PASAS

PLATEFORME D'ANALYSE, DE SUIVI ET D'APPRENTISSAGE AU SAHEL

PORTÉ PAR

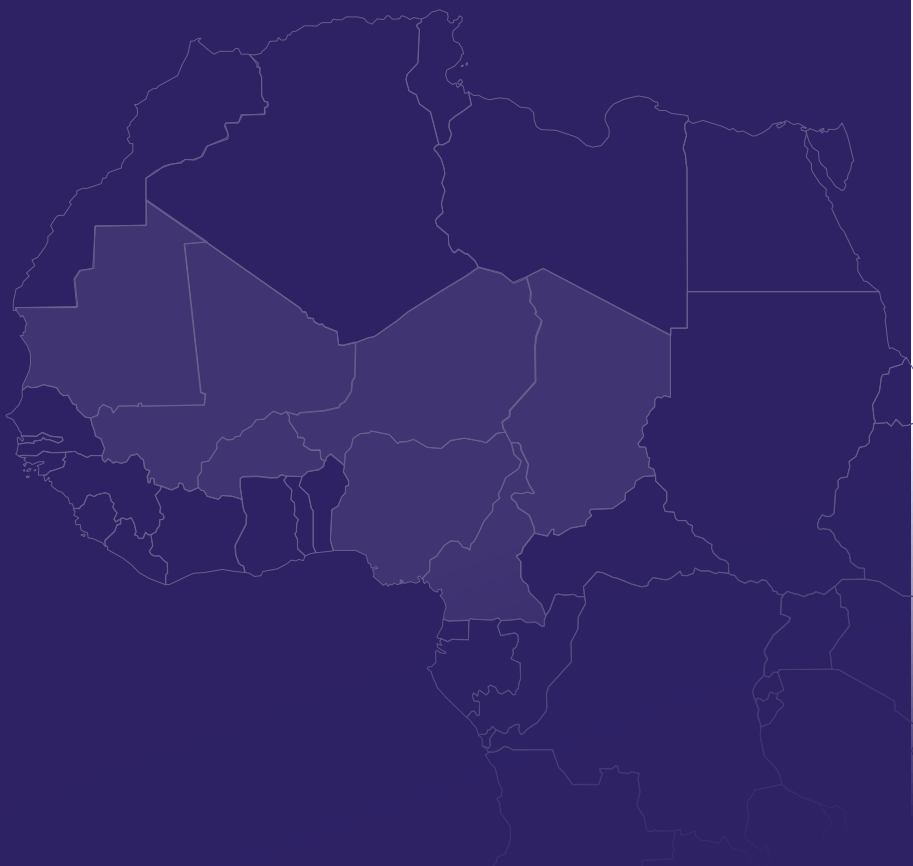
MINKA | AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

Challenges and Issues of digital sovereignty in West Africa in 2024: From the principle of sovereignty to a strategic, adaptive, and resilient digital autonomy

Julien Gavelle

11 août 2024

Public



IRD Institut de Recherche pour le Développement FRANCE | ICE FRANCE | UK International Development Partnership | Progress | Prosperity | ALLIANCE SAHEL

The opinions expressed in this document are those of the authors and do not necessarily reflect the views of AFD, its partners, or funders.

Merci de citer cet ouvrage comme suit :

(11 août 2024), Challenges and issues of digital sovereignty in West Africa in 2024, Plateforme d'Analyse du Suivi et d'Apprentissage au Sahel, Production Pasas. https://pasas-minka.fr

[West Africa]

[Sovereignty, digital, cybersecurity, regional cooperation]

SOMMAIRE

Like the concepts of neoliberalism[1], austerity[2] or resilience[3], digital sovereignty is a multifaceted concept with connected issues, whose fundamental ambiguity is also masked by its overuse in political discourse. Broadly speaking, it lies in the tension between, on the one hand, the pursuit of digital independence and, on the other, the inherent dependencies on global infrastructures and technologies. Moreover, in an increasingly heterogeneous and fragile globalized context, the implementation of genuine strategies of 'shared or complementary autonomy' becomes even more complex. In West Africa, in particular, nationalisms are expressed through repertoires and processes of rupture in favor of a more or less radical defensive sovereignty, while increasingly engaging with exploitative and invasive external partnerships. In response to these dynamics, the technical aspects of digital sovereignty, often neglected in favor of more political approaches, must be addressed. Indeed, the technical value chain of digital sovereignty schematically includes the crucial development of digital infrastructures such as data centers and internet connectivity, as well as local data management, including their collection, secure storage, technical protection, and analysis. Simultaneously, technological innovation plays a central role, supported by initiatives aimed at promoting startups and fostering the development of innovative software. Furthermore, improving digital skills through education and professional training is essential to strengthening this technical infrastructure. On the political level, establishing robust legal and regulatory frameworks for data protection and cybersecurity is a priority. Finally, respecting collective and individual freedoms promotes consideration of these dimensions. Given the breadth of these sub-themes, this policy brief focuses only on certain key elements, particularly the immediate issues, such as the growing cybersecurity challenges affecting West Africa or the issues related to AI: this, in light of national and regional challenges, in a rapidly evolving global geopolitical context, adding significant challenges to the objectives of sustainable digital sovereignty

I. Introduction

West Africa is being transformed by digital technologies. Investments in digital infrastructure (although declining in 2023)[4], the implementation of online public services and the development of the FinTech sector, for example, are contributing to a notable

1 Harvey, David. Spaces of global capitalism: towards a theory of uneven geographical development. Verso, 2006

2 Blyth, Mark. Austerity: the history of a dangerous idea. Oxford university press, 2013

3 Chandler, David. Resilience: the governance of complexity. Routledge, 2014. These authors take a critical approach to economic and political concepts which, though complex, are often simplified and used rhetorically to obscure underlying realities and inequalities.

4 In 2023, African tech startups raised $2.3 billion, marking a 54% drop compared to the previous year. This decrease, the largest ever recorded on the continent, even surpasses the decline seen during the COVID-19 crisis. The number of equity funding rounds also fell by 32%. This trend reflects the global economic slowdown, which is impacting the African ecosystem with a slight delay, similar to what is observed in other emerging markets such as Latin America and Southeast Asia. Despite this decline, funding levels remain nearly double those of pre-2021 figures, highlighting significant growth over the past five years. In Nigeria, concerns over startup governance played a central role in slowing down investments in tech companies, with the notable exception of fintechs, which continue to grow (see note 7). It is also worth noting that 52% of African countries with recorded transactions were Francophone (14 out of 27), compared to 46% the previous year. Additionally, Francophone countries accounted for 68% of equity funding outside the four main markets (South Africa, Nigeria, Kenya, Egypt), a significant increase from 38% in 2022. (Partech, 2024, Africa Tech Venture Capital Report 2023, https://partech-admin.prod.unomena.io/media/documents/2023_Partech-Africa-Tech-VC-Report.pdf)

improvement in administrative efficiency and financial inclusion. However, it continues to face unique challenges in terms of digital sovereignty[5], intensified by socio-economic, political, and technological contexts that further complicate its efforts to catch up on its digital lag. First of all, despite an increase in user accessibility[6], investments in digital infrastructure often remain insufficient, resulting in low internet coverage[7] and significant disparities between urban and rural areas, as well as between countries. These limitations hinder equitable access to digital technologies and slow down innovation and regional emulation dynamics.

Moreover, legal and regulatory frameworks related to cybersecurity and data protection are generally insufficient or poorly implemented, compromising the ability of states to protect their digital infrastructures and data. This situation is exacerbated by a dependency on foreign technologies and infrastructures, which calls into question some of the key objectives of digital sovereignty, potentially jeopardizing the region's overall sovereignty in the long term. Additionally, the region is particularly vulnerable to cyberattacks due to limited cybersecurity capacities and a low level of public, corporate, and even governmental awareness and education on these issues, creating a chain of impacts on growth and efforts to transition toward greater digital governance. The lack of qualified professionals in information technology and cybersecurity is another issue, further exacerbated by educational systems often ill equipped to provide adequate training in digital skills.

Ghana, Senegal, and Nigeria provide relevant examples for addressing these challenges. Ghana stands out for its proactive adoption of blockchain technologies, which aim to modernize and secure its digital infrastructures[8]. Senegal, as the Francophone

5 See Annex 1, Table of the African Union's Objectives for Africa's Digital Transformation (2020-2030).
6 For example, in 2023, Senegal reached an internet penetration rate of 108.31%. In Ghana, this rate was around 70% in January 2024, up from 68% in 2023. In Nigeria, internet penetration stood at 45.5% at the beginning of 2024, with an increase of 2.2 million users between January 2023 and January 2024 compared to the previous year, showing a rapid rise in users. See https://datareportal.com/reports/digital-2024-nigeria ; https://www.statista.com/statistics/1171435/internet-penetration-rate-ghana/ ; https://www.socialnetlink.org/2023/09/30/senegal-le-taux-de-penetration-de-linternet-estime-a-10831/
7 Additionally, while accessibility continues to improve, socio-economic disparities, as well as issues of access, reliability, and particularly cybersecurity, remain significant concerns.
8 Blockchain is a decentralized, secure, and transparent technology for storing and transmitting information. It operates without a central authority, enabling a network of users to share a common database. Each transaction is recorded in a "block" linked to previous ones, forming an unchangeable chain. This decentralization ensures that all transactions are verifiable and nearly impossible to modify without consensus. Blockchain is used for cryptocurrencies like Bitcoin to enable secure financial transactions and for "smart contracts" that automatically execute when specific conditions are met (for a detailed explanation, see Drescher, Daniel, Blockchain basics: a non-technical introduction in 25 Steps, Apress, 2017, pp. 181-193). The transparency and security of blockchain make it a revolutionary technology in various fields, from finance to logistics. For West African governments, the main interest lies in the potential to enhance transparency in administrative processes, reduce corruption, and improve the efficiency of public services, while also strengthening citizens' trust in institutions. For example, see Blockchain Adoption in Africa: Trends in Market Activity and Policy Development, November 2023, background note prepared for the African AI and Blockchain Policy Forum, 15-16 November 2023, OECD, https://www.oecd.org/finance/blockchain/Blockchain-adoption-in-Africa-background-note.pdf. David Mhlanga's article is also an excellent introduction to these issues: The Pivotal Role of Blockchain Technology in Africa's Development: A Comprehensive Review, College of Business and Economics.

leader in the region, is at the forefront with initiatives such as the CFA, a national cryptocurrency[9], illustrating a strategic approach to financial innovation[10] or more recently, the investment in 'neutral' data centers. Finally, Nigeria, the regional hub for fintechs [11], embodies a model of economic and technological dynamism. These countries play a key role in establishing regional standards and legal frameworks to support the sustainable development of digital technologies[12]. Nevertheless, despite their undeniable progress, these countries face significant challenges in areas such as regulation, financing, cybersecurity, and infrastructure, underscoring the need for tailored regional strategies. Furthermore, the regional expansion of these advances is challenged by politically complex neighboring environments, which are increasingly

9 Due to space constraints, this note will not address the issue of cryptocurrencies in West Africa, which nonetheless presents its own challenges in the context of sovereignty. For an insightful overview, see for example: ChainAnalysis, The 2023 Geography of Cryptocurrency Report: Everything You Need to Know About Regional Trends in Crypto Adoption, October 2023, https://www.chainalysis.com/blog/africa-cryptocurrency-adoption/ ; Agence Ecofin, "Afrique subsaharienne : les transactions en cryptomonnaies ont atteint 117,1 milliards entre juillet 2022 et juin 2023," https://www.agenceecofin.com/actualites/2909-112229-afrique-subsaharienne-les-transactions-en-cryptomonnaies-ont-atteint-117-1milliards-entre-juillet-2022-et-juin-2023 ; Henri Louis Vedie, L'émergence des cryptomonnaies en Afrique : réalité ou surévaluation? Research Paper - No. 10/22 - December 2022. It is worth noting that cryptocurrencies contribute to generating positive dynamics around complex development issues within the Fintech sector (Ankun Liu, Orria Goni, and Aiaze Mitha, Cryptocurrency in Africa: Alternative Opportunities for Advancing the Sustainable Development Goals? UNDP, December 2022). At the same time, they pose serious economic challenges, particularly in terms of taxation, as well as significant security risks (ADF, "Islamic State Group Uses Cryptocurrency to Fund Attacks in Africa," Daily News, March 26, 2024).

