Stronger digital voices from Africa

Building African digital foreign policy and diplomacy

November 2022

DiPLO

www.diplomacy.edu

Stronger digital voices from Africa: Building African digital foreign policy and diplomacy

Published by DiploFoundation

Lead authors: Sorina Teleanu, Jovan Kurbalija

Key contributors: Katarina Bojović, Andrijana Gavrilović, Katharina Höne, Marília Maciel

Research support: Arvin Kamberi, Grace Mutung'u, Mwende Njiraini, Judy Okite, Barrack Otienoo

Reviewers: Amr Aljowaily, Souhila Amazouz, Adama Ndiaye, Nanjira Sambuli, Million Hailemichale Tolessa, Mesfin Fikre Woldmariam, Seble Girma Workneh

Copy-editing: Írj Jól Kft.

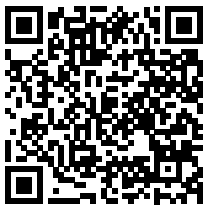
Layout, design, and illustrations: Mina Mudrić and Viktor Mijatović, Diplo CreativeLab

The publication of this study is possible thanks to funding from Switzerland's Federal Department of Foreign Affairs (FDFA). The study does not necessarily represent the views or positions of the FDFA.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

Download the pdf version



About this study

Africa's voices are weak in negotiations on digital topics, from cybersecurity to the future of data and e-commerce. The continent's participation in global policy-making does not reflect its current digital dynamism, with millions becoming connected, e-commerce growing rapidly, and new solutions being created.

As Africa's digital dynamism grows, its participation in global digital policy must increase. In this transition, African countries have to navigate the geopolitical realities of our times.

This study provides a snapshot of Africa's digital diplomacy by examining the holistic representations of national and continental interests in the digital realm. In addition to the role of official diplomacy, this study also looks at the roles of tech developers, businesses, local communities, and others with the necessary skills and expertise for participation in international digital policy.

It is critical that many African countries mobilise all human and institutional resources to enable their active engagement in digital foreign policy and diplomacy. While most African countries are in the early phase of their digital diplomacy journey, there are many practices and initiatives that could help a faster take off of digital diplomacy in Africa. These practices and initiatives are identified in this study with many concrete examples, 55 charts and infographics, over 500 references, and case studies of 8 African countries.

Although the study is focused on Africa, it is fundamentally about digitalisation worldwide. The digital realm cannot be developed into an enabling, secure engine for human prosperity without Africa's active involvement in digital diplomacy.

We invite everyone to join us on this policy and learning journey towards *Stronger Digital Voices from Africa*.

Sorina Teleanu and Jovan Kurbalija

Table of contents

Executive summary

As late-comers to digitalisation and digital transformation processes, countries in Africa lag behind in terms of digital development. But while internet penetration rates are still at low levels (although the growth rates are considerable) and digital divides within countries remain high, governments and regional institutions are putting in place policies and strategies to encourage the uptake of digital technologies as drivers of development and to foster inclusive digital economies and societies.

Beyond initiatives focused on advancing digital development at a national, regional, and continental level, Africa also needs stronger voices in global digital governance. And while countries across the continent do not have dedicated digital foreign policy strategies, elements of such policy can be found in various digital strategies and other national documents, as well as identified in contributions of African countries to global digital policy processes. Our study explores such elements and makes the case for a more active engagement of African stakeholders in organisations and processes that tackle key internet and digital policy issues.

There is a strong opinion that Africa could – and should – use digital transformation as an opportunity to take the destiny of countries, citizens, and communities in the continent's own hands, instead of being on the receiving end of global geopolitical and geoeconomic battles (as has happened many times in the past). A sustained engagement in global digital governance could contribute to this, by ensuring that African interests, priorities, and goals are meaningfully considered.

Global trends in digital foreign policy and diplomacy

Before diving into the African digital (foreign) policy scene, we look at one emerging trend in digital diplomacy: the adoption of digital foreign policy strategies. Countries have begun elaborating such strategies as a way to anchor digital issues more firmly in their foreign policy.

An analysis of the digital foreign policy strategies of Australia, Denmark, France, the Netherlands, and Switzerland reveals several key issues: digital infrastructure, digital as a factor in development, cybersecurity, economic issues (e-commerce and trade in particular), and human rights (e.g. privacy, freedom of expression). In addition to outlining goals and objectives to be achieved in relation to these issues, the strategies also emphasise an integrated dual approach to digital foreign policy: the *whole-of-government* approach, in which ministries of foreign affairs are joined by other ministries and agencies in conducting foreign policy, and the *whole-of-society approach*, which recognises that non-state actors – the business sector, the technical community, civil society, and academia – have an important role to play as well.

The adoption of dedicated digital foreign policy strategies, however, is not the only way for countries to integrate digital issues into their foreign policies. This can also be done through embedding digital issues into general foreign policy strategies, or through including elements of foreign policy in digital-related strategies and policies dealing with issues such as cybersecurity, digital economy, and infrastructure.

Elements of digital foreign policy in Africa

Holistic approach

Despite not having elaborated specific digital foreign policy strategies, African countries have embedded elements of foreign policy in various strategies and plans, be they related to the overall digitalisation and digital transformation of the economy and society, or focused on specific issues such as cybersecurity, broadband, or digital economy.

When countries elaborate plans and policies focused on digitalisation and digital transformation in a holistic manner (e.g. Kenya's *National Digital Master Plan* or Côte d'Ivoire's *National Digital Development Strategy*), they often outline outward-looking goals. Such goals are related to enhancing countries' competitiveness on international markets; building partnerships with international entities (e.g. donors, development agencies and banks, regional and international intergovernmental organisations, multinational tech companies) to help achieve domestic digital transformation goals; fostering overall international cooperation on digital policy topics; and harmonising ICT/digital-related domestic policies and legal and regulatory frameworks with relevant international frameworks.

Similar goals also appear in continental and regional policies adopted at the level of the African Union (AU) and various regional economic communities (RECs). The AU's *Agenda 2063* and the *Digital Transformation Strategy* talk, for instance, about strengthening the continent's presence in the global digital economy (as both a producer and a consumer), fostering cooperation with international entities on issues such as advancing digital skills and supporting digital entrepreneurship, and increasing participation in international internet governance and digital policy processes.

Beyond domestic policies, countries' priorities and goals are also reflected in their contributions to international processes that address digital policy issues. To illustrate, the number of African countries raising digital topics – digital inclusion, cybersecurity, digital economy, and human rights – in their interventions at the UN General Assembly (the General Debate) increased from 8 in 2017 to 24 in 2022. But this still represents less than half of all countries in the region. At the UN Security Council, Ghana, Kenya, and South Africa – which have held non-permanent member seats recently – have been particularly active in discussions on the interplay between digital technologies and peace and security.

Over the past five to six years, there has been a sustained engagement of African actors – in particular, civil society – in meetings of the Internet Governance Forum (IGF). This engagement has also led to the launch of a growing number of national and regional IGF initiatives across the continent – forums that governments and regional institutions could help strengthen and then leverage as spaces to advance a whole-of-society approach to digital governance and foreign policy.

Digital infrastructure and standards

Policies related to strengthening or expanding internet infrastructures propose actions to be implemented at a national, regional, or continental level, but also include international dimensions. National broadband or 5G policies (e.g. in Kenya, Nigeria, Senegal, and South Africa), the AU's *Digital Transformation Strategy,* and various initiatives across RECs talk about working with international partners/investors to boost infrastructure deployment, ensuring regional and international coordination on radio frequency matters and enhancing participation in relevant forums (e.g. the International Telecommunication Union (ITU)), and garnering support from international institutions to develop enabling policy environments.

The adoption and enforcement of international technical standards and strengthened participation in relevant standardisation processes are also envisioned as goals in several domestic policies and strategies (e.g. Ghana, Kenya, Namibia, Nigeria, Senegal, and South Africa).

Actors from all African countries participate at ITU; these include not only specialised ministries or agencies, but also academic institutions, telecom operators, internet service providers (ISPs), and other private entities. Some of these actors – from countries such as Algeria, Côte d'Ivoire, Egypt, Ghana, Morocco, Nigeria, Rwanda, Sudan, and Tunisia – also hold leadership roles across several study groups of ITU Sectors. There is also a relatively strong engagement of African actors – in particular from the technical community and civil society – in the work of the Internet Corporation

for Assigned Names and Numbers (ICANN). Compared with the relatively good participation of African actors in ITU standardisation work, there is less involvement in other international standardisation processes such as the International Organization for Standardization (ISO) and the Internet Engineering Task Force (IETF).

Human rights

Privacy and personal data protection in the context of digital services and technologies is a concern that most African countries have tried to address through data protection laws. But differences between such laws and enforcement difficulties create a complex and unharmonised environment, which tends to put Africa at a disadvantage in the global digital economy. The *AU Data Policy Framework* is expected to contribute to addressing some of these challenges.

Other challenges the continent faces when it comes to human rights in the digital space take the form of internet restrictions (e.g. social media shutdowns, content throttling measures, or complete internet blackouts). In 2019, the African Commission on Human and Peoples' Rights (ACHPR) called on countries to refrain from measures involving removing, blocking, or filtering content, unless they comply with international human rights law.

Civil society groups are particularly active in matters related to digital rights, as demonstrated by their leadership in the development of the *African Declaration on Internet Rights and Freedoms*. Many of them are also actively contributing to various international processes and initiatives, such as the IGF and the Human Rights Council (HRC). In recent years, there has also been some African government involvement – such as Egypt, Ghana, Namibia, Nigeria, South Africa, and Tunisia – in HRC discussions on issues related to digital technologies and human rights.

Cybersecurity, cybercrime, and child online protection

Statistics place Africa among the regions with the highest exposure to cyberattacks, but less than half of the African governments have adopted or drafted cybersecurity strategies. The situation is better with cybercrime laws, which are in place or under development across most of the continent. Several countries have also included aspects related to the protection of children online in various digital-related policies or strategies.

Where cybersecurity or cybercrime policies exist, they also include elements of foreign policy, as they highlight objectives related to greater international cooperation in areas such as collaboration between computer emergency response teams (CERTs), fostering capacity building and knowledge sharing on fighting cybercrime, upholding international cybersecurity norms, and promoting the application of international law. Strengthening regional and international cooperation is also a shared goal of several strategies, policies, or model laws on cybersecurity, critical infrastructure protection, and cybercrime adopted by RECs.

The AU's most ambitious cybersecurity initiative – the *Convention on Cyber Security and Personal Data Protection (Malabo Convention*) – is yet to reach the threshold number of ratifications to come into force. The convention's main goal of bringing some harmonisation to cybersecurity and cybercrime policies remains a challenge. At the same time, the number of African countries that join the Council of Europe (CoE) *Convention on Cybercrime (Budapest Convention)* is constantly increasing.

