Centre for International
Governance Innovation

SPECIAL REPORT

Negotiating Africa's Digital Partnerships amid Geopolitical Competition

Folashadé Soulé

Centre for International
Governance Innovation

SPECIAL REPORT

Negotiating Africa's Digital Partnerships amid Geopolitical Competition

Folashadé Soulé

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Director, Program Management Dianna English
Program Manager Ifeoluwa Olorunnipa
Program Manager Jenny Thiel
Publications Editor Susan Bubak
Publications Editor Christine Robertson
Graphic Designer Sepideh Shomali

Copyright © 2024 by the University of Oxford

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.

The text of this work is licensed under CC BY 4.0. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

For reuse or distribution, please include this copyright notice. This work may contain content (including but not limited to graphics, charts and photographs) used or reproduced under licence or with permission from third parties. Permission to reproduce this content must be obtained from third parties directly.

Centre for International Governance Innovation and CIGI are registered trademarks.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Folashadé Soulé is a CIGI senior fellow and senior research associate at the Blavatnik School of Government, University of Oxford. She is currently a visiting scholar at the University of Ghana. Her research areas focus on Africa-China relations, asymmetrical negotiations, the study of agency in Africa's international relations and the politics of South-South cooperation. She is a principal investigator of the Negotiating Africa's Digital Partnerships policy research project that examines Africa's relations with rising partners in the digital sector. As part of this project, she has led a series of interviews with African senior policy makers, ministers, academics, experts, and private and civic actors that aims to shed light on how African stakeholders build, negotiate and manage strategic partnerships in the digital sector in a context of geopolitical rivalry.

She was a post-doctoral fellow at the London School of Economics and a former Oxford-Princeton Global Leaders Fellow. Her research has been published in several peer-reviewed journals. Folashadé also teaches as a guest lecturer in politics and international relations at the University of Oxford, Department of Politics and International Relations, Oxford School of Global and Area Studies.

As a policy-facing academic, connecting policy and research, she is the initiator of the Africa-China negotiation workshop series, bringing together African negotiators and senior policy makers to exchange and build better negotiation practices when dealing with China. She has also served as a policy analyst and consultant for several institutions.

Acronyms and Abbreviations

5G	fifth-generation
ADRH	Africa Digital Rights Hub
AfCFTA	African Continental Free Trade Area
AI	artificial intelligence
ANCy	Agence Nationale de la Cybersécurité
APEC	Asia-Pacific Economic Cooperation
ASIN	Agency for Information Systems and Digital of Benin
AU	African Union
AUCSEG	African Union Cyber Security Expert Group
CDA	Cyber Defense Africa
CDB	China Development Bank
CERT	computer emergency response team
CERT-MU	Computer Emergency Response Team of Mauritius
CIRT	computer incident response team
COMESA	Common Market for Eastern and Southern Africa
CSOs	civil society organizations
DPGs	digital public goods
DSR	Digital Silk Road
DTSA	Digital Transformation Strategy for Africa
ECCAS	Economic Community of Central African States
ECDPM	European Centre for Development Policy Management
ECOWAS	Economic Community of West African States
FATF	Financial Action Task Force
FMST	Federal Ministry of Science and Technology
GDPR	General Data Protection Regulation
GuiLab	Guinéenne de Large Bande
HP	Hewlett-Packard

ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information and communications technology
ID	identification
IDRC	International Development Research Centre
IP	intellectual property
ISO	International Organization for Standardization
IT	information technology
ITU	International Telecommunication Union
M&E	monitoring and evaluation
MOU	memorandum of understanding
NASRDA	National Space Research and Development Agency
NATO	North Atlantic Treaty Organization
NCB	National Computer Board
NGOs	non-governmental organizations
OST	Outer Space Treaty
PKI	public key infrastructure
PPPs	public-private partnerships
R&D	research and development
SIN	Société d'Infrastructures Numériques
SOC	security operations centre
SSTL	Surrey Satellite Technology Limited
UNECA	United Nations Economic Commission for Africa
WAEMU	West African Economic and Monetary Union

Introduction

Amid growing geopolitical rivalry between major players such as China and the United States, African stakeholders negotiating partnerships toward achieving various digital development goals are faced with a myriad of constraints to their agency. Negotiating Africa's Digital Partnerships — a Centre for International Governance Innovation- (CIGI-) supported policy research project hosted at the Blavatnik School of Government, University of Oxford — studies how African governmental actors negotiate and manage partnerships in the digital sector with new and rising partners in a context of great-power rivalries. It involves interviews with African ministers, policy makers, private sector executives and civil society actors from both francophone and anglophone Africa with a focus on digital connectivity, infrastructure, digital sovereignty, norm-setting and governance issues.

The findings reveal African actors' awareness of geopolitical tensions and their innovative strategies, such as setting negotiation tactics, diversifying partnerships and forming joint ventures, to meet national digital transformation goals. The project also examines the roles and perceptions of African private and civic actors and the efforts toward better multilateral coordination among African governments. Through an interview series published on a dedicated online portal, policy briefs published by CIGI and a policy dialogue organized in collaboration with the Ministry of Foreign Affairs and Regional Integration of Ghana, the project provided valuable insights into the perceptions of African strategies in digital governance as well as actionable recommendations for African governments and stakeholders negotiating digital partnerships across a range of subjects. The project is co-led by Folashadé Soulé with research assistance provided by Leslie N. L. Mills.

Africa's Choice of China as a Preferred Partner Is More Pragmatic than Geopolitical

In their search to find partners to execute various digital projects, African governments make decisions based on national digital strategies enshrined in various policy documents. The choice of one partner over another is guided more by the alignment of the potential partner's capacity to deliver on the priorities detailed in these policy documents than by geopolitical considerations. Despite the source of funding having an impact on the alignment toward the East or the West regarding technology, China tends to be a frequent choice for African governments as the country is seen to be more flexible in negotiations for development cooperation. This is because Chinese technology providers often provide attractive financial arrangements thanks to Chinese state-backed funding. Furthermore, Chinese firms such as Huawei have excelled at developing effective business relations and operating in diverse cultural, political, economic and institutional conditions across Africa.

However, this does not mean that China is the only actor when it comes to digital partnerships in Africa. Several countries favour a diverse portfolio of partners on digital projects. Togo works with India on its digital identification (ID) platform, with partners in Poland on its cybersecurity infrastructure and is in talks with Estonian partners to develop an interoperability platform.[1] Benin has chosen Estonia and Rwanda as partners as the country develops its e-government offerings.[2] African governments also continue to benefit from European development cooperation agencies on a range of technical support and capacity-building projects. What remains important for African governments and leaders is maintaining a pragmatic stance in favour of working with whichever partner has the best offer in terms of technology and cost to achieve their goals, instead of choosing to align with one geopolitical rival over another. The choice of China may be a signal to the West, especially the United States, that African leaders still wield the agency to pursue their partnerships according to their interests. Ultimately, the determining factor for the increasing cooperation between Africa and China in the digital sphere is the lack of viable alternatives from the West that respond to African needs as well as the Chinese players do.

1 See interview with Cina Lawson in this report.

2 See interview with Marc-André Loko in this report.

African Civil Society Organizations Are an Untapped Resource for Africa's Digital Governance Objectives

Civil society organizations (CSOs) have an important role to play in shaping Africa's digital cooperation. They offer governments access to expert networks that can more quickly conduct analyses to come up with findings that improve the quality of government agencies' decision making regarding negotiations with international counterparts and the private sector on digital transformation issues. One example of such a CSO is the Africa Digital Rights Hub in Ghana, which has consolidated expertise on digital rights issues to address the lack of highly qualified digital rights experts in public agencies. African governments should consider developing strong institutional frameworks and coordination mechanisms to ensure ministries and related agencies engage development partners and the private sector with one voice and a common national agenda. Engagements with civil society should expand beyond agencies with historically more resources, such as finance, health and education, to improve the participation of citizens in policy-making processes.

CSOs are important institutions when it comes to holding authorities accountable for the constitutional and legal rights of citizens in the digital sphere. Polycentric and multi-stakeholder organizations can help develop and operationalize standardized strategies to bring private actors together to find solutions in specialized fields that are beneficial to all actors. One example of such a polycentric approach is the collaboration between Mastercard, AfricaCDC and Afreximbank, which led to the creation of the Africa Medical Supplies Platform, which immediately enabled access to products from vetted manufacturers to African governments during the COVID-19 pandemic. Such a platform had the potential to cut health-care delivery costs by allowing continent-wide procurement and leveraging bargaining power to reduce the cost of medicines.[3] CSOs can play a role in encouraging such collaborative efforts.

Achieving consensus at the continental level is a daunting task due to the sheer number of states involved and the diversity of interests. African CSOs also perform the task of engaging with intergovernmental initiatives to help develop a unified African agenda on digital governance. The strong presence of CSOs in intergovernmental cooperation through fora, such as the Global Forum on Cyber Expertise and the Africa Internet Governance Forum, is essential for promoting a unified, comprehensive and effective strategy in addressing the digital challenges facing Africa, ranging from digital governance, digital rights and digital public goods to cybersecurity.[4]

Joint Ventures Can Be Effective Public-Private Partnerships to Deliver Digital Projects

Many African countries grapple with a shortage of top talent in key digital sectors, such as cybersecurity, data protection and software engineering. To mitigate this, some countries, notably Togo, have used joint ventures as an effective strategy for integrating operational expertise in areas lacking local specialization. The Government of Togo has leveraged public-private partnerships (PPPs) in the form of joint ventures to enhance large-scale digital projects and improve service delivery.[5] Such partnerships enable the government to de-risk private partners' participation in the project, which is part of its strategy to attract reputable partners. Involving reputable private partners is beneficial for several reasons. First, it provides access to highly qualified specialists for specific assignments, as it is possible to offer attractive remuneration packages that are not available in the public sector. Second, credibility plays a pivotal role in establishing joint ventures, in particular in sensitive sectors such as cybersecurity.[6] In Togo, a successful joint venture with the Polish software firm Asseco led to the development of major digital infrastructures, including a security operations centre and a computer emergency response team. Another notable achievement is the Woezon joint venture with CSquared, which aims to build and operate a landing station for Google's Equiano submarine

3 See interview with Bright Simons in this report.

4 See interview with Nnenna Ifeanyi-Ajufo in this report.

5 See interview with Cina Lawson in this report.

6 Ibid.

fibre-optic cable, expected to significantly boost the country's economy by 2025. Third, the insistence on knowledge transfer and local talent support obligations in the PPP structure is a powerful tool for building local capacity. The Togolese government's commitment to this approach is evident in its insistence on knowledge transfer and operational training in its biometric ID contract, demanding that local staff be trained to international standards, reinforcing local project ownership and bolstering digital sovereignty. However, fostering fruitful partnerships between the private sector and governments in digital development requires overcoming certain challenges. African governments often exhibit protectiveness over national assets and skepticism toward private sector motives.[7]

For successful partnerships, private companies must alleviate governmental concerns by putting effort into building open and collaborative relationships. Governments, on the other hand, should create conducive environments for profitable business, including transparency in partner selection and clear engagement rules. Fiscal discipline and legal protections are essential to attract private sector interest in joint ventures. Trust, transparency, regulatory clarity and collaboration are fundamental for successful partnerships that foster economic growth and digital development, especially for ventures backed by significant funders such as the World Bank.

Africa Needs to Challenge the Hegemony of International Standards

African private sector players navigating partnerships with both Western and Asian counterparts face the complex challenge of reconciling diverse international standards and institutional practices. While adhering to globally recognized standards, such as ISO (International Organization for Standardization) or GS1, Asian partners often have their own unique internal standards, leading to varied interpretations and implementations. African companies, therefore, find themselves arbitrating between Western (United States, Europe) and Eastern (China, India) conformance expectations.[8] Addressing this situation requires lobbying for the international recognition of African standards and achieving technical interoperability with existing ones. The African Continental Free Trade Area (AfCFTA) presents a promising avenue for developing and implementing norms and solutions rooted in African experiences and standards, potentially extendable to international partnerships. This process requires intensive collaboration with local private sector entities actively engaged across the geopolitical spectrum.

Multilateralism Presents Powerful Opportunities to Achieve Goals Despite Challenges

To significantly influence global norm formation, African countries must unite and leverage their collective strength. The African Union and regional multilateral organizations have been instrumental in addressing digital sector issues, fostering multilateralism in Africa's digital development. This collaboration has been pivotal in cross-border infrastructure projects and supranational agreements to harmonize digital economy regulations, including cybersecurity, data protection, payments and trade. The Malabo Convention, adopted in 2014, and the African Union's Digital Transformation Strategy for Africa (DTSA) (2020–2030) are prime examples of such efforts, promoting common regulatory frameworks and multi-stakeholder alliances. Additionally, subregional alliances such as the Mano River Union, in partnership with the African Development Bank, have launched projects such as the digitization of government payments to enhance transparency and resource management. Despite these efforts, a common African voice on international digital transformation issues remains elusive, as larger nations often negotiate independently with major digital partners, focusing more on attracting foreign direct investment than representing a collective stance. Furthermore, at the African Union level, physical conflicts tend to be prioritized over cyberattacks. African countries also rely on funding and capacity building provided by external states, which compounds the lack of a harmonized approach.[9]

7 See interview with Lanre Kolade in this report.

8 See interview with Bright Simons in this report.

9 See interview with Nnenna Ifeanyi-Ajufo in this report.

The Smart Africa alliance stands out for its role in African multilateral digital initiatives. Comprising 36 member states and diverse stakeholders, Smart Africa works in concert with the African Union to drive the digital economy's contribution to socio-economic development. Smart Africa stands out among other multilateral organizations for its initiatives that involve private sector actors more deeply in its goal of creating an African digital single market with links within the AfCFTA and with other markets.[10] It provides technical support, feedback and expertise in pilot projects, assisting African countries in pooling resources. Smart Africa has developed various blueprints covering aspects such as smart cities, broadband, digital economy and artificial intelligence (AI), offering member states models for policy development. This approach is exemplified by Sierra Leone's National Digital Development Policy, inspired by Kenya's Digital Economy Blueprint. Major tech firms, such as Google, Huawei, Orange and Econet, as significant financial contributors to Smart Africa, gain privileged access to policy makers and heads of state, fostering direct negotiations. Additionally, intergovernmental projects such as the Economic Community of West African States-led Amilcar Cabral project for a submarine fibre-optic cable exemplify regional efforts to enhance broadband capacity. However, achieving a digital single market in Africa faces challenges due to inconsistent policies and varied digital development levels across the continent. A unified approach is crucial for harmonizing laws and advancing shared digital projects.

African Digital Sovereignty Hinges on Unified Approaches to Reduce Reliance on Foreign Tech

Digital sovereignty is a state's control over digital infrastructure and data within its territory, regardless of the data's hosting location. This concept is shaped by a country's social, economic and political interests; technological capabilities; domestic priorities; and digital foreign policies.[11] This vision requires national frameworks and a continental data governance framework, urging African policy makers to build domestic and regional frameworks to harmonize regulatory spaces and enable economies of scale for African firms.

Efforts to address digital sovereignty in Africa are growing. The African Union's DTSA aims to adopt emerging technologies for sustainable development. The Malabo Convention and the AfCFTA offer standards for data protection, cybercrime prevention and regional data flow facilitation. African governments are drawing from the European Union's General Data Protection Regulation (GDPR) model, with variations in localization approaches.

However, some interviewees observed "cyber militarization" as a significant aspect of African perceptions of digital sovereignty, with governments often viewing cybersecurity through a national security lens, leading to internet shutdowns and service blocking in response to crises. African countries frequently align with China and Russia in cyber diplomacy, as reflected in their cybersecurity governance interpretations and implementations. This approach is evident in the ongoing negotiations of article 5 of the UN Cybercrime Treaty where African countries have tended to side with China and Russia.[12]

However, African digital sovereignty faces major challenges, including the continent's infrastructural deficit, dependence on foreign technology providers, data localization issues and a lack of regulatory harmonization.[13] Many African countries face a shortage of technology skills and financial resources for indigenous information and communications technology development, leading to reliance on foreign technology and services. While some countries, notably Senegal, have adopted data localization rules replicating Chinese data governance and moved all government data to a Huawei-built data centre near Dakar, several African countries cannot consider similar policies due to the lack of local data centres.[14] Even so, data localization poses its challenges. While it can

10 See interviews with Thelma Efua Quaye and Nnenna Ifeanyi-Ajufo in this report.

11 See interview with Melody Musoni in this report.

12 See interview with Nnenna Ifeanyi-Ajufo in this report.

13 See interview with Mandira Bagwandeen in this report.

14 See interview with Tin Hinane El Kadi in this report.

benefit local data centre owners and employees, it may also harm the broader economy by limiting access to data. Forcing firms to store data locally may not necessarily lead to digital development or better protected data, especially given other factors such as the fact that many countries struggle to provide reliable electricity and high-speed connectivity.[15] Policy makers face the task of balancing the need for digital sovereignty with the economic impacts of data localization regulations.[16]

To foster digital sovereignty, African policy makers must focus on building domestic and regional frameworks to harmonize regulatory spaces, thereby enabling seamless data flow and use. Major investments are needed to increase Africa's share of global data centre capacity from the less than one percent it is today. African stakeholders must leverage the continent's untapped youth potential to develop local digital industries and foster the emergence of indigenous tech products and software. Prioritizing education and developing the youth ecosystem across Africa's 400 technology hubs in 42 countries will put the continent on the path to digital sovereignty.[17] This strategy will also set the foundations for Africa's emergence in other highly specialized domains where the continent is also underrepresented such as space governance.[18]

15 See interview with Bulelani Jili in this report.

16 Ibid.

17 See interview with Jane Munga in this report.

18 See interview with Timiebi Aganaba in this report.

Compilation of Interviews

Hon. Cina Lawson, Minister of Digital Economy and Transformation (Togo): "Executing a deal well in the digital sector requires thorough collaboration among many actors."

Cina Lawson is Togo's minister of digital economy and transformation. Drawing from more than 20 years of experience and expertise in digital policy and regulation, she has led Togo's transition to an inclusive digital economy.

African governments want to work with multiple partners (public and private) in their digital development objectives and strategic priorities. How does Togo choose its strategic partners to carry out its digital transformation strategy, especially with regard to digital infrastructure and services?

To put it simply, we are guided by our priorities. First and foremost, we define our priorities, and then we look for partners with the required expertise and ability to execute, depending on which project we want to push. Let me give you two concrete examples.

In 2018, we started our cybersecurity journey by designing a strategy. Studies and reports have clearly shown the growing impact of cybercrime. We had to strengthen our cybersecurity as a matter of urgency, with the obligation to protect people and businesses in this technology-driven change era.

We passed laws and different decrees to provide our country with significant legislation for a coherent strategy to monitor and defend against cyberthreats at the national level, and we created the regulatory entities such as Togo's national cybersecurity agency (Agence Nationale de la Cybersécurité [ANCy]) in 2019. But our newly formed ANCy was required to rapidly establish the necessary technical framework for the constant monitoring and implementation of proactive defence mechanisms in response to cyberattacks. This required two critical pieces of infrastructure: a computer emergency response team (CERT); and a security operations centre (SOC).

Our vision was to operate these two infrastructures as a service delivered with high quality for the citizens, the administration and the private sector. However, we did not yet have enough specialized human resources locally, technologies and processes to build and run these kinds of services at the quality and at the scale that we desired. We did not want to only buy the equipment and training from a partner because delivering the service is a different skill set that requires practice, understanding the commercial and technical aspects of it, and, most importantly, building trust.

Given our urgent need to make our newly established ANCy operational in the shortest possible time, it became clear to us that partnering with an established private sector player would be the best way to address our cybersecurity needs. We needed a broader partnership where interests were aligned.

We had been talking to Asseco Group, a partner in Poland, about digitalization of government services, such as geo-portals and cybersecurity, among others. Asseco Group is a leading NASDAQ-listed Polish information technology (IT) firm — the sixth-largest software firm in Europe — with over 25 years of software and expertise in cyberspace protection.

In 2019, we entered a PPP with Asseco to set up a joint venture called Cyber Defense Africa (CDA) to bring in the operational expertise in our cyberspace protection.

Our partnership with Asseco on CDA is unique in that it combines the CERT with a national SOC. It is also unique because Asseco is not only a technical partner but also an investor in the joint venture. This is to ensure that the joint venture is operated efficiently and profitably.

Infrastructure aside, perhaps an even more important reason for us going with the private sector and Asseco was for credibility. Working with a private-sector player like Asseco, with its strong track record and prominent clientele such as the North Atlantic Treaty Organization (NATO), instills the confidence and credibility that CDA needs to function from day one.

Furthermore, we emphasized the importance of service delivery by ensuring that our partner Asseco has a vested interest in training our technical team — which is entirely Togolese — during their

mandate of 10 years. The vested interest was expressed by being a minority shareholder and through decision making such as the CEO selection.

The second example is the landing of Google's submarine cable Equiano in Togo, through a partnership that would transform our country's broadband landscape. In March 2022, Togo became the first landing point in Africa of Equiano, a fibre-optic cable running from Portugal to South Africa. The operationalization of this submarine cable is carried out by a joint venture between the Société d'Infrastructures Numériques (SIN), a public telecommunications asset company, and CSquared, a private, open-access, wholesale broadband infrastructure company. The entity created, CSquared Woezon, is 56 percent owned by CSquared and 44 percent owned by SIN.

With the main objective, in 2019, to deploy a new submarine cable in Togo at the earliest [time possible], we were having conversations with both Google and Facebook, just before Google announced a US$1 billion investment in Africa. We had to convince Google that Togo could integrate the Equiano project's first phase, without affecting their overall schedule, for which implementation had already begun. In parallel, we had to work on developing a market for high-speed internet connection that is lucrative, compared to much bigger countries such as Nigeria, South Africa, etc. Our priority here was to partner with the private sector to accelerate the deployment of high-speed internet connectivity and, particularly, to ensure that the price of fibre-to-the-home internet access drops by about 70 percent, which would bring it within the reach of many Togolese households.

During the implementation of the project, we were faced with two major issues: the determination of a partner likely to provide financing alongside the Togolese state; and the choice of a partner who was entitled to sell international capacity on the Equiano cable and to operate a landing station. We devised a clear partnership structuring mechanism integrating not only the state but also private investors. Like the cybersecurity deal, we would have a state-owned company that would be interested in operating the cable, but we also reached out to private companies, including all the wholesalers on Equiano for private investment, with a particular focus on the training of our teams.

CSquared Woezon is now responsible for the maintenance and operation of the Equiano submarine cable as well as the existing terrestrial fibre-optic networks of the e-government and the fibre on the high-voltage network that links Togo and Benin. For the commercialization of international capacity, CSquared Woezon will provide open access to all national and regional operators on an objective, transparent and non-discriminatory commercial basis, in accordance with industry standards and international best practices. When activated, the Equiano cable will offer 20 times more bandwidth than any other cable currently serving West Africa and should enable Togo to attract even more investment and further stimulate its dynamic start-up culture. Equiano is an essential and strategic tool in realizing Togo's ambitious digitalization projects.

In terms of applications and platforms, our choice is to use open-source technology whenever possible to avoid vendor lock-in. We keep this in mind even as we continue talks with Estonia to establish an interoperability platform and work with the World Bank on a new biometric ID for all our citizens. We have been inspired by India's experience deploying Aadhaar, its national biometric ID system.

In this larger digital strategy that you have explained, where does China, a strategic digital partner for Africa, fit in with its offers in terms of digital infrastructure and digital services?

In the digital infrastructure sector, Chinese firms have been known to provide the funding and technical expertise necessary for network development. This approach has been beneficial for African countries, as they would not have been able to build their networks without Chinese involvement.

In Togo, we view telecom and digital as a service, and we believe that whoever operates the service should have a stake in the asset. Our approach to infrastructure deployment in Togo prioritizes collaboration with the private sector to de-risk projects and focus on service delivery, rather than taking on the responsibility of building infrastructure ourselves. While other countries and partners may have different business models, we prioritize identifying the specific project structure we need and searching for partners who can offer it.

For example, we obtained financing from the World Bank and partnered with India to develop our new biometric ID system. We are also working on a digital social registry for the country and

taking inspiration from successful models in Latin America and the Middle East. We welcome partnerships with any country that can provide the necessary expertise and financing for our projects.

What are the best strategies to negotiate digital projects, especially in terms of technology transfer, local employment, and local content and data protection? Is there an internal strategy for this? Based on Togo's experience, what would be your key recommendations?

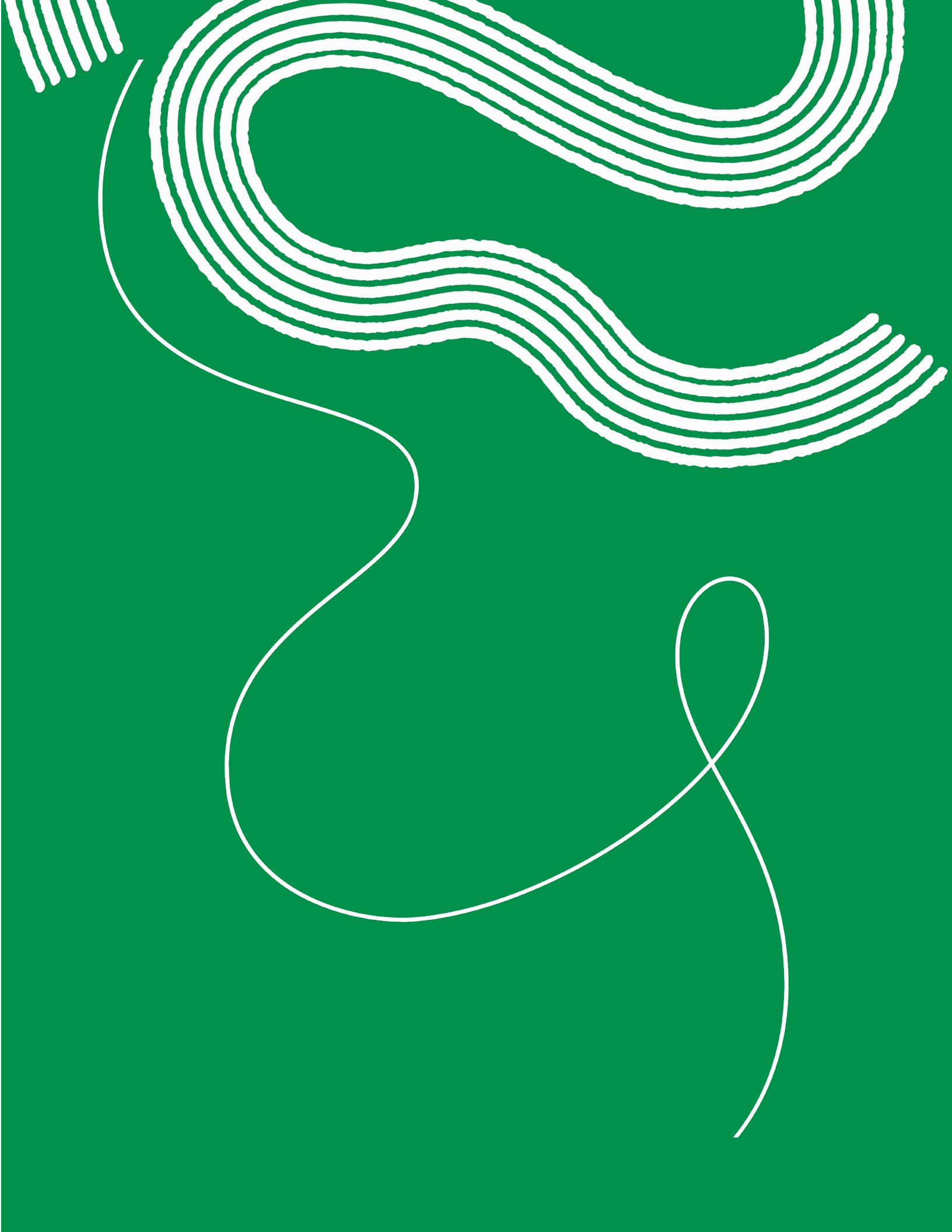
One issue we have on the continent is execution. Deals may be poorly structured, not necessarily because the people in charge are dishonest, but because they may not know how to execute well. In Africa, we must specialize in checking the credentials of every person we hire and emphasize structuring a highly skilled execution team. Executing a deal well requires thorough collaboration among many people. There is no room for improvisation; a team of people with the right expertise in their fields is essential.