10 https://african.business/2017/05/economy/senegal-creates-digital-currency-history

11 The term "fintech" is an abbreviation of "financial technology," which refers to the set of technologies and innovations applied to the financial services sector. It includes mobile payment applications, crowdfunding platforms, automated wealth management systems, online banking services, and much more. Fintechs generally aim to improve and automate the delivery and use of financial services. Nigeria has emerged as a regional hub for fintechs in Africa, particularly within the tech ecosystem of Lagos, often referred to as "Silicon Lagoon." This rise is based on various factors, including a young and dynamic population, a high mobile penetration rate, and innovations in financial regulation. See Occasional Paper No 76 - Fintech Evolution and Development in Nigeria, Central Bank of Nigeria, https://www.cbn.gov.ng/Out/2023/RSD/OCCASIONAL%20PAPER%20NO%2076%20-%20Fintech%20Evolution%20and%20Development%20in%20Nigeria.pdf. It is important to highlight that this growing position is also associated with significant investment in ongoing research and analysis, driving major advancements in this strategic digital sector.

12 Togo, according to the company Perf, ranks at the top in terms of mobile connectivity performance in West Africa, followed by Benin and Senegal: Baromètre des connexions Internet mobiles en Afrique de l'Ouest, (May 2024), tests conducted from 01/01/2023 - 31/12/2023, https://media.nperf.com/files/publications/BF/2024-05-02_Barometre_connexions_mobiles_Afrique-de-l-Ouest-2023.pdf. To avoid reporting potentially biased data influenced by underlying commercial or lobbying interests, we have limited the use of references produced by commercial entities without completely excluding them. Particular attention and methodological caution regarding information sources on these topics will need to increase in the coming years, as the issue of digital sovereignty is also becoming a geostrategic concern, including in terms of communication.

vulnerable to foreign influence[13]. China and Russia indeed advocate for a restricted and controlled version of the internet, thereby undermining considerable opportunities for digital development[14] and techno-political autonomy in West African countries. China, for example, offers highly attractive techno-financial solutions as part of the Digital Silk Road (DSR), but their medium- and long-term impacts are concerning. The potential to build a digital model based on transparent cooperation and mutualisation remains essential for the region's sovereignty and overall development. In the short and medium term, as global economies are shaken by increased geopolitical tensions, digital growth driven by innovative regional cooperation dynamics represents one of the key resilience factors, particularly in the face of fluctuations in FDI[15] or potential reductions in ODA following economic recessions in donor countries[16].

II. Risks, impacts, and challenges of digital sovereignty in West Africa

1. Cyber threats: cyber resilience as a key pillar of digital sovereignty

Cyber threats have significant impacts on African economies, with losses estimated at around 10% of the continent's GDP in 2021 and a 70% increase in cyberattacks in 2023[17]. Both the private and public sectors are affected, with attacks targeting critical infrastructures such as energy, transportation, and healthcare systems, as well as government institutions and private businesses. The operational impacts of cyberattacks are also concerning, with service disruptions that can compromise the delivery of medical care, disrupt financial transactions, and undermine consumer confidence in

13 The creation of the Alliance of Sahel States (AES) in September 2023 by Burkina Faso, Mali, and Niger is undoubtedly the most striking example, as it represents a major shift in West African geopolitics. This initiative, driven by successive military coups since 2020, led these countries to withdraw from ECOWAS, ultimately disrupting regional regulatory efforts. Consequently, attempts to harmonize regulations on cybersecurity and data protection may become fragmented, complicating the attraction of necessary investments for the development of digital infrastructure. Alternatively, this strengthens the position of Chinese companies such as Huawei (https://traceinfos.fr/international-le-mali-et-huawei-signent-un-memorandum-dentente-pour-accelerer-le-projet-mali-numerique/). For more on the AES and its challenges, see https://www.orfonline.org/expert-speak/the-alliance-of-sahel-states-a-regional-crisis-in-troubled-west-africa; https://www.africanresearchers.org/decoding-the-alliance-of-sahel-states-west-africas-geopolitical-shift-and-implications/

14 Refer to annex 2 for a sample: Table 2: Sovereignty and digital opportunities in West Africa: challenges and deployment conditions.

15 FDI (foreign direct investment) flows to Africa decreased by 3% in 2023, while the estimated value of international project finance deals on the continent dropped by 50% in 2023, following a 20% decline in 2022. However, certain sectors such as the chemical industry, electronics, and green hydrogen projects demonstrated notable resilience. It is also worth mentioning that intra-regional investments showed strong momentum, including in the digitech sectors. See World Investment Report 2024: Investment Facilitation and Digital Government, UNCTAD, 2024

16 ODA (Official Development Assistance) appears to be making relative progress but may not withstand further shocks, as the impacts and developments of the war in Ukraine were already putting donor countries under pressure by the end of 2022. A major crisis could be on the horizon, according to the OECD. Global Outlook on Financing for Sustainable Development 2023: No sustainability without equity, OECD, 2022.

17 Julie Le Bolzer, "En Afrique, la menace cyber enfle au rythme de la digitalisation », Les Échos, https://www.lesechos.fr/thema/articles/en-afrique-la-menace-cyber-enfle-au-rythme-de-la-digitalisation-2085287

online services. Additionally, cyberattacks hinder socio-economic development by diverting necessary resources and creating an atmosphere of uncertainty and mistrust, which can deter investors and delay essential reforms aimed at strengthening system security and resilience. Finally, on the national security front, cyberattacks pose a direct threat, with the potential to steal sensitive data, disrupt essential operations, and erode public trust in institutions. These threats highlight the critical need to integrate cyber resilience into the goals of building effective digital sovereignty.

2. Types of cyber threats in Ghana, Nigeria and Senegal

When examining cyber threats and the issues of digital sovereignty in West Africa, particularly through the cases of Ghana, Nigeria, and Senegal, several key elements emerge.

On the one hand, the threats are diverse, ranging from traditional attacks such as phishing[18] or spear phishing[19] and ransomware to sophisticated assaults like distributed denial-of-service (DDoS) attacks[20]. On the other hand, the actors involved in these malicious activities vary, ranging from hacktivists to organized cybercriminals, as well as nation-states[21] and cyberterrorists[22].

18 Phishing is a fraudulent technique where cybercriminals send deceptive messages, often via email, to trick recipients into revealing their personal information. These messages appear legitimate but are designed to steal login credentials, financial data, or other sensitive information. See Whitty, M. T., & Doodson, J. (2020). The Real Online Threats to Real People: How Online Interactions Affect Our Offline Lives. Journal of Research in Crime and Delinquency, 57(3), 324-355; Kumaraguru, P., Rhee, Y., & Acquisti, A. (2017). Protecting people from phishing: The design and evaluation of an embedded training email system. International Journal of Human-Computer Studies, 98, 179-201.

19 Spear phishing is a targeted form of phishing where cyber attackers craft deceptive messages specifically aimed at individuals or organizations. Unlike traditional phishing emails, which are sent in bulk, spear phishing uses personalized information to appear legitimate, with the goal of tricking the victim into revealing sensitive information or performing malicious actions (see Halevi, Tzipora & Memon, Nasir & Nov, Oded. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. SSRN Electronic Journal. And more specifically, the socio-psychological mechanisms of spear phishing in Xu, Tianhao & Singh, Kuldeep & Rajivan, Prashanth. (2023). Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. Applied Ergonomics. 108). From 2020 to 2022, a campaign called "DangerousSavanna" targeted major financial institutions in Francophone African countries such as Senegal and Côte d'Ivoire using spear phishing. This campaign involved French-language emails containing malicious attachments to infect the systems of targeted companies. The hackers also used similar domains to impersonate other financial institutions ('DangerousSavanna' hackers targeted financial institutions in Africa for two years, Infosecurity Magazine, 7 September 2022).

20 Distributed Denial of Service (DDoS) attacks are cyberattacks in which multiple computer systems simultaneously target a single system, overwhelming its capacity and rendering it inaccessible to its users. See Hayes, M., & Akam, N. (2017). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA) (pp. 1-8); Dohaji, Mazen. "DDoS Attacks On The Rise In Africa." CIO Africa, 1 September 2023.

21 See section 1.3

22 Cyber terrorism refers to the use of computer technologies and networks, including the internet, to carry out attacks aimed at causing disruptions, damage, or fear for political, ideological, or religious purposes. In 2016, Nigeria's oil and gas sector experienced sophisticated cyberattacks, disrupting oil and gas production and distribution, leading to significant financial losses and compromising sensitive information. See Achunike, Victor U., & Egbuna, Fidelis C. (2020). Synopsis of Cyber-attacks Incidents and Impacts on Oil and Gas Critical Infrastructures: A Nigerian Perspective. International Journal of Advances in Engineering and Management (IJAEM), 2(3), 335-343. In 2019, during the general elections, hackers attempted to manipulate results by infiltrating the systems of the Independent National Electoral Commission (INEC), raising major concerns about electoral integrity. Nigerian financial institutions were also targeted by Distributed Denial of Service (DDoS) attacks and phishing campaigns, disrupting online banking services and threatening the security of financial transactions.

These evolving threats[23] have multidimensional impacts, ranging from direct financial losses to consequences for socio-economic development, political stability, and national security.

Cyberactivism[24] in West Africa has become a powerful tool for social mobilization, exposing corruption, and calling for political reforms. Movements such as #EndSARS in Nigeria demonstrate the ability of online campaigns to attract international attention and galvanize massive support. However, this form of activism raises crucial questions about digital sovereignty and its interpretations concerning public liberties, especially in contexts where states seek to control and regulate the digital space to preserve stability and national security. Governments in the region often view cyberactivism as a threat to their control of information, leading to the adoption of legislative frameworks intended to combat cybercrime but which are increasingly restrictive or overly interpreted, risking a shift towards Russian or Chinese models[25], when these models are not directly implemented[26]. Laws such as the Cybercrimes Act of 2015 in Nigeria and the Electronic Communications Code of 2018 in Senegal, although initially intended to prevent cybercrimes, are often criticized for restricting freedom of expression and targeting online activists or journalists[27], which does not necessarily extinguish all dissent but can, in turn, stimulate its radicalization. For example, the hacker group Mysterious Team made several Senegalese government websites inaccessible in May 2023 through distributed denial-of-service (DDoS) attacks. They claimed responsibility for these attacks on Twitter using the hashtag #FreeSenegal, protesting against political repression. Regardless of the legitimacy of the political motivations behind these attacks, they indeed fall under the penal code and the law on cybercrime[28]. However, cyber activists are increasingly compelled to navigate complex legal frameworks and growing mechanisms of cyber repression, aligned with geopolitical shifts[29].

3. West African digital sovereignty challenged by the digital Silk Road and the techno-political 'RuNet' model

The dynamics of state multipolarisation in Africa have heightened concerns related to digital sovereignty and resilience. The diversification of international partnerships and a redefinition of

23 For example, ransomware, which poses a major threat by regularly targeting critical infrastructure. Its impact is further exacerbated by the emergence of new organizational models among cybercriminals, such as affiliate programs and ransomware-as-a-service platforms. These programs allow for the professionalization and streamlining of operations, thereby increasing the efficiency and impact of attacks. The evolution of cybercriminal tactics also shows a rapid adaptation to both human and technological vulnerabilities. Email phishing remains a major attack vector, exploited by criminals for various cyber offenses, including ransomware and online scams (Kshetri, N. 2019. Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), see also the 2024 Interpol report on cybersecurity in Africa).

24 Cyberactivism includes online petitions, hashtag activism, the exposure of wrongful behaviors (the disclosure of misconduct or secret documents by platforms like WikiLeaks), and hacktivism, which combines hacking and activism for direct action.

25 Polyakova, A., & Meserole, C. (2010). Exporting digital authoritarianism: The Russian and Chinese models. Democracy and Disorder,Brookings, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf; Cipesa. (2019). Digital Rights in Africa: Challenges and Policy Options.

26 « Modification de la loi sur la cybercriminalité au Niger : RSF alerte sur les risques pour les journalistes », Reporter sans Frontière, 19 juin 2024, https://rsf.org/fr/modification-de-la-loi-sur-la-cybercriminalit%C3%A9-au-niger-rsf-alerte-sur-les-risques-pour-les

27 https://www.article19.org/resources/senegal-fake-news-and-disinformation-laws-threaten-freedom-of-expression/; https://www.theafricareport.com/348123/nigeria-cybercrime-law-still-used-to-harass-citizens-despite-amendment/

28 The articles 431-8, 431-9, and 431-10 of the Senegalese penal code, as well as articles 431-1 and 431-3 of Senegal's cybercrime law. (https://adie.sn/sites/default/files/lois/4-cybercrime.pdf) .

