World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

The intersection of digital policy and cybersecurity: Implications for sustainable development

Ifeyinwa Nkemdilim Obiokafor [1,*] and Ogochukwu Mbonu [2]

[1] *Department of Computing Sciences, Cybersecurity Programme, Admiralty University of Nigeria.*
[2] *Department of Information Technology, National Open University of Nigeria.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 14(03), 077-085

Publication history: Received on 16 January 2025; revised on 26 February 2025; accepted on 01 March 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.14.3.0094

Abstract

As the world becomes increasingly interconnected through digital infrastructure, the nexus between digital policy and cybersecurity has emerged as a critical area of concern, particularly for sustainable development. This study explored the intersection of digital policy and cybersecurity, focusing on their implications for achieving sustainable development goals (SDGs). With growing reliance on digital technologies, safeguarding data, infrastructure, and services through robust cybersecurity measures is essential. Digital policy creates an enabling environment for secure, inclusive, and sustainable digital transformation. This research argues that well-structured digital policies, aligned with robust cybersecurity frameworks, can foster innovation, protect critical infrastructure, and promote sustainable economic, social, and environmental development. This research employs a mixed-methods approach, combining a literature review, policy analysis, and case studies, to investigate how the interplay between digital policy and cybersecurity affects the achievement of sustainable development objectives. The paper concludes with policy recommendations for harmonising digital policy and cybersecurity to support global sustainable development efforts.

Keywords: Cybersecurity; Critical Infrastructure; Data Protection; SDGS; Digital Policy; Digital Transformation; Sustainable Development

1. Introduction

In an era dominated by rapid digital transformation, the interplay between digital policies and cybersecurity has become a significant factor in the global pursuit of sustainable development. Governments, corporations, and individuals increasingly rely on digital infrastructure and systems, from basic communication to critical economic activities [6]. The digital age has brought unprecedented opportunities for economic growth, social development, and environmental sustainability. However, this dependence is coupled with new vulnerabilities including cyber threats, data breaches, and potential digital inequalities. The digital age has also introduced new challenges, including the need for effective digital policies and cybersecurity measures [19] and [23]. The intersection of digital policy and cybersecurity is critical for sustainable development as it has significant implications for protecting personal data, preventing cybercrime, and promoting digital inclusion [1] and [6].

Digital landscapes have become integral to global development. The United Nations' Sustainable Development Goals (SDGs) recognize the transformative potential of digital technologies in addressing various global challenges, from poverty reduction to climate action. Sustainable development, as outlined by the United Nations Sustainable Development Goals (SDGs), [28] emphasizes the need to balance economic growth, social inclusion, and environmental protection [24] and [25]. Digital policies and cybersecurity frameworks are increasingly being recognized as essential enablers of this balance, ensuring that digital technologies can support sustainable development goals without

* Corresponding author: Ifeyinwa Nkemdilim Obiokafor.

compromising security or exacerbating inequalities. However, increasing reliance on digital infrastructure exposes nations and communities to new vulnerabilities in cyber threats and digital divides [1]; [15] and [18].

This study explored the intersection of digital policy and cybersecurity, addressing how they collectively influence sustainable development. It highlights the potential benefits, risks, and challenges of digital transformation, and provides recommendations for crafting inclusive, secure, and forward-thinking digital policies. It examines the complex relationship between digital policy, cybersecurity, and sustainable development. It offers to answer the following research questions:

- How do digital policies and cybersecurity measures interact to shape the digital ecosystem?
- What are the implications of this interaction for achieving sustainable development goals?
- How can policymakers and stakeholders balance the need for innovation and digital growth with the imperative of cybersecurity?

By addressing these questions, this study aims to contribute to the growing body of literature on digital governance and its role in sustainable development. The findings will significantly affect policymakers, development practitioners, and cybersecurity experts working towards a more secure and equitable digital future.

2. Literature Review

2.1. Digital Policy Overview

Digital policy encompasses various regulatory and legislative measures designed to govern the digital sphere. These policies often address issues such as Internet access and infrastructure development, data protection and privacy, the digital economy and e-commerce, digital rights and freedom of expression, artificial intelligence, and emerging technologies [17]. Digital policy refers to laws, regulations, and guidelines governing the use, management, and governance of digital technologies. In their view [1], digital policy states the rules and regulations that govern the digital economy. Research has shown that effective digital policies can promote sustainable development by supporting economic growth, social development, and environmental sustainability [10], and [22]. Digital policies promoting digital inclusion help reduce poverty, the digital divide, and inequality [1] and [27].