Second, in our view, knowledge transfer requires thorough operational training, and we need to consider this in the deals we enter with partners for national projects. In deploying the biometric ID contract, for example, we demanded a road map for knowledge transfer. We want the strategic partner to provide us with the job description of the Togolese who will work with their teams, and they must participate in the selection of these Togolese staff who will shadow them every step of the way. We want the trained staff to pass tests in every project component, so they get what we call "objective certification." The certification must also be internationally recognized. That's what we call "knowledge transfer."

There are two other things: one is subcontracting; the other is hiring of staff. It's very important that our partners hire Togolese staff even at the management level. This requires that they hire Togolese first, but if they really cannot find a suitable Togolese candidate, then there must be a solid training plan in place so that in two to three years, a Togolese from the existing team can grow into the needed role. You must be very hands-on as it is crucial to scrutinize the details of things to ensure that what partners are doing aligns with your vision. This can certainly be more demanding, but you cannot do without it.

A final question about global digital governance: Africa's participation in multilateral fora governing the internet and telecommunications world has been limited so far. What bargaining leverage do African governments have in shaping the global discourse and norms on digital governance?

Well, based on what we have observed so far, it seems that the only way for African countries to have a significant impact in shaping the continent's future is through critical mass and leveraging multilateral organizations such as the African Union. It is clear that no single country can accomplish this alone. Some of the larger countries like Kenya, Nigeria and South Africa may have enough influence to make a difference on their own. However, the rest of us need to unite as a continent. The challenge here is that we often have trouble speaking with one voice due to disagreements between countries. When the larger countries take charge, they often only focus on their own issues. That is why we believe it would be beneficial for these larger African countries to reach out to smaller countries and represent them as well. For example, Nigeria could become the voice of West Africa. If we don't function this way and come together with an aligned agenda, decisions that affect us will be made without our input.



Joanne Esmyot, Public Digital: "Digital decolonization in Africa is a two-way street."

Joanne Esmyot is a director at Public Digital. She has 16 years of experience working in both the private and public sectors. Before joining Public Digital, Joanne was the executive director of the National Computer Board (NCB) of Mauritius for three years. Under her leadership, the NCB successfully delivered several digital transformation initiatives for the Government of Mauritius, such as the establishment of the first Mauritian Certificate Authority, which enabled the launch of online birth certificates in Mauritius and laid the foundation for many more trusted digital services. She also notably led the national computer incident response team (CIRT) of Mauritius, namely, the Computer Emergency Response Team of Mauritius (CERT-MU).

Disclaimer

The views and opinions expressed in this interview are those of the interviewee and do not represent or engage in any way the Government of Mauritius, the NCB, the people, institutions or organizations that the interviewee may or may not have been associated with in a professional or personal capacity.

Your work at the NCB to build out the cybersecurity framework and digital economy of Mauritius led the country to be ranked first in Africa in the International Telecommunication Union (ITU) Global Cybersecurity Index. How can other African governments, especially of smaller countries, strike partnerships with the private sector to build out cybersecurity infrastructure to achieve the heights that Mauritius has? Are there any strategies of note?

First of all, Mauritius ranking first on the ITU Global Cybersecurity Index for Africa was not really of my doing; it was already ranked first when I joined the NCB. It is true, though, that our scores on the assessment increased progressively over the time I was at the NCB. I would highlight two things that worked well for us. The first was starting small and incubating new projects and initiatives within the NCB, as was the case for the CIRT team. It started small, first being incubated at the NCB, then gradually maturing them to work well. The Cybersecurity and Cybercrime Act 2021 establishes CERT-MU as a separate entity under the Ministry of Information Technology, Communication and Innovation. This model of starting small, incubating the team and then gradually maturing the team worked well in the context of CIRT, but also for teams of other projects and initiatives.

The second point is that partnerships were key. I would say that what helped accelerate progress was mostly partnerships with international organizations and donor support. We received quite a lot of support through the Cyber4Dev[19] program funded by the European Union. We had good ties and collaborations with other CIRT teams worldwide, mostly through the FIRST [Forum of Incident Response and Security] network.[20] And we also had good collaboration with AfricaCERT[21] more regionally. So, I think partnerships were key to help us lay down the cybersecurity strategy for the country and build the capabilities of the CERT team. Those international partnerships were even more critical to help the team mature and grow. That was extremely helpful.

That said, one point I must make is that the ecosystem in Mauritius was already conducive for these things to happen. Now that I work with other African countries, I am quite conscious that it may not be the case in other countries. The Mauritian government has, for decades, invested in a long-term vision to make information and communications technology (ICT) a pillar of the economy. That meant that some foundational elements were already in place, in terms of talent, for example. While there is still competition for talent, compared to other countries, there has been some work already done around nurturing enough talent to have minimum viable teams within the government. In terms of infrastructure, since there is already a good ICT sector in Mauritius,

19 See https://cyber4dev.eu.

20 See www.first.org.

21 See www.africacert.org/.

there is already an ecosystem of partners that the government can engage with to implement the infrastructure, to outsource and complement the capabilities within the government — because it is impossible to do everything with the small teams present within government. Overall, the ecosystem was already very conducive to that. There were incentives from the government to attract investors in the sector to Mauritius early on and, since then, ongoing dialogue and partnerships.

Going back to the point around PPPs, by the time I left the NCB, there was indeed a stronger partnership between the government's CIRT team and the private sector. For instance, in some sectors like banking, we did a lot of work to build capability, hold awareness sessions, and offer valuable services such as security assessments of certain banks and other private companies in the sector. We offered these to the private sector because, as part of our national strategy, we recognized that some sectors were part of the critical information infrastructure of the country. This made us work more closely with those sectors. Overall, there was a good partnership with the private sector, although the starting point was working with international organizations, in my view.

In what ways do you think that Mauritius and other countries that have excelled at digital transformation can share lessons and strategies toward digitalizing public services with other countries?

In Mauritius, we have always been inspired by what was being done in other countries and looked to adopt the best practices to inform the strategy of the country. I think that, looking back on my experience, our strategy might have been slightly overambitious initially. When you see more mature, more advanced countries doing lots of things, you are tempted to do the same. But it does not work that way. With time, we learned to be more realistic and take into account our own capability. If you compare the latest version of the strategy to earlier ones, you can tell that in the recent revisions, there are fewer focus areas, but these areas are better aligned with priorities and what would have the greatest impact based on where the country was at that time. In general, I would say there are loads of examples or best practices that are available, depending on which sector you look at. It is important, however, to be realistic about where the country currently is. This involves understanding what the readiness factors are to achieve digital transformation. Start with the basics and set a reasonable number of priorities within the strategy for the next few years that you can focus on to make progress and impact.

How do you think the geopolitical rivalry between China, the United States and Europe affects the way some African governments and actors are establishing their strategies, and what is the best way to avoid being affected by this?

That is a good question, albeit not easy to answer. What comes to mind immediately is the question of sovereignty but also digital decolonization. These are not easy questions, and I am not sure I have solutions to any of those.

Let us take the question of sovereignty. I think the good thing about Mauritius is that, in general, there's political stability, and the government has, over the years, consistently invested in a longer-term vision for digital transformation. One of the challenges with other countries is short-termism, i.e., governments not willing to invest in things that will yield longer-term returns. What has been done in Mauritius — again, long before I joined the NCB — was investing in local data centre capabilities and the capacity to be able to develop and host critical government digital services in-house. That does not mean that everything is necessarily developed in-house or hosted on the government cloud, but at least building that capability within the government to keep control of the things that you want to control is key. Of course, this does not happen overnight. It takes longer-term commitment and actions. Building local capability is foundational to sovereignty, and this can only happen over time.

On the question of digital decolonization, it is a two-way street. Digital decolonization should not be considered only as dealing with the tendency for the most powerful, so-called Global North, countries to impose their vision on lower-income countries or the so-called Global South. We need to also consider it as dealing with the mindset of lower-income countries to make their own decisions around what works for them. I think there needs to be a culture shift both ways, not just in the West. I have been in places where, because I am from Africa, I am less listened to than my colleagues coming from Europe, even though we are working on the same team. A mindset change needs to happen. Granted, some noteworthy trends

are promising in terms of digital decolonization. The increased use of open source within government is one example of this, even though there's still skepticism and resistance in many areas. So, that is one way to aim toward digital decolonization. And then there is the ongoing discourse around digital public goods, digital public infrastructure, and sharing and reuse of solutions among governments and countries. While these concepts are promising, they are not without obstacles. It can be much harder to put into practice, particularly where countries do not have the talent and do not have an ecosystem. A lot more attention and investment should be made into building capability to enable the adoption of a digital public goods or digital public infrastructure approach within governments, especially in low settings.

What should governments or the private sector be doing to cultivate the growth of local talent and attract African diasporans to fill the human resource gap needed to achieve this digital decolonization (for example, with regard to cybersecurity and open-source digital public goods and infrastructure)?

Some longer-term actions must be made, and governments must invest in them, even if the results are not going to be immediate. From my perspective, the reason there is a foundational level of digital skills or literacy within the Mauritian government is because of decisions that were made two decades ago at a point where internet connectivity was not as widespread. Since we invested heavily in infrastructure over 10 to 20 years at least, we rank very highly in terms of access to the internet. But when that was not the case, there were initiatives by the government and by the NCB to offer training at the doorstep of citizens through cyber caravans initially, and then gradually giving access to courses regionally to decentralize access to skills. Several policy decisions promoted the acquisition of digital skills or even required people to build those skills and gain knowledge. One remarkably successful example was the decision by the government to require entry-level civil servants to show evidence of a basic level of digital literacy. That compelled a lot of the people who wanted to join the public service to go forward with those courses, which helped create a minimum foundational level of skills within government.

Other than that, there has been a strong PPP for decades to forecast and plan for skills that are needed by the sector. The Human Resource Development Council[22] is a body in Mauritius that holds sectoral committees with representatives of the private sector to make informed decisions and forecast future needs. These partnerships influence the courses for which the government will fund scholarships, future skills in demand and working with educational institutions to make sure that these are reflected in the curricula. There are even placements or training that are delivered by the private sector to make sure that graduates are more employable. So, there have been lots of different initiatives between the private sector and the government.

What is Mauritius's position on issues related to internet governance, digital rights and data protection in international organizations? How can Africa's voice be strengthened in these multilateral fora?

Mauritius enacted its revised data protection law after the GDPR, before the United Kingdom. I find it amusing that we did this even before the United Kingdom did. We pay a lot of attention to making sure that we are implementing best practices. The laws are usually kept very up to date. In terms of cybercrime, Mauritius is a signatory to the Budapest and Malabo Conventions. So, usually, the laws and the policy are driven by what is happening internationally and what we think is relevant for the country. I can't speak on behalf of the country, but from my point of view, I don't think there is a particular bias toward one region or a type of international organization over another. This might be one of the strengths of Mauritius as compared to other countries. We're always open to a lot of collaboration and cooperation with other countries and with other international organizations, irrespective of the region. This allows us to take good things from everywhere. While I was at the NCB, I recall there was one person from the CERT-MU team who was a member of the working group on cybersecurity for the United Nations. This was great as it was an opportunity for us to contribute to shaping more global policy. But this does not happen often enough.

To your question about Africa's voice, I do feel like, more generally, there are a lot of growing success

22 See www.hrdc.mu/.

stories within Africa, but it's just that it doesn't get the kind of visibility that it should. I honestly don't know why that is. My best guess to positively influence that would be international organizations that work with governments, especially donor organizations like the United Nations or the World Bank or the African Development Bank, to play a greater role in shedding light on those success stories. And not just success but highlighting things that work well in Western countries but do not work in Africa. Not enough is being done around really having locally led development programs as opposed to traditional programs that are pretty rigid and dictated by the donor. To some extent, because African countries are dependent on funding, they have no choice. While this is not the full answer, I do believe that sharing more of what is being done in Africa is helpful. There are success stories like Irembo[23] in Rwanda, for instance, that improves access to digital services in low settings and can be a source of inspiration for countries with similar context. Showcasing those examples more is a good way to create awareness on the alternatives available, in my view.

23 See https://irembo.gov.rw/home/citizen/all_services.

Lionel Chobli, La Guinéenne de Fibre Optique (Guinea)

Lionel Chobli is the CEO of La Guinéenne de Fibre Optique (Guinea).

What is the digital development strategy in Guinea? How does this strategy intend to close the prevailing digital gap? How does this strategy fit into the wider African regional context?

Since 2002–2003, successive governments in the Republic of Guinea have devoted themselves to making investments and developing projects in the telecommunications sector and now the digital economy. After the unsuccessful attempt at a strategic partnership with Telekom Malaysia (2005), it was the arrival of Orange (Sonatel) and then MTN (South Africa) that reorganized the sector and gave it renewed momentum. Unfortunately, this dynamic was held back by the lack of investment by the South African group, which allowed Orange to become a dominant operator, even bordering on a monopoly in certain respects. For example, in terms of mobile network infrastructure, Orange has widened the lead over its two competitors to such an extent that, in 2019, the state had to implement physical infrastructure sharing and mutualization.

In terms of legislation, the government of President Alpha Condé has, from 2010 to 2021, increased the number of reforms, including regulatory, competition and fiscal reforms, with the main result being a significant reduction in the cost of communications. Notable progress has been made in telecommunications infrastructure, as a result of heavy strategic investments, sometimes supported by innovative financial arrangements. The submarine cable of Guinéenne de Large Bande (GuiLab) — in which the state has a majority stake (52 percent) — and the investment of all the telecommunications operators and internet service providers approved at the time is an example. Established in 2011, GuiLab became operational in 2014, launching the era of high- and even *very* high-speed broadband in Guinea. There is also the case of the national fibre-optic backbone, an intercity telecommunications network carrying internet capacity to all 33 prefectures of the country, financed by a Chinese export credit loan (via the Export-Import Bank of China) worth US$238 million for 4,300 km of underground networks.

Other projects, both public and private, continue to develop in Guinea and our company, Guinéenne de Fibre Optique, which is a PPP between Electricité de Guinée (producer, carrier and exclusive distributor of grid electricity) and MouNa Group Technology SA (the only Guinean company still operating in the telecommunications sector as an internet service provider), is an example. The state has been an active facilitator and supporter, seizing every opportunity to bridge a gap or an overlooked aspect of the backbone: the networking of metropolises and therefore access to the end customer.

It must be said that these projects effectively respond to the major challenge facing our states in the Economic Community of West African States (ECOWAS) region: access to the internet for the population, businesses and even decentralized and devolved public services. The much-vaunted, desired and solution-oriented digital world cannot do without quality and secure infrastructure. Regional projects exist such as WARCIP [the West African Communal Initiative Project],[24] financed by the World Bank, and its new variant WARDIP [the Western Africa Regional Digital Integration Program].[25] Some institutions, such as the African Development Bank, the West African Development Bank and the European Union, also support connectivity development projects. The United Nations International Children's Emergency Fund in Guinea has embarked on the fight against "illiteracy" by initiating a project to equip 18,000 digital classrooms in primary and secondary schools over five to seven years.

Of course, the challenges of the continent (the proper formulation of projects, their structuring, the quality of negotiations with donors, the transfer of skills, maintenance and, above all, the availability of electrical energy) remain important issues. Beyond intentions and speeches, a country like Guinea is not yet in a position, in 2023, to levy taxes on a pool of 1,000 significant companies using existing digital tools.

What is the role of external partners in the development and implementation of this digital strategy? Who are the main partners?

24 See www.warcip.net.

25 See www.ppiaf.org/activity/africa-west-africa-regional-digital-integration-project.

What is the role of China, which seems to be particularly active both in terms of supplying equipment and developing digital infrastructure? How does Guinea choose its partners according to the type of digital project?

Guinea's external partners have had little involvement in the formulation and implementation of strategies. If we consider the digital economy in the broadest sense, spanning infrastructure and services, it is noticeable that Guinean administration and private sector executives (as well as a diaspora rich in qualified skills) have always been very active and even jealous of their prerogatives. After mining, transport and financial services, the digital sector must be the one that attracts the most entrepreneurs and workers from outside Guinea. This includes public services.

The European Union, the African Development Bank, the World Bank Group and, to a lesser degree, the Islamic Development Bank can be cited as the leading partners in this field. Then come the private companies, both technical (Orange via Sonatel) and financial, which have considerably influenced the organization of the sector through their lobbying and ambitions. Orange is today a global operator in Guinea, holding all possible licences, from telecommunications infrastructure to financial services, with a role and impact that is very important and even worrying for some nationalists.

Finally, China, through the financing and construction of the national backbone, has played a decisive role in Guinea. Most of the possibilities for the development of new infrastructure stem from a possible interconnection with the backbone financed by the Export-Import Bank of China. On the services side, Huawei has supplanted the initially more established ZTE and is taking over most of the active equipment and accessories supply markets for public and private projects.

Nevertheless, at the institutional level, the major investors and the American agencies and those close to the Atlantic axis (United Kingdom, Australia) have, for some years, preferred to decline the use of Chinese equipment for their projects. Political and economic rivalries at the global level, therefore, have concrete repercussions at the local level. One internet service provider in Guinea was informed by a Western chancellery that it would not accept the provider's service if it uses any equipment from Chinese companies.

It should be noted, however, that the famous framework agreement between China and Guinea did not reserve the share that one might have expected for this sector. With a minimum amount of $20 billion, focused on the construction of infrastructure in exchange for the extraction of natural resources, the framework agreement has had a considerable impact on the mining and energy sectors. One might have hoped that telecommunications infrastructure would have been the third pillar to support Guinea's development. In reality, many telecommunications-related projects have not yet been implemented. The inclusion of the sector in the framework agreement could have boosted the realization of these projects, such as the metropolitan fibre-optic loops (complementary to the backbone), the development of digital terrestrial television, the creation of a proper government communications network, etc.

Finally, we should note the increasingly active role of multinational companies, such as Facebook, Google and Netflix, which are structuring infrastructure projects on a global scale by using their financial resources to reduce the cost of connectivity.

How are these contracts negotiated? What about the transfer of technology and skills in these contracts? What difficulties are encountered and how are they overcome?

The major contracts for financing and building digital infrastructures or providing services have until now been within the framework of bilateral cooperation. Whether it is the backbone concluded in 2014 and delivered at the end of 2020 (financed by the Export-Import Bank of China over 30 years with a 10 percent contribution from the state) or the current interconnection projects for all the universities, access to the negotiations is rather limited. What matters for the Guinean authorities is the result — and for the Chinese, the assurance of exclusivity.

The difficulties encountered by SOGEB [Société de Gestion et d'Exploitation du Backbone National] (the national company in charge of managing the national backbone) in the commercial operation and technical maintenance of the backbone illustrate the difficulties of cooperation in terms of training, after-sales service and sometimes the suitability of equipment choices.

Unfortunately, equipment from China is simply replaced in the event of an unknown or insurmountable problem by new equipment acquired in the West, which the local technicians are more familiar with. Whether this is a strategy decided by Guinea or a rule imposed by the Western partners is anyone's guess. What needs to be considered in this regard is the lack of precision and follow-up on issues of after-sales service, repair and preventive maintenance.

Huawei seems to have realized this by recently strengthening its presence and "Africanizing" its technical teams with local and subregional skills.

There is a strong power rivalry in the digital domain, especially between the United States and China. African countries are also demanding more digital sovereignty. What is your analysis?

Power rivalry is very unevenly manifested in the telecommunications sector in Africa. Leaving aside the knock-on effects of American and Canadian — or even Australian and British — restrictions on Chinese equipment, there most confrontation is invisible to the untrained eye.

In the infrastructure sector, China dominates the market with its unrivalled financing and execution capabilities. The United States seems to have less interest in this sector, largely preferring energy and financial services.

As far as services are concerned, Western, Middle Eastern or even Asian companies and some pan-African groups are the ones competing: French (Orange), English (Vodafone), Moroccan (Maroc Telecom via the Moov brand), Emirati (Etisalat), South African (MTN), Malagasy (Axian), Vietnamese (Viettel) or Indian (Airtel). In the digital sector, particularly applications and payment systems, the United States and China are almost non-existent. The Chinese concentrate their efforts on physical telecommunications infrastructures (networks) and more recently, and timidly, on digital ones. North American companies are indeed more dynamic in investing in and developing digital solutions. Let's take the example of the digitalization of customs, commercial and logistical services: no Chinese company has made a name for itself, unlike those from the United States, Europe and sometimes Singapore or Malaysia.

Visa and Mastercard, despite being very prominent and heavily advertised, remain fairly marginal insofar as relatively few Africans have bank accounts, on the one hand, and use bank cards, on the other. There are large markets (Egypt, Nigeria, Kenya and South Africa) where mobile money solutions are flourishing.

It seems that the control of telecommunications at the strategic level in Africa is another field of confrontation between the United States and China that is hidden from view: communication satellites, intelligence, cybersecurity, the fight against maritime insecurity, etc. Information is, therefore, unsurprisingly difficult to obtain.

In this environment, and given the trends observed, it could be said that African states, in general, are wavering between indifference, vigilance and awareness. Some, for historical and/or strategic reasons, have nevertheless taken strong decisions and clear options, whether it be Egypt, [which is] resolutely attached to North American solutions; South Africa, which is rather proud of its independence and the freedom to weave its web with the partners of its choice; or Rwanda, which seems to be taking advantage of the new options available on the market for Africa (Israel, Turkey, Romania, etc.).

In Guinea, access to information related to security, in general, and cybersecurity, in particular, is limited. From the little information available and cross-checking, one can see the strong activity of American, French, but also Russian, Turkish and Israeli companies. With France, the United States and China, the partnerships are more institutional than commercial.

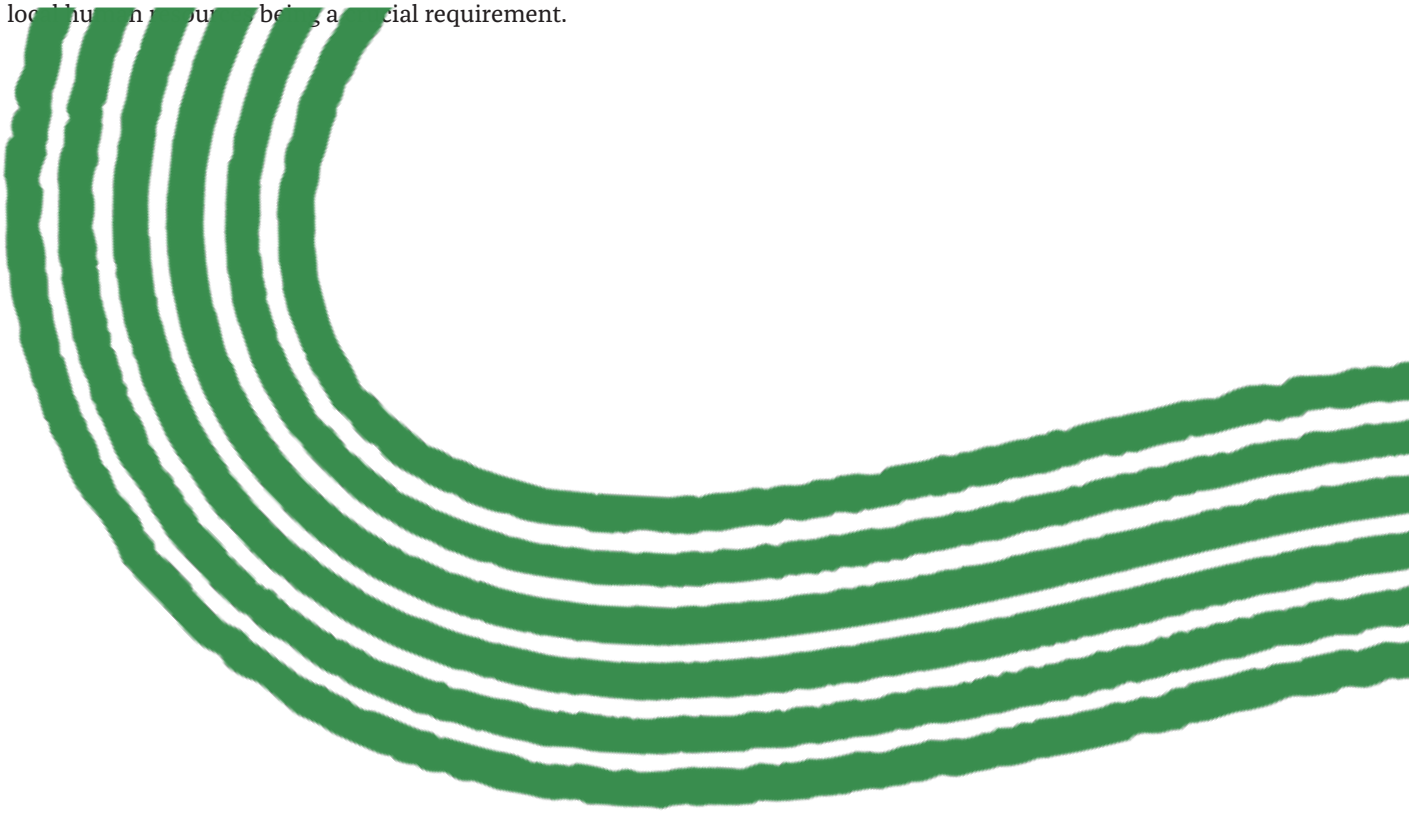
What is Guinea's position on issues related to internet governance, digital rights and data protection in international forums?

Guinea adopted the Law on Cybersecurity and Personal Data Protection in 2016. It has incorporated most of the agencies for the promotion, regulation and management of issues related to cybersecurity, internet governance, etc.

Nevertheless, it is the internal implementation that remains problematic. The state is failing in its efforts to adopt implementing decrees; to set up authorities, notably those that are supposed to be independent or joint; and to finance activities. The political situation that prevailed between 2020 and 2021 did not help matters, since the tensions linked to the opportunistic revision of the Constitution and the presidential election led to major violations of the law, in the broad sense,

and of the law relating to telecommunications (major cuts in free access to services, opportunistic cuts to the internet) and data protection. Critics have denounced the pressure put on operators, the misuse of data collected for biometric identification of populations in the framework of civil status or financial inclusion projects, and the presence of companies known for illegal surveillance of communications and citizens.

Overall, under the exceptional regime that has prevailed in the Republic of Guinea since September 5, 2021, the situation in these areas has eased significantly. Studies conducted by both Orange and Huawei show that the Guinean market has a minimum potential of US$1 billion of turnover for operators by 2030. It is, therefore, necessary to structure it to the best standards, to equip the territory with digital infrastructures and to promote useful services as well as those with added value. Cooperation, PPPs, and balance in the legal and financial structuring and monitoring of projects will be determining factors, with the training of local human resources being a crucial requirement.



Marc-André Loko, Agency for Information Systems and Digital of Benin: "Benin's digital strategy involves a diversified portfolio of best-in-class partners."

Marc-André Loko is the director-general of the Agency for Information Systems and Digital of Benin (ASIN). ASIN was formed following the merger of the four implementing agencies in Benin's digital sector, including the Agency for Digital Development, of which he has been director-general since 2021. He now manages the implementation of flagship digital projects of the Benin government's Action Programme.

What is the digital development strategy in Benin? How does this strategy intend to close the digital gap that prevails in some parts of the country, and how does this strategy fit into the broader African regional picture?

The digital component of the 2016 Government Action Plan was built in collaboration with Monitor Deloitte. The new 2021–2026 plan builds on this and becomes the new framework. This new strategy is to be driven by a new, more homegrown focus on the adoption of digital services. Some aspects of the plan have progressed more rapidly than others. One such area is digital payment infrastructure and platforms as well as projects related to financial inclusion (including mobile money). Building digital skills and entrepreneurship are key priorities if we are to achieve our vision for the benefit of our people. Integrating into the regional context remains a major challenge. We do not have the same frameworks. Benin has a digital code, for example, which covers all the levers needed to put digital at the service of other sectors. In Benin, the digital code was drawn up in collaboration with Jones Day and includes the legal and regulatory framework for electronic communications, cybersecurity and personal data protection. Cybersecurity is the field where there is the most collaboration at the regional level, and the synergy is particularly strong. In terms of digital infrastructure, ECOWAS has brought states together to work on the interconnection of fibre-optic infrastructure. Similarly, in the field of education and research, the West and Central African Research and Education Network promotes synergies between countries on higher education research matters. This facilitates networking among teacher-researchers, particularly in teaching. Having a common infrastructure on different themes makes it possible to link the different education and research networks of these countries in West and Central Africa. Finally, the Smart Africa organization is financing the digital identity project, for which Benin is the project lead. This project will, among other things, put in place a framework for the interoperability of identification data in a secure way, and a technical solution to enable citizens of one country to subscribe to mobile services in another country with their national identity, notably Senegal, Togo and, soon, Ghana.