29 Buss, H. (2022). Digital Rights Are Human Rights: An Introduction to the State of Affairs and Challenges in Africa. Friedrich-Ebert-Stiftung.

traditional alliances have indeed direct implications for how African states manage their cybersecurity and technological autonomy. For instance, national digital infrastructures, often implemented late, are frequently underdeveloped and vulnerable to sophisticated cyberattacks, making these countries reliant on foreign expertise, which increases their vulnerabilities to external pressures and intrusions, including those that are commercially aggressive[30]. Moreover, in an effort to catch up on digital delays at a lower cost and with no real alternative sources of funding, African states are yielding to Chinese technological and financial solutions presented as 'techno-financial packages,' which are turnkey and remarkably attractive. Chinese providers like Huawei and ZTE[31] for instance, attract not only with their technology but also with the financing solutions they offer, such as the 'EPC+F' model (engineering, procurement, construction + financing)[32]. This Digital Silk Road (DSR) initiative is a component of the Belt and Road Initiative (BRI) in effect since 2013[33] and this digital Silk Road has encountered few obstacles or has successfully adapted to efforts aimed at resisting the conditions of its expansion[34].

The January 2017 incident, where IT specialists from the African Union (AU) detected abnormal activities on their servers, reveals major issues[35]. The discovery that data was being diverted every night to Shanghai over a period of five years highlights the vulnerability of African digital infrastructures to sophisticated cyber threats, especially when these are pre-embedded within

30 There is a significant correlation between Chinese aid to Africa and Chinese exports to the continent, across most sectors. For example, see the healthcare sector. Shajalal, M., Xu, J., Jing, J., King, M., Zhang, J., Wang, P., Bouey, J., & Cheng, F. (2017). China's engagement with development assistance for health in Africa. Global Health Research and Policy, 2.

31 ZTE (Zhongxing Telecommunication Equipment Corporation) is a Chinese company founded in 1985, specializing in telecommunications equipment and network solutions. It plays a key role in the global deployment of 4G and 5G infrastructure. However, ZTE has faced criticism for its close ties to the Chinese government and its business practices, which led to sanctions and restrictions by several countries, including the United States, due to concerns over national security and potential espionage. The restrictions were lifted under the Trump administration,https://www.nytimes.com/2018/07/13/business/zte-ban-trump.html.

32. https://theconversation.com/africa-needs-china-for-its-digital-development-but-at-what-price-222905

33 Belt The Belt and Road Initiative (BRI), launched by China in 2013, aims to enhance connectivity between Asia, Africa, and Europe. It is divided into two main components: the Silk Road Economic Belt, focused on transport and energy infrastructure, and the Maritime Silk Road, centered on ports and logistics. While the BRI boosts economic development and infrastructure, it raises concerns related to debt and China's growing political influence, among other issues. For different perspectives on the BRI and the DSR, see for example Philippe Copinschi et al., "La BRI et la stratégie de sécurisation des approvisionnements énergétiques chinois en Afrique," Observatoire de la sécurité des flux et des matières énergétiques, 2019; and for more on the DSR see for example Tugendhat, Henry; Voo, Julia (2021): China's Digital Silk Road in Africa and the Future of Internet Governance, Policy Brief, No. 60/2021, China Africa Research Initiative (CARI), School of Advanced International Studies (SAIS), Johns Hopkins University, Washington, DC.

34 Valerio Fabbri, "The Great Leap of China's Tech Companies in Africa," Geopolitica Info, 2023. https://www.geopolitica.info/great-leap-china-tech-africa/.

35 https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html ; https://www.bbc.co.uk/news/resources/idt-sh/Huawei, A subsequent event was also reported by Raphael Satter, "Exclusive-Suspected Chinese hackers stole camera footage from African Union - memo," Reuters, December 16, 2020. For a very insightful approach to the dynamics of Chinese national and global surveillance, see the conference by Sheena Chestnut Greitens, Surveillance with Chinese Characteristics: The Development and Global Adoption of Chinese Policing Technology,
(draft available at https://ncgg.princeton.edu/IR%20Colloquium/GreitensSept2019.pdf).
The author describes the processes of repression associated with digital usage in China and highlights that political analyses have largely underestimated the extent of the use of Chinese surveillance technologies and policing strategies across the world, as well as the speed with which they have been globally adopted.

the framework of 'EPC+F' schemes. The African Union building had, in fact, been entirely donated and financed by the China State Construction Engineering Corporation (CSCEC), a major player in the BRI[36] and digitized by Huawei. This data breach, which occurred from January 2012 to January 2017, underscores the ability of foreign actors to exploit the weaknesses of African digital systems, in this case by implementing vulnerabilities or backdoors[37], thereby compromising directly the sovereignty of states and regional institutions. It is also important to consider that the financing scheme also creates a debt with multiple variables[38], leading to a dispersion of the intended effects in terms of governance and fundamental rights linked to the conditionality of ODA [39], if not a strict exportation of repressive approaches and population

36 Chinese companies investing in Africa maintain high profit margins, even in politically complex environments. Studies of these companies reveal profit margins as high as 20%, encouraging businesses to expand their operations on the continent. Huawei has not hesitated to maximize profits in politically unstable environments, particularly benefiting from the lack of western competition, which is often reluctant to engage under such conditions in Africa. See the insightful chapter by Bulelani Jili, "The Spread of Chinese Surveillance Tools in Africa: A Focus on Ethiopia and Kenya," in Africa–Europe Cooperation and Digital Transformation, 1st edition, Routledge, 2022, as well as the analyses of William C. Kirby, Billy Chan, and John P. McHugh, "Huawei: A Global Tech Giant in the Crossfire of a Digital Cold War," Harvard Business School Case 320-089, March 2020. Overall, China's economic transition influences its relations with Africa, introducing significant changes in trade, investment, fiscal stabilization, the internationalization of the renminbi (RMB), and cultural and educational exchanges. While China remains a major trade partner for Africa, the trade balance remains highly asymmetrical. Chinese public investments in infrastructure have decreased, in favor of a more industrialization-focused approach through foreign direct investments (FDI). Furthermore, China seeks to increase the use of the RMB in Africa while adjusting its investment strategies and fiscal stabilization based on national and continental developments. At the continental level, its prevailing strategy is to reschedule debt rather than reduce it (a recent innovation from Beijing). This financial restructuring allows China to strengthen its influence and access to key sectors such as digital technologies, as well as through control over strategic supply chains in emerging technologies. See Gbadamosi, Olumide. "How Is China's Economic Transition Affecting Its Relations With Africa?" Carnegie Endowment for International Peace, May 5, 2024, https://carnegieendowment.org/research/2024/05/how-is-chinas-economic-transition-affecting-its-relations-with-africa?lang=en&center=russia-eurasia, and Song-Pehamberger, David. "Controlling Tomorrow: China's Dominance Over Future Strategic Supply Chains," The Diplomat, August 21, 2024.

37 A backdoor is a secret method used to access a system, network, or application by bypassing standard security mechanisms. While it is often installed for malicious purposes, allowing unauthorized access to systems, developers can also deliberately implement it for legitimate purposes, such as maintenance, troubleshooting, or testing. However, these privileged access points pose significant risks if proper controls are not in place, as malicious actors can exploit them. In the context of digital infrastructure deployed in West Africa, controlling and managing backdoors, including those potentially integrated by developers, is crucial to ensure security. This generally involves establishing continuous source code audits, verifying software components, and regularly monitoring systems—essential processes for detecting any unauthorized backdoor (with increasing support from AI). This is a major technical challenge in protecting the region's critical infrastructure from cyber threats, particularly those originating from foreign countries with uncertain intentions. There are, however, other implementation techniques and methods available to detect them. See, for example, the well-known intrusive forms here: https://www.mandiant.com/resources/reports/apt41-double-dragon-dual-espionage-and-cyber-crime-operation.

38 Arnold, S. (2024). Africa's roads to digital development: paving the way for Chinese structural power in the ICT sector? Review of International Political Economy, 1–25 (https://www.tandfonline.com/doi/epdf/10.1080/09692290.2023.2297363?needAccess=true).

39 This is undoubtedly one of the frequently mentioned but still insufficiently described causes of the democratic breakdown processes in West African countries, particularly in the Sahel region. See Li, X. Does Conditionality Still Work? China's Development Assistance and Democracy in Africa. Chin. Polit. Sci. Rev. 2, 201–220 (2017).

control[40]. As for the desirable and promised technical transfers (TT) resulting from this massive alignment with Chinese digital technologies, they are very limited and conditioned by the broader political and commercial strategy of the BRI[41].

More recently, Russia also launched a techno-political offensive in Africa, particularly targeting countries such as Libya (Cyrenaica region), Madagascar, the Central African Republic (CAR), South Sudan, Mali, Burkina Faso, and Niger. While the declaration from the second Russia-Africa summit in 2023 appears to align with key principles of digital sovereignty, it is more outwardly oriented towards part of the global digital ecosystem[42]. However, for the past decade, Russia has influenced these regions through propaganda and disinformation via its online media outlets[43] and the Wagner group[44] or African Initiative, new influence platform backed by Moscow, taking over from the private group and its African Back Office following its dismantling[45]. It has thus significantly accelerated the destabilization of West African countries while reinforcing the ideological framework of these new military regimes, which are rooted in a decolonial tropism. Experts explain that Russia is now seeking to unite its African allies around digital independence from the West[46]. Contrary to the July 2023 declarations, Russia is promoting an independent

40 Erin Baggott Carter et Brett L. Carter, "Exporting the Tools of Dictatorship: The Politics of China's Technology Transfers to Africa," Working Paper 122, dec 2022, AIDDATA https://docs.aiddata.org/ad4/pdfs/WPS122_Exporting_the_Tools_of_Dictatorship__The_Politics_of_Chinas_Technology_Transfers_to_Africa.pdf

41 Although ZTE and Huawei have launched localization initiatives promising meaningful connections, they have offered no substantial learning opportunities to improve the technological skills of local entities. What initially appears to be development efforts facilitating technology transfers turns out to be mechanisms for disseminating Chinese infrastructure, hardware, software, processes, and standards, thereby creating distinct and dependent digital systems? See the well-documented article by Tin Hinane El-Kadi, Learning along the Digital Silk Road? Technology transfer, power, and Chinese ICT corporations in North Africa, The Information Society: An International Journal, vol. 40, no. 2, 2024.

42 The declaration from the 2023 Russia-Africa Summit highlights a mutual commitment to strengthening bilateral relations between Russia and African countries, focusing on key areas such as trade, security, culture, and education. The text emphasizes respect for the sovereignty of African states and non-interference, while promoting economic partnerships aimed at developing infrastructure, industrialization, and agriculture in Africa. Security cooperation is also a major focus, with particular attention given to combating terrorism and enhancing military capabilities. Additionally, the declaration underscores the importance of cultural and educational exchanges, as well as the need to reform international institutions for better representation of African countries. While the declaration initially expresses support for open multilateralism, it ultimately positions Russia and Africa as key partner-actors in an evolving multipolar world. https://summitafrica.ru/fr/about-summit/declaration-2023/

43 Audinet, Maxime, et Kévin Limonier. « Le dispositif d'influence informationnelle de la Russie en Afrique subsaharienne francophone : un écosystème flexible et composite », Questions de communication, vol. 41, no. 1, 2022, pp. 129-148.

44 Olech, A. (2024). The Wagner Group in Africa. The sham battle of Russian mercenaries against terrorism. Terrorism – Studies, Analyses, Prevention, no. 5. The recent disbandment of Wagner has allowed Moscow to regain control of the group's disinformation and influence apparatus in Africa.