The digital policy landscape is dynamic, with governments and international organizations continuously adapting their approaches to keep pace with technological advancements. Notable global initiatives include the European Union's General Data Protection Regulation (GDPR), the Nigeria Data Protection Commission (NDPC), and ongoing discussions of digital taxation and platform regulation. These policies encompass areas such as data privacy, intellectual property, digital rights, infrastructure investments, and digital inclusion [8]; [9] and [15].

Digital policy has a direct impact on multiple SDGs, particularly those focused on innovation, infrastructure (Goal 9), inequality reduction (Goal 10), and education (Goal 4). Effective digital policies foster economic growth and innovation while ensuring that the benefits of digitalization are equally distributed. However, weak or poorly aligned digital policies can hinder progress by exacerbating the digital divide, compromising security, and stifling innovation [1]; [4]; and [6].

2.2. Elements of Digital Policy

- **Data Privacy and Protection:** As activities shift to digital platforms, safeguarding personal and organizational data is critical to digital policy. Legal frameworks such as the General Data Protection Regulation (GDPR) in Europe have set global standards for data protection [8] and [9]. Likewise, the Nigeria Data Protection Commission (NDPC), established under the Nigeria Data Protection Act 2023, safeguards data privacy, enforces regulations, and promotes responsible data handling in Nigeria
- **Intellectual Property (IP) Rights:** Digital innovations from software to online content require robust IP protection to encourage creativity and technological advancement.
- **Infrastructure Development:** Policies promoting investments in digital infrastructure, including broadband Internet access and cloud computing, are essential for supporting a thriving digital economy.
- **Digital Inclusion:** Bridging the digital divide is crucial to ensuring that the benefits of digital transformation are equally distributed across all sections of society, including marginalized and underserved populations [2].

2.3. Cybersecurity Landscape

Cybersecurity is the protection of systems, networks, and programs from digital attacks. Cybersecurity encompasses the practices and technologies used to safeguard digital systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction [17] and [18]. The cybersecurity landscape is defined by evolving threat vectors (e.g., ransomware, phishing, DDoS attacks), national and international cybersecurity strategies, public-private partnerships in threat mitigation, capacity building and workforce development, and technological solutions (e.g., encryption and artificial intelligence in cybersecurity) [3] and [4]. As digital technologies have become more pervasive, the importance of robust cybersecurity measures has grown exponentially [16]. High-profile cyber-attacks, such as the SolarWinds hack, the Colonial Pipeline ransomware incident, and identity thefts, have underscored the critical nature of cybersecurity in maintaining economic stability and national security [28] and [29].

Cybersecurity encompasses practices, technologies, and policies that safeguard digital systems, networks, and data from unauthorized access, attacks, and damage [18]. It is a critical component of digital policy because without effective cybersecurity measures, the integrity of digital systems and services can be compromised, posing significant risks to both national security and sustainable development. Research has shown that effective cybersecurity measures can promote sustainable development by protecting sensitive information, preventing cybercrime, and promoting digital trust [7] and [30]. For instance, cybersecurity measures that protect critical infrastructure can help prevent disruptions to essential services such as healthcare and finance [16].

2.4. Sustainable Development Goals

The United Nations 2030 Agenda for Sustainable Development outlines 17 Sustainable Development Goals (SDGs) designed to address global challenges [24] and [25]. Digital technologies and cybersecurity directly or indirectly impact several of these goals, SDG 11: Sustainable Cities and Communities, SDG 4: Quality Education, SDG 9: Industry, Innovation, and Infrastructure, SDG 8: Decent Work and Economic Growth, SDG 16: Peace, Justice, and Strong Institutions, SDG 17: Partnerships for the Goals. Achieving these goals increasingly relies on secure and accessible digital infrastructure, making the intersection of digital policy and cybersecurity a crucial area of study in the context of sustainable development [13] and [14].

2.5. Cybersecurity's Role in Sustainable Development

Cybersecurity is fundamental to achieving sustainable development, particularly in areas such as innovation, infrastructure, and social inclusion [5]. However, if the digital infrastructure is compromised, the economic and social benefits of digitalization can be severely curtailed. Additionally, cybersecurity vulnerabilities can deepen inequalities because marginalized populations are often the least equipped to recover from cyber incidents [23]. Cybersecurity intersects with multiple SDGs, particularly Goal 9 (Industry, Innovation, and Infrastructure), Goal 16 (Peace, Justice, and Strong Institutions), and Goal 17 (Partnerships for the Goals), to achieve secure digital environments that are essential for fostering innovation, building resilient infrastructures, and enabling inclusive and sustainable development.