When it comes to international processes, some countries – such as Côte d'Ivoire, Egypt, Ghana, Kenya, Morocco, Nigeria, and South Africa – have actively contributed to the UN Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security (later renamed OEWG on security of and in the use of information and communications technologies). Algeria, Egypt, Ghana, Namibia, and South Africa are among the African countries that have engaged in the work of the Cybercrime Ad Hoc Committee. The African region also has some participation (through governmental and non-

governmental bodies) in multistakeholder processes and initiatives, such as the Global Forum on Cyber Expertise (GFCE) and the Paris Call for Trust and Security in Cyberspace.

Digital economy

Africa's digital economy is on a growing trend, but there are significant differences between countries, both in terms of growth rates and the development of enabling policy frameworks. For instance, in 2020 the internet economy represented 7.7% of Kenya's GDP and only 1.27% of Ethiopia's GDP. At the end of 2021, only 28 African countries had consumer protection laws in place, while 33 had adopted e-transaction laws. There are also variations in policy and regulatory frameworks dealing with data flows and digital service taxes.

Some countries, such as Côte d'Ivoire, Kenya, and Senegal, have adopted plans for the development of the digital economy, which also include outward-looking goals, from supporting the expansion of e-commerce beyond national borders to advancing a single digital market across Africa. In the area of digital payments and financial services, countries tend to share common goals: advancing financial inclusion, creating a resilient and inclusive digital payments ecosystem, harmonising rules, and ensuring alignment with international standards and principles.

As the adoption rate for cryptocurrencies and crypto assets is on a continuously growing trend, and Africa is becoming increasingly attractive for crypto companies, policy and regulatory initiatives are also taking up. These range from the Central African Republic's decision to accept cryptocurrencies as legal tender and Nigeria's launch of a central bank digital currency, to South Africa looking into bringing crypto assets into the regulatory remit.

At the continental level, the African Continental Free Trade Area (AfCFTA) is expected to unleash the potential of a large single (digital) market and foster inter-Africa digital trade, while RECs also have various policies and initiatives related to e-commerce and trade that could play a key role in advancing the integration of markets at the regional level.

Seven African countries (Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Kenya, Mauritius, and Nigeria) participate in the Joint Statement Initiative (JSI) on e-commerce at the World Trade Organization (WTO). On matters of taxation, 25 African countries have joined the agreement on new global corporate tax rules led by the Organisation for Economic Co-operation and Development (OECD). Two major economies in the region – Kenya and Nigeria – have opposed the agreement.

Artificial intelligence

Artificial intelligence (AI) investment, innovation, and implementation are taking up across Africa – in particular in countries such as Egypt, Nigeria, Kenya, and South Africa – and multinational companies (e.g. Google and IBM) are tapping into the region's AI research potential. At the same time, governments increasingly understand the importance of adopting AI policies. Egypt and Mauritius have AI strategies, while Ethiopia, Ghana, Rwanda, South Africa, and Uganda are among the countries working on policies focused, for instance, on encouraging AI innovation and research and fostering the development of AI-related capacities and skills.

At the continental level, the AU is also looking into the development of a pan-African AI strategy, while the ACHPR has been calling for legal and regulatory frameworks to ensure that AI is developed and implemented in a human-centric manner.

A few African governments have contributed to the discussions taking place within the United Nations Educational, Scientific and Cultural Organization (UNESCO) on the *Recommendation on the Ethics of AI*. There has also been some involvement of African countries in multilateral discussions on lethal autonomous weapons systems (LAWS).

Sociocultural issues

As governments and regional institutions advance digital ID initiatives, sometimes with the support of international partners, there are calls to foster interoperability among national solutions, and to ensure that privacy and security concerns are properly addressed.

With Africa still one of the regions with the widest digital gender gaps, governments are taking steps to advance gender equality and facilitate women's and girls' access to digital technologies and the digital economy, while also strengthening their protection in the digital space.

Aware that advanced digital skills are essential in building sustainable digital societies and competitive digital economies, governments are outlining actions and goals related to digital capacity development in various policies and strategies. Some countries, like Kenya, Ghana, Rwanda, and South Africa, aspire to leverage their human talent to become regional or even global leaders in certain digital areas, while Nigeria's goal is to become a global outsourcing destination for digital jobs. The development of digital skills is the goal behind multiple capacity development initiatives conducted throughout Africa with the engagement of regional and international organisations, as well as the technical community and civil society.

Geopolitics

Digital topics are becoming increasingly prominent in Africa's relations with its partners. On broad governance issues, the EU, the USA, and China are all aiming to attract the support of African nations for initiatives such as the USA- and EU-led *Declaration for the Future of the Internet* and the Chinese *Initiative on Jointly Building a Community with a Shared Future in Cyberspace*. All three actors are engaged in various initiatives to support the development of digital infrastructures across the continent, including China's Belt and Road Initiative (BRI) and the new Global Development Initiative; the G7 Partnership for Global Infrastructure and Investment, spearheaded by the USA; and the EU's Global Gateway.

These actors are also paying more attention to other digital topics in their relations with African countries. China's approach to Africa is evolving from one focused on infrastructure to a more comprehensive approach also covering other digital governance issues, including e-commerce and the digital economy, cybersecurity, and capacity development. The EU is looking into supporting the growth of the digital economy across the continent, as well as the development of enabling policy and regulatory environments for inclusive and human-centric digital economies and societies. The USA is increasingly seeing Africa as the place to carry out its digital competition with China. India has also placed digital as a priority for its cooperation with Africa, in particular in areas such as digital health, e-government, and digital IDs.

In the fast-changing digital geopolitical landscape, African countries aim to follow their own priorities and avoid taking sides, for instance in the USA-China digital competition. Instead of looking to be strategically aligned with major digital political powers, African nations tend to be more interested in diversifying their technological base and strengthening digital governance by making tactical decisions based on the affordability of technology and its impact on social and economic growth.

Recommendations

African countries might not have specific digital foreign policy strategies, but they do outline foreign policy priorities and goals in various other plans and strategies dealing with digital issues (digital economy, cybersecurity, broadband, skills, etc.). Several governments also actively follow

the digital agenda in the work of intergovernmental organisations, such as ITU, OECD, and the HRC, or have made it a goal for themselves to strengthen engagement in international processes. Moreover, stakeholders from the business, technical, civil society, and academic communities can be seen as actors of foreign policy, as they represent regional and national interests through their participation in international processes such as the IGF and ICANN.

Governments and continental and regional initiatives should build on these realities to strengthen their engagement in international digital processes and ensure that their interests and needs are meaningfully considered. As guidelines, policies, and rules set at the international level have implications at national and regional levels, it is important to ensure that such frameworks are shaped in a way that reflects as many national and regional realities as possible. Moreover, the active participation of African actors in global digital policy is not only about advancing their interests, but also the key to building an inclusive, safe, secure, and sustainable digital future for humanity. To this end, actions that could be undertaken by African governments and regional and continental organisations should focus on the following:

- Ensuring that digital priorities are clearly reflected in foreign policies/international relations.
- Prioritising engagement in specific international digital governance processes that reflect national, regional, and/or continental priorities.
- Strengthening participation in International Geneva, where many digital policy issues of relevance for Africa are addressed (e.g. infrastructure issues at ITU and e-commerce issues at the WTO).
- Continuing to prioritise economic and development considerations related to digital issues – over geopolitical ones – in bilateral and multilateral relations, in line with national priorities and interests.
- Strengthening the whole-of-government and whole-of-society approaches to digital governance and digital foreign policy.
- Fostering coordinated positions of African countries in international digital governance, for instance through the AU or RECs.
- Devising long-term approaches for building academic, research, and digital policy capacities of the next generation of African diplomats and policymakers.

The publication of this study is possible thanks to funding from Switzerland's Federal Department of Foreign Affairs (FDFA).

This study does not necessarily represent the views or positions of the FDFA.

Introduction

Over the past two decades, digital issues have emerged on diplomatic agendas at bilateral, regional, and global levels. Countries and other actors have been addressing cybersecurity, standardisation, privacy, e-commerce, and more than 50 other digital policy issues.

Digital issues are addressed in a wide range of policy spaces. At the UN specialised agencies, countries discuss telecommunication infrastructure (International Telecommunication Union – ITU), e-commerce (World Trade Organization – WTO), digital health (World Health Organisation – WHO), and digital aspects of many other global policy issues. Multistakeholder spaces and processes have also been created, such as the Internet Corporation for Assigned Names and Numbers (ICANN) for managing critical internet resources, or the Internet Governance Forum (IGF) for addressing digital issues in inclusive and holistic ways.

To respond to the need to negotiate internationally, countries worldwide have started defining digital priorities and interests. Put together, these priorities and interests form a country's digital foreign policy. In some cases, they are clearly spelled out in dedicated digital foreign policy strategies or integrated into overall foreign policy strategies. In other cases, countries include foreign policy elements in their various strategies and plans focused on digital topics (e.g. digital development, cybersecurity, digital economy).

Against this backdrop, this study focuses on the digital policy landscape in Africa and explores the following research and policy questions:

What are Africa's digital policy priorities and how are they reflected in the countries' foreign policies and international relations?

How can African digital voices be strengthened globally to ensure that their priorities are advanced and interests protected?

As of October 2022, no African country had a digital foreign policy strategy codified in one dedicated document. However, many of them have started developing principles and practices as building blocks for digital foreign policy strategies.

Our study identifies these building blocks in the holistic approach of African countries to digital transformation as well as in their policies dedicated to several focus areas (digital infrastructure and standards; cybersecurity, cybercrime, and child protection online; digital economy; human rights; sociocultural issues; and artificial intelligence (AI)). We do so through a two-tier approach.

We first look at official digital and information and communications technology (ICT) policies and strategies of selected countries, identifying aspects that relate to international relations, engagement in international processes, and positioning on international markets.

For instance, when countries draft strategies covering various digital policy issues (e.g. cybersecurity, e-commerce, broadband), to what extent do they include goals and actions related to engagement in international organisations dealing with such issues? Do they refer to aligning national policies and legislation with relevant international frameworks? Do they count on support from international partners (e.g. donors, development banks) to achieve goals such as meaningful universal access?

Eight focus countries

While the study covers Africa broadly, our more in-depth analyses (overview of policies and regulations, and contributions to selected international processes) focus on eight countries: Côte d'Ivoire, Ghana, Kenya, Namibia, Nigeria, Rwanda, Senegal, and South Africa. Other countries are also mentioned sporadically.

Annex I provides an overview of digital diplomacy and foreign policy elements of these eight countries. The first part sets the stage by offering an illustrated comparative analysis of these eight countries, which differ in digital developments, priorities, and involvement in international activities. The second part includes a digital profile for each country, with statistics and rankings, national strategies and legislations, and the involvement levels of respective countries in global digital policy.

Relevant national digital developments are also covered to the extent that they (may) impact countries' foreign policies. For example, we look at whether countries have cybercrime and data protection laws and regulations. Where they exist, they can provide the basis for engagement in relevant international processes (e.g. UN negotiations on a cybercrime treaty); where they do not, we recommend that countries follow regional and international good practices and reflect them in their national context and regulatory landscape.