45 https://disinfo.africa/african-initiative-russias-new-mouthpiece-in-africa-65aa76fcc255

46 https://incyber.org/article/offensive-russe-sur-la-souverainete-numerique-en-afrique/

digital ecosystem similar to the "Runet"[47], allowing for strict political control[48] and the defense of conservative values. Combined with anti-imperialist geopolitical storytelling (against the global West) and drawing from the pan-Africanist repertoire, Moscow also offers sophisticated digital censorship approaches to African countries, potentially deploying tools used within Russian territory for this purpose[49]. Thus, Russia and China, despite a multisector convergence that

47 Runet refers to Russia's sovereign digital ecosystem, composed of websites, online services, and technological infrastructures controlled and regulated by the Russian government. Created to protect the country against foreign cyber threats and ensure strict control of information, Runet includes local alternatives to Western platforms, such as the Yandex search engine and the VKontakte social network. This system allows Russia to monitor and filter online content, thereby reinforcing its political control. Runet illustrates an approach to digital sovereignty where a state aims to reduce its dependence on foreign technologies while maintaining strict surveillance of its cyberspace. See Kevin Limonier, « Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », EchoGéo [56 | 2021. However, it is important to note that this drive for hegemonic control does not come without national resistance, starting with Russia itself. Between 2014 and 2016, the 'Yandex.News' service was at the center of an intense political conflict between the Yandex company and the Russian government. Yandex's algorithm, designed to select and publish online news, was accused by Russian authorities of political bias, particularly in relation to the Ukrainian crisis. In 2016, Roskomnadzor, the Russian communications watchdog, eventually took control of the Yandex.News algorithm. This conflict ultimately led to the split between Yandex NV, the Netherlands-based parent company, and its operations in Russia. In 2024, a consortium of Russian investors completed the acquisition of Yandex's Russian operations, marking the largest withdrawal transaction of a Western company from Russia since the beginning of the war in Ukraine. See « La scission de Yandex est presque achevée : les traders russes finalisent l'échange d'actions », 10 juillet 2024, Reuters (https://www.zonebourse.com/cours/action/YANDEX-N-V-8037501/actualite/La-scission-de-Yandex-est-presque-achevee-les-traders-russes-finalisent-l-echange-d-actions-47352959/).
This emblematic case sparked a heated debate about content aggregation algorithms and the need for them to be transparent and independent to support democracy, as well as the independence of states that use such algorithms. Similar debates in Europe concerning Google led to the Digital Services Act. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0825. The Digital Services Act (DSA) imposes strict obligations on digital platforms regarding algorithm transparency, including the disclosure of criteria used for content ranking and personalization, in order to protect users' rights and enhance platform accountability.
48 The 2016 Russian legislation (Yarovaya Law) requires telecommunications operators to store user data and provide this information to security services. It illustrates the state's desire to control information flows by establishing an effective hybrid governance model through the involvement of power-aligned partners, with the state remaining the central decision-maker (once resistance has been overcome, see note 47). Oligarchs and other economic elites, being integrated into this control structure through ownership stakes, have a direct interest in maintaining the political status quo, thus consolidating the existing regime. See also the excellent report by Alena Epifanova, Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet. DGAP Analysis No. 2, German Council on Foreign Relations (DGAP), 2020.
49 Roskomnadzor and the Russian Federal Security Service (FSB) have "backdoors" to national internet platforms, in accordance with the Yarovaya Law (note 48). TSPU (an acronym for "threat control devices" in Russian) are notable for their efficiency. These optimized DPI (Deep Packet Inspection) boxes—devices that allow for detailed examination of the content of data packets transmitted over the internet—are installed at network nodes of internet service providers, enabling the filtering of internet traffic, including VPNs (Virtual Private Networks, which mask IP addresses and encrypt browsing data). While there are legitimate and important advantages to using DPI for a country's public infrastructure—such as the ability to detect threats and attacks hidden within data packet content, prevent data leaks, and identify where data is being sent—their misuse for political control and censorship is becoming increasingly prominent, including in Africa. See Christian Fuchs, "Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance," Journal of Communication, vol. 63, no. 6, 2013, pp. 1328-1359; What is Deep Packet Inspection (DPI)?, PagerDuty (www.pagerduty.com/resources/learn/what-is-deep-packet-inspection/); Russia's digital authority pushes DPI tools and IP geolocation to surveil Internet traffic, Meduza, May 2023 (www.meduza.io/en/news/2023/05/24/russia-s-digital-authority-pushes-dpi-tools-and-ip-geolocation-to-surveil-internet-traffic); A new anti-democratic tool: The Deep Packet Inspection technique, Democracy in Africa.org, 2023 (www.democracyinafrica.org/a-new-anti-democratic-tool-the-deep-packet-inspection-technique/). See also Rio, 2024, infra note 46.

is more nuanced than it appears, are simultaneously intensifying the digital rights divide between two trends. On one hand, there is a collegial approach (i.e., multi-stakeholder, which does not strictly imply consensus or homogeneity[50]) to the legal regulation of the internet, adopted by European and American countries. On the other hand, there is an approach based on the concept of digital sovereignty, championed by Russia, Iran, and China, which is supported by some countries in Asia and Africa. This latter approach manifests in its most pronounced nationalist version through hyper-centralized state control, while fostering segmentation in terms of global cooperation, primarily at the regional level[51]. This strategy also aims to create an ideological convergence with authoritarian and neo-conservative regimes in Africa, strengthening Russian and Chinese influence by exploiting both societal and technical internal challenges. Socio-political divisions, such as those fueled by the failure of governance led by the ruling classes and the democratic model, as well as security instability and technological, particularly digital, delays, are presented as consequences of an outward orientation toward the West, which is portrayed as hindering technological development on the continent.

Alternatively, the promotion of centralized digital sovereignty models rapidly deployed, helps bolster the political control and capital of current regimes, but it fragments and slows down the possibilities for more dynamic and secure regional cooperation.

4. Artificial intelligence: current limitations and transformative opportunities for West African states

Artificial intelligence (AI) represents a transformative opportunity for Africa, offering significant potential to address persistent challenges and accelerate socio-economic development. The fields of application are vast, ranging from improving healthcare systems through AI-assisted medical diagnosis to optimizing agricultural yields with precise, data-driven forecasts[52]. Thus, the integration of AI can act as a facilitator in achieving 134 of the Sustainable Development Goals (79%)[53], primarily through technological advancements that could help overcome various current limitations[54]. However, realizing these benefits requires addressing several chal-

50 This introductory outline must indeed be nuanced, as despite common values, Europe and the United States diverge on several aspects of internet governance in practice. Europe, with the GDPR, is strict on data protection, while the U.S. has a more fragmented approach. Regarding net neutrality, the EU maintains a firm stance, unlike the United States, where policies have fluctuated, notably with the repeal of regulations in 2017 by the FCC. Europe is also proactive in regulating large digital platforms with laws such as the DSA (Digital Services Act) and DMA (Digital Markets Act), whereas the U.S. is still debating appropriate regulations. Lastly, Europe imposes stricter restrictions on hate speech, in contrast to the U.S., which largely protects freedom of speech under the First Amendment. For the key differences between Europe and the United States on these issues, see Christopher T. Marsden, Net Neutrality: Towards a Co-regulatory Solution (Bloomsbury Publishing, 2017); Ari Ezra Walman, Privacy as Trust: Information Privacy for an Information Age (Cambridge University Press, 2018).

51 According to the independent Russian organization Roskomsvoboda, the divergence in approaches and understandings of how internet regulation and human rights are exercised could lead to an unprecedented crisis in nature and scale in the coming years (see the report here).

52 Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University. (2023). See also The State of AI in Africa Report 2023, https://cipit.strathmore.edu/wp-content/uploads/2023/05/The-State-of-AI-in-Africa-Report-2023-min.pdf.

53 As a reminder, the Sustainable Development Goals (SDGs) are a set of 17 global goals adopted by United Nations member states in 2015 as part of the 2030 Agenda for Sustainable Development. They aim to eradicate poverty, protect the planet, and ensure prosperity for all by 2030, addressing global challenges such as poverty, inequality, climate change, environmental degradation, peace, and justice. These goals are broken down into 169 specific targets and measured by 232 indicators. See https://www.un.org/sustainabledevelopment/fr/objectifs-de-developpement-durable/.

54 Vinuesa, R., Azizpour, H., Leite, I., et al. (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. Nature Communications, 11, 233

lenges. One of the main obstacles is the disparity in access to the data and resources necessary for the effective adoption of AI. Many African countries suffer from a digital divide that hinders the collection, management, and local use of data[55]. Moreover, the infrastructure remains insufficient, and the development of algorithms and applications tailored to the specific needs of the continent is still limited.

On the other hand, the gap is widening with cybercriminals who are increasingly using AI to, for example, analyze the effectiveness of their attacks in real time. They adjust their strategies to maximize disruptions while minimizing the risk of detection, particularly through DDoS attacks[56]. These AI-assisted attacks can mimic normal traffic, bypassing traditional defense mechanisms. However, AI can precisely enhance cybersecurity by proactively detecting threats through predictive and behavioral analysis, and by responding quickly to attacks through automation. It continuously improves its defenses by learning from new attacks, making it particularly effective against cybercriminals who also use AI.

However, current policies and regulatory frameworks are often not suited to support the development and adoption of AI in Africa. There is an urgent need for policies that encourage innovation while protecting users' rights and mitigating risks related to ethics and data privacy. This requires close collaboration between governments, research institutions, businesses, start-ups, and civil society to ensure that AI is developed and used responsibly, taking into account both national and transnational needs and issues. Democratic setbacks, including the weakening of civil societies, for example, do not favor such collaborative processes of development and appropriation[57]. The export of intrusive and clandestine AI technologies to African countries where human rights are often violated risks reinforcing existing systems of repression and introducing new forms of control. Meanwhile, AI significantly amplifies disinformation and its destabilizing effects on states[58].

The Conference on the State of AI in Africa (COSAA) on March 15, 2023, highlighted these challenges and called for coordinated action to overcome them. The implementation of effective policies and regulations, along with investment in data infrastructure and AI skills, are essential to maximize the benefits of AI while minimizing its potential risks.[59]. However, the issue

55 See section IV.1 on the issue of neutral data centers.
56 Cybercrime and cyber espionage converge in their use of AI. For example, APT41, supported by the Chinese state and also known as "Double Dragon" (reflecting operations of both cyber espionage and profit-motivated cyberattacks), uses spear phishing techniques to compromise target networks. Once infiltrated, the group deploys sophisticated malware and web shells (malicious scripts installed on a web server for remote access) to maintain access and exfiltrate sensitive data. AI is used to automate the analysis of large amounts of data, identify anomalies, bypass security systems, and customize phishing attacks. See SentinelOne, "APT41 Infiltrates Multiple Sectors in a Worldwide Cyberattack," iZOOlogic, 2023; Agrawal, Jatin, Samarjeet Singh Kalra, and Himanshu Gidwani. "AI in Cyber Security." International Journal of Communication and Information Technology, 2023. Also, see the latest actions of APT41 here: https://izoologic.com/region/china/apt41-infiltrates-multiple-sectors-in-a-worldwide-cyberattack/. See also note 38.
57 Gyimah-Boadi, E. (2021, décembre). Le recul démocratique en Afrique de l'Ouest : Caractéristiques, causes et solutions. Fondation Kofi Annan, https://www.kofiannanfoundation.org/app/uploads/2022/02/Le-recul-democratique-en-afrique-de-louest_caracteristiques-causes-et-solutions_Boadi_Decembre2021.pdf See also the report on digital freedoms in Francophone Africa AFD, 2023, https://www.afd.fr/fr/ressources/libertes-numeriques-pays-francophones-afrique.
58 Pauwels, Eleonore. The Anatomy of Information Disorders in Africa: Geostrategic Positioning & Multipolar Competition Over Converging Technologies. Konrad-Adenauer-Stiftung, 2020
59 Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University. (2023). The State of AI in Africa Report 2023, https://cipit.strathmore.edu/wp-content/uploads/2023/05/The-State-of-AI-in-Africa-Report-2023-min.pdf.

of open-source artificial intelligence, which is nonetheless an important vector for the digital empowerment of West African states, remains relatively under-addressed.

III. Impacts and issues

1. Economic and security impacts

Cyberattacks in West African countries such as Nigeria, Ghana, and Senegal have had significant financial, operational, and security repercussions. In Nigeria, losses due to fraudulent operations in the banking sector reached 193.5 billion naira (544 million USD) in 2021, increasing to 273 billion naira (762 million USD) in 2022, and nearly 300 billion naira (833 million USD) in 2023[60]. SIM swap fraud[61], used to hijack mobile money accounts, cost telecommunications consumers over 20 billion naira (55 million USD) in 2022, according to a report from the Nigerian Communications Commission (NCC).CesThese financial losses highlight the vulnerability of mobile money platforms and the need for strengthened security measures. The operational impacts in Nigeria are also concerning. Attacks on energy infrastructure have disrupted the operations of oil and gas companies, which are crucial to the national economy[62]. Moreover, cyberattacks on critical infrastructure demonstrate that cyber threats can be used as a tool for political and social destabilization.

The rapid growth of internet penetration in Ghana, with an increase from 2.31 million to 24.06 million users between 2012 and 2024, when the internet penetration rate reached 69.8%[63], has facilitated the development of numerous online services. However, this growth also exposes the country to cyberattacks that threaten to undermine trust in these services, thereby delaying economic progress. For instance, direct financial losses due to cyber fraud reached $4.32 million (49.5 million GH₵) in 2023[64]. DDoS attacks disrupted financial transactions on online payment platforms, compromising customer trust. Senegal, for example, has faced severe consequences from cyberattacks. Attacks on government institutions and critical infrastructure resulted in the leakage of sensitive documents and disrupted essential operations. Furthermore, DDoS attacks temporarily paralyzed the online services of government websites, demonstrating the vulnerability of existing systems. These cyberattacks on ministries have jeopardized national security and diplomacy, underscoring the urgent need to strengthen cybersecurity measures to protect infrastructure and users[65].