2.6. The Intersection of Digital Policy and Cybersecurity

Although digital policy provides a regulatory framework for digital transformation, cybersecurity also ensures the safety and reliability of digital systems. The intersection of these two domains is critical to ensure that digital transformation is secure and conducive to sustainable development. The intersection of digital policy and cyber security is a critical area of focus for governments, organizations, and individuals. Research has shown that effective digital policies and cyber security measures can promote sustainable development by supporting economic growth, social development, and environmental sustainability [10]; [11]; [12] and [22]. For example, digital policies that promote digital inclusion can help reduce poverty and inequality, while cybersecurity measures that protect sensitive information can help prevent cybercrime and promote digital trust [7] and [27].

3. Methodology

This study employs a mixed-methods approach to examine the intersection of digital policy, cybersecurity, and sustainable development. The methodology comprises three main components.

- Literature Review: A comprehensive review of the academic literature, policy documents, and reports from international organizations was conducted to establish a theoretical framework and identify key themes in digital policy, cybersecurity, and sustainable development.

- Policy Analysis: An in-depth analysis of digital policies and cybersecurity strategies from a diverse set of countries was performed. This analysis identified common approaches, divergences, and potential gaps in addressing the interplay between digital growth and security.
- Case Studies: Four case studies were selected to provide concrete examples of how the intersection of digital policy and cybersecurity affects sustainable development efforts.

The Data for the case studies were collected through document analysis, expert interviews, and secondary data sources. The case studies were analyzed using a framework that considers the following aspects. Policy context and objectives, cybersecurity measures implemented, impact on relevant SDGs, and challenges and lessons learned. This multifaceted approach allows for a comprehensive examination of the complex relationships among digital policy, cybersecurity, and sustainable development across different contexts and scales.

4. Analysis

4.1. Intersections of Digital Policy and Cybersecurity

The analysis revealed several key areas where digital policy and cybersecurity intersect, with significant implications for sustainable development.

- Data Governance: Digital policies often focus on data protection and privacy, which are intrinsically linked to cybersecurity practices. The implementation of data governance [3], and frameworks such as the GDPR has far-reaching effects on how organizations handle personal data and secure their digital assets.
- Critical Infrastructure Protection: Many digital policies address the need to protect critical infrastructure, including energy grids, transportation systems, and healthcare networks. These policies often overlap with cybersecurity strategies aimed at protecting and safeguarding vital systems from cyber threats.
- Digital Identity Systems: The development of national digital identity systems, as seen in the National Identity Management Commission (NIMC) program, requires a delicate balance between accessibility and security. Digital policies must address both the potential for increased inclusion and the cybersecurity risks associated with centralized identity databases.
- Artificial Intelligence and Emerging Technologies: As digital policies evolve to govern the use of AI and other emerging technologies, cybersecurity considerations have become increasingly important. The potential for AI-powered cyber-attacks and the need for secure AI systems highlight the intricate relationship between policy and security in this domain.
- Cross-border Data Flows: Digital policies that regulate cross-border data flows have significant implications for both economic development and cybersecurity. Balancing the free flow of data with security concerns remains a challenge for policymakers, and affects global trade and innovation.
- Digital Economy Policies: As seen in Nigeria's National Digital Economy Policy and Strategy (NDEPS), comprehensive digital economy policies intersect cybersecurity in multiple ways. These policies often address infrastructure development, digital literacy, and innovation, all of which have significant cybersecurity implications.

4.2. Impacts on Sustainable Development

The interplay between digital policy and cybersecurity has both positive and negative impacts [14] on sustainable development goals:

- Economic Growth and Innovation (SDG 8, and 9): Well-crafted digital policies that promote innovation while ensuring robust cybersecurity can foster economic growth and technological advancement. However, overly restrictive policies or inadequate security measures can stifle innovation and hinder economic progress.
- Digital Inclusion and Education (SDG 4, and 10): Digital policies aimed at expanding Internet access and promoting digital literacy contribute to inclusive development. However, cybersecurity concerns, if not adequately addressed, can lead to digital exclusion, particularly among vulnerable populations.
- Effective Governance (SDG 16): E-governance initiatives, supported by appropriate digital policies and strong cybersecurity measures, can enhance government efficiency and transparency. Conversely, cyberattacks on government systems can undermine public trust and impede progress towards effective institutions [3].
- Sustainable Cities and Communities (SDG 11): Smart city initiatives guided by digital policies have the potential to improve urban sustainability. However, the increased connectivity of urban infrastructure exposes cities to cyber risks, necessitating robust security measures.