The national overview is followed by a look at relevant continental and regional initiatives – in particular within the African Union (AU) and various regional economic communities (RECs) – and their (potential) international dimensions.

Our study then focuses on the participation of African stakeholders – governments, businesses, the tech community, and civil society, as relevant – in global processes such as the UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies (previously known as OEWG on developments in the field of information and telecommunications in the context of international security), ITU, the IGF, and the Global Forum on Cyber Expertise (GFCE).

We find out that Africa needs stronger voices in global digital governance. While some African countries participate in certain international negotiations on digital rules (e.g. at ITU, the WTO, or the Organisation for Economic Co-operation and Development (OECD)), such participation can be strengthened and expanded. There is more vibrancy when it comes to the engagement of the African technical community and civil society in multistakeholder processes such as ICANN and the IGF. Leveraging such engagement and the expertise of these stakeholders could contribute to raising the visibility of African voices in global settings.

The study is inspired by the three-circle approach to digital diplomacy and governance (Figure 1):

- **A whole-of-diplomacy** approach connects via digitalisation all segments of diplomatic service: headquarters and diplomatic missions; bilateral and multilateral departments; and consular, cultural, and other specialised departments.
- **A whole-of-government** approach connects various government ministries and departments involved in digital foreign policy (e.g. defence, security, culture, finance, trade).
- **A whole-of-country or whole-of-society** approach galvanises all national talents and resources to support foreign representation including business, academia, technical community, and civil society.

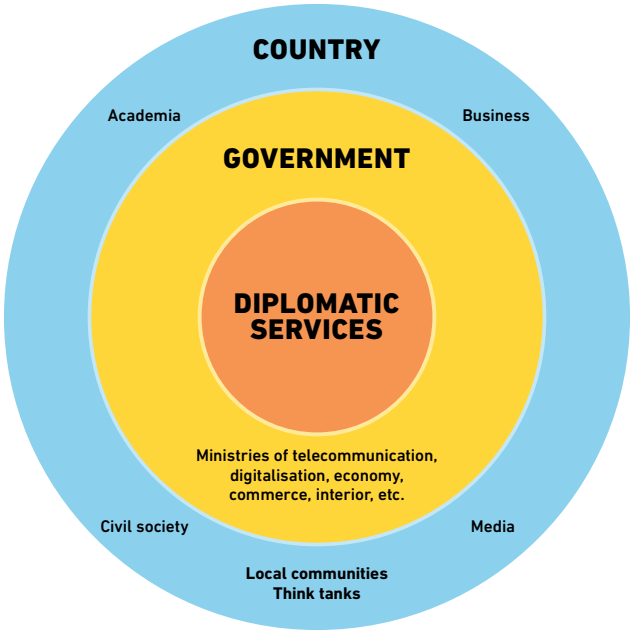


Figure 1. Whole-of-country approach to digital foreign policy.

As African countries and regional organisations shape their digital policies and priorities, other countries become relevant allies in promoting these policies globally and in shaping debates and agendas. We dedicate a section to exploring relations with the EU, the USA, China, and India not only because they are important actors in global governance processes, but also because of their own priorities and presence in Africa.

Finally, the study provides concrete recommendations on what African countries can do to strengthen their voices in global digital governance. This starts with low-hanging fruit, such as strengthening participation in digital negotiations happening in International Geneva, one of the global digital capitals hosting many intergovernmental organisations. It then shifts into more medium-term perspectives, such as galvanising existing national capacities in the business and tech sector to enhance the countries' participation in international digital policy, and strengthening diplomatic capacities. Also included are recommendations for long-term approaches for building academic, research, and policy capacities of the next generation of African diplomats and policymakers.

In sum, this study identifies existing building blocks (and missing pieces) for African digital foreign policies and diplomacy, and outlines the picture of African involvement in international policy processes in the digital realm. It also proposes practical steps for the development of African digital diplomacy by strengthening the voices of national and regional actors.

I
Global trends in digital foreign policy and diplomacy

Chapter summary

In recent years, digitalisation and digital issues have started to be more firmly anchored in foreign policy. Several countries have begun to elaborate dedicated digital foreign policy strategies, establish specialised ambassadorial posts (e.g. tech ambassadors), and create dedicated teams within ministries of foreign affairs (MFAs) to address digital issues.

As the digital foreign policy strategies of Australia, Denmark, France, the Netherlands, and Switzerland illustrate, key topics of digital foreign policy include digital infrastructure, digital as a factor in development, cybersecurity, economic issues (e-commerce and trade in particular), and human rights (e.g. privacy, freedom of expression).

Given the breadth of digital foreign policy, there is an emphasis on *whole-of-government* and *whole-of-society* approaches. The whole-of-government approach means that MFAs conduct foreign policy in coordination with other ministries and agencies. The whole-of-society approach recognises that non-state actors – the business sector, the technical community, civil society, and academia – are affected by digital foreign policy and have an important role to play in its conduct.

Digital foreign policy strategies can be developed to different levels of detail and maturity, each with its advantages and disadvantages. Very detailed strategies include values, priorities, goals, proposed measures, and ownership for implementation. More lightweight strategies might include a vision and general principles but stay away from details and specific measures. Overall, strategies can benefit from embedding the following principles: vision, context, comprehensiveness, clarity, and coordination.

But having a dedicated digital foreign policy strategy is not the only approach. Some countries tackle digital issues in their overall foreign policy strategies, and others have various digital-related strategies and policies that touch on foreign policy issues. When deciding which approach to follow, governments should assess the various options against the backdrop of their own national contexts, priorities, and resources.

Foreign policy describes the sum of policies that a state has adopted towards its external environment.[1] This can take the form of articulated strategies and priorities, but also more implicit positions that derive from domestic policies, domestic and international dialogues, and interactions with domestic and international stakeholders. Foreign policy is a way for a state to define and safeguard its interests abroad. Some scholars also include tools of implementation in the overall framework of foreign policy. They argue that 'reduced to its fundamental ingredients, foreign policy consists of two elements: national objectives to be achieved and the means for achieving them.'[2]

The emergence of *digital* foreign policy is a relatively recent development. Digitalisation and digital issues were put on the global agenda around 20 years ago. After the 1990s, during which digital issues were largely perceived as technical issues to be handled by technical experts and highly specialised organisations, governments and MFAs have started to pay closer attention.

The World Summits on the Information Society (WSIS 2003 and 2005) were pivotal in beginning to position digital issues on the global agenda. Yet, it is only over the last five years or so that digitalisation and digital issues have become more firmly anchored in foreign policy. This observation is based on three points. First, since 2017 countries have begun to release dedicated and comprehensive digital foreign policy strategies. Second, at the same time, specialised ambassadorial posts – tech ambassadors, for example – have been established by several Western countries. Third, dedicated teams to address digital issues have emerged in selected MFAs.

Note on terminology: Digital and digitalisation

In our work, we use the term *digital* as an umbrella term for a variety of issues related to digitalisation. Digitalisation describes technological developments but also their social, economic, and political impact. Hence, digital foreign policy includes topics such as cybersecurity, e-commerce, human rights online, and many others. It also includes the various actors relevant in the digital space and necessitates taking a multistakeholder perspective.

Digital foreign policy exists at the intersection of several more traditional foreign policy fields, including security, economy, and development. In addition to impacting these traditional fields, digital foreign policy also raises a number of unique questions that do not easily fit into these established categories. This includes for example privacy and data protection, which are both no longer only issues of national concern. In addition, governing the internet has moved from a technical question to a political one and brings infrastructure and standardisation issues into sharper focus. Frontier digital technologies such as AI and quantum computing bring with them a host of new questions and challenges – including security, economic, and human rights implications – for foreign policy.

Defining digital foreign policy: A three-part typology

This study defines digital foreign policy as more than the 'continuation of foreign policy by technological means'.[3] Rather, we use a three-part typology for digital foreign policy. It consists of

- digital as a **topic** for diplomacy and foreign policy;
- digital as a **tool** for diplomacy and foreign policy; and
- digital as something that impacts the geopolitical and geoeconomic **environment** in which diplomacy and foreign policy take place.

---

1 Berridge, G.R. & James, A. (2003). *A dictionary of diplomacy* (2nd ed.). Palgrave Macmillan.

2 Crabb Jr., C.V. (1972). *American foreign policy in the nuclear age* (3rd ed.). Harper and Row, p. 1. Quoted in Adesina, O.S. (2017). Foreign policy in an era of digital diplomacy. *Cogent Social Sciences,* 3(1), 1–13. https://doi.org/10.1080/23311886.2017.1297175

3 Adesina, O. (2020, September 18). *The Nigerians in Diaspora Commission (NIDCOM): An example of digital diplomacy in practice*. African portal. https://www.africaportal.org/features/nigerians-diaspora-commission-nidcom-example-digital-diplomacy-practice/

In terms of relevant actors, digital foreign policy also goes beyond a traditional conception of foreign policy and diplomacy. Non-state actors – the business sector, the technical community, civil society, and academia – play an increasing role. Big tech companies, due to their economic power and the far-reaching security, economic, and societal implications of their products, have become important dialogue partners for states and their representatives.

Academic and research institutions are crucial for developing networks, bringing about new types of cooperation, and contributing to innovation and the skill development of the next generation. Civil society raises concerns of public interest and addresses, for example, the human rights dimension of digitalisation. In other words, the governance of the digital field has been defined by multistakeholder practices. The IGF and ICANN are some of the most prominent examples of multistakeholderism in the digital field. These are developments that shape digital foreign policy and can no longer be ignored by state actors.

1. Overview of digital foreign policy strategies

To date, five countries have released comprehensive digital foreign policy strategies: Australia, Denmark, France, the Netherlands, and Switzerland. Beyond these five, the discussion on whether or not a dedicated digital foreign policy strategy is needed has also reached other developed countries.[4]

Defining the elements of digital foreign policy strategies

In our work, we define a comprehensive digital foreign policy strategy as 'a strategy document that outlines a country's approach to digital issues and digitisation in relation to its foreign policy. It touches on numerous digital issues and connects the dots between the ministry of foreign affairs and various other ministries and key stakeholders. It also outlines areas of policy priorities regarding digitalisation and how these priorities are pursued as part of the country's foreign policy.'[5]

It is worth stressing, however, that having a dedicated digital foreign policy strategy is not the only approach. Some countries, for example, have foreign policy strategies that include aspects of digitalisation. Some countries have digital or digitalisation strategies that touch on foreign policy issues. There are also strategies dedicated to specific topics, such as cybersecurity or AI.