What is the role of external partners in the development and implementation of this digital strategy? Who are the main partners? What is the role of China, which seems to be particularly active both in terms of supplying equipment and developing digital infrastructures?

The partnerships we have can be grouped into two categories. The first category are those that complement our strategic objectives through partnerships to develop expertise, as with Estonia and Rwanda, with which Benin is developing a long-term approach. They provide solutions (including e-government) that we implement with technology companies such as Cybernetica and eGA. The other category consists of business-oriented partnerships that are set up through specific projects included in our project specifications. Here, Chinese companies are privileged partners because they provide financing (Huawei or CITCC [China International Telecommunication Construction Corporation] via China Development Bank [CDB] and the Export-Import Bank of China, for example) and offer favourable debt payment deferrals. We also have partnerships with companies certified by Microsoft and Oracle. Feasibility studies for infrastructure projects have often been commissioned from French companies such as Sofrecom, Tactis or Horus. This allows us to benefit from French skills and know-how. As far as its digital strategy is concerned, Benin is developing a diversified portfolio of best-in-class partners. Among them are Tunisian firms such as Digitalis or MGI BFC [Business & Financial Consulting] providing economic studies on digital service adoption and economic models such as public key infrastructure (PKI). This South-South

collaboration was strengthened in 2021 by the implementation of the delegated management contract of the Beninese digital infrastructure company with Sonatel, the Senegalese telecom operator and subsidiary of the Orange Group.

How are these contracts negotiated? What about the transfer of technology and skills in these contracts?

In general, China is a flexible partner in negotiations, provided that one has a robust and structured negotiating team. Beyond the global challenge of competing technological standards, there is a sense that they are eager to do business, which leads them to be less rigid. Chinese companies also have local subsidiaries established in Africa with which we can dialogue directly. Huawei, for example, puts a lot of emphasis on the skills transfer dimension. This is not the case with a number of Western companies that are more rigid and come with pre-established frameworks into which we are expected to fit. As soon as the project reaches a certain size, Benin uses Western auditing firms such as AMOA from the definition of the project, during its execution and for evaluation after the project.

In addition, the Smart Africa alliance provides technical support, feedback and pilot project expertise, and helps African countries to pool resources. The alliance appears more reactive than the African Union, which tends to be more bureaucratic. Benin, for example, shares its expertise in digital identity, while Kenya shares its expertise in broadband infrastructure. Smart Africa is financed by many private actors. Each country leads a project. They can also help to finance a supervisory firm, but on regional projects.

For the conclusion of contracts, Benin has a public procurement code that incorporates a collective component, requiring the presence of national consultants for the public procurement of intellectual services. It also promotes consortia between international and national partners to reduce dependence. But this practice is still marginal and not deliberate enough, especially for PPP contracts. With regard to the execution of projects, there is a strong presence of local companies to boost the local ecosystem. Issues of change management, training and skills transfer are now systematically included in project specifications and addressed in negotiations with the same degree of importance as financial issues.

There is a lot of rivalry between powers in the digital domain, especially between the United States and China. African countries are also calling for more digital sovereignty. What is your analysis?

It seems to me that the business attitude that I observe in Benin is pragmatic: the enemy of my friend is not necessarily my enemy, at least in the context of concluding contracts. These rivalries are, above all, driven by protectionist thinking. Companies like Huawei are bigger than the European leaders like Ericsson and Nokia combined. For us, the challenge is to accelerate our digital transformation.

We are well aware that there is a global battle around digital sovereignty issues. African countries have identified the cybersecurity risks to which they are exposed, and the war in Ukraine has reinforced this geopolitical reality. Concerted action on a national cybersecurity strategy/policy, particularly for critical infrastructures, is consistent thanks to the regulatory framework in place. All infrastructures and information systems with systemic risks will soon be required to undergo an audit and inspection process. There is also more collaboration between the government structures whose countries are known to be the origin of cyberattacks, notably China.

Public financing that Benin has received is mainly for energy and roads, but opportunities could open up in the current geopolitical context. USAID [the United States Agency for International Development] funding is mainly focused on feasibility studies in the digital sector for digital applications in the health and social sectors, for example.

We have observed in other countries in the subregion that, when it comes to matters such as the implementation of video surveillance projects, rivalries can have an impact on the choice of technological partners. In addition to the factors linked to conditions of financing and technologies used in the equipment, the dimension of digital sovereignty is becoming increasingly important. It is worth mentioning that Benin has built its first tier 3 data centre. This project allowed the Beninese to be trained at the national level, which increased our technical skills and contributed to the progress of our digital maturity. The purpose of this national data centre is to be able to store sensitive data locally for better control of the use of our data.

But there is still a huge gap when it comes to digital sovereignty. This sovereignty requires the acceleration of projects to develop digital skills and facilitate the emergence of Beninese technological players in the digital sector. Strictly speaking, however, this sovereignty is a challenge for all countries: our data is everywhere, and data is trafficked via various international operators and carriers. We are going to invest in our local internet exchange point in order to confine as much traffic as possible to the local level and improve the quality of services to users.

Current efforts are helping to bring this concern of digital sovereignty to the forefront. In the meantime, it is necessary to choose and collaborate with actors who evolve in a legislative framework closer to our own. This will help to reduce our sources of vulnerability.

What is Benin's position on issues related to internet governance, digital rights and data protection in international forums?

Benin will soon ratify the Malabo Convention on Cyber Security and Personal Data Protection, and the Budapest Convention on Cybercrime. The country is aware of these issues and participates in multilateral bodies such as the ITU and the Internet Corporation for Assigned Names and Numbers (ICANN). We do not yet have a lobbying strategy to have more influence on the policy directions. The negotiation teams are not very influential. However, there is an awareness internally that we need to build a strategy and forge alliances. The Ministry of Digital Affairs coordinates these multilateral issues.

Lanre Kolade, CSquared: "The private sector needs to understand exactly what the government requires to find common ground during negotiations."

Lanre Kolade is the group CEO for CSquared, a technology company making commercially driven investments into broadband-enabling infrastructure throughout Africa. Lanre has more than 21 years of experience in the telecommunications industry, spanning both Francophone and Anglophone Africa. Before joining CSquared, he was managing director of Vodacom Business in Nigeria. He also previously served as managing director of Vodacom Business for the western, eastern, central and southeastern regions in Africa.

How does CSquared, as a private actor, partner with African governments to develop digital infrastructure projects?

Our ethos is to build open-access wholesale digital infrastructure for Africa. Historically, this kind of infrastructure has been the reserve of governments to build. It was built in Europe and the Americas by governments. For example, British Telecom laid significant telecommunication and fibre-optics infrastructure as a government entity. Later, the government decided they needed to unbundle the fibre and open access to other operators. Government finance was used to fund those assets. CSquared is trying to replicate the same thing in African countries using private funding. We need government because it is a big player in most of these markets. The only way to acquire right-of-way to access legacy assets like optical ground wire on power infrastructure is through working with government. The choice of who to work with is not up to us. It is about which government is easier to work with.

CSquared's positioning — and particularly one thing that we found, for example, with Togo — is that for us to actualize our mandate, we cannot do it on a commercial basis alone. There must be a PPP component to it, and this is what we have demonstrated in Togo. Governments in a lot of markets tend to hold a monopolistic view about telecommunications infrastructure that they want to protect. However, we are bringing private capital to allow them to do what they are trying to do. We would choose to work with governments that we believe are transparent and with those that we believe are ready to adopt the open-access model, which often challenges the posture of many governments.

Take Niger, for instance, where the government monopoly is still strong. Niger Telecom does everything. In this context, our interest could be misconstrued as wanting to compete with Niger Telecom. The only way we can do it in a place like Niger is if we strike a partnership with Niger Telecom. The government then builds the regulatory framework to switch from their assets being closed to being open-ended. So, in Niger, to build out fibre networks, you need to use Niger Telecom's infrastructure. But in Togo, they have taken a different approach. They decided to set up a wholesale framework. Through our discussions with the digital transformation minister, the so-called open-access rule in Togo was established. Even though the government knew they needed open access, the historical operator there, Togocom, was not giving other partners access to its assets. However, the government felt that they needed to liberalize the country's system and licensed CSquared as an open-access wholesale provider.

Our choice of whom to engage with also depends on alignment with transparency that our shareholders, including the World Bank, Google, Mitsui and Converge partners, demand. We need to make sure that everything we are doing is transparent and that the laws in the country where we operate will facilitate that. We often help the governments to consider these laws. Many countries have already built infrastructure, sometimes with a loan from the Chinese government, they want to use for open access, but they have not commercialized it very well. CSquared comes in to re-educate them and give them a more thorough understanding of the financial aspects of better commercialization. We make it clear to the partner government that we are not coming into the market to take away their mandate. We are only coming into the market to facilitate their mandate and to help them better monetize their assets while maintaining a stake in the entity. Ultimately, this is a symbiotic relationship.

What are the most difficult points to tackle with regard to working with governments to deliver digital projects? What strategies have been useful to deal with limiting factors you have found?

I would say the most difficult one from my experience of two years negotiating with the

Government of Togo, for example, is getting government to understand that they need to let go of the highly protective mindset of "This is my asset. You can't tell me what to do with it." Re-education is necessary for them to understand that the private sector is not necessarily anti-government. The private sector is just more transparent. That said, the private sector needs to understand exactly what government wants. If you understand what they are trying to achieve, you can find common ground during negotiations.

In summary, the biggest issue is their inability/unwillingness to let go. Governments naturally tend to be very protective of their sovereign assets. They often do not trust the private sector, but it is important to allay their fears that some private sector partners are only there to extract money out of their country. Rather, we are bringing in foreign direct investment into their country, not the other way around, but any investments must be profitable to attract us to start business there. Governments need to create the enabling environment for private businesses to be satisfied. One thing that I told the Togolese minister of digital economy is that there is nobody that will come into Togo that can swindle the government because they withhold considerable authority and veto power. If CSquared appointed someone who fulfills the expectations of the Togolese government according to the laws, the government retains the power to remove them. While the power of veto is important, and governments must know how to use it, they must also understand that rule of law must prevail and that these powers must be used very carefully.

From your experience, what differences/similarities exist with regard to negotiations in francophone versus anglophone Africa?

I am Nigerian. I am anglophone. But I lived in Benin for two years and in Cameroon for eight years, so I know the nuances of both worlds. Partners from French-speaking countries tend to spend a long time in deliberation without necessarily reaching a compromise. Negotiating changes in a single line of a contract can take a lot of back and forth. There is a lot more deliberation before they get to where they want to go to. On the other hand, English-speaking African partner countries tend to be more direct — what the law says is exactly that. Negotiating contracts is easier because the partners tend to go straight to the point. This might be a legacy of the differences between English versus French legal culture. It takes a special kind of mindset to deal with challenge, but our Paris-based law firm understands the cultural subtleties from both contexts. Importantly, though, understanding the nuances of each of the countries and what they are trying to achieve gets you to a point.

With regard to the outcomes of African government negotiations with local and international partners on large-scale digital infrastructure projects, what are African governments doing right and what is not working, in your opinion?

I think that government coming to the realization that they need a partner is the first thing that is working. They know that they cannot do it alone. So, a lot of people are opening their markets to deal with it. But there is a lack of transparency in the way many African governments choose partners. At CSquared, we only want to strike clean deals. On the one hand, in some countries, the first thing they see from our credentials and integrity is that there will be no room for kickbacks or corruption by working with us. On the other hand, for others, having the World Bank and IFC [International Finance Corporation] as backers of CSquared signals access to funding, which can be reassuring.

A lot of governments still believe in ownership by government. But in markets where the government wants to liberalize, then you can understand that. Take Benin, for example, where the government is trying to privatize everything, but that privatization is not a transparent process. In that market, they will tell you they have a tender process, but there is already a predetermined winner. The key point here is that deals are not done in the way we expect them to be done every time.

Considering the geopolitical rivalry in the digital space and issues related to cybersecurity, what is your analysis on how the interplay between these topics has an impact on Africa's digital transformation, both in terms of opportunities and challenges?

I am going to be very partial here because the source of your funding determines what you are aligned to. He who pays the piper dictates the tone. If your funding comes from the West, you tend to align to the West. My shareholders say that I cannot use Chinese equipment, so on our entire network, we do not have any Chinese equipment. When we buy any such assets in any country, we will have to

replace those assets. Unfortunately, that is where a lot of African countries have found themselves.

Should we be non-aligned in this context? I think, yes. But the reality is that we do not have the technology ourselves in Africa. We would not have had phones in Africa without the Chinese. They have democratized the ability to own a cellphone. It was prohibitively expensive when Ericsson, Alcatel-Lucent and others were doing it. The Chinese offered cheaper alternatives, and now we have it. It is a balancing act and difficult to navigate for a lot of governments because if they do not toe the line, they do not receive donor funding.

It is a very convoluted question that requires careful analysis. African countries need to understand exactly what money they are collecting and how they are collecting it.

How do you see the position of subregional multilateral actors (for example, Smart Africa, AfCFTA, ECOWAS, the West African Economic and Monetary Union [WAEMU]) in the delivery of cross-border digital projects (for example, cross-border roaming, terrestrial regional fibre-optic solutions)? What are the major barriers to negotiating these partnerships and some recommendations on how they can be addressed?

Smart Africa, the AfCFTA and the African Development Bank are enablers to these conversations. Because a lot of African countries are members of Smart Africa, for example, when you go and sell an idea to them, you can have multi-country impact. ECOWAS makes it easier to travel across West Africa, which facilitates commerce. The challenge that arises, though, stems from the fact that these multilateral entities already have their own agenda, making it difficult to sell an idea to them. I understand that this is not necessarily because they do not want to be flexible, but because of the need for them to satisfy different interests, which requires extensive negotiations and significant compromise.

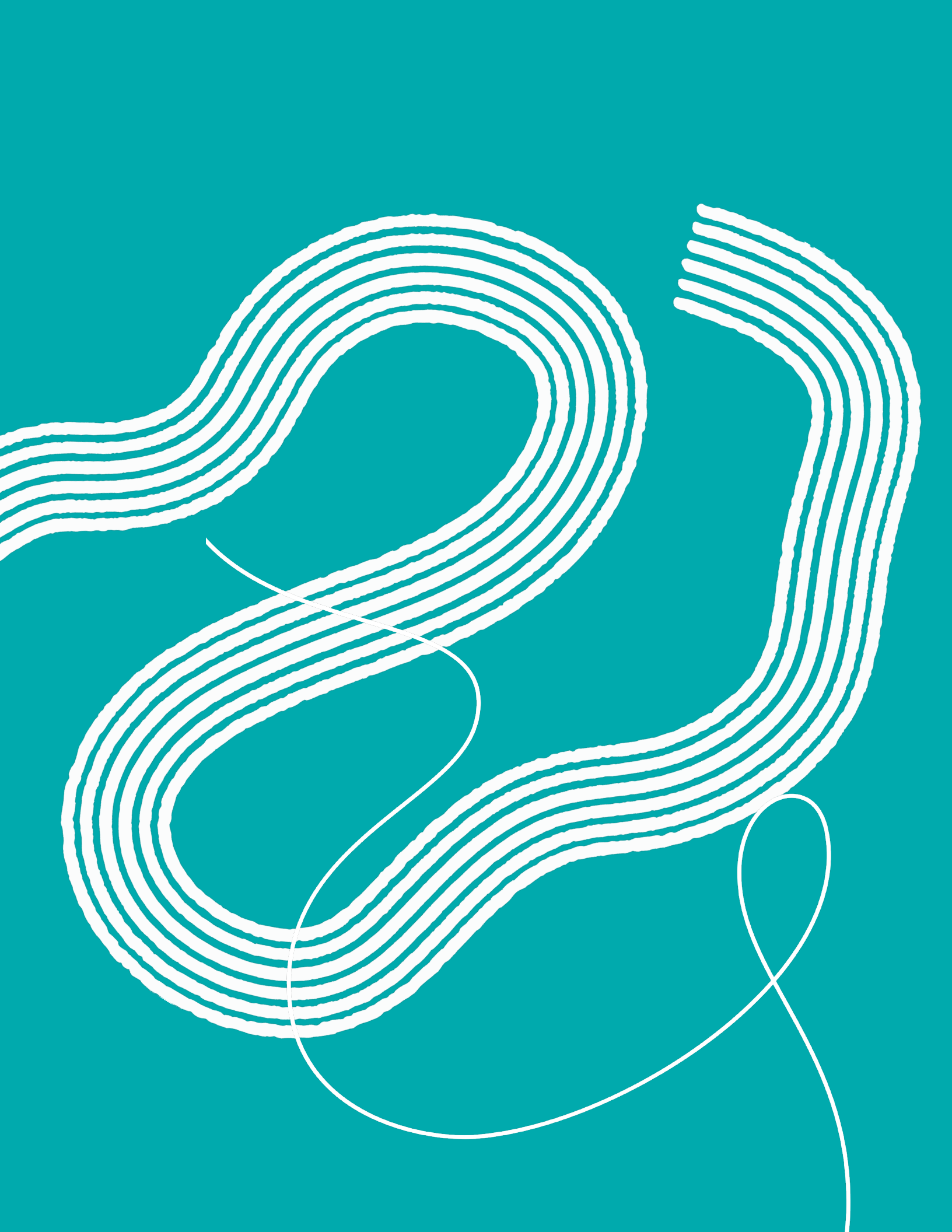
At CSquared, we are currently in talks with the West African Power Pool, a partnership between West African countries who have pulled their power grids together. From Nigeria all the way to Guinea, you have power lines that have fibre capability. If you can deal with the West African Power Pool, you are practically connecting 16 countries at one go. Now, for you to solve that challenge, it might take you two years or even five years, but once you solve it, you would have connected a whopping 16 countries. The disadvantage is that it will take a longer time to come to an agreement because you need to attain the consent of all 16 member states. Invariably, because the fact that they are together does not mean that they don't have their own local nuances and their own agendas.

African Development Bank provides good funding and favourable low-interest rate loans, which are beneficial for us because our investments need what I call "patient capital." Also, having the backing of the major blocs like ECOWAS and Smart Africa, boosts our credibility, making it easier to get into conversations on partnerships and projects. So, for me, there are more positives than negatives when it comes to working with multilateral entities.

In what ways can governments improve their engagements and involvement of African private actors in the governance of the digital sector and cybersecurity?

There are several of them, including clear rules of engagement before you start, fiscal discipline and respect of the rule of law. The regulator should be transparent and working along clearly laid guidelines (for example, on acquiring licences). Clear rules and regulations are important because they make it easy for companies to deal with the government. The other thing governments need to do better is to make sure that once you have a partnership with them like a PPP, for example, there is no risk of arbitrary nationalization of the entity.

Moving on to the second part of your question, the framework for cybersecurity is essential. Every country talks about what they call data sovereignty. It is important that those rules are also clear. Governments need to be bringing the right skills to study this within their unique market and understand exactly how, for example, data centres are going to be operating in the market, what kind of data stays in the country and the cybersecurity initiatives at the national level. While private organizations will have their own cybersecurity rules, the government laying out the right framework for that to happen is critical because the private sector works within the contours of rules they set. So, government must take the lead on that, but they must take guidance from the private sector who have more expertise in the technical aspects than they do.



A digital development specialist at an international financial institution: "Coordination is a critical enabler for integrated digital services and a wider digital economy agenda."

Disclaimer

This anonymous interview has been carried out with a digital development specialist with an international financial institution, where they are providing technical expertise and advice on policy, institutional reform, project development and execution to support the digitization of public administration and public services delivery in client countries. The interviewee is delivering these remarks in their personal capacity. Their remarks do not necessarily reflect the views of the institution.

Regarding the outcomes of African government negotiations with local and international partners on large-scale digital projects, what is your analysis of what African governments are doing right, and what could be done better, in your opinion?

Most African countries are either developing or have developed a national digital development policy and strategy for coherent implementation of digital initiatives across the government. Some countries go a step further to develop implementation road maps to achieve the short-, medium- and long-term country national goals set out in the digital policy and strategy. An example is the Kenya National Digital Master Plan launched in 2022. This is critical to government partnerships with international development partners on large-scale digital projects.

The reason is that by defining a policy and strategy, a country clearly outlines a blueprint that captures its national goals, objectives and priority projects. This helps to see the bigger picture of areas of interventions where [these] will be the most impactful and enable socio-economic growth. Therefore, an international development partner coming into the country must align proposed projects and initiatives to the already defined national goals in the policy and strategy. This enables the countries to reduce the risk of fragmentation and duplication of digital projects.

An area that countries need to improve on is regarding institutional frameworks and coordinating mechanisms among ministries and agencies. More often than not, there have been situations where mandates are not properly defined, and ministries and agencies tend to overlap on implementation, creating confusion on who is doing what. Coordination is a critical enabler for integrated digital services as part of the wider digital economy agenda.

Another area to look at is the rigid and reactive regulatory framework of some African governments, where there is a challenge of how to regulate new and rapidly evolving digital technology. Governments must protect their citizens by putting in place cybersecurity measures, data protection and privacy regulations. In summary, strengthening regulatory frameworks is critical for developing a digital public infrastructure, which has become an aspiration of almost every government.

Considering the multiplicity of donors and the complexity of digital solutions (providers, technologies, service level agreements, interoperability solutions, etc.), how can African governments navigate the geopolitical rivalries and choose the best partners according to their interests?

This is a very complex area to navigate. As mentioned earlier, African governments must first set their strategic priorities and approach for a government-wide digital public infrastructure. Then the government must define an enterprise architecture and interoperability framework leading to the development of a digital platform or government stack comprised of reusable building blocks. Examples of countries that have taken this path are India, Singapore, Estonia, etc.

The next step then would be to leverage the extensive repository of digital public goods (DPGs), which are open-source software, open data, open-AI models and open standards to develop sector-specific digital solutions. The DPGs combine three fundamental characteristics: they are non-rivalrous, non-excludable and globally available. It is important for African

governments to prioritize open-source applications and platforms to avoid vendor lock-in.

Some of our interviewees for this series have mentioned that some deals in the digital sector are poorly structured because those in charge may not know how to execute well. What is your analysis of the pitfalls in executing digital projects on the continent?

Project implementation is primarily the responsibility of the borrower, but the funder provides effective implementation support to improve results, help manage risks and increase institutional development. Unfortunately, country institutions are not always sufficiently developed to undertake project implementation. Particularly challenging may be multi-sectoral projects involving multiple ministries and implementing agencies or projects with new clients lacking experience with the funders' projects.

To mitigate this problem and ensure the borrower can convert investment funds to completed projects, it is important to assign a unit, which ensures that staff are assigned full time to the project tasks. The organization then funds the project management in various ways, including using loan or grant components for project administration. The funder also supports capacity development through advisory technical assistance to the projects. Technical assistance activities consist mostly of training and capacity building, studies and work-plan development.

How do you see the position of subregional multilateral actors (for example, Smart Africa, AfCFTA, ECOWAS, WAEMU) in the delivery of cross-border digital project solutions (for example, cross-border roaming, terrestrial regional fibre-optic)? What are the major barriers to negotiating these partnerships and some recommendations on how they can be addressed?

Alliances and regional organizations, such as Smart Africa, AfCFTA, ECOWAS and WAEMU, have all referenced the need for Africa to create an enabling environment for digital integration and the creation of a single digital market in Africa. The major barrier to this goal is the inconsistency in policies and laws in African countries. Many countries are at different levels of maturity in digital development.

In recent times, Smart Africa has developed a number of blueprints with different member states covering smart cities, smart broadband, digital economy, e-payments, AI, digital ID, etc., to provide countries with a template on how to develop similar policies and strategies in their context. For example, the Sierra Leone National Digital Development Policy, developed in 2021, was inspired by the Kenya Digital Economy Blueprint developed by Smart Africa and the Kenya government.

Another example is the ECOWAS-led initiative of having a subsea fibre-optic cable that will increase international broadband capacity and guarantee redundancy of member states: Cabo Verde, the Gambia, Guinea, Guinea-Bissau, Liberia and Sierra Leone. As part of the memorandum of understanding (MOU) signed by member countries, they affirmed their commitment to sharing policies and strategies in efforts to coordinate the implementation of the project. This regional initiative is captured by the ECOWAS ICT strategy, which identified access to infrastructure and high price levels for broadband as some of the areas that require political intervention/will and appropriate frameworks.

What strategies have proven effective as ways that African governments can work together to achieve consensus and concrete action toward digital goals, especially concerning cross-border digital trade and international infrastructure projects in partnership with the private sector?

Many African member states have elaborated their own strategies and policies on digital transformation, but there is a great degree of variation in terms of the digital preparedness and needs of different African countries. The African Union Digital Transformation Strategy for Africa (2020–2030), which builds on many existing frameworks such as PRIDA [the Policy and Regulation Initiative for Digital Africa], PIDA [the Programme for Infrastructure Development in Africa], AfCFTA, SAATM [the Single African Air Transport Market], etc., has been widely adopted by member states. The document highlights the need for common regulatory frameworks, developing multi-stakeholder African alliances and the promotion of PPPs.

Aside from this, there are also subregional alliances, such as the Mano River Union (consisting of Côte d'Ivoire, Guinea, Liberia and Sierra Leone), which aim to achieve greater unity and solidarity. In 2019, the Union, in partnership with the African

Development Bank, launched a cross-border project for the digitization of government payments that will enhance public resource management transparency, security and optimization.

Are there any best practices that African governments can learn from each other in the process of negotiating digital partnerships with development partners, the private sector and involving civil society in the process?

The best practice is for African governments to develop strong institutional frameworks and coordination mechanisms to ensure their ministries and agencies engage development partners and the private sector with one voice and a common national agenda. Over the last 10 years, I have seen ministries of developing countries with more resources (for example, finance, health, education) engage development partners and the private sector with sector-specific objectives and not the national agenda, thus the government loses on the ability to negotiate for lower prices or volume discounts for services.

Cheikh Bakhoum, Sénégal Numérique S.A.: "Geopolitical rivalries in the digital sector can foster positive competition beneficial to African countries."

Cheikh Bakhoum is the director-general of Sénégal Numérique S.A. (formerly Agence de l'Informatique de l'Etat). He was the head of the IT department of the presidency between 2012 and 2014. Bakhoum is also the director of the Smart Senegal program and led the construction of a national data centre in Diamniadio and the establishment of digital spaces called Senegal Services in all departments of Senegal.

What are the main axes of the digital development/digital transformation strategy in Senegal? How does this strategy fit into the wider African regional context?

At the state level, this is the so-called SN2025 strategy (Sénégal Numérique 2025), which was drawn up in 2016 as part of the implementation of the Plan Sénégal Émergent to serve as a catalyst for modernizing the economy and improving competitiveness. Digital technology is, in fact, one of the driving sectors of the economy and contributes to GDP growth in all other economic sectors. And this transversality must be strengthened for greater productivity.

This strategy embodies Senegal's ambition to maintain its position as an innovative leader in Africa. It is within this framework that the Smart Senegal program, which is linked to the Smart Africa project, has made it possible to put in place structuring digital infrastructures and systems. These include the deployment of a large-scale, fibre-optic network spanning the entire country and interconnecting most of the public sector facilities, and a tier 3 data centre. In addition, our digital strategy focuses on the digitization of administrative procedures, the promotion of innovation through the creation of an innovation laboratory, the development of skills by setting up a Digital Academy, the security of information systems, expanding our undersea fibre-optic links, and developing a national network of Senegalese service centres to provide a one-stop "phygital" shop for the delivery of administrative services in all 45 regions of the country — to name but a few.

How does Senegal choose its external partners in the development and implementation of this digital strategy? Who are your main partners?