- Partnerships and Collaboration (SDG 17): Digital policies that promote international cooperation in cybersecurity can strengthen global partnerships. However, divergent approaches to digital governance and cyber sovereignty can create barriers to collaboration in development initiatives [17].
- Financial Inclusion (SDG 1, 8, and 10): As demonstrated by Nigeria's FinTech sector, digital financial services can significantly contribute to financial inclusion. However, the success of these initiatives depends on robust cybersecurity measures to protect users and to maintain trust in the system.

4.3. Case Studies

To provide a focused examination of the intersection of digital policy, cybersecurity, and sustainable development in an African context, the authors analyzed four case studies from Nigeria:

- Nigeria's Digital Identity System - The National Identity Management Commission (NIMC): The National Identity Management Commission (NIMC) represents a critical intersection of digital policy, cybersecurity, and sustainable development in Nigeria. Launched to provide a unified digital identity platform, the initiative aims to address multiple sustainable development challenges.
- Nigeria's National Digital Economy Policy and Strategy (NDEPS): In 2019, Nigeria launched the NDEPS, a comprehensive plan to transform the country into a leading digital economy. This case study examines how the policy addresses key areas, such as digital literacy, soft infrastructure, solid infrastructure, service infrastructure, and digital service development. The authors analyzed the policy's implications for cybersecurity and its potential impact on sustainable development goals, particularly in the areas of economic growth, education, and innovation.
- Nigeria's Cybercrime Act of 2015: This case study focuses on Nigeria's legislative approach to cybersecurity through the Cybercrime Act of 2015. The authors examined the Act's provisions, implementation challenges, and effectiveness in addressing cyber threats. This study also explored how this legislation has influenced the digital landscape in Nigeria, its impact on digital rights, and its role in creating a secure environment for digital innovation and sustainable development.
- Financial Technology (FinTech) and Mobile Money in Nigeria: Nigeria has experienced significant growth in its FinTech sector, particularly mobile money services. This case study examines the regulatory environment for FinTech in Nigeria, including the Central Bank of Nigeria's policies regarding mobile money operations. This study analyzes how these policies have balanced the need for innovation with cybersecurity concerns and their impact on financial inclusion and economic development.

Data for these case studies were collected through a combination of document analyses, including policy documents, government reports, and academic literature, as well as secondary data sources such as industry reports and news articles.

5. Finding

5.1. Case Studies

- National Identity Management Commission: The National Identity Management Commission (NIMC) represents a critical intersection among digital policy, cybersecurity, and sustainable development in Nigeria. The crucial findings include the following:
  - The policy creates a comprehensive digital identity system, enhances financial inclusion, improves government service delivery and establishes a secure digital infrastructure
  - Implementation challenges include cybersecurity vulnerabilities such as significant concerns about data protection and privacy, risk of identity theft and fraud, inadequate initial security infrastructure and limited technological capabilities in the early stages
  - Digital privacy and data Protection lacks robust legal frameworks for data protection, unclear protocols for data sharing between government agencies and limited public trust in digital government systems
  - The policy has the potential to accelerate progress towards economic inclusion (SDG 8, and 10) enabling easier access to financial services, reduced barriers for informal sector workers, simplified process for obtaining government services and governance improvements (SDG 16)
- Nigeria's National Digital Economy Policy and Strategy (NDEPS): This demonstrates Nigeria's commitment to harness digital technologies for sustainable development. The significant findings are as follows.
  - The policy's holistic approach addresses various aspects of the digital ecosystem, from infrastructure to skill development.