Five digital foreign policy strategies

- France: *Stratégie internationale de la France pour le numérique* (*International Digital Strategy of France)* (2017): 'The strategy covers digital governance, economy, development, and security. On the normative side, the document stresses the importance of an open and inclusive digital international environment, the promotion of universal access to diverse digital technologies, and the need to build trust on the internet.'[6]
- Netherlands: *Digital Agenda for Foreign Trade and Development Cooperation* (2019): 'The strategy focuses on four priority areas: (a) digitalisation and the Netherlands' international position, (b) digitalisation for development, (c) digital security and freedom online, and (d) digitalisation in the trade system. The strategy emphasises the need to cooperate internationally to benefit fully from the opportunities of digitalisation.'[7]
- Switzerland: *Digital Foreign Policy Strategy 2021–24* (2020): 'There are four areas of priority: (a) digital governance, (b) prosperity and sustainable development, (c) cybersecurity, and (d) digital self-determination. The strategy aims to "raise Switzerland's profile in the area of digital governance, further develop its digital foreign policy and position International Geneva as a prime location for discussing digitalisation and technology".'[8]
- Denmark: *Strategy for Denmark's Tech Diplomacy 2021–2023* (2021): 'The strategy is structured along three pillars: responsibility, democracy, and security. It aims for a more inclusive, sustainable, and human-centred technological development.'[9]

4 Garson, M. & Beverton-Palmer, M. (2021). *Response to Foreign Affairs Committee Inquiry on Tech and the Future of UK Foreign Policy*. Tony Blair Institute for Global Change. https://institute.global/policy/response-foreign-affairs-committee-inquiry-tech-and-future-uk-foreign-policy

5 DiploFoundation. (n.d.). *Digital Foreign Policy*. https://www.diplomacy.edu/topics/digital-foreign-policy/

6 Kurbalija, J. & Höne, K.E. (2021). The era of digital foreign policy: Comprehensive approaches to digitalisation. *Revista Política Internacional,* 130 (July–December). https://adp.edu.pe/revista

7 Ibid.

8 Ibid.

9 Ibid.

- Australia: *International Cyber and Critical Tech Engagement Strategy* (2021): 'This strategy comes after the initial 'Australian International Cyber Engagement Strategy' of 2017 and the 2019 progress report. The strategy is structured along three main areas: (a) values, (b) prosperity, and (c) security. The values include democracy, human rights, ethics of critical technology, and diversity and gender equality.'[10]

The key topics of digital foreign policy that are emerging are digital infrastructure, digital as a factor in development, cybersecurity, economic prosperity (including e-commerce), and human rights (including the protection of privacy and freedom of expression). All of these are covered by the strategies of Australia, Denmark, France, the Netherlands, and Switzerland. There are, however, differences in emphasis (Table 1).

Table 1. Coverage of specific issues based on the frequency of certain terms.[11]

Terms	Australia (2021)	Denmark (2021)	Switzerland (2020)	Netherlands (2019)	France (2017)
No. of total words	23 213	4 051	23 285	10 753	18 177
data & privacy	27	7	135	98	76
AI	22	1	53	19	8
security	165	13	45	25	58
human rights	75	9	39	16	30
governance	32	3	60	1	26
development	17	31	94	71	74
science	9	0	28	2	3
economy/economic	82	3	68	47	59
cooperation	62	16	57	41	25
research/education	58	5	40	24	24
health(care)	7	3	16	11	2
SDGs	5	0	6	5	2

What is also noticeable when comparing the strategies (Table 2) is that there are substantial differences in terminology. Australia employs the term *cyber* while the Danish strategy favours the term *tech diplomacy*. France, Switzerland, and the Netherlands focus on *digital*.

Table 2. The use of prefixes in five digital foreign policy strategies.[12]

Prefixes	Australia (2021)	Denmark (2021)	Switzerland (2020)	Netherlands (2019)	France (2017)
No. of total words	23 213	4 051	23 285	10 753	18 177
cyber	425	13	66	25	89
online	81	1	16	28	12

[10] Kurbalija, J. & Höne, K.E. (2021). The era of digital foreign policy: Comprehensive approaches to digitalisation. *Revista Política Internacional,* 130 (July–December). https://adp.edu.pe/revista

[11] Ibid.

[12] Ibid. This table counts the number of occurrences of a particular term or prefix across the whole text corpus.

digital	82	37	312	209	223
virtual	2	0	6	0	1
net	0	0	1	0	0
tech	14	77	4	2	0
e	11	0	1	2	2

These differences in terminology are noteworthy as they reflect a larger tendency towards terminological diversity. In some cases, differences in terminology convey differences in meaning. Cyber, for example, often carries security connotations, as in cybersecurity. Tech, more often than not, implies a focus on the economy and relations with the business sector. In other cases, the terms are interchangeable. Cyber diplomacy is also sometimes used in a broader way, going beyond cybersecurity to include any area that shapes, or is impacted by, digitalisation.[13]

This, however, is more than a linguistic or scholarly concern. Subtle terminological differences might lead to potential confusion regarding the subject of discussion, the wasting of resources and loss of potential synergies, and overall greater difficulties in overcoming policy silos and reaching international or multistakeholder agreements.[14] As these differences in terminology, however, are here to stay, it is important to be clear about the terms used and the scope of their meaning.

These strategies serve both as internal and external guidance. Internally, a digital foreign policy strategy helps to define primary goals and thereby serves to unite various domestic actors under one broad aim. It is also helpful in guiding the actions of diplomats, members of the ministry of foreign affairs and other ministries, and other stakeholders. Externally, a digital foreign policy strategy communicates priorities to other state and non-state partners and can serve as the basis for finding mutual understanding and agreements. In both cases, the advantage of the strategy lies in the fact that all digital topics with foreign policy relevance are gathered under the same roof.

Given the breadth of digital foreign policy, there is an emphasis on *whole-of-government* and *whole-of-society* approaches. The whole-of-government approach acknowledges that digital foreign policy is not conducted by MFAs alone. Rather, a host of other ministries and domestic agencies are involved; they need to be consulted regularly, are more directly involved in working with their counterparts abroad and are crucial for implementation. To facilitate this process, the Australian digital foreign policy strategy, for example, suggests an *International Cyber and Critical Technology Engagement Group*, which brings together five different ministries, the prime minister's office, the attorney general's office, federal police, and the cybersecurity centre.[15]

The whole-of-society approach recognises that many different stakeholders are affected by digital foreign policy and are also crucial for successful digital foreign policy.

Digital foreign policy strategies can be developed to different levels of detail and maturity. On one end of the spectrum, very detailed and mature strategies include values, priorities, goals, and proposed measures, and allocate ownership for implementation. All strategies discussed here are located more towards the higher level of maturity, but the strategies of Australia, Denmark,

---

13 The Australian strategy uses cyber in this way. Australian Government. (2021). *Australia's International Cyber and Critical Tech Engagement Strategy*. https://www.internationalcybertech.gov.au/sites/default/files/2021-05/21066%20DFAT%20Cyber%20Affairs%20Strategy%202021%20update%20Internals%201%20Acc.pdf
Germany includes international cyber policy in its list of key foreign policy topics. Cyber policy is described with a strong focus on security issues but also goes beyond that. Federal Foreign Office. (2017). *International Cyber Policy*. https://www.auswaertiges-amt.de/en/aussenpolitik/themen/cyber-aussenpolitik
For the context of Africa, see Allen, K. (2022, January 3). *Africa must get up to speed on cyber diplomacy.* Institute for Security Studies. https://issafrica.org/iss-today/africa-must-get-up-to-speed-on-cyber-diplomacy

14 Kurbalija, J. (2015, April 17). Different prefixes, same meaning: cyber, digital, net, online, virtual, e-. *Diplo*. https://www.diplomacy.edu/blog/different-prefixes-same-meaning-cyber-digital-net-online-virtual-e/

15 Australian Government. (2021). *Australia's International Cyber and Critical Tech Engagement Strategy*. https://www.internationalcybertech.gov.au/sites/default/files/2021-05/21066%20DFAT%20Cyber%20Affairs%20Strategy%202021%20update%20Internals%201%20Acc.pdf

and Switzerland are among the most mature.[16] The Danish strategy for example includes key performance indicators to measure progress. Mature strategies have the advantage of giving clear strategic guidance. But they might face the disadvantage of being inflexible and very resource-intensive to prepare.

On the other end of the spectrum, relatively lightweight digital foreign policy strategies might include a vision and general principles but stay away from details and specific measures. Their advantage lies in strategic ambiguity, flexibility, and being comparatively less resource-intensive in their preparation. Disadvantages might include reduced effectiveness and limited value as a guiding document.

Lastly, a digital foreign policy strategy, or the intention of developing one, also raises questions about personnel and institutional structures to support the development and implementation of the strategy.[17] As mentioned, some countries have created dedicated ambassadorial posts, while others have created dedicated teams or units within their MFAs. In addition, digital foreign policy also raises challenges of coordination among ministries and with non-state actors. As previously stated, the Australian strategy includes reference to institutional structures that facilitate coordination. Whether such elements are included in the strategy depends to some extent on the maturity of the strategy. In either case, digital foreign policy raises institutional challenges that need to be considered from an early stage in the process, if possible.

2. Building digital foreign policy strategies

The previous analysis of the five digital foreign policy strategies should not be read as a suggestion that all countries should draft such a document. Other approaches are possible as well, such as covering foreign policy aspects in strategies and plans dealing with various digital issues. We recommend that African countries analyse all these options; assess them against the backdrop of their own national contexts, priorities, and resources; and choose the model that works best for them.

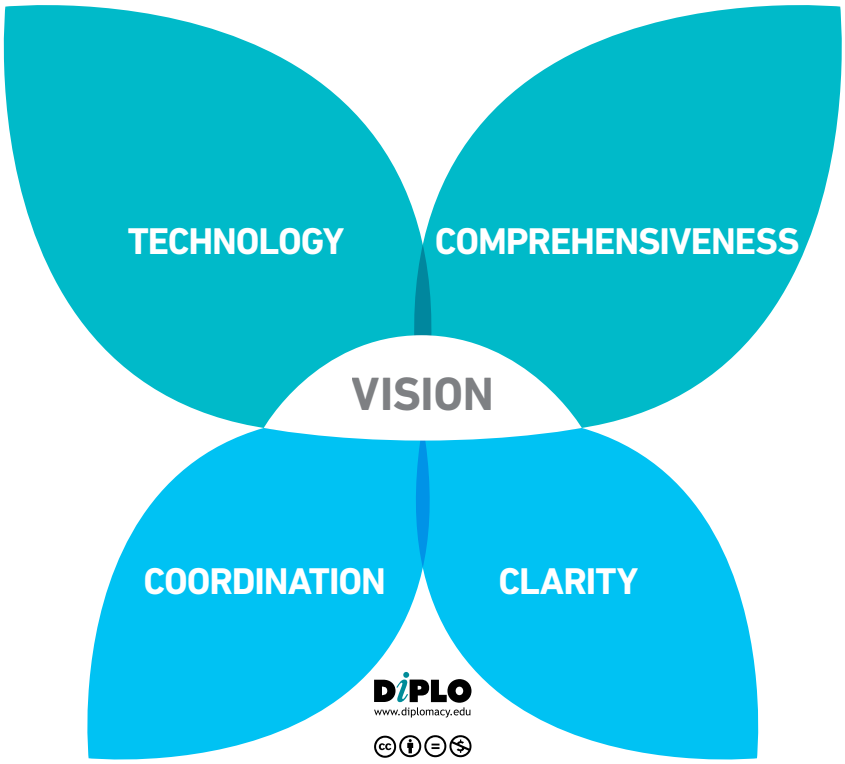
If countries choose to develop digital foreign policy strategies, the following principles (Figure 2) can be followed:

- **Overall vision.** The strategy should serve as a guideline for future actions and cooperation. The clearer this overall vision and priorities can be articulated, the better.
- **Context.** The strategy needs to be specific to the country and its unique circumstances, interests, priorities, and capabilities.
- **Comprehensiveness**. It is important to address a broad range of issues related to digitalisation and their impact on foreign policy. Among them are digital infrastructure, digital as a factor in development, cybersecurity, the digital economy, and human rights.
- **Clarity**. Clarity in communication is important and the choice of words, given their various connotations, needs to be deliberate. The strategy itself needs to start with utmost clarity to facilitate future cooperation.
- **Coordination**. Developing and implementing the strategy requires coordination among many ministries and agencies. This is encapsulated in the *whole-of-government* approach. Coordination also means multistakeholder consultations and collaboration. This includes civil society, the technical community, the business sector, and academia. This is described as the *whole-of-society approach.* These processes can be time-consuming but are crucial for the future success of the strategy.