In the field of technology, benchmarking is an essential practice, and we regularly practise it at Sénégal Numérique S.A. to find out what the best practices are in other countries to implement them in Senegal, in accordance with the guidelines of our national strategy. In this regard, we regularly interact with partners such as Estonia, the United Arab Emirates, Quebec (Canada), Rwanda and Cabo Verde. The interactions with these partners revolve around issues relating to the digitalization of administrative procedures, digital health, the operation of "phygital" counters, customer experience (to better address the concerns of end users of the public service), the promotion of ICTs among young people, and the launch of an ambitious training program for one million coders over the next three years, among others.

Also, following study visits to Senegal, cooperation projects have been completed or are being negotiated with counterpart African agencies (for example, Niger, Benin, Chad, Cameroon, the Comoros, Gabon, Burkina Faso and the Gambia).

Finally, we collaborate with many other countries, such as France, Germany, Belgium, Luxembourg, Canada, the United States and China, in bilateral cooperation projects. The areas of cooperation are diverse and varied depending on the partner: dematerialization, cybersecurity, geomatics, operating licences and infrastructure deployment, among others.

What is China's role in the development of digital infrastructure in Senegal, particularly in the establishment of the Diamniadio data centre? What are China's comparative advantages as a digital partner?

The SN2025 strategy provides a framework for the reforms undertaken in the digital sector as well as the major projects of the president. Collaboration with China began with the establishment of the connectivity infrastructure now managed by Sénégal Numérique S.A., which connects the various state agencies. The various phases of this turnkey project are financed by an Export-Import Bank loan from China to the Senegalese government.

It must be said that cooperation between Senegal and China in the digital field has grown significantly in recent years. Our two countries have signed several cooperation agreements to promote the development of ICTs in Senegal, notably, the Smart Senegal program, which has led, among other things, to the establishment of a data centre in the new city of Diamniadio, some 40 km from Dakar.

Regarding the Diamniadio data centre, it should be noted that although China's role as a partner was important, it was Senegalese expertise that was at the forefront during all the design, construction and operation phases. Today, all the engineers operating in this state data centre are exclusively Senegalese. In addition to the data centre, we have worked with China as a partner on other projects, such as the deployment of fibre optics, the SHARE [Senegal Horn of Africa Regional Express] submarine cable and the departmental digital spaces, commonly known as Senegal Services.

How is the transfer of technology and skills negotiated in these contracts? What difficulties are encountered and how are they overcome?

The highest authorities of our respective states have steered the negotiation phase according to the guidelines and needs identified. And the experts concerned took over at each phase of implementation. The fact that Senegalese experts and engineers have taken over all the infrastructure developed with China without difficulty shows that the transfer of technology and skills in these contracts is effective. Sénégal Numérique S.A. has the advantage of having all the engineering profiles necessary for the proper management of our infrastructures.

There is a strong rivalry between powers (the United States/China/the European Union) in the digital field, especially between the United States and China. How does this affect Senegal in its digital development strategy?

Rivalries between the two countries can foster positive competition for the benefit of African countries, and thus contribute to their economic and technological development. However, African countries with relatively fragile economies can be adversely affected by these rivalries, which, in some cases, negatively impact their political and economic stability.

As mentioned, Senegal's digital strategy provides a framework for the president's major projects. Given the nature of digital technology, which offers a broad spectrum of infrastructures, solutions and innovative and technological applications, African states would benefit from multiplying and diversifying their partnerships by establishing cooperative relationships with all parties, including those in the same sector. From this point of view, the Government of Senegal maintains partnerships in this field with China, the United States and/or EU countries. We do not note any particular constraint to access other Western partners as a result of the partnership relationship with China. In fact, in many cases, it is these countries that are now coming to us with proposals for partnerships with different funding mechanisms.

We are cooperating with China, through Huawei, on the development of the state's digital infrastructure (data centre, Senegal services centres, optical fibre, safe city, etc.). However, the equipment, applications and other licences are not exclusively Chinese, as Sénégal Numérique S.A. works with other companies, including American firms, notably Microsoft, in the digitalization of the Senegalese administration (for example, through the government messaging system set up in state structures). The EU delegation in Senegal and bilateral cooperation agencies from Germany, France, Belgium and Luxembourg are supporting Senegal Numérique S.A. and the Senegalese government in its policy of digitizing procedures and securing information systems.

Ultimately, this rivalry has not impacted our sector because the state knows how to collaborate with its partners in an intelligent manner. To date, we do not perceive any direct or even indirect negative impact from this rivalry.

At the same time, African countries, including Senegal, are also demanding more digital sovereignty. What is your analysis?

Senegal has always played a pioneering role in the field of ICTs. In terms of digital sovereignty, initiatives are regularly taken to establish this digital sovereignty. The latest act, to date, is the commissioning of the new state resource centre (Diamniadio National Datacenter). During its inauguration on June 22, 2021, the president of Senegal emphasized its essential character in the national digital system, stating: "This infrastructure is the repository of all

these resources and of the billions of data generated in our country, which circulate and are exchanged within our administration, with our partners and users of public services. This is our documentary and audiovisual heritage in a world where the stakes and threats are enormous. This state-of-the-art datacentre allows Senegal to better control its destiny and to definitively resolve the issue of its digital sovereignty."

Thanks to this infrastructure, we can host and secure our most critical data, protect our competitive advantages, make forecasts, learn through AI and big data, compile, recreate and innovate.

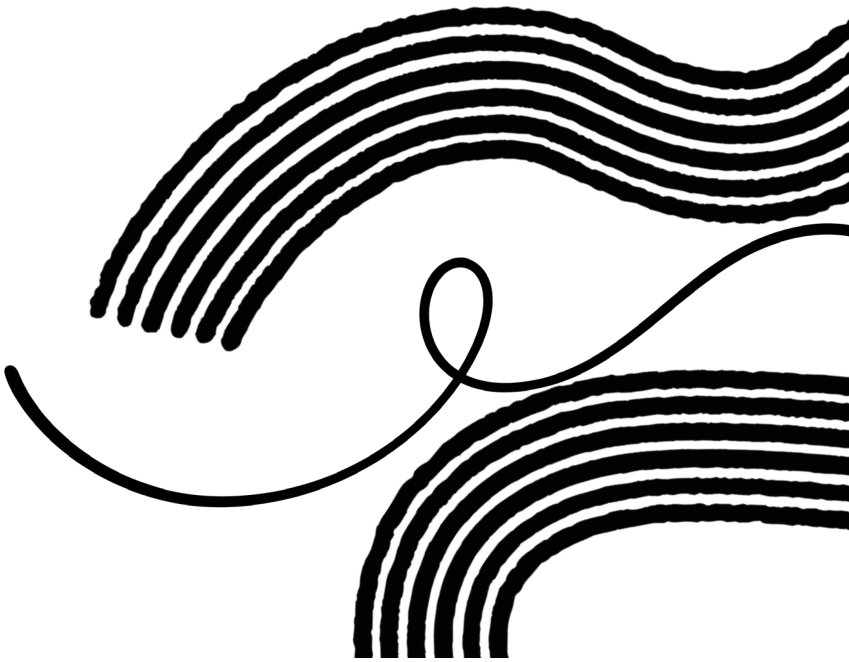
It is for this reason that the president of the republic has firmly instructed the government to host, from now on, all the state's data and platforms in this facility, aligned with international norms and standards, and to proceed with the rapid migration of data hosted abroad or elsewhere. This instruction makes the Diamniadio National Datacenter the primary solution for the country as well as its technical and financial partners.

What is Senegal's position on issues related to internet governance in international institutions, digital rights and cybersecurity in international forums?

Senegal is involved in these issues primarily as an active member of several international organizations that deal with these issues, such as the ITU, a UN agency responsible for regulating electronic communications worldwide. Senegal is also a member of ICANN, a non-profit organization responsible for managing domain names and internet protocol addresses.

With regard to digital rights, Senegal adopted a law on the protection of personal data in 2008, which aims to protect the privacy of citizens in the digital context. Our country also acceded to the Budapest Convention on Cybercrime in 2015, thus strengthening its international cooperation in the fight against cybercrime. It has been represented in various international forums such as the Internet Governance Forum, where it has taken part in discussions on internet-related policies and practices.

Finally, Senegal is collaborating with other African countries to strengthen cybersecurity on the continent. In this regard, Senegal, as a member of the African Union, adopted in 2014 the Convention on Cyber Security and Protection of Personal Data, which aims to fight cybercrime and protect citizens' rights in the digital space. Senegal also participates in regional awareness-raising and capacity-building initiatives on cybersecurity in the West African regional body ECOWAS.



Teki Akuetteh, Africa Digital Rights Hub: "Civil society organizations have the power to hold governments accountable on digital rights enforcement."

Teki Akuetteh is an ICT/telecom lawyer, a privacy/data protection consultant and senior partner at a law firm based in Accra, Ghana. She is also the founder and executive director of the Africa Digital Rights Hub, a member of the UN Global Pulse Data Privacy Advisory Group, and a non-resident fellow of the Center for Global Development. Previously, Teki has worked for the Government of Ghana in the development of several key legislations for the ICT sector.

Compared to the West, African data protection authorities have one-tenth of the average budget to effectively carry out data governance. What recommendation do you have for policy makers negotiating digital partnerships (especially with Chinese firms and Western firms) to bolster their data governance capacities while protecting digital sovereignty?

In terms of funding, it is a tricky issue. Apart from governments negotiating with multilateral corporations like the World Bank and the IMF [International Monetary Fund], it is challenging for governments to negotiate funding for a data protection authority, especially when it comes to dealing with major private corporations. One significant reason for this is that an extremely crucial feature of any effective data protection authority is independence. It becomes even more complicated to negotiate policy or funding requirements for a regulator that is supposed to be independent of the government itself.

So, you realize that under the law, data protection authorities can typically receive support from donor agencies and other corporations. However, this support must be provided in a way that ensures their independence. I would not suggest that governments subject themselves to corporations and request funding to support data protection authorities. Nevertheless, supporting data protection authorities is an essential part of our society, as it enables the protection of individual or fundamental rights.

It is high time that we engage in discussions regarding policy support and the implementation of legal frameworks that benefit the ICT industry as a whole, specifically addressing cybersecurity and data protection issues at the multilateral level. In my experience working with the Ghana Data Protection Commission and as a consultant on a World Bank project, I focused on creating an enabling legal environment for the country, which involved passing several laws. After the laws were passed, we made sure to allocate resources to support the implementation of the legal framework. This process goes beyond policies and laws; it requires substantial resources.

For example, during the second phase of the E-Ghana Project (renamed e-Transform) at the Data Protection Commission in Ghana, we secured funding components from the World Bank to support the implementation of the law. However, it was not deemed adequate due to the significant amount of resources required.

They need a physical space. They need technologies to support them. They need to hire competent staff to efficiently implement the laws. They need to raise awareness because that is also part of ensuring an ecosystem that deeply respects these rights. Having that understanding is extremely important. With that understanding, you can then consider appropriate funding. I must say that sometimes there is a lack of knowledge regarding the actual costs to fund these institutions. Therefore, when creating these institutions, it is important to assess what kind of institution is being built and conduct a cost analysis, so that funding can be allocated before the project starts.

When it comes to how governments engage with corporations, for instance, if a government is hiring a company like Amazon, Huawei or a telco provider to provide specific services and they will be paid for it, I believe we need to include measures such as data protection impact assessments, compliance with data protection and cybersecurity requirements in the work plans. These aspects should be part of the terms of reference or calls for proposals, and companies should be evaluated accordingly. Funding at the government or international organization level is fine, but I wouldn't recommend direct funding from corporations to these institutions. However,

with corporations, we should ensure that they incorporate data protection compliance into the systems or services they are required to deliver.

You recently co-wrote a blog post[26] about upgrading the AU-EU digital partnership. What do African leaders need to be focusing on within the next five years?

I believe that at the continental level, our focus should be on developing a strategy to harmonize our digital ecosystem. This includes frameworks and laws, as one of the biggest challenges we face as a continent with 54 countries and diverse realities is the difficulty of effectively coming together. I strongly believe that Africa has a strong future, and to achieve that, we need a strategy to unite quickly. This is also our biggest challenge as a continent: ensuring that we can come together to accomplish what we need to do. It is crucial and will make a significant difference for Africa.

Take the GDPR, for example. If it were just one or two European countries implementing it, it wouldn't have had the desired impact on data protection. We need to find a way to work around our differences. When I mention harmonization, I'm not talking about uniformity. This is always a challenge for us as a continent, as there's a tendency to seek the same kind of laws when we think of harmonization. However, insisting on uniformity will pose challenges. We should focus on achieving harmonization by working around the differences in our laws and finding common ground where they exist to speak with one voice.

That's the first point I want to emphasize. Secondly, when we discuss the continental free trade area and digital transformation strategies, we need to consider what implementation truly entails. Reading about text data policies, interoperability frameworks and continental-level digital transformation strategies may sound promising, but what matters is the actual implementation. Over the next five years, we should prioritize moving beyond rhetoric and executing these well-designed strategies and plans for the future of the continent.

Lastly, we need to think about what resources in the digital space we have as a continent or, better, that we can claim as originating from Africa. I recently had a conversation with someone who wondered if it was too late for Africa to claim any such digital resource as its own. Their view, although painful, resonated with reality. People on the continent are primarily consumers, benefiting from technologies, platforms, services and infrastructure that originate from elsewhere. For instance, considering digital infrastructure, most of it is not even located in Africa. This made me realize that we need to come up with something entirely different, something that doesn't solely rely, for example, on AI technology that we don't even own. It got me worried because I wondered where we should even start. Therefore, for the overall socio-economic development of the continent, we must think beyond the digital and consider how Africa can carve its own niche, just as the rest of the world has done, and become a driving force for the rest of the world.

On the topic of harmonizing our regulations, are there any common areas that already exist today that represent opportunities for further alignment?

When it comes to data protection laws, most of our current laws already recognize the fundamental right to privacy. Across countries, there is general agreement that this right is crucial and must be protected. So, it's not a point of disagreement. Moreover, many countries on the continent have data protection laws in place, which acknowledge key principles such as safeguarding personal data, lawful processing of information and recognizing certain rights for data subjects. While the extent of these rights may vary, there is more common ground in the legal texts than differences.

Where differences arise is in the implementation of these laws. Countries have varying approaches to implementation, including the level of independence of their data protection authorities and the effectiveness of enforcing the laws. Many laws have been passed to enable enforcement to some extent. Once we identify the commonalities, or what I call the "low-hanging fruits," in terms of harmonization, we can make progress. For example, we don't need all 55 African countries to have data protection laws to respect and recognize each other's data protection authorities.

A notable example is the recent MOU signed between Mauritius and the South African data protection authority. This bilateral agreement

26 See Akuetteh and Pisa (2022).

between the Mauritian Data Protection Office and the South African information commissioner focuses on data flows and transfers. Encouraging such arrangements at the regional level can be facilitated by the African Union Commission. It is relatively easier for countries like Ghana to engage with Senegal, Mauritius or South Africa individually, rather than convening all countries at the same table. Therefore, we should start establishing a network of arrangements or strategies that include MOUs for data movement and transfer, particularly within the continent, aligning with initiatives like the AfCFTA and the single digital market for Africa.

These are a few areas that we can focus on if we want to promote harmonization.

How can civil society fit itself/contribute to the national drive to deliver large-scale digital projects (for example, in infrastructure or software solutions) to ensure digital rights issues are considered throughout project development?

In the last two decades, I have observed the crucial role of civil society, particularly in our region, not only as a voice for the people, but also in holding governments accountable for constitutional and legal rights. How do we achieve this? We advocate for more transparency in processes and better structures and strategies for implementing various frameworks across the continent. Another important role for civil society is research, which is why we established the Africa Digital Rights Hub (ADRH). Through ADRH, we aim to address the lack of government offices equipped to handle digital rights challenges. For example, during my work with the Government of Ghana, I noticed a shortage of individuals with deep expertise in digital rights and the necessary knowledge for implementing laws in the sector, including ICT and telecoms.

Most of the few individuals with expertise in this field have been absorbed by telecom companies due to their higher salaries. To have me on board, the Government of Ghana had to pay me under the World Bank project since they couldn't match the competitive salaries offered by the private sector. This is one of the major challenges we face. Civil society can help bridge this gap, as governments may not be able to immediately change their salary structures or afford to hire all the required skill sets within the public sector. Civil society organizations like ADRH have the opportunity to conduct research and bring in consultants from around the world to delve into specific issues, which governments may not have the resources to do. Non-governmental organizations (NGOs) can also convene stakeholders and shape relevant policies for our ecosystems.

Without these efforts, we see governments signing on to projects where the World Bank's consultancy processes require international competitive bidding due to implementation costs. Consequently, non-Africans often end up implementing these projects in Africa. During my time working for the World Bank, we introduced parameters within our procurement processes to include local context requirements. For instance, if drafting a law in Ghana, the consultant had to work with a local law firm familiar with the legal system to facilitate the process. However, I believe that civil society is sometimes better positioned to work quickly, publish its findings and enable governments to address these issues. They also have the ability to bring stakeholders together, which is crucial for a thriving ecosystem.

In cases where legal frameworks are not effectively working, civil society organizations have the power to hold governments accountable. For example, we've seen strategic litigation in Kenya related to the Duma number, which led to the development of their data protection law. In a continent where the enforcement of rights may not be as progressive as in other parts of the world, and where holding individuals accountable can be expensive, civil society plays a vital role in supporting these endeavours.

With the emergence of other influential pieces of legislation (Digital Services Act, EU AI Act, Digital Markets Act) and the inevitable influence that will have on Africa's governance of the sectors at which these pieces of law are targeted, how much agency do African states have to determine the way they would like to address these topics? How can they increase their agency?

The level of agency that individuals or regions have depends on themselves, as no specific country or region decides for an entire continent. However, having agency requires being informed, knowing one's identity and position, and understanding what one wants to achieve. Europe, Asia and others approach Africa because they recognize the continent's significance and how it can benefit their interests. Unfortunately, Africa often lacks a solid presence at the negotiating table, even from a government perspective. Therefore, for Africa to have agency, it needs

a strong position that goes beyond defining a strategy or having a document stating its goals. Concrete steps must be taken to effectively achieve those objectives. This determination of action also shapes the approach to these issues.

As a continent or country, understanding the challenges, the ecosystem, limitations and opportunities is crucial. Simply adopting another region's approach, such as the European GDPR, may not work seamlessly in a different context. African countries are now realizing that implementing the GDPR requires adaptation to their unique circumstances, infrastructure and regional factors. In my view, agency should be closely tied to self-awareness, knowing who you are, and having a comprehensive strategy for approaching these issues.

Hon. Eliud Owalo, Cabinet Secretary, Ministry of ICT and the Digital Economy (Kenya): "Complex negotiations require a more strategic approach."

How does Kenya choose its external partners to carry out its digital transformation strategy (Kenya National Digital Master Plan 2022–2032), especially on digital infrastructure and services?

The government has identified its key priorities in several documents, including the Kenya Vision 2030 economic blueprint, the Kenya National Digital Master Plan, the Digital Economy Blueprint, the Plan (Manifesto), the National ICT Policy 2019 and the Bottom-Up Economic Transformation Agenda. These priorities aim to address various areas, such as job creation, poverty eradication and revenue generation, by expanding the tax base, food security, reducing the cost of living and improving the foreign exchange balance.

When engaging with external partners, the government considers their contributions to these key development priorities. Partnerships can take different forms, including government-to-government collaborations, engagement with development partners, PPPs and involvement of private partners. To ensure proper funding and implementation of digital infrastructure and services, the government follows a consultative process and has secured a pathway for funding. This process involves procurement and engaging with relevant stakeholders.

Furthermore, all government projects undergo a public investment management process, which includes project identification and conceptual planning, feasibility and appraisal, project selection for budgeting and other necessary steps. This process helps ensure effective management and allocation of resources for government initiatives.

China has been a key partner in Kenya's digital transformation strategy. What are the key incentives for the Kenyan government to engage extensively with China?

China is one of Kenya's strategic partners in its digital transformation journey. Kenya is committed to collaborating with various development partners to achieve its development agenda, always prioritizing Kenya's interests in these engagements. Through the partnership with the Government of China, Kenya has successfully implemented and expanded its ICT infrastructure. This includes the establishment of fibre connectivity, the Konza National Data Center and the development of smart-city facilities.

Additionally, Kenya has also benefited from partnerships with other development partners, including with France on the implementation of the National Optic Fibre Backbone Infrastructure Phase 1 through SAGEM; with Belgium on the Last Mile Connectivity Project facilitated by Soulco; and with the United States through Google's connectivity project. These collaborations with various partners have played a significant role in advancing Kenya's digital infrastructure and connectivity initiatives.

How to best negotiate digital projects with external partners? What are the best practices in terms of technology transfer, local employment, and local content and data protection? Please provide examples.

All the digital projects pursued by the Government of Kenya are aligned with our key priorities. The Government of Kenya handles negotiations proactively. They are based on the government's strategic plans and other guiding documents. It does not simply react to moves by other parties. While this approach may work in many cases, complex negotiations require a more strategic approach. Considerations for such negotiations include starting with a plan, identifying limits and boundaries, understanding the external partner's motivations, building solid relationships, being flexible and recognizing that hard stances rarely achieve much.

In the case of PPP projects, there is a dedicated department at the National Treasury. Furthermore, all projects are guided by the public investment management processes, ensuring proper oversight and management.

The effectiveness of these practices ultimately depends on the specific industry and context in which they are implemented. However, some general best practices are applicable.

In terms of technology transfer, it is crucial to incorporate a strong component of local capacity building into project implementation. This ensures a clear understanding of the

technology and strengthens the internal capacity to support it. Attention should also be given to proprietary licences, intellectual property (IP) rights and the establishment of proper agreements between the involved parties.

Promoting local employment opportunities and the use of local materials is a requirement during project implementation. The government encourages youth to pursue technical-vocational courses to prepare for these opportunities. Additionally, efforts are made to create a diverse and inclusive work environment that respects local customs and practices. It is important to identify and collaborate with local market and service providers to promote local content whenever possible. This not only creates local jobs but also contributes to the development of the local economy. It is essential to establish realistic and achievable local content requirements and provide adequate support to the local market to meet these requirements.

Since the enactment of the Data Protection Act in 2019, compliance with data protection aspects has become a legal requirement. Organizations must implement robust security measures, such as access controls, encryption and regular backups, to protect data. Data policies should align with relevant legal and regulatory requirements. Regular training for staff on data protection best practices and security threats is also essential, and guidance can be sought from the Office of the Data Protection Commissioner.

Overall, the key to effective technology transfer, local employment, local content and data protection practices is to collaborate with local communities and stakeholders, understand their needs and priorities, and tailor interventions accordingly. This approach builds trust, promotes sustainability and delivers long-lasting benefits for all parties involved. Kenya has ongoing bilateral agreements with countries worldwide, development partners and the private sector.

What is the Kenyan government's approach to digital sovereignty? How to best push forward the establishment of digital norms and digital governance on issues like cyber surveillance?

Digital sovereignty for Kenya is an important factor, as is the case for territorial integrity. This is so because it gives us control of our digital infrastructure, systems and data. This ensures the protection of our national security, economic security and individual privacy. It also gives us power as a country on how our data is used.

Kenya's approach to digital sovereignty is through the development of our trusted digital infrastructure that encompasses networks, data centres and applications.

Another approach is to regulate technology partners, guaranteeing compliance with our legal and regulatory frameworks, policies, common standards, best practices and digital norms for the digital world. Kenya also advocates for cyber diplomacy, building trust among nations and fostering cyber hygiene.

However, several challenges persist, including the high costs associated with developing and maintaining our digital infrastructure, difficulties in regulating technology partners based outside Kenya, and non-compatibility between national laws and international standards. Despite these challenges, digital sovereignty remains a crucial objective for many countries. As the digital world becomes increasingly interconnected, it becomes essential for nations to exercise control over their digital infrastructure and data. Several examples demonstrate the growing importance of digital sovereignty around the world. The European Union has implemented various initiatives to enhance digital sovereignty, such as the GDPR and the European Cybersecurity Act. China has made substantial investments in its digital infrastructure, including fifth-generation (5G) networks and AI. The United States is also working toward strengthening its digital sovereignty through initiatives like the CHIPS Act (Creating Helpful Incentives to Produce Semiconductors) and Science Act.

Digital sovereignty is a complex issue, but its significance continues to grow. With the increasing interconnectedness of the digital world, countries must retain control over their digital infrastructure and data to ensure their sovereignty.

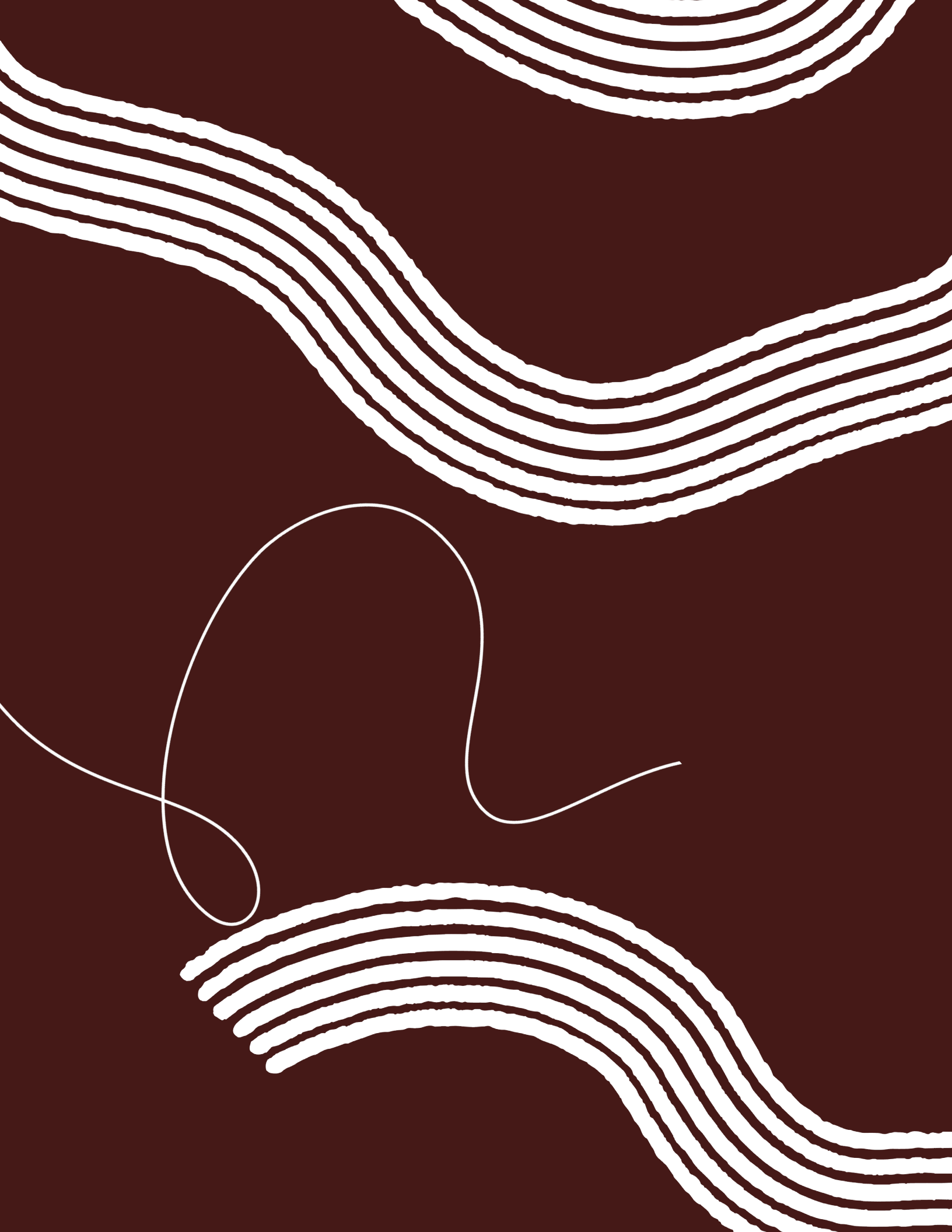
What is your opinion on the geopolitical rivalries in the digital sector, especially when it pertains to Africa? To what extent does it affect the way Kenya carries out its digital strategy? How should African governments manage this rivalry?

