), 75–88.

[4] Adetunji, M., & Sanyaolu, A. (2021). Public-Private Partnerships for AI Development in Nigeria: The Role of Local Innovation Ecosystems. Journal of Emerging Technologies in Governance, 4(2), 112–127.

[5] Adetunji, T., & Sanyaolu, A. (2021). Addressing Algorithmic Bias in AI Systems: Implications for Public Service Delivery in Lagos State. Journal of African Technology and Society, 4(1), 12–28.

[6] Afolabi, K., & Ibrahim, M. (2022). Enhancing Government Data Security in Lagos State through AI: Opportunities and Pitfalls. Nigerian Journal of Cybersecurity Studies, 1(1), 22–35.

[7] Afolabi, R., & Ibrahim, M. (2022). Leveraging Machine Learning for Public Sector Cybersecurity in Nigeria: A Case Study of Health and Finance Ministries. Journal of Cybersecurity and Public Administration, 5(1), 78–93.

[8] Ayoade, J., & Oladejo, R. (2020). Building Cybersecurity Capacity in Nigeria's Public Sector: The Role of AI Skills Development. African Journal of ICT Policy and Governance, 5(2), 44–59.

[9] Ayoade, O., & Oladejo, M. (2020). Human Capital Development for AI-Driven Public Sector Cybersecurity in Nigeria. Journal of African Digital Policy, 3(1), 45–60.

[10] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute, University of Oxford.

[11] Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cybersecurity Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

[12] Crawford, K. (2021). Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press.

[13] Cybersecurity Nigeria. (2022). Annual Cybersecurity Threat Report. https://cybersecuritynigeria.org/reports

[14] Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press.

[15] European Commission. (2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[16] Eze, C., & Olatunde, J. (2022). Understanding Adversarial Attacks on AI Cybersecurity Systems in Nigeria. Cybersecurity Review, 3(1), 15–29.

[17] Eze, J. O., & Olatunde, M. A. (2022). Adversarial AI and the Threat Landscape in Nigeria's Public Sector: Emerging Challenges and Strategic Responses. Journal of African Cybersecurity Studies, 3(2), 55–70.

[18] Gbenro, D., & Akinyemi, O. (2023). AI-Driven Security and Human Capacity Needs in Nigerian e-Government Platforms. International Journal of Government Technology, 8(1), 75–91.

[19] Gunning, D., & Aha, D. (2019). DARPA's Explainable Artificial Intelligence Program. AI Magazine, 40(2), 44–58.

[20] Kayode-Bolarinwa, G., 2025. Cybersecurity Awareness and Risk Management in the Public Sector. International Journal of Intelligent Systems and Applications in Engineering, 13(1), pp.146–152.

[21] Kayode-Bolarinwa, G., 2025. Responsive AI with Cybersecurity*:* A Synergistic Approach to Modern Threat Management*.* Harbin Gongcheng Daxue Xuebao/Journal of Harbin Engineering University*,* 46(7), pp.609–617.

[22] Khan, R., McLaughlin, K., Sezer, S., & Imran, M. (2021). AI-Driven Threat Detection for Critical Infrastructure: https://doi.org/10.1109/ACCESS.2021.3100254

[23] Lagos State Government. (2023). Digital Lagos Initiative: Transforming Public Service with AI. Ministry of Science and Technology. https://lagos state.gov.ng/digital-lagos

[24] Lagos State Government. (2023). Ministry of Science and Technology Annual Report 2023: Enhancing Digital Infrastructure and Cybersecurity. Government Press.

[25] National Bureau of Statistics (NBS). (2022). State GDP Report 2021–2022. https://nigerianstat. gov.ng

[26] NDPC (Nigeria Data Protection Commission). (2023). Nigeria Data Protection Act 2023. Federal Government of Nigeria.

[27] NITDA (National Information Technology Development Agency). (2019). Nigeria Data Protection Regulation (NDPR). Abuja: NITDA. https://nitda.gov.ng/ndpr/

[28] OECD. (2021). OECD Principles on Artificial Intelligence. Organisation for Economic Co-operation and Development. https://www.oecd. org/going-digital/ai/principles/

[29] Ogunleye, A., & Adeoye, F. (2023). Regulatory Gaps in AI Governance: A Lagos State Perspective. International Journal of Public Policy and Administration, 9(3), 99–115.

[30] Ogunleye, A., & Adeoye, M. (2023). AI Policy Readiness in Subnational Governments: A Study of Lagos State. African Journal of Public Administration and Technology, 5(2), 44–60.

[31] Olaniyi, O., Adeyemi, L., & Balogun, T. (2023). AI Adoption in Nigerian Public Sector: Cybersecurity and Ethical Implications. Journal of Emerging Technologies in Government, 6(1), 33–47.

[32] Oyedele, A., & Adebayo, T. (2021). Cyber Threat Landscape and the Resilience of Public Institutions in Lagos State. Nigerian Journal of Information Security and Governance, 4(2), 101–117.