[16] Ersze, A. & Garson, M. (2022). *A leaders' guide to building a tech-forward foreign policy*. Tony Blair Institute for Global Change. https://institute.global/policy/leaders-guide-building-tech-forward-foreign-policy

[17] Sahin, K. (2022, April 1). Außenpolitische Digitalstrategien (Foreign digital policy strategies). *SWP-Aktuell*. https://www.swp-berlin.org/publikation/aussenpolitische-digitalstrategien

Figure 2. Principles for drafting a digital foreign policy strategy.



II
Elements of digital foreign policy in Africa

African countries do not have readily available digital foreign policy strategies. And digital topics do not play a prominent role within the existing foreign policy strategies. **Namibia** is an exception. The country places cybersecurity among its 'contemporary global factors' and lists ICT as an issue of national priority in its 2017 policy on international relations and cooperation.[1] Also worth mentioning is Tunisia: Reducing the digital divide between industrialised and developing countries is embedded into the country's foreign policy objective related to 'rectifying the disequilibria characterising international economic relations'.[2]

In contrast to this, nearly all African countries have explicit digital agendas. These are outlined in national development plans and dedicated strategic documents or take the form of strategies and policy documents covering specific issues such as infrastructure, cybersecurity, or e-commerce.[3] The AU and RECs also have digital priorities and initiatives focused on issues such as advancing digital transformation and facilitating the harmonisation of legal and regulatory frameworks. In some cases, these national, regional, and continental policies and strategies contain elements of foreign policy, as they outline goals and objectives related, for instance, to international cooperation or engagement in international processes.

This chapter maps elements of digital foreign policy in Africa by first drawing on relevant strategies and policy documents. But because understanding these elements requires a grasp of local realities, challenges, and concerns, we start with an overview of key developments and initiatives at the national, continental, and regional level.

This overview, as well as the analysis of relevant policy documents and their international/foreign policy dimensions (where they exist), is built around the following specific topics: digital infrastructure and standards; human rights in the digital space; cybersecurity, cybercrime, and child online protection (COP); digital economy; AI; and sociocultural issues (e.g. digital identities, gender equality, and skills). This selection of topics is in part inspired by the mapping of existing digital foreign policy strategies introduced in the previous chapter, and in part based on our assessment of key digital policy priorities across the region.

We then zoom out and look at the extent to which African countries and their stakeholders participate in various international processes related to digital policy issues, from UN agencies and dedicated working groups, through technical organisations such as ICANN, and to multistakeholder processes and initiatives, such as the IGF and the GFCE.

This overview builds on the whole-of-government and whole-of-society perspectives. While foreign policy is the primary purview of MFAs, digital foreign policy challenges this traditional understanding. Other ministries, in particular ministries of ICT, and agencies, for example in the area of cybersecurity, become increasingly relevant. At the same time, non-state actors, in particular, the business sector and civil society, are crucial in bringing about digital transformation and in raising concerns about societal and human rights issues. These two perspectives, whole-of-government and whole-of-society, need to be adapted to local circumstances.

Over 1.4 billion people live in Africa. Applying various economic and development indicators, it is a region of great diversity. In terms of development, there are also substantial differences within countries, for example between rural and urban areas. This is especially true when it comes to digitalisation. This means that any generalisation across the region can lead to oversimplification and the erasure of important distinctions. To address this challenge, in this study we work as much as possible with indices and rankings that depict the whole of Africa, while focusing on analysing a select number of countries in greater detail: **Côte d'Ivoire**, **Ghana**, **Kenya**, **Namibia**, **Nigeria**, **Rwanda**, **Senegal**, and **South Africa**.

---

1 Ministry of International Relations and Cooperation of Namibia. (2017). *Namibia's Policy on International Relations and Cooperation.* https://mirco.gov.na/webdav/mirco.gov.na/document_library/Documents/Downloads/Namibia%27s%20Policy%20on%20International%20Relations%20and%20Cooperation

2 Ministry of Foreign Affairs, Migration and Tunisians Abroad, Republic of Tunisia. (n.d.). *Foreign policy of Tunisia.* https://www.diplomatie.gov.tn/en/foreign-policy/foreign-policy-of-tunisia/

3 Abimbola, O., Aggad, F., & Ndzendze, B. (2021, September 23). *What is Africa's Digital Agenda?* APRI Policy Brief. https://afripoli.org/what-is-africas-digital-agenda#

1. Holistic approach

Section summary

Africa lags behind other regions in terms of digital development. To encourage the uptake of digital technologies as drivers of growth and development, countries have developed or are working on various strategies, plans, and other policy documents that cover digital topics, from digitalisation strategies to broadband plans and digital economy policies. Some of these documents also include elements of foreign policy, as our analysis of the eight focus countries indicates. Such elements relate to enhancing countries' competitiveness in international markets; building partnerships with international entities (e.g. donors, development agencies and banks, regional and international intergovernmental organisations, multinational tech companies) to help achieve domestic digital transformation goals; fostering overall international cooperation on digital policy topics; and harmonising ICT/digital-related domestic policies and legal and regulatory frameworks with relevant international frameworks.

At the continental level, documents such as the *Agenda 2063* and the *Digital Transformation Strategy* outline goals for Africa to achieve an integrated and inclusive digital society and economy. Strengthening the continent's presence in the global digital economy (as both a producer and a consumer), fostering cooperation with international entities on issues such as advancing digital skills and supporting digital entrepreneurship, and increasing participation in international internet governance and digital policy processes (UN, ITU, IGF, ICANN, etc.) are some of the outward-looking elements outlined in such documents. RECs have their own strategies and policies related to ICT and digitalisation, which also include certain international dimensions, from goals related to the coordination of regional initiatives with relevant ones at the international level to those focused on strengthening engagement in international processes and the coordination of national positions.

At the international level, some countries raise digital topics when they contribute to debates at the UNGA and/or the Security Council. If in 2017 8 countries mentioned digital topics in their statements at the GA general debates, this number grew to 24 in 2022. Topics covered include digital inclusion, digital economy, cybersecurity, and human rights online. At the Security Council, Ghana, Kenya, and South Africa (which have held non-permanent member seats recently) have been particularly active in discussions on the interplay between digital technologies and peace and security, raising issues such as the need for international support for developing and least-developed countries (LDCs) to strengthen their cybersecurity capabilities and address the misuse of digital technologies by terrorist and extremists.

There is also some participation of African actors (in particular civil society) in meetings of the IGF. For instance, statistics on IGF participation place Africa as the second-best represented region in 2017, 2018, 2019 and the third in 2020 and 2021. Civil society and the technical community are usually the most active in terms of IGF session speakers and organisers. Across Africa, 1 continental IGF initiative (the African IGF – AfIGF), 5 regional initiatives, and 31 national ones facilitate multistakeholder dialogue and cooperation on relevant digital policy topics. Governments and regional institutions could tap into the potential of such IGFs to advance the whole-of-society approach to digital governance and foreign policy.

1.1. National overview

Almost all African countries have national strategies, plans, and other policy documents that cover digital topics. These can be either documents specifically focused on digital issues (e.g. broadband plans, digitalisation strategies, e-commerce policies) or broader development plans, which include certain digital components (Figure 3).

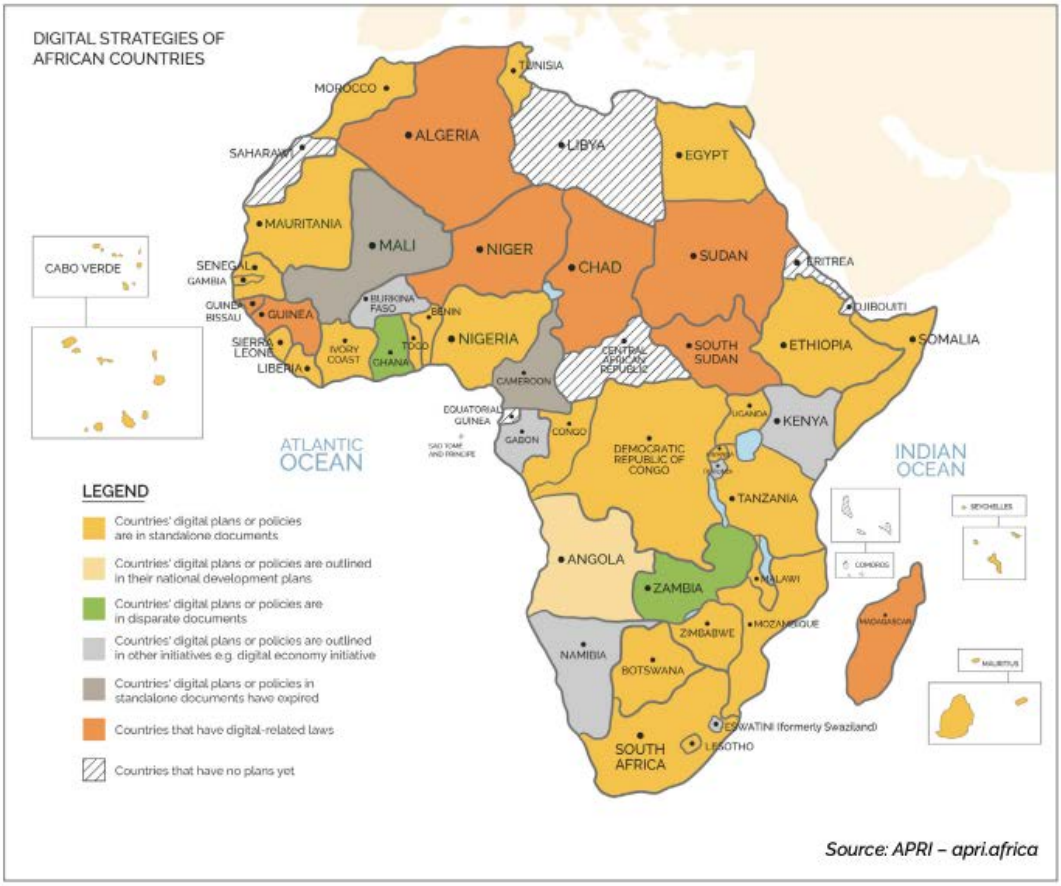


Figure 3. Digital strategies of African countries.[4]

Digital development across Africa is gradually picking up, but the region is significantly behind compared to developed countries. For instance, the eight focus countries have relatively low scores in various indices tracking issues such as network readiness, connectivity, and overall digital development (Table 3). Against this backdrop, when countries outline strategies and policies related to digital issues, these generally focus on setting priorities, goals, and measures to advance overall digital transformation at the national level and help speed up the uptake of digital technologies as drivers of growth and development.