My view is that geopolitical rivalries in the digital sector should be managed through peaceful competition. Kenya does not take sides in

technological rivalries. For example, our country enjoys cordial bilateral relationships with both the United States and China. Recently, Kenya successfully hosted the American Chamber of Commerce business forum, where the president announced several mutually beneficial undertakings. As a nation, we remain open to engagement with other countries that are willing and able to provide digital solutions.

What is the Kenyan perspective on data governance debates in multilateral institutions? What bargaining leverage do African governments have in shaping the global discourse on internet and data governance?

Kenya continues to engage multilateral bodies like the European Union and the United Nations on the issue of cross-border data transfer and the need to ensure full compliance with the Data Protection Act. Data governance debates in multilateral institutions are a crucial factor that cannot be left out in the digital transformation agenda of African Union member states. Bargaining leverage for African governments on shaping the global discourse on the internet and data governance can be achieved through dialogue and communication between the state and non-state actors. In these forums, we advocate for our national interests in cyberspace through diplomacy and cybersecurity policies, the protection of human rights in cyberspace and the development of international cyber laws.



Bright Simons, mPedigree: "The geopolitics of standards play a significant role in how innovation-focused organizations can have agency."

Bright Simons, a patent-holding enterprise technology inventor, is the president of mPedigree, an award-winning technology social enterprise reinventing the supply chain on three continents to enhance patient and consumer safety in such vital categories as medicines and agro-inputs. He previously served on the World Economic Forum's Africa Strategy Group. He is also honorary vice president at the IMANI Center for Policy and Education, a Ghanaian think tank dedicated to policy and research on rule of law, market growth and development, individual rights, and human security and institutional development.

As a CEO of an African tech company and patent holder, how does the geopolitical rivalry between the United States and China (and also Europe) affect your business and how you forge partnerships?

Our company mPedigree has operations in China. In terms of our work, we primarily specialize in supply chain transformation. Initially, we aimed to address the issue of counterfeit products, starting with counterfeit medicines. China is a significant source of both counterfeit and legitimate medicines in Africa, making it crucial for us to collaborate with pharmaceutical companies and Chinese technology subcontractors. One of our key contributions is helping manufacturing companies apply unique identifiers, such as RFID [radio-frequency identification] or serialized security labels, to track products as they move through the supply chain. A significant portion of these application technologies is produced in China and India. We procure these tagging technologies from our partners in China and provide them to our pharmaceutical clients in India and China, who apply them on the packaging of products for further shipping to Africa.

Additionally, we work closely with a few large American pharmaceutical companies, but also predominantly with European companies in the pharmaceutical industry, such as Sanofi, F. Hoffmann-La Roche and Novartis. We integrate our solutions with their production processes in various locations, including Morocco, India, South Africa and the United States. In the agricultural sector, we collaborate with companies like Monsanto and Syngenta to track and trace food products in Africa and South Asia. These collaborations involve applying specialized markings or tags to the outer packaging, allowing customers to interact with them and providing valuable supply chain data.

Working with Western companies, especially in terms of IP protection, has presented challenges. While we've tried partnerships with companies like Hewlett-Packard (HP) and Xerox, the complexities of IP balance and market deployment hindered joint efforts. For example, HP was keen on working with us in India but not very much so in China due to concerns of IP leakage. In contrast, we found working with Asian companies more favourable due to their experience with strategic IT alliances and a history of signing agreements that constrain their actions — a strategy I could term as "strategic humility." Europe remains an important market for us, particularly serving European pharmaceutical companies that emphasize quality assurance and inspections in Indian and Chinese factories.

We had to arbitrate between the various conformance expectations between our Asian and European partners. For instance, while the Asians have their own internal standards, they also subscribe to ISO and other similar standards. However, based on our experience, when it comes to the practical implementation of these standards, they are not always as harmonious as they may initially appear. The interpretation of ISO standards can vary based on the environment in which they are implemented. As a result, we have had to navigate these mediation issues between European companies and Indian manufacturers, as well as between Chinese and American manufacturers. This experience demonstrated to us that so-called global standards for traceability and supply chain management like ISO or GS1 can often exhibit Western-leaning hegemonic tendencies and may need updating to stay relevant. Implementing these standards in Africa sometimes faces scrutiny from American consultants and advisers who question deviations from the standard. However, we believe that Africa has been at the forefront of traceability since 2010, evident from our systems enabling tracking of pharmaceutical products from factories to patients in Nigeria. This achievement surpasses what is currently available in the United States or the United Kingdom due to a more streamlined coordination process and a

willingness to experiment and learn. Nevertheless, GS1's growing influence poses challenges as local systems, developed independently, struggle to align with Western-centric models. This issue is apparent in India, Ghana, Nigeria, Kenya and Ethiopia, where efforts to impose GS1-based systems clash with existing local capacities. Geopolitics of standards significantly impact these dynamics, despite the progress made in African and Indian contexts. The influence of global best practices, which tend to be Western-centric, perpetuates the struggle.

In simple terms, the geopolitics of standards play a significant role in our work. The dominance of Western-centric models, particularly in global standards like GS1, can hinder local innovations and impede progress. Africa and India have made strides in traceability and supply chain management, but the challenges arising from Western-centric perspectives persist.

Considering the clash between international standards and local standards that are developing independently, are there any avenues for African tech companies to benefit from this situation? How can they seize these opportunities, and what precautions should private sector actors take, based on your experience?

Let's focus on the discussion about fintech and innovation in Africa. Fintech is the fastest-growing segment of digital innovation on the continent. In terms of the payment ecosystem, there are big players like Mastercard and Visa, which are heavily influenced by Western, predominantly American, standards and regulations, particularly regarding anti-money-laundering and counterterrorism measures. These standards are designed in the West and therefore gravitate toward Western-centric interests on what is considered risky for the financial system. International watchdogs such as the Financial Action Task Force (FATF) operate on these standards.

The FATF's grey listing of Nigeria and South Africa thus introduces complexities for African fintech startups. When entrepreneurs in Africa try to build fintech startups, they face challenges when connecting to the global systems dominated by these big players. Furthermore, since the databases and risk management systems are designed based on Western standards, local startups without significant investment struggle to operate. Without a robust venture capital ecosystem in Africa, many early-stage fintech companies struggle to scale and compete with well-funded players.

To overcome these challenges, African startups have two options. They can focus on areas that are not easily platformable, such as health care, agriculture, education and national security. By building local platforms that cater to specific needs and contexts, they can operate more efficiently and at lower costs. Alternatively, they can embed themselves in global practices and seek investment from Western venture capitalists who understand the Western-centric risk-reward functions in highly platformable areas like payments and financial services. While embedding in global structures can lead to rapid scaling, marketing and fundraising challenges may still arise.

However, it's important to note that the global landscape is changing. As digital platforms become more dominant, there is a growing tension between global platforms and local solutions. The introduction of standardized taxation and regulatory systems, driven by organizations like the OECD [Organisation for Economic Co-operation and Development], may level the playing field and make it easier for global platforms like Facebook or Google to enter local markets and out-compete smaller players. Therefore, African startups need to consider the evolving landscape and find the right balance between local innovation and global integration.

Another side of this clash between local and international standards, and opportunities for African startups, has to do with the role of the public sector in platformization efforts. In areas such as social media and digital connectivity, the public sector is increasingly regulating these platforms due to concerns like addiction, cyberbullying and illegal content. The question remains as to whether regulation may slow down the degree of platformization in these areas. What we have done at my company is that we have found ways to work with the government and embed regulatory measures into their architecture from the beginning.

For example, we developed a platform for agricultural data management called Agrotrack in collaboration with the Common Market for Eastern and Southern Africa (COMESA), a large regional bloc made up of 21 African member states. Our aim was to establish a regional platform that enables seamless digital data flow and analysis

to address concerns like food security and quality across borders. After a successful trial in Kenya, COMESA requested for the platform to be extended across the bloc. By integrating seed regulators like the Kenya Plant Health Inspectorate Service into the system, the platform ensures that agricultural products meet regulatory standards right at the start. They issue the certificate of seed quality that is used by the platform and that farmers can verify. This approach, which I would refer to as "over solving," reduces friction that we might have encountered if we had opted to do it alone and navigate regulatory obstacles as they emerged. My view is that social innovation platforms often need to over solve from the beginning, anticipating regulatory pressures and incorporating public sector elements into their models. It also creates a feedback loop between farmers, regulators and the platform, reducing issues such as low-quality products and improving issue tracking. The over-solving approach may initially be slower, but offers more stability and reduces fluctuations as the platform scales.

By contrast, traditional global platforms aim to "under solve" problems and maximize returns. It is a limitation of global platforms that African entrepreneurs must be aware of and seek opportunities to arbitrage. This involves identifying areas where over solving can provide unique benefits and creating digital extensions or specialized services that exploit these under-solving tendencies of global platforms. African entrepreneurs with a deep understanding and mastery of the specific needs and challenges of local contexts can bridge gaps between local and global networks, and create opportunities for collaboration between the public and private sectors.

In the context of geopolitical rivalry, efforts have been made to convince major global players to partner with local entrepreneurs in extending their services. Management approaches to over solve or under solve can be seen in the Chinese-American dynamic. Take the payments industry, for example: to avoid direct involvement in highly domestic and sensitive mobile money markets, firms like Mastercard and Visa strike agreements with local entrepreneurs who create digital extensions to bridge the local mobile money system to their global platforms. Meanwhile, considering the case of Alibaba in e-commerce reveals that the success of their approach in Africa lies in their ability to over solve issues specific to African commerce operators, rather than relying on the over-standardization of platforms like Amazon. By designing around risk, developing escrow mechanisms and providing innovative management approaches, Alibaba has found success in Africa. African entrepreneurs can identify arbitrage opportunities that align with the specific needs of their region. I think that these opportunities will increase as we go forward.

Regarding the outcomes of African government negotiations with local and international partners on large-scale digital projects (for example, in Ghana, the national addressing system, Ghana.gov, the Ghana Card system, SIM registration and GhanaPostGPS), what are African governments doing right and what is not working, in your opinion?

Well, because I'm an activist, I'm often more inclined to focus on what is not going right. So, I appreciate the fact that you started off with what is going right, which is a brilliant way of getting me to reconsider my routines and think differently. I think what is going right is, first of all, the focus on quality. If we consider the Ghana Card system, it is widely regarded as the highest quality card we've had in a very long time in terms of its features. They have globalized their standards and adopted best practices in every department. Various companies, including CryptoVision, have come together to create the best-in-class PKI and other necessary components. This reflects the importance of global standards and worldwide collaboration.

However, it's worth mentioning a contrasting example from India. The former Infosys boss Nandan Nilekani, who conceived and was the architect of Aadhaar, emphasized the need to build something specifically for the Indian market, rather than replicating ID card systems from around the world. He aimed to address the unique challenges faced in India, rather than focusing solely on standardization. In Ghana's case, it seems that we have over invested in the solution, partly due to a lack of understanding. The involvement of Moses Baiden[27] was influential in convincing the government to pursue a

27 According to Moses Baiden, Jr., CEO of Margins ID Group, "The [Ghana Card ID system] is run through a public-private partnership between Ghana's National Identification Authority and subsidiaries of Margins ID Group, Intelligent Card Production Systems (ICPS) and Identity Management Systems (IMS)."

particular approach, resulting in a project cost of $1.2 billion. However, there are concerns that this cost may double due to ongoing cost inflation.

One of the issues we face in Ghana's policy making is the lack of proper documentation and understanding. Parliament has not thoroughly reviewed the matter, and there is a potential for a significant problem in the future. Cost inflation may lead to tensions between the government and the private sector. For example, the private sector claims that the government owes them $170 million, and they have withheld 3.5 million cards to prevent their use. This situation demonstrates a vendor lock-in problem, where the system cannot be operated despite payment to the vendor. The lack of operational capability stems from disagreements or other issues including non-payment. This highlights the complexities of the PPP model and the outsourced nature of the system, especially considering the security, privacy and data protection concerns involved.

It is concerning that most of the data is stored outside Ghana and is in the hands of the contractor. Although the contractor may be brilliant, they played a mostly integrator role in managing the challenge of the lack of top-notch in-house engineers, which complicated the initial stages of the project. The ownership of critical IP also raises issues. Ghana's attempt to build value-added steps on top of the system has faced resistance from various quarters. For instance, the Ministry of Communications has opposed using the system for SIM card registration due to its preferred vendor. This has led to multiple competing private sector players in Ghana's digital space, depending on which government department favours them the most.

While private-sector involvement in building the country's digital infrastructure and ecosystem is not inherently bad, it requires careful governance and clear policies. In the United States, for example, the defence industry is private, but laws and policies ensure they are subservient to the state when it comes to risk management and critical decision making. In Ghana's case, such control and oversight seem to be lacking. Consequently, there is a lack of strategic flexibility on the part of the government, and issues of system abuse and policy vacuum have emerged. Access control policies, as well as rules and regulations for data access, are not properly established or documented, leading to challenges in enforcing proper testing and accountability, such as determining who has access to certain data or call records.

In summary, while there are positive aspects, such as the focus on quality and global standards, there are significant challenges and shortcomings in the implementation of the PPP model for the Ghana Card system. Lack of documentation, strategic oversight and clear policies has resulted in potential problems and vulnerabilities. It is essential to address these issues to ensure effective governance, protection of data and proper functioning of such systems.

How can civil society place pressure on governments to invest more in data privacy and governance issues? What are the stakes at hand, in your view?

I wrote an article recently in which I discussed a concept called "transmutation" (Simons 2021). However, I admit that I haven't defined or operationalized it well. Transmutation refers to a valuable concept that challenges the traditional understanding of intermediaries. While most people perceive intermediaries as maintaining stability, some types of intermediaries go beyond their role and focus on preserving the system. These intermediaries, known as transmedia intermediaries, are better suited for society and non-private/non-public actors.

As an activist, I have often played the transmedia role in the systems I've been part of, such as in Malawi, where I was deeply involved in policy design and prioritizing the common good over immediate private sector interests. It was not an easy position, as it required shifting focus and dealing with conflicting priorities. Generally, people in society and the non-profit sector rely on different types of non-profits. If you primarily serve as a service provider in the non-profit sector, you also have vested interests. However, if you work as a systems builder in the non-profit world, you can adopt a transmedia role.

Transmedia intermediaries are crucial and can be exemplified by organizations like GS1, an international NGO that acts as a treasurer and uses standardized strategies to bring together private and public actors and find solutions that benefit everyone. With the rise of platforms and the need for critical thinking and objective analysis, transmedia intermediaries are essential, especially in areas like agriculture and health. During the

COVID-19 pandemic, we witnessed collaborations between Mastercard, AfricaCDC, Afreximbank and the creation of the Africa Medical Supplies Platform, which aimed to address health-care supply shortages. Although Mastercard played a catalytic role, it couldn't fully transition from an intermediary to a transmedia entity due to limited influence over other parts of the system. Nevertheless, the platform highlighted the need to extend platform logic to bridge existing divides.

The new digital divide encompasses aspects of our lives that cannot be fully addressed by platforms but still require platform plasticization to increase efficiency, transaction efficiency and reduce costs. For instance, the Africa Medical Supplies Platform had the potential to cut health-care delivery costs by allowing continent-wide procurement and leveraging bargaining power to reduce medicine prices. However, achieving this requires more than just intermediaries like Mastercard. Transmedia intermediaries are necessary to maintain system stability by actively engaging governments and lobbying for collaborative efforts, as demonstrated by the challenges faced in Nigeria's political landscape.

To solve these complex problems, a polycentric and multi-stakeholder approach is crucial. The presence of transmedia intermediaries becomes instrumental in maintaining system stability and addressing gaps. Societal groups need to recognize and embrace the role of transmutation, similar to how organizations like ICANN operate as transmedia entities in specialized areas. The internet itself is managed by a private entity functioning as a transmedia intermediary, although in highly contained contexts. Acknowledging and leveraging this role can significantly contribute to addressing various challenges.

Timiebi Aganaba, Arizona State University: "Space governance is an area where Africa could punch above its weight."

Timiebi Aganaba is an assistant professor of space and society in the School for the Future of Innovation in Society at Arizona State University. She previously worked for the Nigerian National Space Research and Development Agency.

As an adviser on the first legal team of Nigeria's space agency in 2006, how were partnerships established back then? Which countries were key to Nigeria's space program development? Tell us more about Nigeria's negotiation processes and strategy back then. Were there specific challenges, and how were these addressed?

I was a trainee in the Legal Affairs and International Cooperation department of the Nigerian Space Agency in 2006, as a requirement of my National Youth Service Corps. I was part of the first legal team of the agency, and it was a very interesting experience. Nigeria's space ambitions date quite far back. In 1987, the Federal Ministry of Science and Technology (FMST) created a national committee on space applications. In 1993, the National Agency for Science and Engineering Infrastructure set up a committee to develop a draft space policy and, in 1999, a National Space Research and Development Agency (NASRDA) was established.

NASRDA conducted an open international competition for its first satellite, the NigComSat-1 using Telesat Canada, a Canadian company, as an intermediary, and if I recall correctly, received 21 expressions of interest from American, European, Russian, Israeli and Chinese companies. China Great Wall, a Chinese state-owned enterprise, was the only bid received by the deadline that met the specifications. This was a significant deal as it was China's first satellite export sale. Included in the contract was the satellite, based on China's DFH-4 platform, the launch, insurance and a technology-transfer package, a capacity-backup provision and options on future satellites.

Nigeria was also an early adopter for the United Kingdom's small satellite offerings, developed by the UK Surrey Satellite Technology Limited (SSTL), supported by the British government. SSTL made an optimistic statement that the NigeriaSat-1 satellite it built, with Nigerian engineers, earned 3.87 million naira (£16,400) in royalties in the first six months of commercial operations of the satellite developed as part of the Disaster Management Constellation. They use the example that NigeriaSat-1 was the first satellite to share images of Hurricane Katrina in the United States, a feat described by the United States as a "proud achievement" for Africa.

I will highlight two challenges from both satellite deals with the Chinese (NigComSat-1) and the British (NigeriaSat-1).

As reported in *SpaceNews* in 2005, the Russian and Israeli bidders were unable to meet the contract terms, and the major manufacturers in Europe and the United States appeared not to believe that the Nigerian government would follow through on the contract work, as well as coping with stringent export control rules. NigComSat-1 ended up failing in orbit due to a malfunction in its solar arrays. The public did not take well to this news. One of my first tasks was to write a legal opinion on a loss of the satellite, at the launch site, but I certainly underestimated what the effect of an in-orbit loss would mean in terms of morale and the ability of Nigerians to begin to adopt this solution, rather than remain with trusted foreign offerings.

Another challenge arose with the Earth observation satellite. According to Adigun Ade Abiodun, founder of the African Space Foundation, the purchase and sale agreement between the Nigerian FMST and the United Kingdom's SSTL signed on November 7, 2000, in Abuja, Nigeria, stated that "FMST shall not remove or alter any copyright or other proprietary on any of the know-how." According to Abiodun, this clause foreclosed Nigeria's ability to modify the design and software codes it was to receive from SSTL, codes which are very critical to a successful technology transfer and subsequent technology development in Nigeria. The issue at hand is that it is the buyer's responsibility to obtain the rights to use the software in the way it is needed, but while commercial off-the-shelf software licences rarely grant a right to modify, pre-2000, one could say these exchanges were still "experimental," and so could have been possible (Flynn, Buffington and Pennington 2020). The Canadian International Development Research Centre (IDRC) model could have worked well in this instance, whereby as part of Canada's foreign affairs and development efforts, IDRC champions and funds research and innovation within and alongside developing countries. In the IDRC model (Bhagavan 1997), when a promising

technology is still under development and testing in the Global North, its usefulness and capacity to help solve development problems in the Global South can often be explored. IDRC believes that an efficient way to prepare people to use a technology is to encourage their participation in its early fine tuning. This seems a more "honest" approach.

Rwanda and Nigeria have signed the US deal on space governance at the latest US-Africa summit in Washington, DC, in December 2022. What is your analysis of the geopolitics of space, and how can African countries best navigate these?

These two countries came up in the global space arena at very different times and "eras" of space, so I refer to them as Traditional Space (Nigeria) and New Space (Rwanda). According to the European Space Agency, there have been four eras of space:

> "The first era of space, 'Space 1.0', can be considered to be the early study of astronomy (and even astrology). The next era, 'Space 2.0', came about with spacefaring nations engaging in a space race that led to the Apollo moonlandings. The third era, 'Space 3.0', with the conception of the International Space Station, showed that we understood and valued space as the next frontier for cooperation and exploitation.... Space 4.0 represents the evolution of the space sector into a new era, characterised by a new playing field. This era is unfolding through interaction between governments, private sector, society and politics."[28]

In 2020, the Government of Rwanda formed the Rwanda Space Agency and thus arose Space 4.0 (Walker and Mendler 2022). However, Nigeria's history in space goes quite a bit further back, as mentioned above, to the Space 3.0 era.

At the US-Africa summit in Washington, DC, in December 2022, the first US-Africa Space Forum was held. The United States is currently on a global endeavour to promote a governance regime to guide all the new proposed activities on the Moon in the coming decades, and an agreement known as the Artemis Accords was presented at the forum, with a signing ceremony of the first African signatories (Space in Africa 2022). As of May 3, 2023, there are 24 signatories. Rwanda and Nigeria, as the first African signatories, will have the opportunity to weigh in on significant topics such as the emerging issue of in-space resources like hydrogen and oxygen derived from ice, and use of strategic areas on the Moon (International Space Exploration Coordination Group 2021).

While some African perspectives (Onwudiwe and Newton 2021) exist with differing understandings of the pros and cons of the emerging governance regime that is unfolding through the Artemis Accords, the topic of the evolutions of international law applicable to space and what such new regimes mean (Aganaba 2022), will expose differing perspectives due to geopolitics. As the Artemis Accords foster new exploitation potentials, commodity integration is a key understated issue based on the developing country experience.

Primary commodities, including mineral commodities, are the major source of income and employment for several developing countries. The relevant question here is: To what markets in the short term on Earth will in-situ space resources apply? This is currently unclear. Missions like the NASA- [National Aeronautics and Space Administration-] led Psyche mission are of interest because they may involve significant amounts of nickel. The rising demand for electric cars is the underlying factor influencing the increasing production of cobalt, lithium manganese and natural graphite, much of which is produced in the Democratic Republic of the Congo (United Nations Conference on Trade and Development 2020). There are specific regimes governing how much they are extracted for and how the value is integrated into the global market. More relevant is that serious early discussions for commodity markets are being discussed at forums such as the US National Space Council Users' Advisory Group (2020), which proposes a strategic in-space propellant reserve modelled on the petroleum reserve. Alongside game-changing applications such as space-based solar power,[29] which would require wireless power transmission, Africa is in a position to ensure that these leapfrogging technologies are accessible.

How can Africa leverage its voice and position in space governance debates?

28 See www.esa.int/About_Us/Ministerial_Council_2016/What_is_space_4.0.

29 See https://sa.catapult.org.uk/projects/space-based-solar-power-enablers/.

There has never been a better time to think about article 3 of the Outer Space Treaty (OST) (the seminal space law governance instrument), which states that, "States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding."[30]

As a developing nation, the question is: What does international law mean and stand for? How does the UN Charter apply in space, and how has international cooperation fared toward the objective of article 1 of the OST, which states that "the exploration and use of outer space, including the moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind."[31]

Space governance may, in fact, be one area that a region like Africa could punch above its weight (Tayeb 2021), because it does not require science and technology mastery. As the current global priority is on space sustainability,[32] ensuring the long-term continuation of space activities, Africa has a lot of heritage to contribute to these kinds of governance objectives.

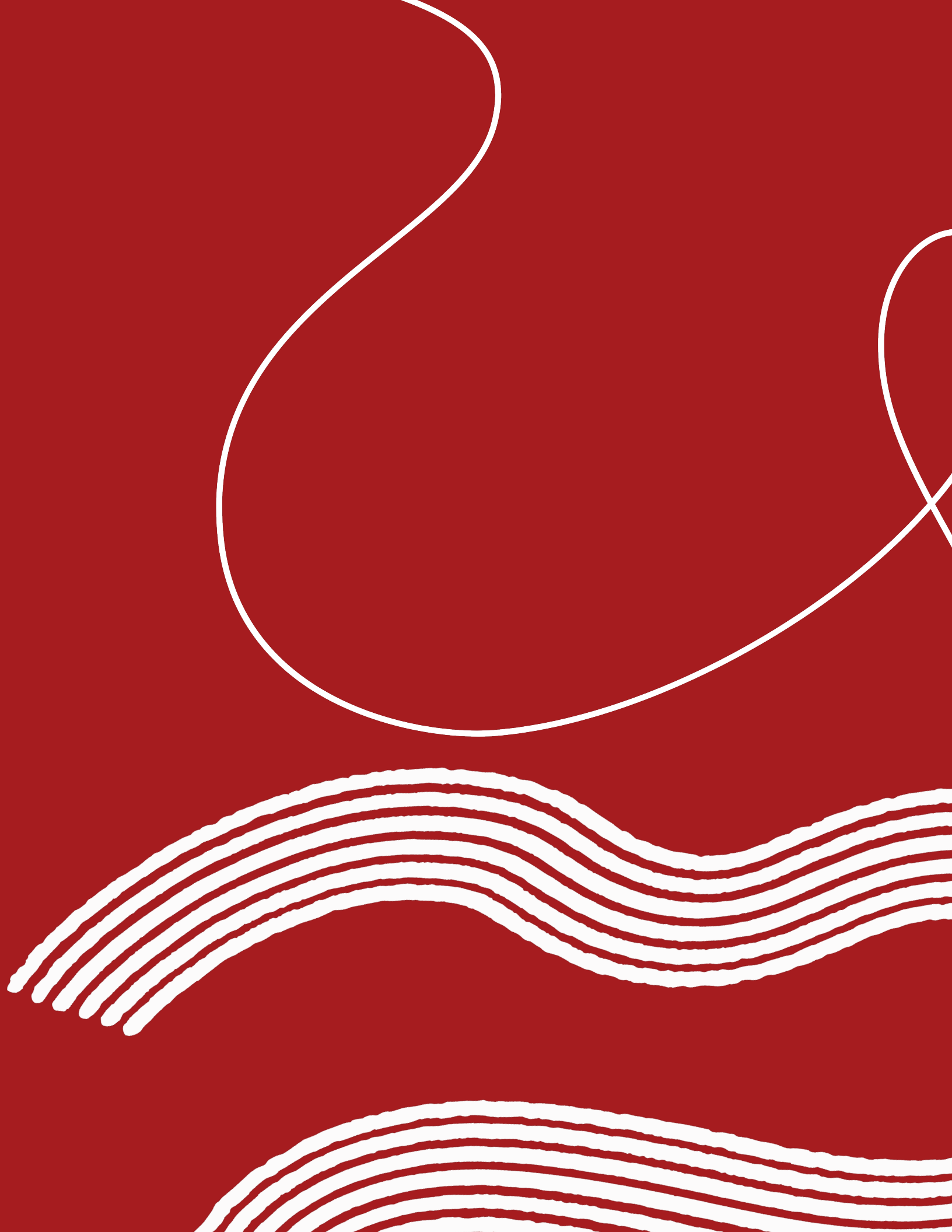
In fact, the first definition of what is now sustainable development, as well as the first Declaration of the Right to Environment, can be found in African governance instruments such as the 1968 African Convention on the Conservation of Nature and Natural Resources, the 1976 Algiers Universal Declaration of the Rights of Peoples and the 1981 African Charter on Human and Peoples' Rights. With the global spotlight on space debris, Rwanda clearly articulates that "Fighting space debris should start from the design of the space object to include smart collision avoidance mechanism and systems to safely de-orbit at the end of the object's mission…[while recognizing that] the trend of low cost/small satellites will tend to oppose the move of additional mechanism and complexity for collision avoidance and deorbiting mechanism" (Rwanda Space Agency 2021).

With 42 percent of global youth expected to be African by 2030, fostering the children, youth and early-career professionals and their solutions will also be important as they give practical insights to addressing issues such as space debris and sustainability (Haroun et al. 2021). Therefore, Africa will need to prioritize education on the continent to prevent brain drain and to future-proof the region. In an editorial in the journal *Science*, my colleague and I propose a space education summit on the continent (Aganaba and Offiong 2022).