2. Impacts on development

In Nigeria, the financial inclusion initiative launched by the Central Bank of Nigeria in 2012 aimed to integrate 80% of the adult population into the formal financial system by 202066. However, credit card fraud and online account hacking quickly undermined public trust in

60 Nigerian communications commission annual report 2023, (https://www.ncc.gov.ng/documents/885-annual-report-2022/file); Banks lose N18bn to fraudsters in 2023 -NIBSS, 29 avril 2024 (https://punchng.com/banks-lose-n18bn-to-fraudsters-in-2023-nibss/)
61 Ekeh, G.E., Afolabi, Y.I., Uche-Nwachi, E.O., Ekeh, L.K., & Eze-Udu, E. (2022). Awareness of BVN, SIM Swap and Clone Frauds: Methods and Controls. Science World Journal, 17(2). Department of Computer Science, Alex Ekwueme Federal University, Ndufu Alike-Ikwo, Ebonyi, Nigeria.
62 https://punchng.com/hackers-attack-39-nigerias-oil-sector-computers-report/;
63 Digital 2023: ghana; https://datareportal.com/reports/digital-2023-ghana; https://www.askyazi.com/useful-data-sources-for-africa/ghanas-digital-statistics-2023#:~:text=There%20were%2023.05%20million%20internet,percent%20of%20the%20total%20population.
64 Bank of Ghana Annual Report 2022](https://www.bog.gov.gh)
65 Osiris, Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal. 2024. "La souveraineté numérique, une question de sécurité nationale." 26 février 2024. http://www.osiris.sn/La-souverainete-numerique-une.html.
66 National financial inclusion strategy, 2012, https://www.afi-global.org/wp-content/uploads/publications/mfg-en-paper-national-financial-inclusion-strategy-oct-2012.pdf

digital banking services, resulting in losses of 3 billion naira (8.3 million USD) in 201867. In Senegal, the healthcare system modernisation project, supported by the World Bank, was severely disrupted by ransomware attacks in 2016. These attacks paralyzed hospital IT systems, resulting in financial losses and interrupting healthcare services. Similarly, in Ghana, the agricultural development project aimed at improving the productivity of smallholder farmers was compromised by cyberattacks in 2018. Cybercriminals targeted mobile payment platforms, stealing funds and eroding farmers' trust in digital technologies. These incidents demonstrate that cybercrime leads to direct financial losses, a decrease in public trust, and delays in project implementation, thereby compromising development goals.

3. Impacts on social and political stability

Cybercrimes in West Africa, particularly in Nigeria, Senegal, and Ghana, have devastating effects on social and political stability. In Nigeria, while cybercrime has resulted in revenue losses for businesses, it has also led to increased unemployment and exacerbated social tensions. The exodus of investors, as seen after the 2017 attack on a major Nigerian bank, slowed economic growth and compromised development projects, sparking protests against the government[68]. In Senegal, cyberattacks such as the May 26, 2023 DDoS attack on government websites disrupted the local economy and had a significant impact on investor confidence[69]. Similarly, in Ghana, during the 2016 elections, cyberattacks on the Electoral Commission[70] raised doubts about the integrity of the electoral process, contributing to post-election violence. These are not isolated events, and they are increasingly alarming experts[71]. Beyond the immediate economic losses, cybercrimes threaten citizens' trust in their institutions, undermine development efforts, and can destabilize already fragile societies.

IV. Responses and challenges of digital sovereignty in West Africa

1. Initiatives in strengthening digital sovereignty

The efforts of African countries such as Senegal, Ghana, and Nigeria to strengthen their digital sovereignty reflect a growing awareness of the importance of controlling and protecting infrastructure and data in an ever-evolving digital environment. These initiatives include the creation of secure data centers, the development of regulatory frameworks, and adherence to international conventions such as the Malabo Convention on Cybersecurity and Personal Data Protection72.

67National financial inclusion strategy revised, 2018, https://www.cbn.gov.ng/out/2019/ccd/national%20financial%20inclusion%20strategy.pdf
68https://www.vanguardngr.com/2017/07/hackers-target-nigerian-banks/;https://www.premiumtimesng.com/news/top-news/228166-north-korean-hackers-attack-banks-in-nigeria-17-other-countries-kaspersky.html?tztc=1
69 https://incyber.org/en/article/a-cyberattack-hits-government-sites-in-senegal/
70 BBC News. 2016. "Ghana Election Commission Website Hit by Cyber Attack." 8th December 2016. https://www.bbc.co.uk/news/world-africa-38247987.
71 Sarah O'Connor, Fergus Hanson, Emilia Currey, Tracy Beattie. Cyber-enabled Foreign Interference in Elections and Referendums. ASPI, Policy Brief Report No. 41/2020.
72 Union Africaine. (2014). Convention de l'Union Africaine sur la Cyber Sécurité et la Protection des Données à Caractère Personnel. Récupéré de https://www.afapdp.org/wp-content/uploads/2018/06/CONV-UA-CYBER-PDP-2014.pdf.

Senegal has established a data center in Diamniadio, supported by the State IT Agency (ADIE)73. Meanwhile, Ghana has created the Ghana Cyber Security Authority (CSA) and invested in improving its telecommunications infrastructure to ensure resilient connectivity. Similarly, Nigeria has taken significant steps with the Nigerian Communications Commission (NCC) and the National Information Technology Development Agency (NITDA), focusing on regulating the telecommunications sector and promoting network security in 2022. An essential component of these efforts also appears to be the rise of "neutral" data centers74. These approaches enable the control and protection of local data, stimulate local technological innovation, and ensure greater strategic autonomy in the digital domain. Between $5 and $6 billion are expected to be invested in such data centers across Africa over the next 3 to 5 years (driven by companies like Equinix, Vantage, and Digital Realty). Simultaneously, an increasing number of African governments are adopting policies, laws, and regulations on data localization and privacy protection.

Countries like Nigeria75, Ghana76, South Africa77 and Kenya78 have implemented data protection and privacy laws, while others are considering similar measures to strengthen their legal frameworks on cybersecurity79. The adoption of the Malabo Convention on Cybersecurity and Personal Data Protection is an example of African states' commitment to developing national laws that align with the standards and principles outlined in the text. However, with only 15 out of 55 countries having ratified the convention, questions remain about the reasons behind this situation, highlighting the need to promote awareness and engagement on cybersecurity issues in Africa.

73 ADIE (Agence de l'Informatique de l'État). (s.d.). Datacenter de Diamniadio, lieu d'impulsion de la transformation digitale du Sénégal. https://www.adie.sn/actualites/le-datacenter-de-diamniadio-lieu-d%E2%80%99impulsion-de-la-transformation-digitale-du-s%C3%A9n%C3%A9gal.

74 A "neutral" data center is a facility independent of any specific telecommunications or cloud provider. It gives customers the freedom to choose their operators and service providers, ensuring high flexibility and interconnectivity. These data centers host critical infrastructure independently, which enhances the security and resilience of digital systems while ensuring that data is stored within the users' country. This contributes to local technological innovation and the digital sovereignty of nations.

75 National Information Technology Development Agency (NITDA). (2019). Nigeria Data Protection Regulation (NDPR). Abuja : NITDA, https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf ainsi que le cadre d'application deux ans plus tard https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf

76 Government of Ghana. (2012). Data Protection Act, 2012 (Act 843). Accra: Government of Ghana, https://www.dataprotection.org.gh/data-protection/data-protection-acts-2012#:~:text=OVERVIEW%20OF%20DATA%20PROTECTION%20ACT%2C%202012%20(ACT%20843)&text=It%20recognises%20a%20person's%20right,accordance%20with%20the%20individual's%20rights

77 South African Government. (2013). Protection of Personal Information Act (POPIA), 2013. Pretoria: South African Government, https://www.justice.gov.za/legislation/acts/2013-004.pdf

78 Kenya Law. (2019). Data Protection Act, 2019. Nairobi: Kenya Law, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

79 See in this regard the successive reports from 2019 to 2021 by the United Nations Conference on Trade and Development (UNCTAD), Value Creation and Capture – Implications for Developing Countries, Geneva: UNCTAD, https://unctad.org/topic/ecommerce-and-digital-economy/digital-economy-report. The acceleration of legal data protection measures in some countries over a few years has been spurred by the COVID-19 crisis, during which digital alternatives played a central role in maintaining minimal economic activities.

Finally, Nigeria's strategic roadmap and action plan for data protection, launched by the Nigeria Data Protection Commission (NDPC) in December 202380, reflect the efforts made to strengthen data security and increase user trust in the digital environment.

2. Challenges and perspectives

The challenges encountered in the quest for digital sovereignty in West Africa are numerous and complex. Firstly, the technological dependence on partnerships with foreign companies raises concerns about the security and autonomy of digital infrastructure. These partnerships can increase vulnerability to the business practices and political influence of foreign companies, thereby jeopardizing data confidentiality and the protection of national interests.

The dominance of global tech giants such as the GAFAM (Google, Apple, Facebook, Amazon, Microsoft) and Chinese web giants exacerbates this dependence and threatens Africa's digital sovereignty.

These companies often control the most widely used digital platforms and services on the continent, placing them in a significant position of power to influence policies and regulations in the digital domain81.

Another major challenge is the lack of qualified human resources in cybersecurity and digital infrastructure management. The shortage of trained personnel in these areas makes it difficult to effectively protect networks and data against growing threats, such as cyberattacks and

80 National Data Protection Commission. (2023). Strategic Roadmap and Action Plan (SRAP), https://ndpc.gov.ng/Srap.pdf.

81 The GAFAM (Google, Apple, Facebook, Amazon, Microsoft) dominate African digital markets, limiting the growth of local businesses and posing challenges related to data sovereignty and privacy protection, while also influencing local socio-cultural dynamics. Their interdependent relationship with governments, which support them geopolitically and economically, complicates efforts for strict regulation and dismantling, as these companies are deeply embedded in both national and international economies (IRIS - Les GAFAM et l'État : quelles évolutions du champ du pouvoir, https://www.iris-france.org/167483-les-gafam-et-letat-quelles-evolutions-du-champ-du-pouvoir/). Despite substantial institutional and financial resources, European regulations struggle to curb this dominance. Joëlle Toledano highlights the fragmentation of European regulators and the lack of adequate control resources, which allows GAFAM to bypass new regulations (DMA and DSA). She proposes consolidating regulatory missions into three European hubs for better coordination (Le Monde - Sans régulation efficace, la politique de souveraineté numérique européenne échouera selon l'auteur, https://www.lemonde.fr/idees/article/2023/09/01/sans-regulation-efficace-la-politique-de-souverainete-numerique-europeenne-echouera_6187365_3232.html). The lessons learned from Europe are instructive for Africa, which must develop clear and coordinated regulations to manage GAFAM's influence and protect its digital sovereignty. Investing in local capabilities and ensuring that regulations are precise and binding is crucial to prevent global tech companies from circumventing imposed obligations. In Senegal, the recent approach focuses initially on enforcing a strict fiscal constraint. Since July 1, 2024, GAFAM and other foreign providers must collect and remit VAT on digital services provided in Senegal, marking a step forward in regulating digital transactions, despite concerns over foreign suppliers' compliance (Digital Business Africa - Les GAFAM vont collecter et reverser au fisc sénégalais la TVA sur les activités numériques dès le 1er juillet 2024, https://www.digitalbusiness.africa/les-gafam-et-cie-vont-collecter-et-reverser-au-fisc-senegalais-la-tva-sur-les-activites-numeriques-des-le-1er-juillet-2024/). However, there are fears that these companies may pass the costs onto consumers or reduce their investments in the region. Overly strict regulations could discourage foreign investments and slow down local innovation, which flourishes in a balance between generating fiscal revenue and promoting an environment conducive to economic and technological growth (Social Net Link - Taxer les GAFAM, un pari risqué pour les pays africains, https://www.socialnetlink.org/2024/07/03/taxer-les-gafam-un-pari-risque-pour-les-pays-africains/).

privacy violations. It is crucial to invest in specialized education and training programs to build a skilled workforce capable of addressing these issues.

Cybercrime is the most urgent and rapidly growing challenge in West Africa, particularly in Nigeria. Cyberattacks, such as ransomware, online fraud, and data theft, have become frequent and can cause significant harm to individuals, businesses, and governments. Tackling these threats requires effective coordination between national and international actors, along with strong security measures and proactive prevention strategies.

Funding ambitious digital projects is, overall, a major hurdle. Initiatives aimed at reinforcing digital sovereignty require considerable investments in infrastructure, technology, and human capacities. However, access to adequate funding sources remains limited, which hampers the implementation of strategic projects in this domain.