In **Kenya**, for example, the *National Digital Master Plan* (2022–2032) has as an overall objective the development of a 'robust, secure, affordable, accessible and reliable digital ecosystem that benefits the public and private sector, and improved quality of life'.[5] **Nigeria**'s *Digital Economy Policy and Strategy* (2020–2030) outlines objectives related to accelerating digitalisation processes,

4 Abimbola, O., Aggad, F., & Ndzendze, B. (2021, September 23). *What is Africa's Digital Agenda?* APRI Policy Brief. https://afripoli.org/what-is-africas-digital-agenda#

5 Ministry of ICT, Innovation and Youth Affairs, Kenya. (2021). *The Kenya National Digital Master Plan.* https://repository.kippra.or.ke/bitstream/handle/123456789/3580/Kenya%20-%20Digital%20Master%20Plan.pdf

expanding broadband penetration, enhancing digital skills, and promoting innovation and entrepreneurship, among others.[6]

Table 3. Digital development level and network readiness score for the eight focus countries.

Country	Digital development level[7]	Network readiness score[8]
Côte d'Ivoire	33,54	35,69
Ghana	40,68	40,86
Kenya	37,14	45,18
Namibia	37,28	35,66
Nigeria	31,76	37,51
Rwanda	30,23	38,65
Senegal	33,04	39,48
South Africa	49,24	48,88
For comparison		
Switzerland	83,80	80,20
Highest score	84,17 (Denmark)	82,06 (Netherlands)

Elements of foreign policy

In addition to outlining goals and objectives to be achieved at the national level, some national policies and strategies also include outward-looking elements. Zooming in to the eight focus countries, we look at the extent to which elements of foreign policy (cooperation with international entities, engagement in international processes, positioning of the country on the international scene, etc.) are referenced in general strategies and other policy documents related to digitalisation, ICT, or broad development plans.

When countries develop general plans and policies focused on digitalisation and digital transformation, they almost always outline **economic goals related to enhancing their competitiveness in regional and international markets**. **Kenya**'s *National Digital Master Plan* highlights among its overarching objectives that of positioning the country as a 'globally competitive digital economy' and creating a 'globally attractive legal, regulatory, and policy ecosystem that provides adequate support to start-ups'.

The plan also envisions Kenya 'as a leader in emerging technology adoption, localisation, and utilisation for development', as well as in global discourses and discussions on issues related to emerging technologies. Similar goals appear in the country's *Digital Economy Blueprint*, which notes that the digital economy offers Kenya a leapfrogging opportunity for economic development, and outlines objectives and actions to help the country 'become a regional and global innovation leader

6 Federal Ministry of Communications and Digital Economy, Nigeria. (2020). *National Digital Economy Policy and Strategy.* https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file

7 eGovernance Academy Foundation. (n.d.). *National Cyber Security Index*. https://ncsi.ega.ee/. The index also includes a digital development level, which is calculated based on the ICT Digital Development Index and the Networked Readiness Index.

8 Portulans Institute. (2021). *Network Readiness Index 2021.* https://networkreadinessindex.org/countries/ The network readiness score combines a series of indicators related to technology (e.g. access to ICT, digital technology produced in the country, whether countries are prepared for technologies such as AI), people (e.g. digital skills, the use of ICT by businesses and governments), governance (e.g. the extent to which policies and regulations promote inclusion and participation in the network economy), and impact (e.g. the economic, social, and human impact of participation in the network economy).

driving a strong sustainable economy and a better society'.[9] Likewise, the *National ICT Policy* wants Kenya to 'gain global recognition for innovation', develop an innovation and start-up ecosystem that can lead globally, and 'become a more prosperous participant in the global economy'.[10]

Nigeria too wants not only to actively participate in the global digital economy but also to leverage digital technologies in order to become 'a leading player', as noted in its *National Digital Economy Policy and Strategy*.

Supporting domestic businesses to increase their competitiveness on regional and global markets – in particular in emerging tech domains – is among the goals included in **South Africa**'s *ICT and Digital Economy Masterplan*.[11]

For **Ghana**, key goals behind its *National ICT for Accelerated Development Policy* include the development of a 'dynamic export-led and globally competitive ICT industry' and 'securing a place for Ghana in the international economic system'.[12] These goals are reinforced in the *Ghana Beyond Aid* policy, which foresees that by 2028, the country 'would have leveraged its abundant human talent to become a leader (at least in Africa) in the digital economy'.[13]

Cote d'Ivoire has a somewhat similar goal outlined in its *National Digital Development Strategy 2021–2025*: accelerate digital transformation at the national level in order to become one of Africa's top five innovation leaders by 2025.[14]

Ensuring that the country is part of the 'global information society' and increasing the competitiveness of ICT businesses on international markets are envisioned in **Namibia**'s *Overarching ICT Policy*.[15]

Rwanda wants to position itself as a globally competitive knowledge-based economy and this goal appears across several documents such as the *ICT Sector Strategic Plan*[16] and the *Smart Rwanda Master Plan*.[17] The country also sees itself as a future regional ICT hub and has a specific strategy in place dedicated to this goal – the *ICT Hub Strategy 2024*.[18]

---

9 Republic of Kenya. (2019). *Digital Economy Blueprint*. https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf

10 Ministry of Information, Communications and Technology, Kenya. (2019). *National Information, Communications and Technology Policy*. https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf

11 Although various online governmental sources indicate that the plan has been approved, we were unable to locate the final version of the document. Therefore, throughout this document we refer to an intermediate draft: Knowledge Executive and Genesis. (2020). *ICT and Digital Economy Masterplan for South Africa. Draft for discussion*. https://www.ellipsis.co.za/wp-content/uploads/2020/08/ICT-and-Digital-Economy-Masterplan-for-South-Africa_Draft-for-discussion_-August_-2020.pdf

12 Republic of Ghana. (2003). *The Ghana ICT for Accelerated Development (ICT4D) Policy.* https://nita.gov.gh/theevooc/2017/12/Ghana-ICT4AD-Policy.pdf

13 Ghana Beyond Aid Committee. (2019). *Ghana beyond Aid Charter and Strategy Document*. http://osm.gov.gh/assets/downloads/ghana_beyond_aid_charter.pdf

14 Ministry of Digital Economy, Telecommunications and Innovation, Republic of Côte d'Ivoire. (2022). *Stratégie Nationale de Développement du Numérique en Côte d'Ivoire (National Digital Development Strategy of Côte d'Ivoire).* https://telecom.gouv.ci/wp-content/uploads/2022/02/Strategie-Nationale-Developpement-du-Numerique-2021-2025.pdf

15 Ministry of ICT, Namibia. (2009). *Overarching Information Communications Technology (ICT) Policy.* http://www.nied.edu.na/assets/documents/05Policies/NationalCurriculumGuide/ICT_in_GRN_Policy.pdf

16 Ministry of Information Technology and Communications, Republic of Rwanda. (2017). *ICT Sector Strategic Plan*. https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/ICT_SECTOR_PLAN_18-24_.pdf

17 Ministry of Youth and ICT, Republic of Rwanda. (2015). *Smart Rwanda Master Plan.* https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/SMART_RWANDA_MASTERPLAN.pdf

18 Ministry of Information Technology and Communications, Republic of Rwanda. (2018). *ICT Hub Strategy 2024.* https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/ICT_HUB_STRATEGY.pdf

Developing a digital economy which is competitive at the regional and international levels is one of the goals outlined in **Senegal**'s *Digital Senegal Strategy 2016–2025*.[19]

It is worth highlighting that some of these countries share leadership-related goals. **Kenya** and **Nigeria**, for instance, aim to position themselves as global leaders in innovation and/or the digital economy, while **Ghana** and **Cote d'Ivoire** aspire to a similar status at least within Africa. Translated into concrete actions, these goals can help advance healthy competition on the digital economy scene within and beyond the region.

Building partnerships with international entities (in particular, but not limited to, donors and development agencies/banks) to help achieve domestic digital transformation goals is another objective shared by several countries. **Kenya** intends to foster links with, and seek support (technical, material, financial, capacity development-related) from international development partners to implement elements of its *National Digital Master Plan* and other ICT and digitalisation policies. It also wants to cooperate with 'international systems and platforms for global reach', **attract foreign direct investments**, and encourage international businesses to open offices in the country (*National ICT Policy*).

Facilitating **partnerships with multinational tech companies** 'to create platforms for indigenous vendors to serve global markets' is envisioned by **Nigeria** (*National Digital Economy Policy and Strategy*), while **South Africa**'s similar goal is to 'facilitate investment and partnerships with global buyers of digitally traded services' (*ICT and Digital Economy Masterplan*). Attracting international corporations through investment-friendly policies and garnering their support in establishing ICT research and development (R&D) centres are among **Rwanda**'s objectives (*Smart Rwanda Master Plan*). **Ghana** too intends to promote partnerships between local R&D institutions and foreign and international centres of excellence (*National ICT for Accelerated Development Policy*).

More **general goals related to fostering international cooperation** are outlined by several countries. **Kenya**, for instance, wants to 'leverage regional and international cooperation and engagement to ensure that [it] is able to harness global opportunities' (*National ICT Policy*). For **Rwanda**, one of the goals behind its *ICT Hub Strategy* is to partner with global organisations/institutions to develop tech-based solutions needed to address socio-economic challenges in areas such as education, health, and agriculture.

The **harmonisation of ICT/digital-related domestic policies and legal and regulatory frameworks with relevant international frameworks** features as a common goal across national documents in **Kenya** and **Ghana.** This implies some level of engagement with the organisations and processes behind those frameworks. Other policy documents are more detailed in this regard, indicating specific instruments and frameworks to ensure harmonisation in areas such as spectrum policies, cybersecurity, and data protection. (We cover these later in the relevant sections.)