30 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, RES 2222 (XXI) art 3 (entered into force 10 October 1967), online: *UNOOSA* <www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html>.

31 *Ibid*, art 1.

32 See https://swfound.org/our-focus/space-sustainability/.



Tin Hinane El Kadi, London School of Economics: "Collective bargaining would help maximize gains from negotiations with leading tech firms."

Tin Hinane El Kadi is a political economy researcher. She is currently writing a Ph.D. thesis at the London School of Economics and Political Science, looking at China's Digital Silk Road (DSR) in North Africa.

How are Egypt and Algeria establishing and negotiating digital partnerships with strategic partners? What is the role of China in their digital transformation strategies?

So far, major negotiations around digital issues have taken place within broader trade negotiations. Both Algeria and Egypt have engaged in trade negotiations on a bilateral basis, whether it is with economic blocs like the European Union or with other countries, limiting their bargaining power. The most contentious point in trade negotiations regarding the digital sphere has been around the free flow of data. Developing countries have increasingly been calling for data localization while global powers like the United States and institutions like the World Trade Organization have been pushing for a global data governance framework that favours the free flow of data across borders.

China is an increasingly important actor in this sphere. Unlike the United States, China has been a vocal proponent of data localization and data sovereignty. Many nations have introduced data governance frameworks that resemble China's. The digital space is a notable aspect of recent China-North African partnerships. Chinese tech firms are becoming ever more important actors in North Africa through the DSR, the digital component of the Belt and Road Initiative. North African governments see the DSR as an opportunity to help bridge the digital divide and bolster their own national efforts to build digital economies and create high-quality jobs for the millions of unemployed university graduates across the region. In recent years, the region has become home to notable DSR projects, such as smart cities, satellite navigation centres, data centres and network infrastructure. So, I would say that China plays quite a significant role in the region's digital transformation strategy.

How are geopolitical digital rivalries between the United States, China and Europe affecting Egypt and/or Algeria, and how do they deal with these rivalries?

Developing countries haven't had to choose between any of these big players so far. Often what we see on the ground is a mix of infrastructures, hardware, software and standards that will mirror the interests of host countries and pre-existing ecosystems and social preferences. Several African countries purchase digital equipment from China because it tends to be of good quality and cheaper than alternatives that Western countries have to offer. Moreover, China provides funding for what is expensive backbone infrastructure. This is an undeniably significant comparative advantage for the globalization of China's ICT industry abroad. Both Algeria and Egypt have avoided picking sides in the current digital rivalries between great powers. Even though the United States has attempted to persuade these countries to stop purchasing Chinese digital equipment, the price competitiveness of Chinese ICT original equipment manufacturers, such as Huawei and ZTE, and the access to loans they both provide through Chinese public banks, has meant that countries like Algeria and Egypt, seeking to expand and update their digital infrastructure, are often left with no other alternatives.

Interviews I conducted with diplomats in both countries have highlighted that not picking sides and continuing to work with whichever firm had the best offer in terms of technology and cost, was the most strategic position for middle-income countries as it allowed them to leverage different powers to achieve their economic, political and security goals.

Both the United States and EU countries are advancing the objectives of decoupling and de-risking strategies when it comes to their technological cooperation with China. How might this affect Africa in the future?

Both the European Union and United States have tried to convince African countries not to use Chinese digital equipment in their infrastructural mix, but they did not have any interesting alternative to put on the table. During the Trump administration, Washington was prompting its Clean Network program. According to Washington, it was a "comprehensive approach to safeguarding the nation's assets including citizens' privacy

and companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party."[33] In practice, they offered loans to developing countries to remove Chinese equipment and replace them with more expensive, but supposedly more secure, US digital equipment. The Egyptian policy makers I have spoken to about this program found it very insulting, considering the huge infrastructural needs of the country. I suppose that the reaction of leaders in other African countries was similar, understandably so.

Huawei is a key choice for several African countries as they build their digital infrastructure. What is the company's strategy?

Huawei has become a significant player in the ICT infrastructure of African countries. An estimate by *Foreign Policy* suggests that Huawei has built 70 percent of Africa's 4G [fourth-generation] network. While this number was challenged by some experts, the reality is likely not too far from this. The shift to 5G will probably also be undergone with Huawei as it is more cost-effective to stick to the same ICT provider.

I believe that Huawei has such a significant footprint on the African market for a set of reasons. First, the Shenzhen-based firm produces high-quality equipment that is cheaper than its competitors' wares. Some analysts have estimated that Huawei's equipment is about 30 percent cheaper than those of its competitors, but estimations vary widely depending on the type of technology. Huawei's remarkable push to internationalize, including its price advantage, can be traced to the financial edge it derives from the Chinese state and the company's commitment to research and development (R&D). Huawei and other Chinese tech firms venturing abroad benefit from access to large loans provided by China's state-backed policy banks, specifically the CDB and the Export-Import Bank of China. For instance, Huawei received one CDB loan to the tune of US$10 billion in 2004 and then received another for twice that amount in 2009. Credit from the CDB allowed Huawei to offer what is termed "vendor financing," which is providing the financial backing for customers to make major purchases.

Second, considerable investments in R&D are a cornerstone of Huawei's global success. The Chinese firm reinvests a far greater share of its profits back into production and R&D compared to US firms like Cisco, which have grown increasingly financialized. This has been especially the case since the 2000s, when Beijing adopted a handful of policies to boost "indigenous innovation" in strategic areas. These policies reflected concerns in the Chinese Communist Party's leadership that its low-value-added export path in the 1980s risked leaving China stuck indefinitely at the bottom of global value chains and vulnerable to the national security implications of foreign-controlled internet infrastructure. In response, new Chinese policies were aimed squarely to support the emergence of competitive domestic actors by offering a wide range of incentives for local public and private firms to enter the digital innovation fray. In this context, Huawei progressively ramped up its own R&D efforts and set out to overtake its global competitors.

Finally, a less-recognized factor behind Huawei's success lies in the firm's capacity to adjust to disparate cultural, political, economic and institutional settings in different regions around the world. The tech giant has flourished in widely varying environments, from democratic Senegal to autocratic Cuba, from the United Kingdom's liberalized telecommunications industry to Ethiopia's state monopoly over telecommunications, and from the stable and prosperous European Union to war-torn Afghanistan. Admittedly, Huawei's operating environment in some of these locations is changing, with the UK government barring the firm from its 5G rollout. Nonetheless, these setbacks reflect geopolitical misgivings more than shortcomings in the firm's technological and business capabilities.

Huawei's bid to internationalize its operations has involved learning and making adjustments. Gaining local knowledge allowed the tech multinational to fine-tune its products on short notice to meet local customers' evolving needs. For instance, in attempting to capture more smartphone market share in Muslim-majority countries, one of Huawei's popular smartphones came with a built-in Muslim prayer reminder function and an app for locating nearby mosques. In Africa and other developing regions where the

33 See https://uk.usembassy.gov/our-relationship/policy-history/policy/the-clean-network/.

need for job creation, training and technological upgrading is pressing, Huawei has emphasized knowledge transfer schemes by creating ICT academies, organizing tech competitions and providing scholarships to outstanding students.

In this context, collective bargaining could be an advantage for African governments. Why, in your opinion, is this not happening?

Indeed, collective bargaining would help maximize gains from negotiations with leading tech firms like Huawei. This could be done by attributing a greater role for African regional blocs. In North Africa, for instance, states could leverage their collective markets to bargain for better deals with Chinese and other foreign multinationals. Moving beyond fragmented bilateral commercial negotiations with China would help level the playing field for all North African governments as they deal with Huawei and other companies whose investments and know-how they hope to attract and harness. However, at the moment, we are witnessing the opposite — more competition between different African countries to attract more tech investments than cooperation, leading in some cases to a race to the bottom. This is often due to political rivalries and domestic agendas, which tend to be short-sighted. In North Africa, the increased political tensions between Morocco and Algeria (largely due to Western Sahara and Morocco's recent normalization with Israel), has made the realization of the United Maghreb impossible. As it stands, the Maghreb is the least economically integrated region in the world.

Several African countries are claiming for increased digital sovereignty. What is your analysis of this? To what extent is this objective effectively included in the negotiation process and implemented in practice?

The success of the Chinese model has inspired other developing countries. With the rapid rise in digitization since the COVID-19 pandemic, several African countries have adopted data localization strategies. It is estimated that roughly 33 African governments adopted data flow regimes that subject data to contractual safeguards, prior authorization or mandatory localization. Countries like Egypt, South Africa, Chad, Senegal, Tunisia, Kenya, Uganda and Zimbabwe have all adopted conditional flow regimes for data protection purposes, with some taking stricter data localization measures than others.

Notably, to achieve greater data sovereignty, Senegal was the first African country to replicate the Chinese data governance model that requires all servers to be located within a country's borders. The West African state moved all government data and digital platforms from foreign servers to a Huawei-built data centre in Senegal. The data centre was financed through a 46 billion CFA francs (€70 million) Chinese loan. But this creates several issues. The danger of relying on Chinese surveillance technologies for African countries' own cyber sovereignty has been somewhat concealed by China's advocacy for data sovereignty in various global digital technology standard-setting bodies. Yet an investigation published by *Le Monde* (Kadiri 2018) showed that confidential data from the Chinese-built African Union headquarters was diverted every night from Addis Ababa to Shanghai. Of course, China is by no means the only power involved in using the internet for spying. US intelligence services have accessed the data of millions of citizens across the world through the help of US tech giants. Ultimately, data sovereignty will remain an elusive goal without building endogenous technological capabilities.

This discussion on negotiations with great powers inspires a serious rethink on that old chestnut: regional integration. Integration will contribute to improving the bargaining power and competitiveness of Africa as a continent in a way that can allow each country to better harness the benefits of foreign investment, in general, and Chinese investments, in particular. Moving beyond the current bilateral relations with China is, hence, a necessary step to help even out the unbalanced relationships of the Asian giant with the region.

Bulelani Jili, Harvard University: "African policy makers should see digital development, data flows and data governance as mutually reinforcing."

Bulelani Jili is a Meta Research Ph.D. fellow at Harvard University. His research interests include ICT development, Africa-China relations, cybersecurity, post-colonial thought and privacy law. He is also a visiting fellow at Yale Law School, a visiting fellow at the University of Hong Kong Faculty of Law, a fellow at the Atlantic Council, a research associate at Oxford University, a former cybersecurity fellow at the Harvard Kennedy School, a former scholar-in-residence at the Electronic Privacy Information Centre and a former public policy fellow at Google.

How do you assess the policies set up by various African countries to pursue "digital sovereignty"?

Digital sovereignty is an analytical aperture and strategic posture that seeks to reassert the authority of state actors over cyberspace, including the development of digital technology. As such, this vision demands the recognition of individual countries' rights to craft and employ the requisite policy instruments to govern cyber activities within their juridical territory. Yet the shifting constellation of global networks and the privately owned technical infrastructure of the internet suggests an opposition to this statist approach. Accordingly, advocates of the concept, on the one hand, seek to recentre the nation-state as the principal vector to govern cyberspace while also wishing to leverage private firms and investment to pursue digital development.

One thread of digital sovereignty is data localization. Briefly, data localization is a protectionist policy measure that may result in marginal gains for some local stakeholders, including enterprises and workers, but it may also cause more significant harm to the broader economy. The benefits of data localization would accrue to the small number of data centre owners and employees who operate locally. However, the wider ecosystem may suffer from limited or poor access to data. Although data centre infrastructure is critical for the use of data for development, many governments focus on forcing firms to store data locally, even though it does not necessarily lead to digital development or better-protected data, never mind the fact that many countries struggle to provide reliable electricity supply and high-speed connectivity. Currently, it is unrealistic to expect every firm that manages data to set up data storage facilities and business operations in every country. Meanwhile, not having domestic controls in place would be equally problematic. This highlights the need for national frameworks and a continental data governance framework. Accordingly, African policy makers need to focus on building both domestic and regional frameworks to harmonize diverse regulatory spaces and enable economies of scale for African firms. Being able to acquire, use and move data seamlessly across borders allows firms and government agencies to provide digital goods and services. Seamless data flow also supports the use and reuse of data within the African data ecosystem, which is critical to leveraging data-driven emerging technologies that empower innovations in public service delivery and new business ventures on the continent. Inversely, restrictions on the movement of data result in the loss of entrepreneurial opportunities.

How do foreign actors like China, European countries, the United States and private actors understand and deal with the local African discourse on data ownership?

In the context of African data localization, China is promoting its notion of cyber sovereignty. Cyber sovereignty can be simply defined as respecting an individual country's right to choose its own digital development path and cyber management policies. Following this logic, state actors should principally discourage the interference of other nation-states in the internal affairs of other governments. Accordingly, this statist approach privileges the ambitions of governments over those of private firms and civil society. And, in turn, this commitment is antithetical to current US commitments. The US government advocates for more open and multi-stakeholder approaches that promote the leadership of private firms and civil society engagement. However, China and its principle of cyber sovereignty is attractive, in part, because it provides legitimacy and cover for state and substate actors who wish to further restrict online activity in the name of political stability. While this push for cyber sovereignty and its seemingly commensurate emphasis on localization ostensibly empowers local stakeholders, it does raise questions about the capacity of African stakeholders to promote

rights against local government abuses and private firms' excesses. It must be said that China's cyber sovereignty commitment does not result in neutral outcomes or even the supposed local empowerment, but it can be an obfuscating frame that loses sight of the technological asymmetries between itself (a power realized through the tightening grip over domestic corporations) and its African partners that come to rely on its technical expertise to realize digital development.

How can regional and international organizations better support a shared vision of data governance and regulation, and cybersecurity in Africa?

Firstly, it must be said that policy makers should see digital development, data flows and data governance as mutually reinforcing, not something that needs to happen sequentially. Of course, digital development only gets harder given that it also depends, in part, on African policy makers addressing other major economic and political issues like urbanization, cybercrime, youth unemployment, poverty and climate change. But, again, rather than conceptualizing digital developments independently from these challenges, policy makers should recognize that digital tools and development can also play a constructive role in addressing them. For example, the COVID-19 pandemic illustrated the significance of free data flows. Free data flows are critical to the management of public health crises. Timely and unhindered access to data has ensured appropriate policy responses that go toward improving health outcomes. Data governance's cross-cutting significance means it should not be segmented or seen as some sort of dislocated aspiration from development goals.

Again, for example, the push for data localization in Africa might have consequences for the trade liberalization ambitions envisioned by the AfCFTA. While the free trade agreement's e-commerce protocol remains to be finalized, data localization requirements have consequences for several provisions under the services protocol. Accordingly, the African Union can learn from other regional bodies, such as those in the Asia Pacific, via the Asia-Pacific Economic Cooperation (APEC). APEC has not let similar socio-economic hurdles stop them from the arduous work of building a regional data governance framework while also addressing associated issues like digital infrastructure gaps.

To its credit, the African Union has demonstrated an interest in building a regional digital economy. The African Union has designed the Digital Transformation Strategy for Africa to adopt emerging technologies for sustainable development. The framework acknowledges and seeks to correct the historical deficiency of continental cooperation, aiming to promote further cohesion across distinct policy environments. In addition, the Malabo Convention, which has been signed by 15 countries, offers a standard level of data protection that seeks to prevent cybercrime and privacy violations while also mitigating the need for strict localization requirements. Accordingly, it also facilitates regional data flows for African states. AfCFTA offers a similar tangible opportunity to work toward a shared policy infrastructure, particularly under the e-commerce protocol. A regional approach to data governance would support the development of a single digital market in Africa that leverages data-driven technologies. A single market would lay the foundations for regional cooperation on other major issues such as data protection, privacy, cybersecurity and government access to data for purposes such as law enforcement requests and regulatory oversight of firms.

The ability of African countries to fully realize their ambitions for sustainable, safe, inclusive and effective digital development is contingent on their ability to work together. Likewise, policy makers in Africa should focus on developing national and regional data governance frameworks that account for the continent's distinct challenges while enabling data flows across countries. The promotion of data flows needs to happen in parallel with discussions about how they can also work together on related policy objectives, including cybersecurity, data privacy and human rights. What is salient is that, regardless of the issue, local legal responsibilities move with the data, and firms can be held accountable if they breach these shared laws. Ultimately, policy makers need to recognize that a regional data governance framework is a critical ingredient to ensure the region's people, firms and governments are better positioned to meet this digital inflexion point.

Jane Munga, Fellow, Carnegie Endowment for International Peace: "Developing a vibrant tech ecosystem in Africa will put the continent on the path to digital sovereignty."

Jane Munga is a digital policy expert and a fellow at the Carnegie Endowment for International Peace. Jane leads the work on technology policy in the Africa program. Her career has focused on policy making, emphasizing the potential of digital technologies for digital transformation. Jane has previously worked for the Government of Kenya as an adviser in the Ministry of ICT, Innovation and Youth Affairs, Ministry of Education and Ministry of Interior. She also served as an economic expert at the National Communications Secretariat, an ICT policy advisory body for the Government of Kenya, where she focused on developing digital economy policies and regulations, which included Kenya's Digital Economy Blueprint for Africa, and designing digital transformation programs for the Government of Kenya.

What are the dynamics of the US-China technology decoupling in Africa? How is it affecting the continent?

The tensions between the United States and China over digital technologies are growing, with wide-ranging implications for Africa's digital economy on issues from infrastructure and platforms to hardware devices. Like other regions of the world, African countries must contend with the ramifications of great-power competition in their digital agenda. African nations, however, must navigate the prospects of such decoupling alongside China's substantive investments and dominance in telecommunications infrastructure.

The same tension between the United States and China over technology has given rise to techno-nationalist approaches in which each party contests to promote ideological values through the reshaping of institutions and standards (Capri 2020). Both the United States and China have launched initiatives to counter each other's influence. The United States has put in place export control measures that limit trade between the country and China (Nellis, Freifeld and Alper 2022). In return, the Chinese government introduced several measures to counter US restrictions (Mozur and Liu 2023). African countries rely heavily on imported technology from both sides, however, with greater investments from China. For example, Africa, a mobile-first continent, connects to the internet primarily through mobile phones. About 70 percent of Africans access the internet using mobile devices. A large share of these mobile phones is from vendors incorporated in China. Out of the 42 vendors with market share in the continent, 19 are incorporated in China, while just four are incorporated in the United States. Chinese brands not only have a larger market share but also offer variety with options for phones specifically designed for African consumers.

Given this background, the ramifications of US-China technology decoupling will have repercussions for African consumers. Some mobile users are already feeling the effects of technology decoupling. In 2019, the US Department of Commerce's Bureau of Industry and Security added Huawei and its affiliates to its Entity List. The list designates foreign organizations with restrictions on their ability to export specified items to the United States. The addition of Huawei to the Entity List hinders the company from trading with US tech companies such as Google and those in the markets of US trading partners without US government approval. Google was prohibited from including Gmail, Google Maps, YouTube or the Play Store on Huawei phones. Mobile phone users with Huawei devices manufactured after 2019 must thus contend with limited accessibility to key mobile applications, depleting the digital dividends of such devices for millions of Africans across the continent.

Beyond restricting access to mobile apps, US-China technology decoupling has made for vibrant policy conversations, especially on the future of the internet. As debates on internet standards unfold in multilateral organizations such as the ITU, African policy makers must engage in digital foreign policy. For example, at the ITU's Telecommunication Standardization Advisory Group meeting in 2019, China Mobile, China Unicom, Huawei and the Chinese Ministry of Industry and Information Technology proposed the standardization of a new set of internet protocols (dubbed "New IP"), which would support a new internet by 2030. Ten African countries, a cohesive front from the continent, supported the proposal. The proposal on "New IP" slowed when the World Telecommunication Standardization Assembly was postponed due to the coronavirus pandemic. However, the conversation on the future of the internet has continued to elicit debate, studies and

political alignments, causing African countries to engage more disparately and cautiously on the matter. This is evident from the US-led Declaration for the Future of the Internet, which garnered just three African signatories (Cabo Verde, Kenya and Niger), although one of those countries (Kenya) stated its signature was added prematurely before government officials reached an official decision.

No doubt cyberspace is a major arena, where US-China technology decoupling will take centre stage. African countries will have to contend with the fragmentation of the internet, considering that China and the US telecom companies are the leading providers of ICT infrastructures on the African continent, with Chinese ICT firms Huawei and ZTE accounting for building more than 70 percent of the ICT infrastructure on the African continent.

How can African actors best navigate the prospects of such decoupling?

African countries can diversify manufacturing and technology supply chains. For example, African businesses can effectively engage in the smartphone-manufacturing industry, to help meet the rising demand of its burgeoning population. Currently, the continent's large demand for mobile phones is met through imports. There have been several attempts by African countries, such as Rwanda and South Africa, to manufacture smartphones, but large-scale success has yet to be achieved. However, new endeavours continue to launch; for example, Kenya has launched a smartphone assembly plant (Musau 2023). Efforts to kickstart smartphone manufacturing in Africa should seek to build regional value chains. Recent research by the African Union — *Made by Africa: Creating Value through Integration* — examines the vast potential of multi-country integrated value chains in sectors such as pharmaceuticals, apparel and automobiles for economic diversification and job creation in Africa (International Trade Centre 2022). Thus, the manufacturing of affordable smartphones can similarly aim to build regional value chains. African governments and businesses can participate in the smartphone manufacturing process at national and regional levels and examine ways of leveraging the AfCFTA to advance the continent's industrialization process and safeguard from technology decoupling effects. This would also ultimately reduce Africa's dependency on Chinese imports and promote supplier diversity.

What does this tell us about the need for more local technology innovation and local data ownership?

To cultivate a truly robust digital economy, African countries must invest in developing their own digital industry, and this starts with local digital products. Africa needs a digital industry built by Africans for Africa. African states must move from being passive recipients of blueprints developed elsewhere and build their ICT sectors with locally developed solutions. Indigenous tech products are crucial to establish digital sovereignty, enable policy control and drive economic growth. A homegrown digital industry will focus on solving challenges specific to African nations by providing locally tailored solutions. They also create high-skill job opportunities and help retain talent.

Africa has been termed as a continent rich in resources, bursting with innovative ideas and blessed with a huge youthful population, who are regarded as the continent's untapped potential. These youth are powering the innovative ecosystem on the continent with Africa's 400 technology hubs in 42 countries (African Union 2020, 19). However, despite the strong entrepreneurial mindset, youthful numbers and a growing number of tech innovations, Africa has not translated its innovative potential into a vibrant or comprehensive digital entrepreneurial ecosystem.

African governments need to develop digital economic policies that will promote innovation and create opportunities for their growing youth. Africa needs high-potential digital innovations/products that can be scaled up to build an indigenous digital ecosystem. This can only be done through a healthy innovation ecosystem that will help harness the power of technology to grow innovative ideas to scale. Developing a vibrant tech ecosystem in Africa will put the continent on the path to digital sovereignty, building the technology and setting the rules that will shape its future. By investing in indigenous digital industry, African governments and businesses can accelerate digital transformation on their own terms. The future is digital, and the time for Africa to shape its own digital destiny is now. African tech providers are best positioned to deliver the infrastructure for Africa's digital revolution. By keeping the digital industry within the continent, they enable a faster digital transformation and lower costs, paving the way for African businesses and consumers to fully utilize and benefit from technology.

Mandira Bagwandeen, Nelson Mandela School of Public Governance, University of Cape Town: "The domination of foreign companies in Africa's digital landscape could impact a country's digital sovereignty."

Mandira Bagwandeen is a senior research fellow at the Nelson Mandela School of Public Governance at the University of Cape Town. She also lectures at various South African universities on international relations and the political economy of Africa-China ties.

What are the common and specific challenges posed to sovereignty by data governance and digital transformation in Africa?

Data sovereignty and digital transformation pose various challenges to sovereignty, specifically state sovereignty. The two primary global challenges are around data privacy and data protection, and cybersecurity threats and cyber espionage.

In the age of big data and surveillance capitalism, protecting people's data privacy and ensuring it is managed ethically and securely is a significant challenge. Like many countries worldwide, African states are at various stages of developing data protection regulations and frameworks. As of February 2023, 36 of 54 African countries had adopted data protection laws (Hogan Lovells 2023, 4). Drawing on best practices, many of these laws were influenced and modelled after the European Union's GDPR. The impetus to adopt GDPR-like data laws stems from the need to develop a legislative framework that facilitates data protection as well as economic growth, innovation and trade between African countries and their Western trading partners, notably the European Union, the continent's biggest trade partner. Approved in 2017, Benin's Digital Code is so evidently informed by the GDPR that it's been described as having "enacted the most GDPR-like legislation outside the EU" (Daigle 2021, 8).

Like many countries around the world, African states have to deal with cybersecurity threats such as hacking, phishing and malware, which can harm a computer system or network, damage data or disrupt digital activities. Additionally, several cyber-espionage incidents (also known as cyber-spying or cyber-collection) have been reported in recent years. Some popular headlines include allegations of Chinese state-sponsored cyber espionage. For example, in 2018, reports emerged that China had spied on servers at the Chinese-built African Union headquarters for more than five years, gaining access to confidential information (Dahir 2018). Following this, in December 2020, a Chinese hacking group nicknamed "Bronze President" reportedly "rigged a cluster of servers in the basement of an administrative annex to quietly siphon surveillance videos from across the AU's [African Union's] sprawling campus" (Satter 2020). And in May 2023, allegations were reported that a Chinese state-linked hacking group calling themselves "Backdoor Diplomacy" conducted a cyber-espionage campaign over three years, targeting the Kenyan government to gain sensitive information about their debt owed to China (Ross, Pearson and Bing 2023).

There are three additional challenges that are noteworthy and specific to the African continent. These have to do with the continent's infrastructural deficit and the resulting dependence on foreign technology providers, issues around data localization and the lack of regulatory harmonization.

Many African countries lack the necessary ICT infrastructure, including a reliable electricity supply, broadband internet and data centres. Another challenge is a shortage of technology skills in the labour market and a lack of financial and material resources to develop ICT infrastructure indigenously. As such, many African countries depend on foreign technology and digital services. With foreign companies dominating Africa's digital landscape, they could impact a country's digital sovereignty. For example, foreign suppliers could influence digital governance practices or threaten national security.

The infrastructural deficit also has an impact on any aspirations toward data localization. While data localization is considered a means to ensure data sovereignty, it is challenging to achieve, primarily because of the financial resources and technical capabilities required to develop data centre infrastructure. Nonetheless, many commentators consider it essential for African states to build data centres to ensure digital sovereignty. Currently, most of the data content consumed in Africa is hosted outside the region, and the market is severely underserved. With digitization increasing across Africa and the increasingly important issue of digital

sovereignty garnering more attention, several African countries have — or are in the process of building — data centres with the assistance of foreign investment and companies. So far, Chinese companies, especially Huawei, a Chinese telecoms giant, have made significant inroads into Africa's ICT sector and data centre market.

Furthermore, achieving regulatory and legal harmonization on cyber laws and regulations at the regional and continental level in Africa is very challenging due to diverse legal frameworks, different forms of governance and linguistic differences. For example, the African Union's Malabo Convention received lacklustre support; it took nine years for the convention to obtain 15 ratifications, eventually coming into force in June 2023.

How do you assess the different policies set up by various African countries to pursue "digital sovereignty"? What are the variations that you see?

African countries have produced various policies to achieve digital sovereignty, which can be simply understood as a state exerting control over digital infrastructure, data and technology to protect national interests. Some of the various policies include (but are not limited to) data localization and protection laws; establishing national internet exchange points, content regulations and internet censorship; national digital platforms; and e-government initiatives. While many policies, especially data localization and protection laws, draw on global best practices, some legislation such as Nigeria's Data Protection Act, 2023, has some unique provisions. It includes a new classification of data controllers and processors "of major importance" and specific obligations attached to them, as well as broader protections for exempt processing activities (King'ori 2023).

How do foreign actors like China, European countries, the United States and private actors understand and deal with the discourse on local data ownership?

China takes a state-led or authoritarian approach to data sovereignty, stressing the importance of local data ownership. The Chinese government requires all data generated within the country to be stored locally and subject to Chinese laws and regulations, allowing the government to exert considerable control over data access and usage.