However, digital investment facilitation measures have a significant economic impact on the business environment and are crucial for attracting foreign direct investment (FDI) in a context of marked fragility82. The OECD suggests that reducing administrative complexity in developing countries to the median level could increase the stock of FDI by 20%83. Due to their relatively low cost, these digital measures particularly benefit smaller economies and those with limited resources to attract investment. They improve governance and institutions, especially in countries with weaknesses in these areas, and promote economic diversification by further supporting FDI in the manufacturing and service sectors. SMEs, often hindered by administrative barriers, benefit significantly from digital investment facilitation, making the process more accessible and attractive84. Similarly, concrete commitments, such as those related to the Addis Tax Initiative (ATI), have demonstrated an acceleration in the digitization of public services. For instance, in Ghana, an online platform has been established for the publication of tax information and financial reports of public administrations, as well as for online payment services 85. This initiative has improved the perception of transparency and enabled citizens to track the use of public funds86.

However, the digitalization of public services, while an essential strategy, does not address all challenges.

West African countries need to adopt a more comprehensive approach to preserve their digital integrity, rapidly acquire essential technical skills, manage regional financial variations such as the increasingly responsive expectations of FDI, while promoting balanced and mutually beneficial partnerships with international actors. Regardless of the combinations considered to

---

82 As underlined previously (see note 10)

83 Coopération pour le développement 2023 : quel système d'aide pour demain ?, OCDE, 2023, https://www.oecd.org/fr/publications/cooperation-pour-le-developpement-2023_83b806cb-fr.html

84 Iyaji Danjuma, "Insurgency, Political Risk, and Foreign Direct Investment Inflows in Nigeria: A Sectorial Analysis," CBN Journal of Applied Statistics, vol. 12, no. 2 (December 2021), Adewale Samuel Hassan, "Does Country Risk Influence Foreign Direct Investment Inflows? Evidence from Nigeria and South Africa," Journal of Contemporary Management, vol. 20, no. 1, 2023, https://www.bloomberg.com/news/articles/2024-02-17/nigeria-s-capital-inflows-fell-26-in-2023-amid-economic-turmoil.

85 https://gra.gov.gh/file-and-pay-taxes/e-commerce/

86 However, this point highlights two important dimensions: on one hand, the challenges related to fiscal balancing and sequencing, with Ghana seeking to exploit opportunities offered by digital technologies and Fintech to expand its tax base by taxing digital services, while risking discouraging potential users. On the other hand, a positive perception of digitization processes does not necessarily translate into effective public engagement with them. Ofosu-Ampong K thus emphasizes the crucial importance of properly structuring the fiscal components as well as facilitating the use of the implemented system (Ofosu-Ampong, K. (2024). New policies, new behaviors: How digital taxation shapes mobile money use in Ghana. Engineering Reports, https://onlinelibrary.wiley.com/doi/epdf/10.1002/eng2.12860).

achieve these goals, they seem to require the integration of a few key strategic elements. Three can be identified.

The first element is rooted in a logic of empowerment through financial diversification. It involves strengthening an approach that focuses on alternative financing mechanisms and continuous diversification, including at the local (national or regional) level. This helps foster more resilient dynamics in the face of the economic impacts of global crises and aggressive political-commercial penetrations that exploit circumstantial or structural vulnerabilities.

The second strategic component revolves around increased collaboration, particularly at the regional level, and resource sharing. The principle is to maximize available resources and promote efficiency by fostering enhanced cooperation between the public and private sectors, as well as pooling regional infrastructures. This, in turn, boosts financial diversification.

Finally, the third element focuses efforts on technological innovation and the enhancement of local skills. This approach aims to strengthen technological autonomy through open source, technology transfer, and the promotion of local expertise, particularly in the field of cybersecurity. Several proposals can be made in this direction.

Autonomy through financial diversification

Financial diversification is essential to empower investments in West Africa. Whether through official development assistance (ODA) or foreign direct investment (FDI), both of which are under pressure, the trend seems to lean toward projects that offer both economic and social returns. For instance, the financial inclusion brought by fintechs has managed to attract venture capital and private equity funds, reducing their reliance on traditional FDI. This ongoing and more intensive diversification strategy, at the local or regional level, aims to create resilient economic dynamics in the face of global crises and aggressive political-commercial penetrations exploiting local vulnerabilities.

The creation of digital sovereign wealth funds could also play a crucial role, fueled by revenues from natural resources or other public assets, and aimed at financing digital infrastructure, tech startups, and research projects in digital innovation. For example, mining revenues could be at least partially reinvested in digital initiatives, ensuring a strategic use of national resources for technological development87. The adoption of cryptocurrencies and digital assets, such as the eCFA in Senegal, could offer alternatives to traditional financial systems, thereby facilitating access to capital for startups and small businesses. Furthermore, blockchain technology can be leveraged to create collaborative savings and credit systems, strengthening financial inclusion and stimulating local entrepreneurship. Cryptocurrencies can also serve as a store of value

87 To convince governments and political classes, it is crucial to demonstrate the short-term economic benefits and the robustness of dividend redistribution in the ICT sector. This can be achieved by highlighting efficiency and transparency gains in public services, providing evidence and case studies, and emphasizing the positive social impacts. Additionally, proposing concrete policies and strategies to support ICT development can enhance the credibility and appeal of investments in this sector. Rwanda is a pertinent illustration in this regard. The country implemented a national ICT development strategy (Vision 2020) and successfully attracted significant foreign investments in the ICT sector, creating jobs and stimulating local innovation. Kigali has become a regional tech hub, hosting major tech events and startup incubators. On the structural dividend front, besides improving public administration through the digitization of government services (which has led to greater transparency and efficiency), the tax base has expanded significantly due to the economic growth driven by ICTs. See, for example, IFC report shows digitalization holds immense promise, economic potential for african businesses of all sizes, May 2024 (https://pressroom.ifc.org/all/pages/PressDetail.aspx?ID=28167). The full report is accessible through the IFC portal: https://openknowledge.worldbank.org/server/api/core/bitstreams/e6f2cc1b-ad12-460f-9f17-ff95b69cb378/content.
.

for sovereign wealth funds, diversifying assets and reducing dependence on foreign currencies88. The development of crowdfunding platforms could also provide a supplementary solution for raising funds through popular contributions, thus supporting innovative projects with high social impact. Simultaneously, the creation of local venture capital funds focused on African tech startups would help channel investments toward promising projects. These initiatives could also attract foreign investors looking for growth opportunities on the continent. However, support in capital management for startups is essential, particularly in terms of entrepreneurial governance, to avoid some of the failures observed in Nigeria and Ghana.

Resilience through increased collaboration and resource sharing

Regional collaboration and resource sharing would maximize the deployment, efficiency, and use of infrastructures. Public-private partnerships (PPP), akin to what could be called Digital Investment Groups (Groupements d'Investissement Numérique or GIN), would enable the pooling of private and public capital to fund data centers and telecommunications infrastructures. The GINs, inspired by Agricultural Land Groups (Groupements Fonciers Agricoles or GFA), would be civil organizations where each share is proportional to the capital contributed, ensuring a fair distribution of revenues. The state would play a limited but strategic role, ensuring the sovereign management of data. This approach would theoretically encourage intermediate investments, diversifying funding sources and reducing risks while promoting cooperation between the public and private sectors and, eventually, the pooling of regional infrastructures89. Regional cooperation, building on these national PPP dynamics, could indeed play a key role in creating a favorable environment for investment. As mentioned earlier, by accelerating the reduction of administrative complexity through digitalization and harmonizing regulations at the regional level, West African countries could attract more Foreign Direct Investment (FDI) and facilitate access to capital.

Beyond this, the creation of special economic zones (SEZs)90 dedicated to digital technologies could also stimulate investment by offering fiscal incentives. Finally, the sharing of infrastructure,

88 Interview with a crypto-economy expert based in Africa, 18/07/24.

89 At first glance, there are similar, more global and ambitious approaches, such as the Smart Africa Alliance in support of ICT, backed by the African Union's Agenda 2063 (https://au.int/en/agenda2063/overview). However, these essential initiatives face challenges in mobilizing financial resources, partly due to a lack of a more dynamic diversification strategy. This sustains a marked dependence on international funding, which is itself increasingly fragile.

90 A Special Economic Zone (SEZ) is a designated region within a country where economic, fiscal, and commercial rules differ from those applied in the rest of the territory. These zones are designed to attract foreign investment, boost economic development, and promote specific industrial sectors. They offer various advantages, such as tax exemptions, more flexible regulations, easier access to infrastructure, and sometimes a distinct legal framework. The main goal of SEZs is to stimulate economic growth, create jobs, and foster technological development in strategic areas. According to UNCTAD, their performance in Africa often falls short of set objectives due to institutional challenges, harmful competitive dynamics, and weak strategic frameworks. However, the implementation of highly specialized SEZs (dedicated to digital industries) that are well-defined strategically, territorialized at the national or cross-border level, or even "despatialized" (which could stimulate the harmonization of regulations across different national stakeholders in the digital sector) could represent a more operational model. In particular, this could be supported by leveraging the African Continental Free Trade Area (AfCFTA). See United Nations Conference on Trade and Development (UNCTAD). Guide sur les zones économiques spéciales en Afrique : vers une diversification économique à travers le continent. UNCTAD/DIAE/IA/2021/3, 2021. Furthermore, given the challenges posed by Chinese models of economic cooperation zones implemented in Africa, which have created long-term political and economic issues, well-conceived SEZs focused on the digital sector could represent an alternative. For relevant warnings, see Bräutigam D, Xiaoyang T. African Shenzhen: China's special economic zones in Africa. The Journal of Modern African Studies. 2011;49(1):27-54.

such as data centers and telecommunications networks, through regional initiatives could reduce costs and improve access to advanced technologies. The approach of mesh networks (meshing91) could enhance connectivity, particularly in underserved areas, promoting broader access to technology and fostering regional economic integration. For example, a collaboration between Senegal, Côte d'Ivoire, and Ghana could pool telecommunications infrastructure to improve coverage and reduce costs. Technical incubators could also be integrated into these regional structures to foster skill development across the different countries. Regarding neutral data centers, a regional approach would allow for the creation of shared data centers among several countries, ensuring technological independence and enhanced data security while reducing infrastructure costs through resource sharing92.

Technological innovation, technology transfer, and local capacity building

Focusing efforts on technological innovation and strengthening local skills, particularly in terms of cybersecurity, is crucial for technological autonomy. The promotion of open-source technology and technology transfer are key elements in consolidating the achievement of digital sovereignty objectives. For example, training programs in open-source software development, hackathons93, and technology startup incubators would encourage local innovation.

---

91 Meshing, or mesh networking, is an innovative approach to building decentralized and resilient communication infrastructures. In West Africa, this method offers a viable and cost-effective solution to improve connectivity and strengthen digital sovereignty. It provides broad coverage, increased resilience through redundancy and self-repair, and cost savings via shared infrastructure. For an educational presentation on the principles of meshing, see https://www.intechopen.com/chapters/66938. For examples of local meshing projects in Africa, see initiatives such as https://tunapanda.org/ or https://www.internetsociety.org/issues/community-networks/success-stories/ (Uganda, Morocco, South Africa). These projects are small-scale but highly effective. If scalable, they can be developed in peripheral and border areas where connectivity is still limited or nonexistent. Also, refer to the following sources for additional insights: Sanchez, Alain, Joe Robertson, and Courtney Radke. "Cybersecurity Roundtable: Fortinet CISOs Discuss Mesh Architectures." FORTINET, February 22, 2022, https://www.fortinet.com/blog/industry-trends/cybersecurity-mesh-architectures-fortinet-cisos-discuss-the-importance/; "Internet access in Africa - Are mesh networks the future?" BBC News, https://www.bbc.com/news/av/world-africa-47723967.

92 Au Given the current national sensitivities regarding sovereignty issues, it is necessary to clarify the possible operational framework for these regionally shared systems. First, data encryption, both in transit and at rest, protects sensitive information. Partitioning and logical isolation ensure the separation of data from each country, even if they are physically located in the same place. Restricted and controlled access is essential, using role-based policies and multi-factor authentication to limit unauthorized access. In this regard, European initiatives such as Gaia-X can inspire shared governance systems. Strict service level agreements would define the responsibilities of each party regarding security. Continuous monitoring and regular audits would also help detect and quickly respond to potential security breaches. The use of advanced security technologies, such as firewalls, intrusion detection and prevention systems (IDPS), and security information and event management (SIEM) solutions, would further strengthen protection. Compliance with international standards, such as GDPR (see above), would ensure legal compliance. Finally, continuity and recovery plans would guarantee the availability of data in case of an incident. For details on the Gaia X project, see GAIA-X: le projet européen entre dans une nouvelle phase (https://www.entreprises.gouv.fr/files/files/01-nouveau-portail/secteurs-d-activite/Numerique/bmwi_gaia-x_papier_umbrella-master_frz-web.pdf) and Gaia-X: un projet européen trop ambitieux? (https://afee-cedece.eu/gaia-x-un-projet-europeen-trop-ambitieux/).