[19] Ministry of Post and Telecommunications, Republic of Senegal. (2016). *Stratégie Sénégal Numérique 2016–2025 (Digital Senegal Strategy 2016–2025).* http://www.numerique.gouv.sn/sites/default/files/Numerique%202025_0.pdf

South Africa's policy positions on internet governance

Standing out among the documents we have reviewed is South Africa's *Integrated ICT Policy White Paper*, which outlines the country's position on matters of international internet governance.

With the overarching goal of 'ensuring that the internet is governed in the public interest, taking into account the diverse needs of all countries across the world and in line with the principles of the open internet', South Africa outlines the following as specific objectives of its policy on international governance of the internet:

- 'Ensure that international governance and administration mechanisms, processes and institutions reinforce the overarching principles of the Open Internet.
- Reinforce a multilateral approach to Internet governance in line with the principles set by the United Nations.
- Recognise the responsibilities of all governments across the globe to determine public policy on a local, national and international level and ensure equal participation by all governments in Internet governance.
- Strengthen Internet governance mechanisms and processes to ensure they are inclusive and open to all interested stakeholders, in line with the South African constitution.
- Reinforce the importance of meaningful participation and involvement by all stakeholders across the world in international governance processes and decision-making related to this platform. This includes all governments, technical experts, individual users, community and civil society organisations, academics and the private sector in their respective roles.
- Clarify the roles of the different stakeholders in shaping the evolution and development of the principles, norms, rules, standards and programmes that shape the Internet. Ensure that stakeholders involved are globally distributed and that no one country or group of countries has any undue influence on global Internet policies.
- Reinforce accountability mechanisms for Internet governance institutions.'

In line with these objectives, South Africa's position to take in internet governance forums, mechanisms, and processes is to:

'Endorse positions that recognise the central role that governments, as elected bodies representing and accountable to the public, must play in determining Internet governance policy.

Recognise the right of all countries to develop and implement policies in accordance with the principles of self-determination and subject to the UN principles.

Recognise the responsibility of governments to develop public policy on all aspects of the Internet including infrastructure and services deployment and regulation, cybersecurity, cross border taxation etc. These should be subject to both national laws and international treaties.'[20]

1.2. Continental and regional overview

Setting the scene: Regional and continental cooperation

The idea of an integrated and united continent goes back to the Pan-Africanism of the nineteenth century. In the AU's *Agenda 2063*, adopted in 2015, this takes shape in concrete aspirations and goals. The second aspiration of the agenda calls for 'an integrated continent, politically united, based on the ideals of Pan-Africanism and the vision of Africa's Renaissance'. This is more concretely spelled out in terms of working towards 'free movement of people, capital, goods, and services', a 'continent of seamless borders' and 'significant increases in trade and investments amongst African states'. The realisation of these goals will depend to a substantial degree on digital tools

[20] Department of Telecommunication and Postal Services, Republic of South Africa. (2016). *National Integrated ICT Policy White Paper.* https://www.dcdt.gov.za/documents/legislations/white-papers/file/109-the-national-integrated-ict-policy-white-paper-3rd-october-2016.html

and digital policies. Also noteworthy is the Agenda's seventh aspiration, which envisions Africa as a strong and influential global player and partner, and emphasises the need for reinforcing participation in world affairs and multilateral institutions to enable the continent to 'take its rightful place in the political, security, economic, and social systems of global governance'.[21]

Most digital issues cut across state boundaries and cannot effectively be addressed at the national level alone. The full benefits of the digital transformation can best be realised through policies that are coordinated across national jurisdictions. Both the AU and RECs (Figure 4) have a role to play in the coordination and harmonisation of policies.

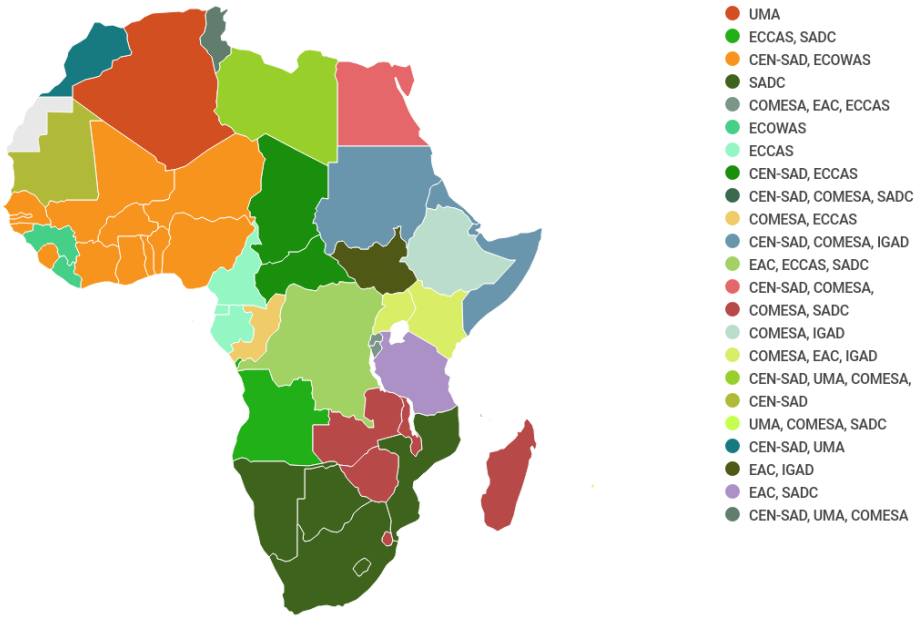


Figure 4. Regional economic communities.[22]

Recent initiatives in the area of digital policy at the level of RECs and the AU point in the direction of increasing cooperation. There is diversity among African countries; this includes substantial cultural and legal diversity; diversity in terms of levels of digitalisation; and significant variations in legal, policy, and technological capacities. Tensions between countries are also inevitable, including on digital matters. Yet, there is also a clear sense that digital issues require multilateral – and multistakeholder – collaboration. And regional and continental approaches that work towards greater integration and harmonisation of digital policy issues have been growing. The African Continental Free Trade Area (AfCFTA) and its e-commerce provisions are just two such examples. On the one hand, collaboration is important to reap the benefits of digitalisation. On the other hand, greater coordination will also strengthen the position of African countries in negotiating with other actors and within key multilateral forums. In this sense, a digital foreign policy for the AU could become a reality in the future.

Throughout this chapter, we cover several key regional and continental strategies and initiatives that present elements of digital foreign policy or could form the basis of such regional/continental policies.

---

21 African Union [AU]. (2015). *Agenda 2063. The Africa We Want. Popular Version*. https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf

22 The map shows countries by their membership to the eight RECs recognised by the AU: Arab Maghreb Union (UMA); Common Market for Eastern and Southern Africa (COMESA); Community of Sahel–Saharan States (CEN–SAD); East African Community (EAC); Economic Community of Central African States (ECCAS); Economic Community of West African States (ECOWAS); Intergovernmental Authority on Development (IGAD); and Southern African Development Community (SADC).

Digital priorities and elements of foreign policy

At the **continental level**, *Agenda 2063* sets an overarching goal of achieving technological transformation and a well-developed ICT and digital economy across the continent by 2063. A strong digital economy will help Africa achieve other goals outlined in the strategy: **become a major economic force in the world, and an active and equal participant in global affairs**.

In 2020, the AU adopted an overall strategy to guide the continent's digital transformation over the period 2020–2030: the *Digital Transformation Strategy for Africa* (DTS), which states that there is a 'need for Africa to make digitally enabled socio-economic development a high priority'. It envisions 'an integrated and inclusive digital society and economy in Africa that improves the quality of life of Africa's citizens, strengthens the existing economic sector, enables its diversification and development, and ensures continental ownership with Africa **as a producer and not only a consumer in the global economy**'. Key themes are solidarity among African countries and African leadership in the process of digital transformation – a transformation 'led and owned by Africa's institutions' and 'embedded in Africa's realities'.[23]

The strategy – which builds on an intricate framework of topics (Figure 5) – highlights the importance of harmonising policies, legislation, and regulations and enabling 'the coherence of existing and future digital policies and strategies at regional and national levels'. Focus areas include the following:

- **Law and policy:** to facilitate fair market regulation as well as broader human and people's rights issues.
- **Digital infrastructure:** including mobile telephony, broadband infrastructure, terrestrial broadcasting data and cloud services.
- **Human resources:** including the issues of labour for the digital market as well as reskilling and upskilling various professionals required for the digital economy.
- **Digital innovation and entrepreneurship**: including creating an enabling environment regarding policies and policy harmonisation.

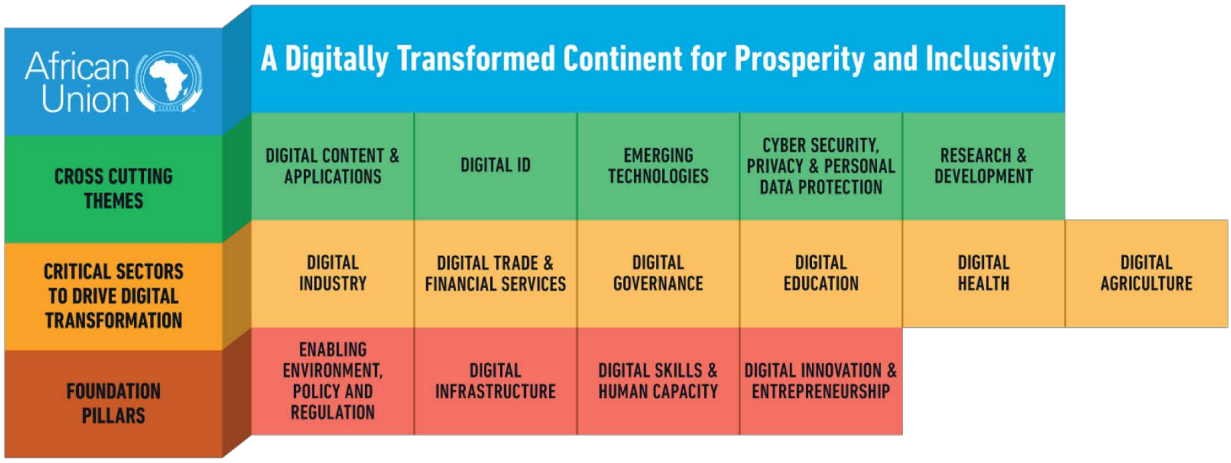


Figure 5. Themes and pillars of AU's Digital Transformation Strategy.

One of the *Digital Transformation Strategy*'s guiding principles is **cooperation.** It refers both to cooperation at the regional and continental levels (between the AU, RECs, and national institutions) and cooperation with international organisations. For instance, collaboration with development partners in the implementation of the strategy is envisioned as a key action line.