As prescribed by the European Union's GDPR, European countries emphasize individual data rights and privacy more. The GDPR limits cross-border data flows and instructs that personal data must be processed following strict privacy and security measures. This empowers users to have more control over their data. Since European countries are concerned about data protection, they often require companies to obtain user consent for data processing.

The United States takes a more market-driven approach to data ownership. Data ownership is often left to individual or corporate discretion, with less emphasis on local data ownership. However, in recent years, there has been a growing concern in American policy circles about the potential of large tech companies, such as Amazon, Apple, Google, Meta and Microsoft, to undermine democratic values and institutions, resulting in increased calls for the US government to implement digital regulations. Some argue that the dominance of a few large tech companies gives them too much power in cyberspace and poses a direct challenge to state authority.

Private entities, especially multinational tech companies, must often balance adhering to data localization requirements of various jurisdictions and ensuring efficient data utilization and analytics.

How can regional and international organizations better support a shared vision of data governance and regulation in Africa?

Developing a shared vision of data governance and regulation in Africa requires that regional and international organizations, governments, stakeholders and communities collaborate earnestly — there must be sustained cooperation and synergy to achieve policy and regulatory harmonization. While several areas require cooperative efforts, I think that four initiatives are key to advancing the establishment of a common African vision on data governance.

First, there is a need for capacity building and policy development initiatives. Regional and international organizations can assist with providing training and capacity-building programs or courses to help African governments and national departments improve their expertise on data governance, equipping them to develop more well-informed and sound policies. Organizations can also contract their staff to

African governments to help develop data governance policies to ensure that legislation aligns with best global practices while reflecting the unique local contexts and priorities.

Second, financial and technical assistance is crucial. Through grants, partnerships and funding programs, organizations can provide financial support to assist African governments in implementing their data governance policies. Technical support can be provided through advisory services and technological transfer initiatives.

Also, collaborative research as well as monitoring and evaluation (M&E) need to be expanded across the continent. To better understand data governance challenges and opportunities across Africa, collaborative efforts should be established between African and international organizations to produce research that can inform the development of comprehensive policies. And regional and international organizations can work together to establish monitoring and evaluation mechanisms to assess the effectiveness of data governance policies. Regular M&E can provide valuable information to tweak or improve policies and regulations.

Finally, regional and international organizations can partner with African ICT departments to promote and establish multi-stakeholder engagements with governments, civil society, the private sector and academia to ensure that data governance policies that are produced reflect the diverse interests of African citizens.

Melody Musoni, European Centre for Development Policy Management (ECDPM): "Diversity in digital sovereignty approaches highlights the global impact of differing national policies in the digital sphere."

Melody Musoni is a policy officer at ECDPM, a think tank, where her work focuses mainly on digital governance and digital economy. She is also an expert adviser on a project on Artificial Intelligence in Primary Education in Africa. She previously assisted the Southern African Development Community Secretariat with its data protection and compliance programs. She has worked for over a decade in legal practice where she specialized in ICT law, data protection and information security.

What are the different approaches to digital sovereignty?

To understand the various approaches to digital sovereignty, it's crucial to first define the concept. Digital sovereignty is essentially a state's control over digital infrastructure and data within its territory, regardless of where this data is hosted. The approach a country takes toward digital sovereignty is shaped by its social, economic and political interests; technological capabilities; domestic priorities; and digital foreign policies.

In the European Union, lagging behind technologically compared to China and the United States, the strategy has been to assert digital sovereignty by setting global legal norms and promoting European technologies. A notable example of this is the GDPR, which is part of the European strategy that involves imposing stringent data governance standards and extending EU authority over data processing, even beyond its borders. The European Union, by setting these norms, encourages other regions to adopt GDPR-like laws. It also collaborates with the African Union in developing Africa's Data Policy Framework, a crucial policy document poised to transform the utilization of African data for the continent's advancement.

The United States adopts a laissez-faire approach, prioritizing unrestricted data flows, which benefits its tech companies who happen to control the largest global market share. However, through the CLOUD Act, the United States maintains sovereignty by requiring US entities to disclose data upon request, regardless of the data's location.

China, on the other hand, exercises tight control over both domestic and international operations. This is evident in its surveillance-oriented data protection law and stringent data transfer requirements. The Chinese government has privileged access to all data originating in China and mandates companies to transfer critical information to state-run servers. Chinese companies are also required to provide access to data for national security review when the state submits a request for access to them.

In Africa, there's a common misinterpretation equating digital sovereignty with data localization. There is a conception that if data infrastructures and data centres are on the African continent and owned by African entities, African governments have more control over the data, the infrastructures and any data-processing activities taking place in their territory, thus exercising digital sovereignty. The African Union's strategies, such as the DTSA of 2020 and the AU Data Policy Framework of 2022, acknowledge the need for sovereignty over data while cautioning against strict local data storage mandates. The 2030 vision of Africa under the DTSA is on building digital infrastructures such as African data centres on the continent and setting up a Digital Sovereignty Fund to attract investment and funding on digital infrastructure. Positively, the Data Policy Framework identifies the importance of maintaining data sovereignty but also cautions against the stringent local data storage mandates as contradictory to sovereignty principles. African countries display varied national data laws and attitudes toward cross-border data flows and local data storage requirements. This diversity in digital sovereignty approaches highlights the global impact of differing national policies in the digital sphere.

How do you assess the policies set up by various African countries to pursue "digital sovereignty"?

Policies regarding digital sovereignty across African nations reveal challenges in standardization and policy harmonization concerning data sharing and transfer, and alignment with continental objectives. For example, Ghana adopts a liberal stance on data sharing outside its borders without local storage mandates, whereas Zambia enforces strict local data storage for cross-border transfers. Several African countries are concerned about foreign dominance in the cloud market affecting their

sovereignty. South Africa is considering a policy for digital sovereignty through data localization, while Djibouti aims to become a hub for African data centres and is conducting a market study and defining a road map on construction and exploitation of regional data centres in Africa.

The AU Data Policy Framework and the AfCFTA could influence changes in African nations' approaches to cross-border data flows. The AU Data Policy Framework advocates for digital sovereignty but opposes data localization as a means to achieve it. The operationalization of the AfCFTA presents an opportunity for African countries to reconsider strict data localization laws and adopt intra-African data sharing as guided by the AU Data Policy Framework. I believe that as African countries implement this framework, they will maintain their own data centres but be more open to transborder data sharing, which could foster trade within Africa.

How can regional and international organizations better support a shared vision of data governance and regulation in Africa?

The progress in data governance in Africa over the last five years has been significant, with countries enacting personal data protection laws, criminalizing unlawful cyber activities and establishing data regulators. The adoption of the AU Data Policy Framework and progress toward operationalizing the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), now ratified by 15 member states, are notable achievements. These, along with efforts toward a continental free trade area and digital single market, position Africa for economic growth, societal advancement and human rights protection.

For further progress, closer collaboration among African countries is essential to align national laws with continental frameworks and bridge policy gaps. Regional economic communities can assist member states in enacting data protection laws. The Smart Africa Alliance and other regional alliances can provide technical and financial assistance to AU member states. The African Network of Data Protection Authorities, under the African Union's leadership, could play a significant role in capacity building, knowledge sharing and conducting workshops on data protection.

The African Union should continue its leadership in guiding member states on regulations for artificial intelligence, digital identities and effective implementation of data policy frameworks. Support from the private sector, civil society and academia is also crucial.

Lastly, the partnership between Africa and Europe can be expanded, with the European Union's Team Europe Initiatives potentially providing technical and financial support to African countries. Africa can benefit from the European Union's experience in data governance to develop and enforce its own frameworks.

Motolani Peltola, Tampere University: "The pursuit of digital sovereignty and local data ownership has implications for local capacity development."

Motolani Peltola (formerly Agbebi), Ph.D., is a university lecturer in the Faculty of Management and Business, Tampere University, Finland. Her research interests include Sino-Africa relations and its implications for socio-economic development in Africa; China's DSR and its implications for Africa's technological future; and human capital development in Africa.

With the significant increase in data centres in Africa, estimated at around 700 new facilities in the coming decade, what are your thoughts on digital sovereignty and local data ownership in this context?

A growing number of African governments are actively fortifying their digital sovereignty through the adoption of policies, laws and regulations pertaining to data localization. This involves increasing investments in digital infrastructure, particularly data centres, and imposing restrictions on the hosting and transfer of data beyond national borders unless officially exempted. Concurrently, the continent is witnessing an escalating trend in the adoption and implementation of data protection and privacy regulations, exemplified by Nigeria's Data Protection Regulation, South Africa's Protection of Personal Information Act, Kenya's Data Protection Act and Ghana's Data Protection Act, among others. Notably, these regulations often draw inspiration from the European Union's GDPR, albeit with certain deviations. In their approach to data localization, African countries exhibit a spectrum of approaches ranging from hard localization to soft localization to hybrid localization regulations.

The surge in efforts by African governments to bolster digital sovereignty and local data ownership encompasses economic, social and political dimensions. The rationale behind the adoption of data localization requirements includes considerations for cybersecurity, data protection and privacy of citizens, economic development, law enforcement, national security and, controversially, government censorship and surveillance. While these motivations hold true for African countries, the predominant reasons often revolve around data protection and economic development. For instance, Nigeria's data localization policy is justified by the aspiration to rectify the negative trade balance in the ICT sector and foster a digital economy for the benefit of its citizens. Similarly, South Africa views data and associated digital infrastructure as strategic national resources.

Through the implementation of data localization regulations, certain African governments aim to mitigate the risk of data colonization, reinforce digital sovereignty and ensure local economies reap the benefits. The prevalence of foreign technology firms in Africa, with their access to valuable user data, exposes African governments and citizens to data and national security vulnerabilities. Local hosting of data is envisioned as a means for African governments to maintain control over critical data and data infrastructure, such as data centres, with some countries designating them as critical information infrastructure[34] to be protected as strategic national assets yielding socio-economic benefits.

The expansion of data centres in Africa, coupled with investments in broadband networks and supporting digital infrastructure for local data storage and processing, contributes to local digital infrastructure development and diminishes dependency on foreign platforms and companies. Given that Africa's share of global data centre capacity is less than one percent (Beard 2021), there is an imperative to develop these digital infrastructures. Moreover, the pursuit of digital sovereignty and local data ownership has implications for local capacity development, fostering expertise in areas such as data services and cybersecurity.

However, the promotion of local data ownership poses a dual perspective. While it may be deemed a legitimate strategy to enhance digital sovereignty, fortify data and national security, as well as curb data colonization by foreign entities, critics argue that if the entire infrastructure, technical expertise and support are provided by foreign firms, concerns about exposure to data vulnerabilities remain unresolved.

34 See *Electronic Communications Act, 2005* (S Afr), No 36 of 2005.

Furthermore, the unintended consequences of data localization on competition, trade and investments may impede economic development. Similar to industrialized Western democracies, African nations face the challenge of balancing the imperative of digital sovereignty facilitated by data localization with economic considerations against such regulations. Consequently, national data regulation policies must be adeptly designed to mitigate negative economic impacts on cross-border data flows and trade while ensuring gains from a data sovereignty regime align with the needs of a burgeoning digital economy.

How do foreign actors like China, European countries, the United States and private actors understand and deal with the African discourse on local data ownership?

The responses of foreign state actors, such as China, European countries and the United States, to the discourse surrounding data localization in Africa can be seen as reflective of their domestic approaches to digital sovereignty, data protection and regulation.

Within the European Union, a comprehensive framework for data protection is embodied in the GDPR, supplemented by additional regulations like the Data Act and Data Governance Act. These instruments are crafted to control, facilitate and safeguard cross-border data flows. The GDPR, as a representation of EU countries' stance on data protection, emphasizes individuals' rights to privacy, control over their data and responsible organizational practices, and governs cross-border data transfers outside the European Union. While the European Union and Africa share concerns regarding the dominance of foreign technology firms and their utilization of citizen data, there are disparities in their approaches to digital sovereignty. The European Union champions a liberal stance on digital sovereignty, emphasizing individual control over data rather than government or private organizations, contrasting with African countries' tendencies to exhibit elements of both state-centric and liberal models in their approaches to data sovereignty to varying degrees.

Conversely, both the European Union and the United States express concerns about the discourse on local data ownership in Africa, particularly with respect to the implications of increasing governmental control over data for civil liberties and the potential misuse of data by authoritarian governments. Also, there are concerns regarding the national security risks posed by digital infrastructure provided by state-led Chinese companies. Additionally, concerns are raised about the competitiveness of European tech companies amid increasing data localization regulations in a sector dominated by Chinese and American technology firms. The European Union's endeavours to enhance its position in the global data value chain, foster competitiveness and negotiate agreements with African countries on digital-related clauses further underscore the complex landscape.

The United States, adopting a more liberal approach to data sovereignty, has historically abstained from imposing federal or comprehensive data localization requirements. Dominance of US technology companies around the world and a historical advocacy for open cross-border data flows reflect a liberal regime on data localization with limited restrictions. While debates persist on data localization, there is yet to be a formal consensus among US policy makers on domestic mandates, and responses to foreign policies are yet to materialize. Having said that, economic concerns about threats to American businesses in the event of restricted cross-border data flows, coupled with concerns of an authoritarian approach to data governance due to China's increasing dominance in the provision of digital infrastructure in Africa, are prominent in US deliberations on increasing data localization in Africa. For example, the US Trade Representative has expressed reservations about data localization measures in Nigeria and Kenya, deeming them discriminatory to foreign businesses (that store and process data globally) and potentially detrimental to the development of the digital economy (Office of the United States Trade Representative 2019).

China, adopting a state-centric view of digital sovereignty, centralizes the role of the state in data governance and citizen data control. Enforcing a strict data localization approach, mandating data to be hosted within the state of its production, China has propelled the growth of its domestic firms at the expense of foreign competitors. In Africa, China's active involvement in financing digital infrastructures, including data centres, and its technology companies' collaboration with governments in designing national digital economy strategies, exemplifies

its commitment to shaping the digital landscape in alignment with its Digital Silk Road aims.

A common thread in the response of foreign actors, namely, the United States, China and the European Union, is a concerted effort to bolster the competitiveness of their technology firms globally and particularly in Africa's technology sector, which still holds substantial investment opportunities. Despite the variations in their domestic stances on data localization, these actors — the United States (Karombo 2020), China (Si 2023), the European Union (Victoria 2020) — demonstrate an interest in capitalizing on the investment opportunities facilitated by the growing trend of data localization in Africa.

How can regional and international organizations better support a shared vision of data governance and regulation in Africa?

In addressing the critical issue of data governance and regulation in the African context, a primary concern revolves around the need to harness the benefits of the digital economy while mitigating the inadvertent challenges posed by data localization to trade and overall economic progress. Therein lies the potential role of regional and international organizations in facilitating a collective vision for robust data governance in Africa. A shared vision of data governance and regulation in Africa can be better supported in the following ways.

First, there is a necessity for capacity-building initiatives and technical assistance. These interventions should be tailored to enhance the expertise of individuals, organizations and government officials in formulating and implementing effective data governance frameworks aligned with their unique priorities. Furthermore, capacity-building efforts should include comprehensive training on principles, regulations and best practices associated with data governance.

Second, the promotion of standardization and policy harmonization is a crucial strategy to counteract the potential impediments to continental trade posed by disparate levels of data localization and governance across African nations. It is crucial to facilitate interoperability and cross-border data flows to bolster continental trade initiatives such as the AfCFTA. The Malabo Convention, albeit pending full ratification, serves as an initial step toward policy harmonization. It is imperative to encourage sustained dialogue and collaboration among African countries, fostering the development of common standards and aligning regional practices with global norms to alleviate barriers that impede economic development and delivery of essential services in sectors such as the health sector.

Moreover, the lack of policy complementarity in data governance within Africa could exacerbate digital divides and inequalities. This is particularly evident when certain data governance regimes, through localization measures, result in disparate access to data, increased prices and limited availability of ICT products and services. Consequently, regional policy harmonization becomes a compelling imperative to address this challenge and promote equitable development.

Third, the establishment of platforms for collaborative dialogue involving all stakeholders, including civil society organizations, regional and international bodies, and the private sector, is crucial for fostering an effective and cooperative data governance ecosystem. This collaborative effort should be oriented toward the protection of individual data, responsible data usage, and the creation of an enabling environment for innovation and economic development.

Fourth, regional and international bodies can play a pivotal role in fortifying democratic institutions and civil society organizations in African countries. The association between data localization and a decline in internet freedom underscores the importance of support in ensuring these entities possess the requisite resources and can exert agency to contest data governance laws that may undermine democratic processes and impede civil liberties.

Finally, financial support for digital infrastructure development remains indispensable. Such financing is instrumental in creating the necessary infrastructure for effective data governance and management in Africa, thus facilitating the overarching goals of economic development and innovation.

Nnenna Ifeanyi-Ajufo, Leeds Beckett University and African Union Cyber Security Expert Group (AUCSEG): "The current state of cybersecurity in Africa is the tendency toward a cyber-militarization approach."

Nnenna Ifeanyi-Ajufo is professor of law and technology at Leeds Beckett University, United Kingdom, and vice chairperson of AUCSEG, and has been actively involved in advising the African Union Commission and member states on existing international, regional and national legal frameworks related to cybersecurity, as well as promoting cybersecurity in the region.

What is your analysis of the state of play in Africa regarding cybersecurity and infrastructure regulation?

Thank you for the opportunity to share my insights. In my view, the state of cybersecurity in Africa is defined by two critical factors: governance and regulation. Given the nature of cyberspace, these elements are of utmost importance. Traditionally, cybersecurity has been focused on technical aspects and legal frameworks, but the role of infrastructure is pivotal. Unfortunately, without adequate digital capacity, governing cyberspace effectively is a challenge.

Africa remains the least digitalized region globally, which impacts its approach to cybersecurity. The disparity in wealth distribution across African countries plays a significant role in this context. In poorer nations, cybersecurity is often not a priority, and in regions like the Sahel, conflicts and political instability further detract from cybersecurity initiatives.

In terms of infrastructure, Africa lags behind due to various factors, including technology dependence, uneven distribution of technology and political issues like corruption. However, some countries, such as Mauritius, Ghana and Tanzania, are making notable progress in developing cybersecurity infrastructure. This encompasses not just technology, but also the establishment of agencies and authorities, and a commitment to multi-stakeholder collaboration in cybersecurity.

Despite some progress, there is a lack of harmonization in efforts across the continent. Countries like Togo have also made strides, such as the agreement with the United Nations Economic Commission for Africa (UNECA) to establish a regional cybersecurity centre, but challenges like funding persist. The African Union is also working on a cybersecurity strategy, yet implementation varies significantly across the continent due to disparities in wealth, approach and existing challenges.

On the regulatory front, Africa is at a crucial juncture. The regional cybersecurity treaty came into force on June 8, 2023. Originating from the 2009 Oliver Tambo Declaration, this convention is ambitious, encompassing electronic transactions, cybersecurity and personal data protection in a single treaty — a unique approach compared to other regions. However, there has been reluctance among African countries to ratify this convention, with only 15 ratifications to date — none from the continent's major powers like Nigeria, Kenya, Egypt or South Africa. Even Ethiopia, the seat of the African Union, is yet to ratify the treaty. This demonstrates the lack of capacity to implement an otherwise powerful regulation. It represents the gap between the presence of regulatory frameworks and their implementation.

At the subregional level, regional economic communities like ECOWAS and SADC [the Southern African Development Community] have their cybercrime directives, indicating a more dynamic subregional approach to cybersecurity. However, the African Union's influence over these regional initiatives is limited. This is because, unlike other regions in the world, regional economic communities are relatively strong. In addition, there's a diversity in legislative approaches among African countries, with some focusing on computer-dependent crimes, while others have broader scopes, as seen in Ghana's 2020 Cybersecurity Act and Nigeria's Cybercrimes Act.

A key aspect of the current state of cybersecurity in Africa is the tendency toward a cyber-militarization approach toward cyber governance. This has contributed to a trend of cyber-authoritarianism, as many African countries view cybersecurity through a national security lens, leading to practices like internet shutdowns, blocking of specific services (for example, Nigeria's Twitter ban between 2021 and 2022) in response to crises rather than focusing on vulnerabilities of citizens in cyberspace. This approach contrasts with the African Union's Digital Transformation Strategy (2020–2030), which advocates for a more

people-centred, multi-stakeholder approach to cybersecurity than a government-centred one.

With regard to the cyber-militarization approach of most African countries that you mentioned, would you say that this approach is unique to Africa, or is it more in line with the approaches of some major geopolitical powers?

In the realm of cyber diplomacy, African countries often align with Russia and China. The influence of these countries is evident in the negotiations around the cybercrime convention and the adoption of their digital sovereignty approaches. This alignment affects how African governments interpret and implement cybersecurity governance. The cyber-militarization approach observed in many African countries is not entirely unique to the continent but aligns with the trends seen in major geopolitical powers. This alignment reflects the dynamics of cyber diplomacy in Africa. For instance, during the negotiations for the UN cybercrime convention,[35] Russia notably spoke on behalf of certain African countries, like Burkina Faso, illustrating this influence.

The contrast between the ratification of the Budapest Convention (the Council of Europe's cybercrime convention) by only a handful of African countries, and the substantial support for the resolution to start the cybercrime convention initiated by Russia, further highlights this leaning toward Russia and China. The influence of these powers is evident not only in the adoption of digital sovereignty approaches, but also in the reliance on technology sourced from these countries.

The relationship between the African Union and China is particularly significant in this context. Despite the evident cyber-authoritarian tendencies, there has been a notable silence from the African Union in taking a stand against these approaches. When deliberating on potential articles of the UN cybercrime convention, the inclination of most African countries toward the perspectives of Russia and China becomes apparent, especially concerning human rights issues. For instance, the ongoing negotiations around article 5 of the potential UN cybercrime convention, which deals with human rights, reveal a tendency among African nations to align with authoritarian stances. This indicates that cyber diplomacy is intertwined with traditional diplomatic relations and influences how African governments interpret and manage cybersecurity governance. Therefore, the cyber-militarization approach in Africa, while having unique regional characteristics, is significantly influenced by, and aligned with, the broader geopolitical strategies of major powers like Russia and China.

With the significant increase in data centres in Africa, estimated at around 700 new facilities in the coming decade, what are your thoughts on digital sovereignty and local data ownership in this context?

The surge in data centre construction in Africa represents a phase of "data capitalism," reflective of the continent's digital dependence. In the European Union, data is regulated and protected under the GDPR, but in Africa, data protection is far less consistent, and we only have the Malabo Convention, which only a few countries have finally ratified. The lack of comprehensive regional data protection laws further complicates this issue.

Many African nations lack robust data protection legislation, often resorting to copying laws such as the GDPR without the capacity for effective implementation. I recall in, 2018, one example when I picked up a data protection bill of one African country, which turned out to be a verbatim copy of the UK Data Protection Act. This raises concerns about whether these emerging data centres can be effectively regulated. Despite some countries like Ghana making progress with digital ID systems, there is a general lack of widespread, systematic data collection across the continent — thousands of people on the continent still have no civil registration records such as birth certificates and, in places where these are present, they are largely not yet digitalized.

An important consideration is the question of who the primary beneficiaries of these data centres are. It is crucial for Africa to approach discussions on data centrality cautiously, addressing digital inequalities to ensure reciprocal and equitable access, use and benefits from this data. Africa's vast market potential makes it attractive for international tech companies, yet this interest in building data centres and similar infrastructure is not necessarily driven by the African Union or African initiatives. This disparity raises questions

35 See www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

about true digital sovereignty and local data ownership in Africa. There appears to be a misunderstanding of digital sovereignty in the African context. For instance, African leaders might readily share comprehensive national data with international corporations like Google, which may fund data centres, without fully considering the implications for data sovereignty and security. This practice extends to areas like election infrastructure, often managed by foreign companies, with data domiciled outside Africa. The critical issue, then, is whether these data centres are being constructed to genuinely build capacity within Africa or to serve external interests, a situation that could be termed "data colonialism." Until there is a broader understanding and discussion about what digital equality means for Africa, it will be challenging to achieve parity in the global digital landscape. This conversation is essential to ensure that Africa's development in the digital age is equitable and beneficial to its people.

In light of the increasing trend of data localization and domiciliation as a response to data colonialism, to what extent do you consider this approach a viable solution for Africa? For instance, countries like Senegal are adopting the Chinese model of data onshoring to protect digital sovereignty. How effective is this strategy?

First, it's important to acknowledge that, in my view, complete data localization is an ambitious goal that may not be entirely achievable. However, we are witnessing a growing trend toward internet fragmentation and data localization efforts, particularly in countries like Senegal, which has been proactive in cybersecurity and vocal about digital sovereignty. Senegal's ratification of both the Malabo and Budapest Conventions reflects its commitment to prioritize cybersecurity. The case of Senegal, which is moving toward data onshoring with China's support, raises crucial points. Reflecting on the incident at the African Union in 2019, where the data servers within Chinese-built AU headquarters were reportedly transferring data covertly to China, it's clear that there can be a significant gap between rhetoric and reality in these initiatives.

The practicality of complete data localization in Africa is questionable. The technology companies and infrastructure are predominantly foreign, and the applications of data often have international dimensions. Furthermore, cybersecurity necessitates some level of international cooperation, implying that external powers may still access data despite localization efforts. This reality underscores the importance of scrutinizing the dynamics of international conventions and treaties from a unified African perspective. While the ambition of countries like Senegal to localize government data is commendable, the actual feasibility of such an endeavour across Africa is uncertain. A more harmonized approach to data protection, where African nations collectively define their priorities and develop a deeper understanding of data governance, is needed.

Localizing government data, particularly sensitive information like electoral data, within the country is a crucial step toward safeguarding digital sovereignty. It's vital for African countries to build their capacity in technology and data governance to make this ambition realistic. While the aspiration to localize data is not far-fetched and is indeed being pursued by other countries, the transition to such a model in Africa needs careful consideration, balancing ambition with the realities of technological dependence and international cooperation.

What strategies have proven effective for African governments to collaborate toward achieving digital goals, particularly regarding digital sovereignty and multinational digital infrastructure projects? Additionally, where do the lapses lie, and how can they be addressed?

The effectiveness of strategies for African governments to achieve consensus and action in digital realms is influenced by a variety of factors, some of which are man-made, while others are inherent to the region's realities, such as political instability and conflict. These factors often shift the priority away from digital goals.

For instance, the African Union experienced a significant cyberattack this year, yet the response was unclear, reflecting the overarching issue of prioritizing physical conflicts over digital threats. The African Union, unlike the European Union, does not have the same regional influence and is relegated to observer status in the cybercrime negotiations. This limitation hinders the African Union from speaking for or holding its member states accountable in digital matters.

The individualized approach to governance in African countries impacts cyber governance. While the African Union has started pursuing

a unified African position on cybersecurity, a mere policy paper doesn't necessarily equate to consensus, as evidenced by the limited impact of the Malabo Convention.

Furthermore, the African Union needs to prioritize funding and capacity building in digital governance and cybersecurity. Currently, many African countries rely on capacity building provided by external states, leading to a lack of a harmonized approach. This situation is compounded by donor superiority, where external countries dictate Africa's digital priorities.

Regional economic communities like ECOWAS play a significant role, but they face their own subregional governance challenges. Even with directives like the ECOWAS cybercrime directive, inconsistencies such as internet shutdowns within member states reveal gaps in implementation and adherence.

Another strategy could involve African "champion" countries like Morocco, Egypt, Ghana and Mauritius leading and guiding others. The Malabo Convention, now in force, could serve as a platform for creating a harmonized approach and amending parts of the convention to better suit regional needs. Africa's digital transformation strategy, if implemented transparently and accountably, could provide a robust framework for the continent's digital evolution. However, there's a lack of clarity regarding its implementation and relevance to individual African countries. Ensuring transparency and accountability in implementing this strategy would help define Africa's digital governance landscape more effectively.

Considering the limitations of the African Union, could engagement with regional economic communities be a more effective solution for addressing digital challenges, or does bilateralism offer a better approach in the short to medium term?