93 A hackathon is an intensive event where participants collaborate to create innovative solutions on a specific topic, often within 24 to 48 hours. They develop functional prototypes or concepts using their diverse skills, such as programming, design, or engineering. At the end, the projects are presented and evaluated, sometimes offering opportunities for funding or partnerships.

More specifically, initiatives such as specialized technical training, coding workshops, and certification programs in open-source software development could be established to train a new generation of local developers and technicians. Additionally, tech startup incubators and hackathons could be organised to stimulate local innovation and identify solutions tailored to the specific challenges of the region and each partner country in the resource-sharing framework. Furthermore, reinforcing technology and skill transfers should be a priority in foreign partnerships (further promoting the implementation of previous proposals). In this regard, it would be both urgent and essential to integrate technology transfer clauses into all international agreements. These clauses should include obligations for foreign partners to share technologies, train local workers, and support educational institutions ideally centred on these technologies. Strategies could include creating training and certification programs in partnership with local and international institutions, promoting collaborative research and development, and implementing monitoring and evaluation mechanisms to ensure compliance with these commitments. Such initiatives would help train specialists in key fields and develop technologies tailored to local needs, while avoiding technological dependency mechanisms that could limit the region's autonomous and sustainable development.

Conclusion

Geopolitical upheavals, such as the rise of multipolarity and growing tensions between major powers increasingly playing out on the continental level, underscore the need for West African states to find a balance between digital independence and global interconnectivity. Failing to do so risks leading to digital stagnation or recession and exposing their national integrity to long-term penetration by foreign techno-political and economic strategies.

Rather than moving toward a closed form of digital sovereignty, which could isolate nations and hinder technological progress in the medium to long term, it is crucial to promote a strategic, adaptive, and resilient autonomy to address these challenges. This should be simultaneously rooted in a logic of resource sharing. The path forward involves developing regional processes of technological cooperation and integration that are tailored to diverse national contexts and informed by ongoing monitoring of technical, political, economic, and sociological factors. More specifically, by developing strong regional collaboration networks, West African states can protect their digital infrastructures from growing cyber threats while promoting harmonized and sustainable technological development.

The promotion of open source, the pooling of regional infrastructures, the informed renegotiation of sustainable technology transfer conditions, and technological and financial innovation supported by enhanced digital education are key pillars of a dynamic and inclusive digital sovereignty. Furthermore, it is essential to more broadly involve national and regional economic actors (with a much more open and transparent capital structure) to foster the emergence of an expanded "eco-digital" class that can support and stimulate national and regional policies geared towards resilient and profitable solutions. This will require a commitment to generating innovative and responsive crosscutting solutions while addressing the specific challenges of each country.

Thus, West Africa's digital sovereignty in the coming years must be envisioned as a delicate and unique balance between national autonomy, regional interdependence, and global connectivity. A proactive and informed digital diplomacy, focused on cooperation and contextual adaptation, would be essential in transforming current challenges into sustainable opportunities, thereby ensuring a strong and resilient role for West Africa in the global digital economy.

Bibliographie

Awoleye, O. M. (2021). Reconfiguring Data Infrastructure Ecosystem in Africa: A Primer Toward Digital Sovereignty. ArXiv

Bagayoko, C., Bediang, G., Anne, A., Niang, M., Traoré, A., & Geissbuhler, A. (2017). Digital health and the need to develop centers of expertise in sub-Saharan Africa: two examples in Mali and Cameroon. Medecine et sante tropicales, 27(4), 348-353.

Baromètre des connexions Internet mobiles en Afrique de l'Ouest. (2024). nPerf

Camara, O. M. (2019). Cellular Telephone Internet, and Electronic Communication in Senegal, Mali, and Gambia. Thèse de doctorat. Fort Hays State University.

ChainAnalysis. (2023). The 2023 Geography of Cryptocurrency Report

Degila, J., Tognisse, I. S., Honfoga, A.-C., Houetohossou, S. C. A., Sodedji, F. A. K., Avakoudjo, H. G. G., Tahi, S. P. G., & Assogbadjo, A. E. (2023). A Survey on Digital Agriculture in Five West African Countries. Agriculture, 13, 1067.

Drescher, Daniel. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps Apress.

El-Kadi, Tin Hinane. (2024). Learning along the Digital Silk Road? Technology transfer, power, and Chinese ICT corporations in North Africa. The Information Society: An International Journal, 40(2).

Epifanova, Alena. (2020). Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet DGAP Analysis No. 2, German Council on Foreign Relations (DGAP)

Evans, O. (2019). Digital politics: internet and democracy in Africa. Journal of Economic Studies

Gehl Sampath, P., & Tregenna, F. (Eds.) (2022). Digital Sovereignty: African Perspectives Johannesburg: DSI/NRF South African Research Chair in Industrial Development.

Interpol (2024). Rapport Interpol de 2024 sur l'évaluation des cybermenaces en Afrique: Perspectives du Bureau pour les opérations de lutte contre la cybercriminalité en Afrique - 3ème édition

Les annales des Mines (2023). La souveraineté numérique : dix ans de débats, et après ?. N° 23 - Septembre 2023.

Mascellino, A. (2021). DangerousSavanna' Hackers Targeted Financial Institutions in Africa For Two Years. Infosecurity Magazine

OECD. (2023). Blockchain Adoption in Africa: Trends in Market Activity and Policy Development

Partech. (2023). Africa Tech Venture Capital Report 2023

Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4).

Statista. (2024) Internet penetration rate in Ghana. Statista

Ude, N., Ude, K., Ugbor, U., Igwe, C., & Ogu, E. (2021). E-Governance and Economic Development in Sub-Saharan Africa: A Case of Nigeria. International Journal of Development Strategies in Humanities, Management and Social Sciences

UNCTAD. (2024). World Investment Report 2024: Investment Facilitation and Digital Government Geneva: United Nations Conference on Trade and Development (UNCTAD).

ANNEXE 1:

Table 1: Main Objectives of the African Union for Africa's Digital Transformation (2020-2030)[94]

Objective	Description
Universal and affordable internet access	Ensure that all African citizens have secure and affordable internet access (6 MB/s at 1/100 of a U.S. dollar per MB) and promote locally manufactured smart devices (priced at a maximum of 100 U.S. dollars).
Investments in infrastructure	Encourage investments to bridge the digital infrastructure gap, ensuring accessible, secure, and affordable broadband for everyone, transcending demographic and geographic differences.
Strengthening intra-African trade	Establish and improve digital networks and services to enhance intra-African trade, investment, and capital flows, and to promote the continent's socio-economic integration.
Policies and regulations	Implement policies and regulations to accelerate digital transformation at national, regional, and continental levels, ensuring coherence in current and future digital strategies.
Cybersecurity and data protection	Raise awareness of cybersecurity and data protection issues, promote open standards and interoperability, and support the enforcement of the African Union Convention on Cybersecurity and Data Protection.
Development of digital skills	Develop inclusive digital skills and human capacity in digital sciences and education, with online training programs aiming to provide basic skills to 100 million Africans per year by 2021, and 300 million per year by 2025.
Telemedicine and tele-education	Support telemedicine and tele-education programs to transform service delivery and make the digital revolution the foundation of African society.
Digital legal identity	Ensure that 99.9% of Africa's population has a legal digital identity by 2030.

94 Table created from the African Union report. (2020). Digital Transformation Strategy for Africa 2020-2030

ANNEXE 2

Table 2: Digital Sovereignty and Opportunities in West Africa: Challenges and Deployment Conditions

This table aims to present an analysis of digital technological opportunities that have already been examined or implemented in various sectors, linking them with the associated sector challenges and the standard conditions required for such opportunities to be effective. This analysis is based on bibliographical references and informal exchanges with experts.

Sector	Opportunities	Challenges	Standard conditions
Governance	Mobile payment and mobile marketing platforms	Improve transparency of government transactions and facilitate access to public services	CYBERSECURITY (strong cryptography, two-factor authentication) INFRASTRUCTURE (high bandwidth, secure servers) LOCAL DEVELOPMENT CAPACITY (mobile application development, system maintenance) LEGISLATIVE FRAMEWORK (data protection regulations, user privacy laws)
	Security and health alerts via mobile (SMS apps)	Strengthen public safety by providing real-time information and encouraging citizen participation	CYBERSECURITY (communication encryption) INFRASTRUCTURE (reliable mobile networks, alert broadcasting systems) LOCAL DEVELOPMENT CAPACITY (skills in alert system development) LEGISLATIVE FRAMEWORK (emergency management laws, sensitive data protection)
	B2B analytics data FinTech	Use analytics to improve public policy and strategic decision making	CYBERSECURITY (protection against cyberattacks, access control) INFRASTRUCTURE (secure data centers, data analysis platforms) LOCAL DEVELOPMENT CAPACITY (expertise in data analysis, FinTech solution development) LEGISLATIVE FRAMEWORK (regulations on financial data usage, financial information protection laws)
Justice	Blockchain for value chain and traceability	Increase transparency and reliability of public registries, reducing corruption and fraud	CYBERSECURITY (robust consensus algorithms, data immutability) INFRASTRUCTURE (decentralized networks, blockchain platforms) LOCAL DEVELOPMENT CAPACITY (blockchain technology knowledge, smart contract development) LEGISLATIVE FRAMEWORK (blockchain adoption regulations, public register management laws)
Agricultural development	Electronic pest and disease monitoring systems	Improve agricultural productivity and reduce crop losses	CYBERSECURITY (securing monitoring data) INFRASTRUCTURE (sensor networks, real-time data analysis platforms) LOCAL DEVELOPMENT CAPACITY (expertise in detection technology, agricultural data analysis) LEGISLATIVE FRAMEWORK (agricultural data collection regulations)
	Precision agriculture and automated agricultural machinery	Optimize agricultural yields by using advanced technologies for crop management	CYBERSECURITY (securing automated systems) INFRASTRUCTURE (IoT networks, advanced agricultural machinery) LOCAL DEVELOPMENT CAPACITY (training in machinery usage and maintenance) LEGISLATIVE FRAMEWORK (agricultural technology regulations)
	Agricultural robotics and agricultural equipment tracking	Increase efficiency and traceability of agricultural operations	CYBERSECURITY (robotic equipment security protocols) INFRASTRUCTURE (communication networks, equipment management systems) LOCAL DEVELOPMENT CAPACITY (robotics expertise, equipment management) LEGISLATIVE FRAMEWORK (agricultural equipment regulations)
	Digital agricultural marketplace platforms in cloud mode	Facilitate farmers' access to markets and real-time information	CYBERSECURITY (securing cloud transactions and data) INFRASTRUCTURE (secure data centers, cloud platforms) LOCAL DEVELOPMENT CAPACITY (e-commerce expertise, cloud solutions) LEGISLATIVE FRAMEWORK (digital transaction regulations)
	Agricultural price forecasting	Help farmers make informed decisions based on market trends	CYBERSECURITY (securing forecast data) INFRASTRUCTURE (data analysis platforms, market data access) LOCAL DEVELOPMENT CAPACITY (market analysis expertise, economic modeling) LEGISLATIVE FRAMEWORK (market data usage regulations)
	Weather-indexed insurance / remote sensing	Provide insurance solutions based on indices to	CYBERSECURITY (protecting weather and risk data) INFRASTRUCTURE (remote sensing systems, climate analysis plat-