  - Cybersecurity is recognized as a critical component, with specific provisions for enhancing national cybersecurity.
  - The implementation challenges include limited resources, inadequate infrastructure, and the need for continuous adaptation to emerging technologies.
  - The policy has the potential to accelerate progress towards SDGs related to education (SDG 4), decent work and economic growth (SDG 8), and innovation (SDG 9).
- Nigeria's Cybercrime Act of 2024: This case study reveals the complexities of implementing cybersecurity legislation in a developing-country context.
  - The Act provides a legal framework for combating cybercrime, which is crucial for creating a secure digital environment.
  - Implementation has been challenging owing to limited technical capacity, jurisdictional issues, and the rapid evolution of cyber threats.
  - The Act raised concerns about potential infringements on digital rights and freedom of expression, highlighting the need for a balance between security and civil liberties.
  - Despite these challenges, the Act has contributed to an increased awareness of cybersecurity issues and has provided a foundation for building a more secure digital ecosystem.
- Financial Technology (FinTech) and Mobile Money in Nigeria: The growth of FinTech in Nigeria offers insights into the interplay between innovation, regulation, and cybersecurity.
  - Regulatory sandboxes introduced by the Central Bank of Nigeria have allowed controlled innovation in the FinTech sector.
  - Cybersecurity concerns, particularly around data protection and fraud prevention, have been central to policy discussion in this sector.
  - Expanding mobile money services has contributed to financial inclusion, particularly in underserved rural areas, supporting progress towards SDG 1 (No Poverty) and SDG 10 (Reduced Inequalities).
  - Challenges remain in balancing the need for robust security measures to ensure accessibility and ease of use in populations with varying levels of digital literacy.

These Nigerian case studies highlight the importance of context-specific approaches to digital policy and cybersecurity. They demonstrated how a developing country is navigating the challenges of building a digital economy while addressing cybersecurity concerns and striving towards sustainable development goals.

5.2. Challenges at the Intersection

Despite the importance of the intersection between digital policy and cybersecurity, several challenges and limitations must be addressed. These include:

- Policy Fragmentation: Digital policies and cybersecurity frameworks often differ significantly across jurisdictions, creating challenges for global cooperation regarding cyber threats. The intersection of digital policy and cybersecurity raises jurisdictional issues, as digital policies and cybersecurity measures may need to be implemented across multiple jurisdictions [12].
- Rapid Technological Change**:** The speed of technological advancement often outpaces the development of regulatory frameworks, leaving gaps in governance and security.
- Digital Sovereignty versus Globalization: Countries increasingly adopt digital sovereignty strategies prioritising national control over digital infrastructure and data. This can complicate global efforts to address cyber threats and digital inequalities.
- Complexity: The intersection of digital policy and cyber security is complex and multifaceted, requiring a deep understanding of both [20] and [21].
- Technical Challenges: The intersection of digital policy and cyber security presents technical challenges, as digital policies and cyber security measures may require significant technical expertise for implementation and maintenance [7].
- Resource Constraints: The intersection of digital policy and cybersecurity may require significant resources, including financial, human, and technical resources [26].

5.3. Implications for Sustainable Development

Digital policies and cybersecurity have widespread implications for sustainable development. Below are several crucial areas in where this intersection plays a critical role.

- Economic Growth and Innovation: Digital economies have the potential to generate significant economic growth, particularly through innovation in sectors such as fintech, health tech, and e-commerce. However, without robust cybersecurity measures, cyber threats can undermine the economic benefits of digitalization. Comprehensive digital policies that prioritize both innovation and security are essential for sustainable economic development [1].
- Reducing Inequality: Digital policy plays a central role in promoting digital inclusion by ensuring that all populations have access to affordable and reliable Internet services. Cybersecurity is equally important because cyber incidents often disproportionately affect marginalised communities. Ensuring that cybersecurity measures are accessible and effective across all societal groups is essential for reducing inequality.
- Environmental Sustainability: Digital technologies, such as smart grids and IoT devices, have the potential to enhance environmental sustainability by optimizing resource usage and reducing waste. However, these technologies have introduced new cybersecurity risks. Digital policies that promote sustainable innovation while ensuring the security of these technologies can help accelerate environmental goals.