The engagement with regional economic communities indeed presents a viable solution, complementing the limitations of the African Union in addressing digital challenges. Various states are also taking initiatives on a unilateral and bilateral basis. For instance, UNECA and Togo's collaboration to host the first Summit of African Heads of State and Government on Cybersecurity last year is a prime example. This summit led to the Lomé Declaration on cybersecurity and the fight against cybercrime, a significant commitment from over 27 African countries to promote cybersecurity and endorse the Malabo Convention, which, at the time, hadn't come into force. This collaborative approach, especially in regional forums, could be augmented by the leadership of countries in each region, like Kenya, for instance, advancing in cybersecurity governance in East Africa. These nations could spearhead workshops and dialogues, fostering a better understanding and implementation of cybersecurity measures across smaller or less-developed countries in their region.

The Africa Internet Governance Forum, under the UN framework, is another platform where substantial progress is being made. This forum, which includes regional and subregional iterations like the West African Internet Governance Forum and the North Africa Internet Governance Forum, focuses significantly on state involvement but also boasts a strong presence of civil society organizations. These organizations, such as Paradigm Initiative and ICT Africa, are growing in number and relevance and working with governments and relevant stakeholders in pushing for digital governance, digital rights, digital public goods and cybersecurity. Moreover, initiatives like the African School on Internet Governance contribute to shaping a unified African agenda in digital governance. The African Union Cyber Security Expert Group, of which I am a member, for example, has been instrumental in advocating for specific priorities in capacity building for Africa within these forums.

The international cooperation fostered by entities like the Global Forum on Cyber Expertise, which focuses on capacity building in Africa, demonstrates the potential of combining efforts beyond bilateral agreements. This collective approach is essential for a comprehensive and effective strategy in addressing the digital challenges facing Africa.

What are your thoughts on the role of an organization like Smart Africa in the African digital transformation ecosystem, particularly in integrating the private sector into the discourse?

Smart Africa plays a unique and significant role in the African digital transformation ecosystem, though its position is complex and raises several questions. This organization, backed by several governments and led by the Rwandan president, operates somewhat

independently of the African Union, focusing on cybersecurity and digital governance.

The creation of the Continental Cybersecurity Blueprint by Smart Africa is noteworthy. However, it leads to questions about the overlap and distinction between Smart Africa's initiatives and those of the African Union. Smart Africa's involvement with multiple African governments and its alignment with heads of state like Rwanda's president is intriguing, especially considering whether these efforts could be more effectively channelled through the African Union.

Smart Africa's position in the digital landscape is somewhat ambiguous: it is unclear whether it should be seen as an independent civil society organization, an intergovernmental organization or a unique entity. This ambiguity is evident in Smart Africa's collaborations with different organizations on various projects, despite seeming to operate independently.

The engagement with private entities is one area where Smart Africa stands out. It provides a regional platform that not only has the attention of many African countries but also collaborates extensively with tech companies and telecommunication firms. This inclusive approach is crucial because there is no other platform with such a regional outlook that actively involves private companies in shaping the digital landscape in Africa. Furthermore, international tech giants like Google and Microsoft, while global in their operations, are establishing a significant presence in Africa, challenging the traditional notion of local versus international tech companies. Their involvement in the region, whether through direct presence or through labour sourced from Africa, is reshaping the digital business landscape.

The emergence of Smart Africa and its increasing influence raise questions about the role of the African Union in championing digital transformation. Is it a matter of political will, funding, capacity or leadership that has led to the rise of Smart Africa as a key player in digital initiatives? These questions are essential to consider as Africa navigates its digital transformation journey, seeking to balance capacity, leadership and prioritization of digital objectives. The future of digital transformation in Africa might hinge on how well regional bodies like the African Union and platforms like Smart Africa can collaborate and align their efforts for the greater good of the continent's digital landscape.

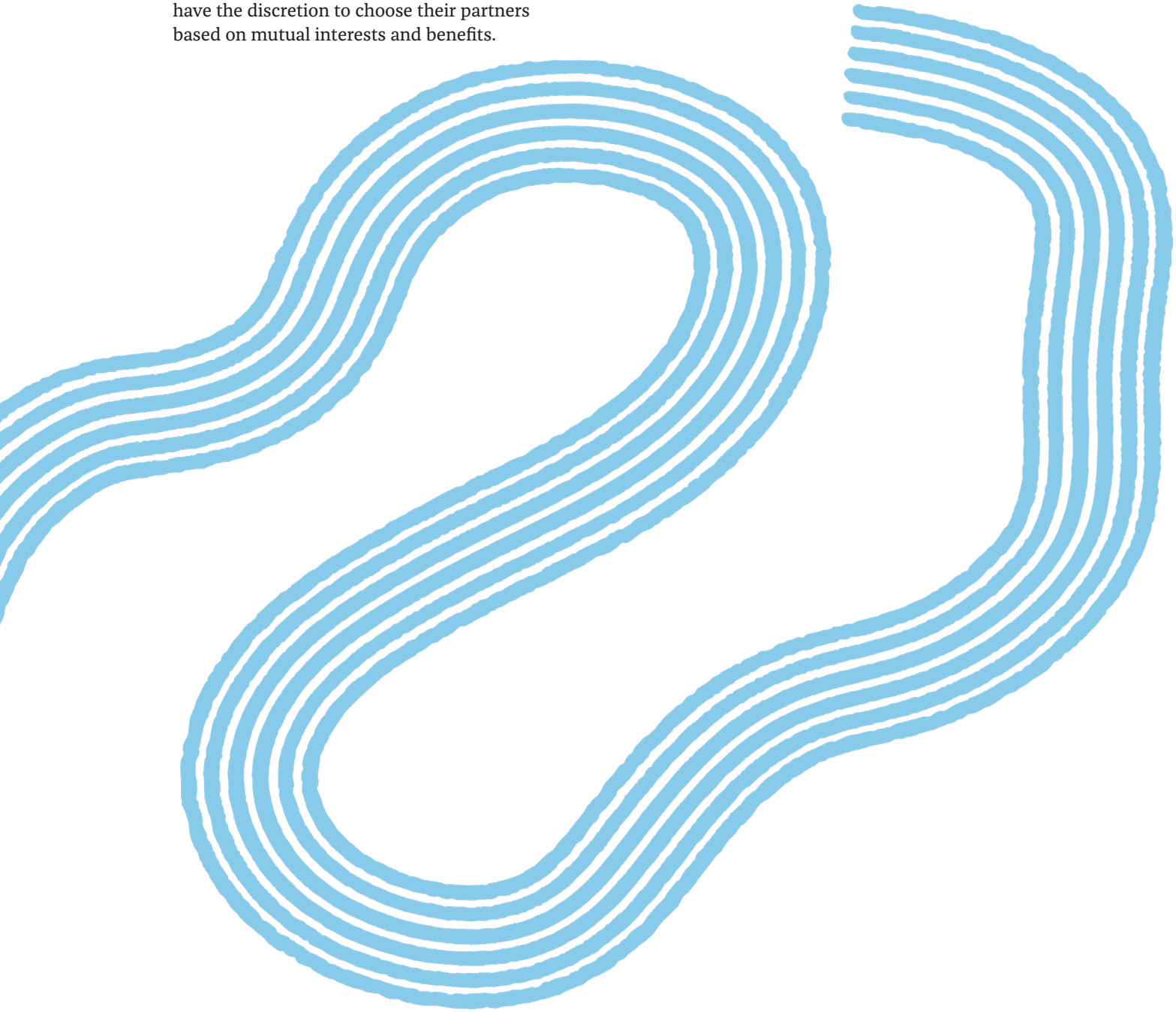
How do China and the DSR fit into African ambitions for digital transformation?

The role of China and its DSR in Africa's digital transformation is multi-faceted and raises questions about international relations and state interests. It's important to consider this in the broader context of global superpower strategies and foreign aid in Africa. When comparing China's approach with initiatives like the White House's digital transformation acceleration program, it becomes evident that foreign aid and cooperation have long been tools of state interest and influence. The apprehension toward China's DSR often contrasts with the reception of similar initiatives from Western powers. This difference in perception could partly be due to the history of colonialism in Africa, which affects how cooperation with different global powers is interpreted. Africa's willingness to cooperate more readily with China or Russia, as opposed to Western countries, might be influenced by a lack of historical colonial ties with these nations.

Regarding China's role in Africa, it's crucial to understand that foreign aid, including digital assistance, is not a new phenomenon. China, like the United States, knows what it stands to gain from its involvement in Africa's digital sphere — a massive market and a testing ground for various technologies. Africa, with its vast population and relative openness to new technologies, presents an attractive opportunity for digital powers like China. The apprehension about China's increasing digital influence in Africa might stem from its status as a digital superpower and its established relationships on the continent. The affordability and accessibility of Chinese technology products make them a preferred choice in many African countries. If China offers digital infrastructure development in addition to its existing contributions, it's likely that African governments would be receptive.

The approach of other superpowers, like the United States and the European Union, which have also pledged significant funds for Africa's digital development, raises similar questions. The mode of implementation of these pledges, whether they involve significant local involvement or are led by foreign experts, can influence the level of acceptance and independence in these partnerships. Ultimately, the dynamics

of international cooperation, historical ties, accessibility of resources and state interests play crucial roles in shaping Africa's digital transformation journey. The choice of partner — whether China, the United States, the European Union or others — will depend on these factors and the specific needs and strategies of individual African countries. As long as international cooperation does not contravene any laws or principles of international relations, states have the discretion to choose their partners based on mutual interests and benefits.



Thelma Efua Quaye, Smart Africa: "Smart Africa navigates through geopolitical competition by diversifying its partnerships and reducing reliance on any single geopolitical entity."

Thelma Efua Quaye heads the Digital Infrastructure Program at Smart Africa. In this role, she oversees projects that will connect every African country to at least two of its neighbours, make internet more affordable and meaningful to citizens, and develop policies to ensure the right balance between the protection of the countries' sovereignty and harnessing the economy around data, among others. Prior to this role, she worked as chief technical officer at Airtel Ghana Limited, and was the first female network director across the Airtel Africa group. She has worked with the ITU, UN Women and the African Union as a lead trainer in coding and soft skills for girls from across Africa.

Smart Africa has become one of the major bodies mobilizing multilateral action on digitalization in Africa. What strategies have proven effective at getting African governments to work together and achieve concrete action toward digital goals, especially concerning cross-border digital trade and international infrastructure projects in partnership with the private sector?

Smart Africa is trusted at both regional and continental levels across Africa and acts as an aggregator. The organization has employed several key strategies to mobilize African governments toward achieving digital goals, especially in cross-border digital trade and international infrastructure projects. One effective strategy that Smart Africa has used is policy harmonization and regional integration, involving the creation of a common regulatory framework that encourages cross-border digital trade and e-commerce. This helps reduce barriers and creates a seamless digital market across African nations.

Smart Africa is positioned as, and focuses on being, the go-to organization for cross-border flagship programs to accelerate the digital agenda of the continent. Unlike regional economic communities, which cover a wide range of topics, Smart Africa is specifically dedicated to digital transformation. This focus allows it to specialize and be more effective in this domain. We also prioritize projects that have a regional scope or impact, supporting countries in their efforts to implement projects with broader cross-border aspirations. This allows countries to focus on both national and regional aspects.

Smart Africa utilizes a multi-stakeholder framework involving African countries, the African Union, the ITU, the UNECA, the African Development Bank, the World Bank, private sector, academia and research institutions. This inclusive approach brings together broad support and mobilizes resources for cross-border digital trade and international infrastructure projects. Furthermore, each member country leads a flagship project involving stakeholders from various sectors. This promotes efficiency, accountability and maintains agility while respecting the sovereignty of African countries.

How does Smart Africa manage the interests of private sector giants (such as telcos) and governments to advance the agenda to create a single digital market in Africa? What roles can/do regional economic communities (for example, ECOWAS, the Economic Community of Central African States [ECCAS], etc.) play to facilitate this?

Smart Africa plays a crucial role in balancing the interests of private sector giants, such as telecommunications companies, and governments to foster a single digital market in Africa. The Private Sector Forum is a consultative organ with the Smart Africa Alliance that discusses matters related to the implementation of its initiatives. This forum includes a diverse range of private sector entities, fostering collaboration and ensuring their interests align with the Smart Africa agenda.

The private sector is also part of our main organs, such as the steering committee where the private sector sits with ministers and the board where the private sector sits with our heads of state, to advise and share their expertise for inclusive decisions taken. Smart Africa emphasizes prioritizing private sector investments, especially in digital infrastructure, recognizing their critical role in achieving a single digital market. As a matter of fact, we say "private sector first" in our manifesto.

Regional economic communities like ECOWAS, ECCAS and others are instrumental in the implementation of Smart Africa's vision. These communities are pivotal in enforcing the guidelines, directives and blueprints developed through Smart Africa's multi-stakeholder approach. Their ability to enforce these standards is vital for the successful realization of the single digital market, ensuring that the initiatives and strategies

formulated by Smart Africa are effectively translated into action at the regional level.

We observe a proliferation of data centres on the continent; one source estimates that as many as 700 new data centres will be built in Africa over the current decade. What is your analysis of the situation regarding the question of digital sovereignty and local data ownership?

The estimated construction of 700 new data centres across Africa in the coming decade marks a pivotal shift in the continent's digital landscape, emphasizing the importance of digital sovereignty and local data ownership. This surge in data centres is a significant step toward bolstering Africa's digital sovereignty, allowing for greater control over local data and reducing reliance on foreign data storage facilities. This is particularly crucial for sensitive information like government records and personal data, which necessitate protection from external jurisdiction.

The growth of data centres supports data localization, where data is stored within its country or region of origin, reinforcing local data ownership, and giving African countries and businesses more control over their data. Economically, this expansion attracts investment, generates jobs and advances technology, while also enhancing the efficiency of digital operations by reducing latency and data storage costs. In the same context, Smart Africa is implementing a project called Regional Data Centre and Cloud, where each region can have a centralized data centre that can interconnect with national data centres.

In conclusion, the proliferation of data centres in Africa presents both opportunities and challenges. By addressing issues related to digital sovereignty, local data ownership and implementing effective regulatory frameworks, African nations can create a resilient and sustainable digital infrastructure that aligns with the broader goals of technological advancement and economic development.

What is your analysis of navigating the digital transformation of Africa within the context of fierce geopolitical competition between the United States, China and Europe? How can African governments/actors exercise more agency despite the asymmetry of this relationship?

Navigating Africa's digital transformation amid intense geopolitical competition from global powers, such as the United States, China and Europe, presents a multifaceted challenge for African governments and actors. This competition, often manifesting in investments and digital infrastructure development, requires a strategic approach to leverage these dynamics for Africa's benefit. African countries can utilize the competitive interests of global powers to negotiate better terms for technology transfer and investments. Establishing clear, independent digital agendas and policies focused on national and regional interests is crucial for aligning decisions with developmental goals free from external influence.

Key to this strategy is promoting regional collaboration through bodies like the African Union and Smart Africa, enhancing bargaining power and presenting a united front in negotiations. Smart Africa's focus on strengthening regional collaborations and supporting member states' national digital programs suggests an approach of fostering regional independence and resilience.

By engaging with a wide range of international organizations and the private sector, Smart Africa navigates through geopolitical competition by diversifying its partnerships and reducing reliance on any single geopolitical entity. At Smart Africa, we are not trying to transform Africa into a single digital island, but rather a single digital market connected with other markets in the world as well.

Based on your experience engaging with African members states, what is your analysis of the African position on issues related to internet governance, digital rights and data protection in international organizations? How can Africa's voice be strengthened in these multilateral fora?

Engagement with African member states on internet governance, digital rights and data protection shows a landscape marked by diversity and evolution. African nations exhibit varied perspectives on internet governance, influenced by their unique political, economic and social contexts. This results in differing approaches, ranging from advocating for an open and free internet to prioritizing state control for reasons like security and political stability. There's a growing acknowledgement of digital rights as human rights across the continent, yet the implementation and enforcement of these rights vary. Many African countries are developing or have recently implemented data protection and privacy laws,

influenced partly by global movements like Europe's GDPR and the Malabo Convention, but effective enforcement remains a challenge.

To strengthen Africa's voice in international fora on these issues, several strategies can be employed. Enhanced regional collaboration, particularly through bodies like Smart Africa, can present a more unified African stance on digital issues, leading to more coherent and influential participation. Capacity building is essential, encompassing training for diplomats, policy makers and stakeholders in internet governance, digital rights and data protection. Active engagement in the formation of international digital policies through regular participation in conferences and working groups is crucial. Forming strategic partnerships with other countries, international organizations and NGOs can amplify Africa's voice, providing support and a platform for shared concerns. Promoting local research and data collection on internet usage and related issues can support African positions on the global stage.

African governments' position is to find a sweet spot between protecting African citizens' rights including privacy, and protecting the sovereignty and interests of African states, while creating an environment that allows African businesses to grow and thrive through greater coordination and cooperation.

Acknowledgements

This compilation of interviews is part of the Negotiating Africa's Digital Partnerships: Interview Series, led by Folashadé Soulé, with African senior policy makers, ministers, and private and civic actors to shed light on how African actors build, negotiate and manage strategic partnerships in the digital sector in a context of geopolitical rivalry. Research assistance was provided by Leslie N. L. Mills. The Negotiating Africa's Digital Partnerships policy research project is hosted by the Global Economic Governance Programme at the University of Oxford and supported by CIGI.

Works Cited

African Union. 2020. *The Digital Transformation Strategy for Africa (2020–2030)*. Addis Ababa, Ethiopia: African Union Headquarters. https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

Aganaba, Timiebi. 2022. "Deriving Meaning through Treaty Interpretation or Is It Time for New Innovative Space Governance Instruments for Space Resources?" *Albany Law Review* 85 (2): 409–38. www.albanylawreview.org/article/55754-deriving-meaning-through-treaty-interpretation-or-is-it-time-for-new-innovative-space-governance-instruments-for-space-resources.

Aganaba, Timiebi and Etim Offiong. 2022. "Africa's growing space enterprise." *Science* 376 (6591): 329. www.science.org/doi/10.1126/science.abq5570.

Akuetteh, Teki and Michael Pisa. 2022. "Upgrading the Africa-EU Digital Relationship." *Center for Global Development* (blog), February 15. www.cgdev.org/blog/upgrading-africa-eu-digital-relationship.

Beard, Stephen. 2021. "Data centres are a growing investment opportunity in Africa." Knight Frank, April 7. www.knightfrank.com/research/article/2021-04-07-data-centres-are-a-growing-investment-opportunity-in-africa.

Bhagavan, M. R., ed. 1997. *New Generic Technologies in Developing Countries*. London, UK: MacMillan.

Capri, Alex. 2020. "Techno-nationalism and diplomacy." Hinrich Foundation, October 2. www.hinrichfoundation.com/research/wp/tech/techno-nationalism-and-diplomacy/.

Dahir, Abdi Latif. 2018. "China 'gifted' the African Union a headquarters building and then allegedly bugged it for state secrets." Quartz, January 30. https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years.

Daigle, Brian. 2021. "Data Protection Laws in Africa: A Pan-African Survey and Noted Trends." *Journal of International Commerce and Economics*. February. www.usitc.gov/staff_publications/jice/data_protection_laws_africa_pan_african_survey_and.

Flynn, Michael, Kirk Buffington and Richard Pennington. 2020. *Legal Aspects of Public Procurement*. 3rd ed. New York, NY: Routledge. www.routledge.com/Legal-Aspects-of-Public-Procurement/Flynn-Buffington-Pennington/p/book/9780367471729.

Haroun, Fawaz, Shalom Ajibade, Philip Oladimeji and John Kennedy Igbozurike. 2021. "Toward the Sustainability of Outer Space: Addressing the Issue of Space Debris." *New Space* 9 (1): 63–71. https://doi.org/10.1089/space.2020.0047.

Hogan Lovells. 2023. *Recent developments in African data protection laws: Outlook for 2023*. February 24. London, UK: Hogan Lovells. www.engage.hoganlovells.com/knowledgeservices/news/recent-developments-in-african-data-protection-laws-outlook-for-2023.

International Space Exploration Coordination Group. 2021. *In-Situ Resource Utilization Gap Assessment Report*. April 21. International Space Exploration Coordination Group.

International Trade Centre. 2022. *Made by Africa: Creating Value through Integration*. Geneva, Switzerland: International Trade Centre. https://au.int/en/documents/20221123/made-africa-creating-value-through-integration.

Kadiri, Ghalia. 2018. "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin." *Le Monde*, January 26. www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

Karombo, Tawanda. 2020. "The US development corp is betting $300 million on Africa's rising demand for data storage." Quartz, December 11. https://qz.com/africa/1945156/us-dfc-bets-300m-on-africas-demand-for-data-storage-centers.

King'ori, Mercy. 2023. "Nigeria's New Data Protection Act, Explained." *Future of Privacy Forum* (blog), June 28. https://fpf.org/blog/nigerias-new-data-protection-act-explained/.

Mozur, Paul and John Liu. 2023. "With Ban on Micron, China Escalates Microchip Clash With U.S." *The New York Times*, May 22. www.nytimes.com/2023/05/22/business/micron-technology-china-ban.html.

Musau, Dennis. 2023. "Kenyan Phones To Retail From Ksh.7,499 As First Assembling Plant Opens In Athi River." Citizen Digital, October 30. www.citizen.digital/business/kenyan-phones-to-retail-from-ksh7499-as-first-assembling-plant-opens-in-athi-river-n330296.

National Space Council Users' Advisory Group. 2020. "Assessing the Utility of a U.S. Strategic In-Space Propellant Reserve: Economic Development in Low Earth Orbit and Cislunar Space." White Paper on Strategic In-Space Propellant Reserve. September 3.

Nellis, Stephen, Karen Freifeld and Alexandra Alper. 2022. "U.S. aims to hobble China's chip industry with sweeping new export rules." Reuters, October 10. www.reuters.com/technology/us-aims-hobble-chinas-chip-industry-with-sweeping-new-export-rules-2022-10-07/.

Office of the United States Trade Representative. 2019. "Fact Sheet on 2019 National Trade Estimate: Key Barriers to Digital Trade." March. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/march/fact-sheet-2019-national-trade-estimate.

Onwudiwe, Memme and Kwame Newton. 2021. "Africa and the Artemis Accords: A Review of Space Regulations and Strategy for African Capacity Building in the New Space Economy." *New Space* 9 (1): 38–48. https://doi.org/10.1089/space.2020.0043.

Ross, Aaron, James Pearson and Christopher Bing. 2023. "Exclusive: Chinese hackers attacked Kenyan government as debt strains grew." Reuters, May 24. www.reuters.com/world/africa/chinese-hackers-attacked-kenyan-government-debt-strains-grew-2023-05-24/.

Rwanda Space Agency. 2021. "Feedback from: Rwanda Space Agency." European Commission, November 18. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13163-Space-traffic-management-development-of-an-EU-strategy-for-safe-and-sustainable-use-of-space/F2752179_en.

Satter, Raphael. 2020. "Exclusive – Suspected Chinese hackers stole camera footage from African Union – memo." Reuters, December 16. www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idINKBN28Q1DB/.

Simons, Bright. 2021. "All Problems are Connected, So Must the Solutions." The Scarab, December 10. https://brightsimons.com/2021/12/10/all-problems-are-connected-so-must-the-solutions/.

Space in Africa. 2022. "Nigeria and Rwanda sign NASA Artemis Accord." Space in Africa, December 13. https://spaceinafrica.com/2022/12/13/nigeria-and-rwanda-sign-nasa-artemis-accord/.

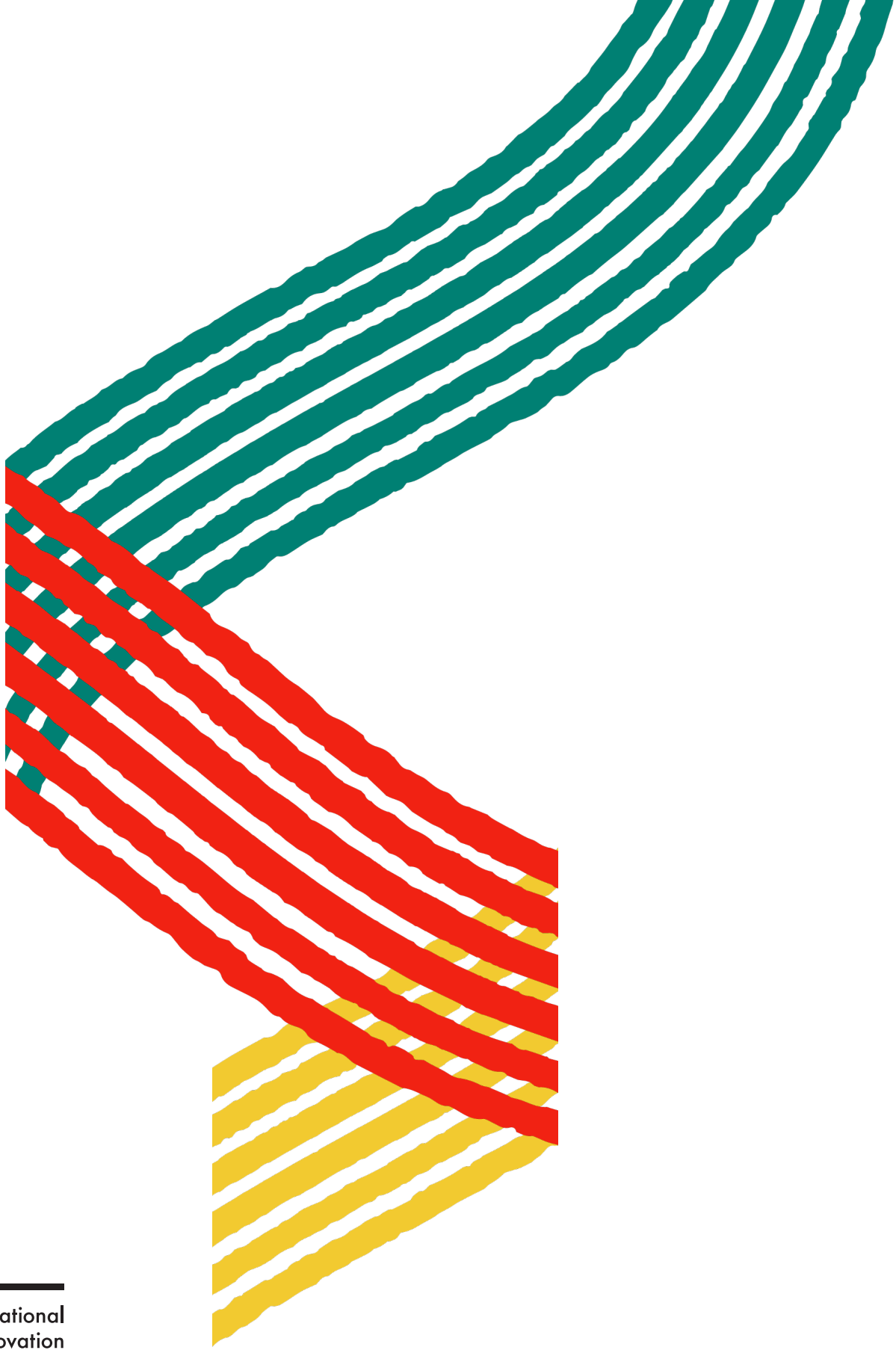
Tayeb, Zahra. 2021. "Africa is poised to be a significant player in the new space age — especially when it comes to governance. Here's why." *Business Insider*, September 19. www.businessinsider.com/africa-space-age-tourism-exploration-governance-2021-9.

Si, Ma. 2023. "China to strengthen digital cooperation with African countries." *China Daily*, October 20. https://global.chinadaily.com.cn/a/202310/20/WS6531e1bca31090682a5e9b92.html.

United Nations Conference on Trade and Development. 2020. Commodities at a Glance: Special issue on strategic battery raw materials. No. 13. Geneva, Switzerland: United Nations. https://unctad.org/publication/commodities-glance-special-issue-strategic-battery-raw-materials.

Victoria, Ana. 2020. "The EU-AU Data Flagship." Digital 4 Development Hub Forum, December 8. European Commission. https://futurium.ec.europa.eu/en/Digital4Development/discussion/eu-au-data-flagship.

Walker, Daniel and Bridgit Mendler. 2022. "International Space Law & Emerging Economies: Rwanda Case Study." ASCEND 2022, October 24–26, Las Vegas, NV. https://arc.aiaa.org/doi/10.2514/6.2022-4281.



Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org