		protect farmers from climate risks	forms) LOCAL DEVELOPMENT CAPACITY (remote sensing expertise, climate analysis) LEGISLATIVE FRAMEWORK (agricultural insurance regulations)
	Real-time soil testing	Improve soil management and fertility of agricultural lands	CYBERSECURITY (securing testing devices and data) INFRASTRUCTURE (sensor networks, data analysis platforms) LOCAL DEVELOPMENT CAPACITY (agronomy expertise, testing technologies) LEGISLATIVE FRAMEWORK (soil data collection regulations)
	Open-source agricultural engineering transfer with tutorials	Facilitate access to advanced agricultural technologies for small farmers	CYBERSECURITY (protecting open-source sharing platforms) INFRASTRUCTURE (open-source platforms, internet access) LOCAL DEVELOPMENT CAPACITY (training in agricultural engineering) LEGISLATIVE FRAMEWORK (open-source regulations, knowledge sharing)
	Simplified price surveys for granular tracking of local markets	Provide accurate and up-to-date information on agricultural product prices, helping farmers obtain fair prices	CYBERSECURITY (securing market data) INFRASTRUCTURE (data collection platforms, communication networks) LOCAL DEVELOPMENT CAPACITY (market data collection expertise) LEGISLATIVE FRAMEWORK (price transparency regulations)
	Electronic mechanization	Improve efficiency of agricultural operations through automation	CYBERSECURITY (securing electronic systems) INFRASTRUCTURE (communication networks, automated equipment) LOCAL DEVELOPMENT CAPACITY (training in equipment maintenance and usage) LEGISLATIVE FRAMEWORK (agricultural technology regulations)
	Partial traceability and supply chain tracking	Ensure traceability of agricultural products from farm to consumer, improving transparency and quality	CYBERSECURITY (securing traceability data) INFRASTRUCTURE (supply chain management platforms, communication networks) LOCAL DEVELOPMENT CAPACITY (supply chain management expertise, traceability technologies) LEGISLATIVE FRAMEWORK (product traceability regulations)
Civil Society and Citizen Participation	Offline advisory services using audio and video tools (tablets)	Improve access to information and services for remote and marginalized communities	CYBERSECURITY (protecting advisory devices and communications) INFRASTRUCTURE (internet access, audio and video devices) LOCAL DEVELOPMENT CAPACITY (training in device usage and maintenance) LEGISLATIVE FRAMEWORK (data protection regulations, access rights)
Health	Health alerts via mobile (SMS apps)	Provide real-time information on health emergencies and improve crisis management	CYBERSECURITY (health data encryption) INFRASTRUCTURE (reliable mobile networks, health alert systems) LOCAL DEVELOPMENT CAPACITY (health alert system development expertise) LEGISLATIVE FRAMEWORK (emergency management laws, health data protection)
Fintech and B2B Analytics	Data analytics for agriculture	Use data to optimize agricultural practices and improve yields	CYBERSECURITY (protecting agricultural data) INFRASTRUCTURE (data analysis platforms, communication networks) LOCAL DEVELOPMENT CAPACITY (data analysis expertise, agricultural technology) LEGISLATIVE FRAMEWORK (agricultural data usage regulations)
Agriculture Observatory	Agriculture Observatory	Track agricultural trends and developments for informed decision making	CYBERSECURITY (protecting monitoring systems) INFRASTRUCTURE (secure data centers, observation platforms) LOCAL DEVELOPMENT CAPACITY (agricultural monitoring expertise, data analysis) LEGISLATIVE FRAMEWORK (data collection regulations)
Education	Online learning platforms	Facilitate access to education for all, especially in rural and remote areas	CYBERSECURITY (protecting learner data) INFRASTRUCTURE (internet access, online learning platforms) LOCAL DEVELOPMENT CAPACITY (educational content development, technology usage expertise) LEGISLATIVE FRAMEWORK (digital education regulations)
	School performance tracking	Enable accurate and continuous assessment of students' academic performance	CYBERSECURITY (protecting school data) INFRASTRUCTURE (school tracking platforms, internet access) LOCAL DEVELOPMENT CAPACITY (data management expertise, performance analysis) LEGISLATIVE FRAMEWORK (educational data collection regulations)
Environment	Biodiversity monitoring	Protect and monitor biodiversity for sustainable management of natural resources	CYBERSECURITY (biodiversity data protection) INFRASTRUCTURE (sensor networks, environmental data platforms) LOCAL DEVELOPMENT CAPACITY (ecology expertise, environmental data analysis) LEGISLATIVE FRAMEWORK (biodiversity protection regulations)
Employment	Online recruitment platforms	Facilitate job search and connection between employers and job seekers	CYBERSECURITY (protecting user data) INFRASTRUCTURE (online recruitment platforms, internet access) LOCAL DEVELOPMENT CAPACITY (platform management expertise,

			algorithmic matching) LEGISLATIVE FRAMEWORK (data protection laws, labor laws)
	Vocational training	Offer online courses and vocational training resources accessible via mobile apps	CYBERSECURITY (learner data protection) INFRASTRUCTURE (online training platforms, internet access) LOCAL DEVELOPMENT CAPACITY (training content development expertise) LEGISLATIVE FRAMEWORK (digital education regulations)
Infrastructure	Infrastructure project monitoring	Use mobile applications to monitor infrastructure projects, collect real-time data, and ensure transparency in public fund management	CYBERSECURITY (securing monitoring systems) INFRASTRUCTURE (communication networks, project management platforms) LOCAL DEVELOPMENT CAPACITY (infrastructure project management expertise, real-time data analysis) LEGISLATIVE FRAMEWORK (transparency regulations, public fund management)
	Preventive maintenance	Implement preventive maintenance systems based on connected sensors to extend infrastructure life and reduce repair costs	CYBERSECURITY (securing maintenance systems) INFRASTRUCTURE (sensor networks, maintenance management platforms) LOCAL DEVELOPMENT CAPACITY (sensor technology expertise, preventive maintenance management) LEGISLATIVE FRAMEWORK (public infrastructure maintenance regulations)
Tourism	Digital tourist guides	Develop mobile applications to provide interactive tourist guides, information on historical and cultural sites, and facilitate online reservations	CYBERSECURITY (protecting tourist data) INFRASTRUCTURE (tourist information platforms, communication networks) LOCAL DEVELOPMENT CAPACITY (tourism app development, cultural content management) LEGISLATIVE FRAMEWORK (data protection laws, tourism regulations)
	Ecotourism promotion	Use online platforms to promote ecotourism destinations, raise awareness of nature conservation, and encourage sustainable tourism	CYBERSECURITY (protecting ecotourism data) INFRASTRUCTURE (tourism promotion platforms, communication networks) LOCAL DEVELOPMENT CAPACITY (ecotourism content management, online promotion) LEGISLATIVE FRAMEWORK (data protection laws, tourism regulations)
Inclusive Finance	Digital microfinance	Facilitate access to financial services for unbanked populations through digital microfinance platforms enabling secure mobile transactions	CYBERSECURITY (securing financial transactions) INFRASTRUCTURE (microfinance platforms, internet access) LOCAL DEVELOPMENT CAPACITY (microfinance management expertise, financial technologies) LEGISLATIVE FRAMEWORK (financial services regulations, financial data protection)
	Collaborative savings and credit	Implement blockchain-based collaborative savings and credit systems to encourage financial inclusion and stimulate local entrepreneurship	CYBERSECURITY (securing blockchain transactions and data) INFRASTRUCTURE (blockchain platforms, internet access) LOCAL DEVELOPMENT CAPACITY (blockchain expertise, financial services management) LEGISLATIVE FRAMEWORK (blockchain regulations, collaborative financial services)
Culture and Art	Promotion of local arts	Use online platforms to promote local artists, facilitate the sale of artworks, and encourage appreciation of African culture	CYBERSECURITY (protecting artist and user data) INFRASTRUCTURE (art promotion platforms, internet access) LOCAL DEVELOPMENT CAPACITY (art platform management, digital marketing expertise) LEGISLATIVE FRAMEWORK (data protection laws, copyright regulations)
	Digital archiving of cultural heritage	Develop digital archives to preserve African cultural heritage, including music, literature, crafts, and oral traditions	CYBERSECURITY (securing digital archives) INFRASTRUCTURE (archiving platforms, internet access) LOCAL DEVELOPMENT CAPACITY (archiving expertise, cultural preservation) LEGISLATIVE FRAMEWORK (data protection laws, copyright regulations)
Technological Innovation	Technological startup incubators	Create technological startup incubators to support local innovation, encourage entrepreneurship, and stimulate the digital economy	CYBERSECURITY (protecting data and innovations) INFRASTRUCTURE (coworking spaces, high-speed internet access) LOCAL DEVELOPMENT CAPACITY (incubator management, startup development expertise) LEGISLATIVE FRAMEWORK (innovation regulations, entrepreneurship support)
	Hackathons and technological competitions	Organize coding events and technological competitions to stimulate creativity, encourage collaboration, and solve local challenges through technology	CYBERSECURITY (protecting participant data) INFRASTRUCTURE (event spaces, high-speed internet access) LOCAL DEVELOPMENT CAPACITY (event organization expertise, tech community management) LEGISLATIVE FRAMEWORK (innovation regulations, entrepreneurship support)

Glossary

Artificial Intelligence (AI)
The simulation of human intelligence in machines that are programmed to think and learn, often used for automation, data analysis, and decision-making processes.
Business to Business (B2B)
Refers to transactions or interactions that occur between businesses, often used in the context of providing services or products, such as digital solutions for financial services.
Cloud Service Agreement (CSA)
A contract between cloud service providers and their clients, detailing the terms and conditions under which services will be provided, including security standards.
Cyber Security Authority (CSA)
An authority responsible for overseeing cybersecurity efforts within a nation, such as the Ghana Cyber Security Authority.
Distributed Denial of Service (DDoS)
A type of cyberattack that overwhelms a server or network by flooding it with internet traffic, rendering it unavailable to legitimate users.
Electronic Currency Franc of Africa (ECFA)
A digital currency initiative introduced in Senegal, which represents an alternative to traditional financial systems, aimed at facilitating financial inclusion and access to capital for businesses.
Engineering Procurement Construction + Financing (EPC+F)
A business model combining engineering, procurement, construction, and financing, often used in large-scale infrastructure projects such as digital or telecommunications developments.
Foreign Direct Investment (FDI)
Investment made by a company or individual in one country in business interests in another country, typically by acquiring business assets in the foreign country or establishing business operations.
General Data Protection Regulation (GDPR)
Règlement européen sur la protection des données personnelles, visant à renforcer la protection des données des citoyens de l'Union européenne et à harmoniser les lois de protection des données à travers l'Europe.
Groupement d'Investissement Numérique (GIN)
Digital Investment Groups inspired by agricultural investment groups, aiming to pool private and public capital for digital infrastructure projects like data centers and telecommunications.
Groupements Fonciers Agricoles (GFA)
Agricultural Land Groups, a type of cooperative structure that pools resources for shared agricultural projects. In the digital context, these serve as inspiration for investment groups in digital infrastructures.
Information and Communication Technology (ICT)
Refers to technologies that provide access to information through telecommunications. It includes the internet, wireless networks, mobile phones, and other communication mediums.
Internet of Things (IoT)
A network of physical objects—devices, vehicles, buildings—that are embedded with sensors, software, and other technologies to collect and exchange data, enabling automation and monitoring across various sectors.
National Information Technology Development Agency (NITDA)
A Nigerian agency focused on promoting digital development and technology regulation within the country, aiming to secure and regulate IT services.
Nigerian Communications Commission (NCC)
The official regulator for communications in Nigeria, responsible for overseeing telecom services and digital infrastructure.
Official Development Assistance (ODA)
Government aid designed to promote the economic development and welfare of developing countries. Often used to fund digital infrastructure and technology projects.
Public-Private Partnership (PPP)
A cooperative arrangement between the public and private sectors to finance, build, and operate projects, typically for infrastructure like telecommunications and digital services.
Special Economic Zones (SEZ)
Areas within a country where the business and trade laws differ from the rest of the country. SEZs are typically created to attract foreign direct investment and foster economic growth, particularly in technology sectors.
Subscriber Identity Module (SIM)
A small chip in mobile devices that stores user information and connects them to mobile networks. SIM swapping is a fraud method used to hijack user accounts.

PASAS

Introduction

PLATEFORME D'ANALYSE,
DE SUIVI ET D'APPRENTISSAGE
AU SAHEL

PORTÉ PAR

MINKA | AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

pasas-minka.fr

Ce rapport a été élaboré dans le cadre d'un financement du Fonds Paix et Résilience Minka.

Le Fonds Minka, mis en œuvre par le groupe AFD, est la réponse opérationnelle de la France à l'enjeu de lutte contre la fragilisation des États et des sociétés. Lancé en 2017, Minka finance des projets dans des zones affectées par un conflit violent, avec un objectif : la consolidation de la paix. Il appuie ainsi quatre bassins de crise via quatre initiatives : l'Initiative Minka Sahel, l'Initiative Minka Lac Tchad, l'Initiative Minka RCA et l'Initiative Minka Moyen-Orient.

La Plateforme d'Analyse, de Suivi et d'Apprentissage au Sahel (PASAS) est financée par le Fonds Paix et Résilience Minka. Elle vise à éclairer les choix stratégiques et opérationnels des acteurs de développement locaux et internationaux, en lien avec les situations de crises et de fragilités au Sahel et dans le bassin du Lac Tchad. La PASAS se met en œuvre à travers d'un accord-cadre avec le groupement IRD-ICE après appel d'offres international dont le rôle est double : (i) produire des connaissances en réponse à nos enjeux opérationnels de consolidation de la paix au Sahel et (ii) valoriser ces connaissances à travers deux outils principaux : une plateforme numérique, accessible à l'externe, qui accueillera toutes les productions et des conférences d'échange autour des résultats des études. La plateforme soutient ainsi la production et le partage de connaissances, en rassemblant des analyses robustes sur les contextes sahéliens et du pourtour du Lac Tchad.

IRD Institut de Recherche pour le Développement FRANCE | ICE FRANCE | UK International Development Partnership | Progress | Prosperity | ALLIANCE SAHEL