6. Discussion

The analysis of the intersection between digital policy and cybersecurity, particularly in the context of Nigeria and other developing African countries, reveals several significant considerations for sustainable development:

- Policy Integration in Resource-Constrained Environments: Nigeria's NDEPS highlights the importance of integrated policy approaches that consider both digital development and cybersecurity. However, this underscores the challenges in implementing comprehensive policies in resource-constrained environments. Developing countries often face trade-offs between investing in digital infrastructure and allocating resources to cybersecurity measures. Policymakers must strive for a balanced approach that promotes digital growth while ensuring adequate protection against cyber threats.
- Capacity Building and Skills Development: The implementation challenges faced by Nigeria's Cybercrime Act emphasize the critical need for capacity building in both technical and legal domains. Many African countries lack the specialized skills to enforce cybersecurity laws and respond to evolving cyber threats effectively. Sustainable development efforts must prioritize education and training programs to build local expertise in cybersecurity, digital forensics, and technological laws.
- Contextual Adaptation of Global Best Practices: While there is value in learning from global best practices in digital policy and cybersecurity, Nigerian case studies demonstrate the importance of adapting these practices to local contexts. Factors such as limited digital literacy, infrastructural challenges, and unique socioeconomic conditions necessitate tailored approaches to digital governance in African countries.
- Balancing Innovation and Regulation: The growth of Nigeria's Fintech sector illustrates the delicate balance required to foster innovation and ensure adequate regulation. Overly restrictive policies can stifle the growth of digital economies, while insufficient oversight can expose vulnerable populations to cyber risks. Regulatory sandboxes and other flexible governance models can help strike this balance, allowing for controlled innovation while maintaining necessary safeguards.
- Digital Inclusion and Cybersecurity Awareness: As observed in the expansion of mobile money services in Nigeria, digital technologies have the potential to promote financial inclusion and contribute to sustainable development goals. However, the rapid adoption of these technologies exposes new users to cyber risks. Policies should emphasize digital literacy programs that incorporate cybersecurity awareness, particularly for vulnerable and newly connected populations [17] and [18].
- Public-private Collaboration in Resource Mobilization: Given the resource constraints faced by many African countries, a collaboration between governments, private sector entities, and international partners is crucial for mobilizing the necessary resources for digital development and cybersecurity initiatives. Policies should create frameworks for such collaborations while protecting public interests and data sovereignty.
- Regional Cooperation and Harmonization: Cyber threats often transcend national borders, making regional cooperation essential. African countries should work towards greater harmonization of digital policies and cybersecurity standards at the regional level, facilitating information sharing and collective response to cyber threats.
- Leapfrogging Opportunities: While facing significant challenges, developing African countries can leapfrog outdated technologies and practices. By learning from the experiences of more digitally advanced nations, countries such as Nigeria can implement cutting-edge solutions that integrate security considerations from the ground up, potentially avoiding some of the cybersecurity pitfalls experienced by early adopters.

7. Conclusion

Examining Nigeria's experiences at the intersection of digital policy, cybersecurity, and sustainable development provides valuable insights into the challenges and opportunities of developing countries in Africa. This study has demonstrated that, while digital technologies offer significant potential for accelerating progress towards the SDGs, realising these benefits is contingent upon implementing robust and context-appropriate digital policies and cybersecurity measures.

Case studies from Nigeria have highlighted several key lessons.

- Comprehensive digital economy policies, such as the NDEPS, are essential to provide a roadmap for sustainable digital development. However, their success depends on their effective implementation and ability to adapt to rapidly changing technological landscapes.
- As Nigeria's Cybercrime Act exemplifies, cybersecurity legislation is crucial in creating a secure digital environment. However, the effectiveness of such laws hinges on building adequate enforcement capacity and striking a balance between security and digital rights.
- As seen in Nigeria's FinTech sector, the growth of innovative digital services can significantly contribute to sustainable development goals such as financial inclusion. However, realizing these benefits requires a nuanced regulatory approach that encourages innovation, while ensuring robust security measures.

Policymakers and stakeholders in developing African countries should adopt a holistic and adaptive approach to digital governance.

- Prioritizes capacity building and skills development in cybersecurity and digital policy
- Fosters public-private partnerships to overcome resource constraints
- Promotes regional cooperation in addressing transnational cyber threats
- Emphasizes digital inclusion while simultaneously building cybersecurity awareness
- Leverages opportunities to adopt advanced, secure technologies that support sustainable development goals

By addressing the complex interplay between digital policy and cybersecurity, African nations can create an environment that enables sustainable development in this digital age. This approach can help bridge the digital divide and ensure that the benefits of digital technologies are realized across all segments of society.

Future research should focus on developing metrics and assessment frameworks tailored to the African context to enable policymakers to evaluate the effectiveness of digital policies and cybersecurity measures to support sustainable development outcomes. Additionally, exploring innovative financing models for digital infrastructure and cybersecurity initiatives in resource-constrained environments could provide valuable insights into policy implementation.

The path towards a secure and inclusive digital future for Africa is challenging but essential for achieving the ambitious goals of the 2030 Agenda for Sustainable Development. By learning from experiences in Nigeria and fostering knowledge sharing and collaboration, African countries can work towards harnessing the full potential of digital technologies while safeguarding their digital futures. This balanced approach ensures that the digital revolution catalyzes sustainable and inclusive development across the continent.

Compliance with ethical standards

Disclosure of conflict of interest

There are no conflicts of interest.

References

[1] Aguboshim, F. C., Obiokafor, I. N., & Onwuka, I. N. (2021). Strategies for coping with Frontier technologies and innovations in Africa. World Journal of Advanced Research and Reviews, 11(1), 022-028.

[2] Aguboshim, F. C., Obiokafor, I. N., & Nwokedi, C. C. (2022). Closing ICT usability gaps for Nigerian women and girls: Strategies for reducing gender inequality. World Journal of Advanced Research and Reviews, 15(1), 056-063.

[3] Aguboshim, F. C., Obiokafor, I. N., & Emenike, A. O. (2023). Sustainable data governance in the Era of global data security challenges in Nigeria: A narrative review. World Journal of Advanced Research and Reviews, 17(2), 378-385.

[4] Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: policy challenges And global inequalities in cyber capacity building. Third World Quarterly, 41(6), 917-938.

[5] Cybersecurity and Infrastructure Security Agency. (2023). National Cybersecurity Strategy.

[6] Dawson, M., & Bacius, R. (2015). Cybersecurity in the 21st Century. In Security Solutions for Hyperconnectivity and the Internet of Things (pp. 1-9). IGI Global.

[7] ENISA. (2020). Cybersecurity in the EU: A Review of the Current State of Play.

[8] European Commission. (2018). General Data Protection Regulation (GDPR).

[9] European Union. (2016). General Data Protection Regulation (GDPR).

[10] International Telecommunication Union. (2020). Global Cybersecurity Index (GCI).

[11] International Telecommunication Union. (2022). Global Cybersecurity Index.

[12] International Telecommunication Union (ITU). (2020). Digital Economy Report 2020.

[13] Internet Society. (2019). Global Internet Report: Consolidation in the Internet Economy.

[14] Klimburg, A. (Ed.). (2012). National cyber security framework manual. NATO Cooperative Cyber Defence Centre of Excellence.

[15] Lewis, J. A. (2018). Economic Impact of Cybercrime—No Slowing Down. Center for Strategic And International Studies.

[16] National Institute of Standards and Technology (NIST). (2019). Framework for Improving Critical Infrastructure Cybersecurity.

[17] Obiokafor, I. N., & Aguboshim, F. C. (2024). Cybersecurity Strategies For Safeguarding Smart Ecosystem Infrastructure: A Narrative Review. ANSPOLY Journal of Advanced Research in Science & Technology (AJARST), 1(1), 49-64.

[18] Obiokafor, I. N. (2024). Strategies to Mitigate Cyber Identity Theft in Africa's Digital Transformation. JASSD-Journal of African Studies and Sustainable Development, 7(4).

[19] Obiokafor, I. N., Onyesol, M. O., Olusanya, F. A., Oboti, N. P., & Ajonuma, M. E. (2024). Cyber Intelligence's Efficacy In Mitigating Cyber Threats: A Narrative Review. ANSPOLY Journal Of Innovative Development (AJID), 2(1), 28-42.

[20] OECD. (2020). Digital Economy Outlook.

[21] OECD. (2021). Digital Economy Outlook 2020.

[22] Organisation for Economic Co-operation and Development (OECD). (2019). Digital Economy Outlook 2019.

[23] Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. Third World Quarterly, 39(5), 821-837.

[24] United Nations. (2015). Transforming Our World: The 2030 Agenda for Sustainable Development.

[25] United Nations. (2015). Sustainable Development Goals.

[26] World Bank. (2019). World Development Report 2019: The Changing Nature of Work.

[27] World Bank. (2016). World Development Report 2016: Digital Dividends.

[28] World Economic Forum. (2021). The Global Risks Report 2021.

[29] Yayboke, E., & Brannen, S. (2020). Promote and Build: A Strategic Approach to Digital Authoritarianism. Center for Strategic and International Studies (CSIS).

[30] Cisco. (2020). Cybersecurity Report 2020.