Other areas of action with **international dimensions** include cooperating with international organisations and donors (as well as public institutions, companies, universities, and NGOs) in

[23] African Union [AU]. (2020). *The Digital Transformation Strategy for Africa (2020-2030)*. https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

the development of programmes focused on digital skills; incentivising international companies to hire and train young Africans 'for local jobs or in the context of circular migration'; attracting international venture capital firms to invest in the African technology ecosystem; and promoting a wider participation of enterprises into international e-commerce.

Besides these two major AU strategies – *Agenda 2063* and the *Digital Transformation Strategy* – elements of digital foreign policy can also be identified in the *Declaration on Internet Governance and Development of Africa's Digital Economy*, issued by AU heads of state and government in 2018. The declaration outlines a series of **principles that could be seen as representing a common African position on key internet governance issues**:

- Promoting inclusive, transparent, and accessible internet governance.
- Maintaining an open internet based on open standards development processes.
- Facilitating a resilient, unique, universal, and interoperable internet that is accessible to all.
- Advancing multistakeholder approaches to internet governance that are open, participatory, inclusive, transparent, collaborative, consensus-driven, and respect cultural, gender, and linguistic diversity, and which seek to promote accountability and full participation of governments, the private sector, civil society, the technical community, and users.

Taking into account these principles, the heads of states and governments call on countries and regional and continental institutions to **increase their participation in internet governance discussions and related public policy processes** such as those taking place at the level of the Human Rights Council (HRC), ICANN, the IGF, ITU, and the UN. They are also requested to facilitate and contribute to national and regional IGFs, as well as encourage the participation of all stakeholders in such initiatives.[24]

At a **regional level**, the various RECs have developed their own strategies, policies, and other initiatives related to ICT and digitalisation. These communities generally approach digitalisation from a market perspective and therefore emphasise market issues, such as enhancing trade and facilitating hubs. Facilitation of cross-border trade, as well as the harmonisation of laws, have been high on the RECs' digital agendas. There has been less emphasis on broader political and social issues, for example, the human rights impacts of ICTs, gender mainstreaming, benefit sharing from the digital economy, and knowledge transfer.

RECs' harmonisation challenges

Harmonisation of digital policies in the various RECs is an important element for strengthening the digital (foreign) policy of the member countries. The various RECs are at different stages of policy development and harmonisation. Despite some positive signs, the implementation of REC policies into national law remains a key challenge. Overlapping memberships lead to multiple, potentially contradictory commitments as well as substantial duplication of efforts. As long as this is the case, the economic benefits of harmonisation for cross-border trade cannot be fully realised.

Some of the policy documents issued by RECs include certain international dimensions. The Economic Community of West African States (ECOWAS),[25] for instance, adopted an *Act on Harmonization of Policies and the Regulatory Framework for the ICT Sector* (2007), which encourages national authorities to **ensure alignment of their policies with regional and international frameworks**, as well as the **coordination of their initiatives with relevant ones at the regional and global level**.[26]

[24] African Union Assembly of Heads of State and Government. (2018). *Declaration 3(XXX) on Internet Governance and Development of Africa's Digital Economy*. https://www.saigf.org/AU-Declaration%20on%20IG.pdf

[25] ECOWAS member states: Benin, Burkina Faso, Cabo Verde, Côte d'Ivoire, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

[26] Economic Community of West African States [ECOWAS]. (2007). *Supplementary Act A/SA.1/01/07 on the harmonization of policies and of the regulatory framework for the information and communication technology (ICT) sector*. http://legaldocs.ecowas.int/_lang/fr/doc/_iri/akn/ecowas/statement/supplementaryAct/2007-01-19/A_SA.1_01_07/eng@/!main

The *Protocol on Transport, Communications and Meteorology* agreed by the Southern African Development Community (SADC)[27] highlights the commitment of member states to develop national telecom networks and take advantage of international technological developments as part of broader efforts to advance economic development. It further calls on countries to **participate in regional and international telecommunications forums** (such as ITU) and outlines an agreement to **coordinate national positions** on 'matters dealt with at all international telecommunications and other relevant fora'.[28] The *e-SADC Strategic Framework* (2010), dedicated to promoting ICT use for regional economic integration, has among its overarching strategies the **promotion of participation in international ICT forums** and the consolidation of SADC positions to present in such forums.[29]

IGF initiatives and the whole-of-society approach

Within Africa, there is a continental IGF initiative – the AfIGF – which has been holding annual meetings since 2012 and is supported by the AU Commission (AUC) and the UN Economic Commission for Africa (UN ECA). In October 2022, there were 5 regional IGF initiatives[30] and 31 national IGF initiatives[31] across Africa recognised by the IGF Secretariat.[32] All eight focus countries have a national IGF (Table 4).

IGFs are typically multistakeholder processes that foster dialogue and cooperation on digital policy issues of relevance at the national and regional levels. The fact that they bring together stakeholders from different groups can make them suitable venues to inform various policy processes. Governments and regional institutions could tap into the potential of IGFs to advance the whole-of-society approach to digital governance. They could run consultations – formal or informal – on their national digital policies or on the positions to take in international processes. And because discussions taking place at the national and regional IGFs usually feed into the global IGF, these initiatives could also act as promoters of national and regional interests, positions, and views. The challenge, however, is to ensure that these processes are truly multistakeholder and inclusive and that they have access to the resources needed to ensure their independence and sustainability.

Table 4. National IGF initiatives across the eight focus countries.

National IGF initiative	Established in	Latest annual meeting (as of October 2022)
Côte d'Ivoire	2020	2021
Ghana	2014	2022
Kenya	2008	2022
Namibia	2017	2021
Nigeria	2013	2022
Rwanda	2014	2021
Senegal	2017	2019
South Africa	2016	2022

27 SADC member states: Angola, Botswana, Comoros, Democratic Republic of the Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia, and Zimbabwe.

28 Southern African Development Community [SADC]. (2006). *Protocol on Transport, Communications and Meteorology in the Southern African Development Community (SADC) Region*. https://www.sadc.int/files/7613/5292/8370/Protocol_on_Transport_Communications_and_Meteorology_1996.pdf

29 Southern African Development Community [SADC]. (2010). *e-SADC Strategic Framework*. https://repository.uneca.org/ds2/stream/?#/documents/789cf54b-73c2-59a6-9536-f894b38ee6ff/page/1

30 Central Africa IGF, East Africa IGF, North African IGF, Southern African IGF, and West African IGF.

31 Benin, Botswana, Burkina Faso, Cabo Verde, Cameroon, Chad, Côte d'Ivoire, Democratic Republic of the Congo, Gabon, Gambia, Ghana, Kenya, Liberia, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Rwanda, Senegal, Sierra Leone, South Africa, South Sudan, Sudan, Tanzania, Togo, Tunisia, Uganda, Zambia, and Zimbabwe.

32 IGF Secretariat. (n.d.). *National and regional IGF initiatives*. https://www.intgovforum.org/en/content/national-igf-initiatives and https://www.intgovforum.org/en/content/regional-igf-initiatives

1.3. International engagement

United Nations General Assembly: Digital policy at the General Debate

Every year, the United Nations General Assembly (UNGA) includes a General Debate (GD) section that sees heads of states or other high-level representatives outline national positions on various matters of relevance to international affairs. Digital policy topics are sometimes among them, as our analysis of GD statements between 2017 and 2022 indicates.

Overall, between 2017 and 2019 there was an increase in the number of statements tackling digital issues: 49 statements in 2017, 78 in 2018, and 84 in 2019. It is noteworthy that in 2018, UN Secretary-General António Guterres included digital issues alongside top priority areas on the agenda. However, in 2020 there was a decrease in the number of statements tackling digital in comparison to the previous year (76). This was despite the vow to improve digital cooperation, digital trust, and security, and the fact that, unlike in previous years, national delegations met online to deliver their respective speeches.

In 2021 and 2022, the upward trend continued, with 84 and 92 speeches, respectively, reflecting on the role of digital technologies in the post-COVID-19 era (from economic, security, and development perspectives) and in addressing major global crises, and reacting to the UN Secretary-General's report *Our Common Agenda*.[33]

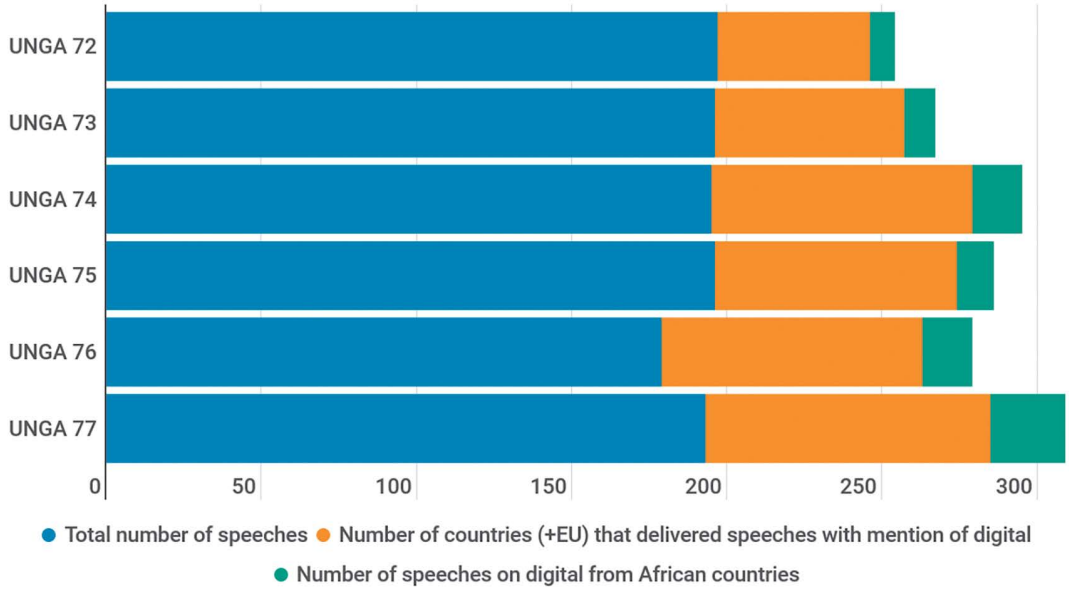


Figure 6. Overview of statements tackling digital issues at the UNGA General Debate between 2017 and 2022.

African countries have followed the overall trend with a steady increase in speeches tackling digital over the first three years observed, followed by a decline in 2020, and again an increase in 2021 and 2022 (Figure 6). Despite the increase in the number of African countries addressing digital, the topic is still predominantly underrepresented in statements from the region, with the majority of countries not tackling it.

In 2017, eight African countries – Algeria, Eritrea, Guinea, **Nigeria**, Eswatini, Morocco, Cabo Verde, and Sierra Leone – mentioned digital topics in their respective national statements. In 2019, the number of countries addressing digital topics doubled (Figure 7). In 2022, the highest number of African countries (24) made reference to digital issues.

[33] DiploFoundation. (2021). *UN General Assembly 76th Session: Analysis of high-level statements.* https://www.diplomacy.edu/reporting-from-the-76th-session-of-the-un-general-assembly/

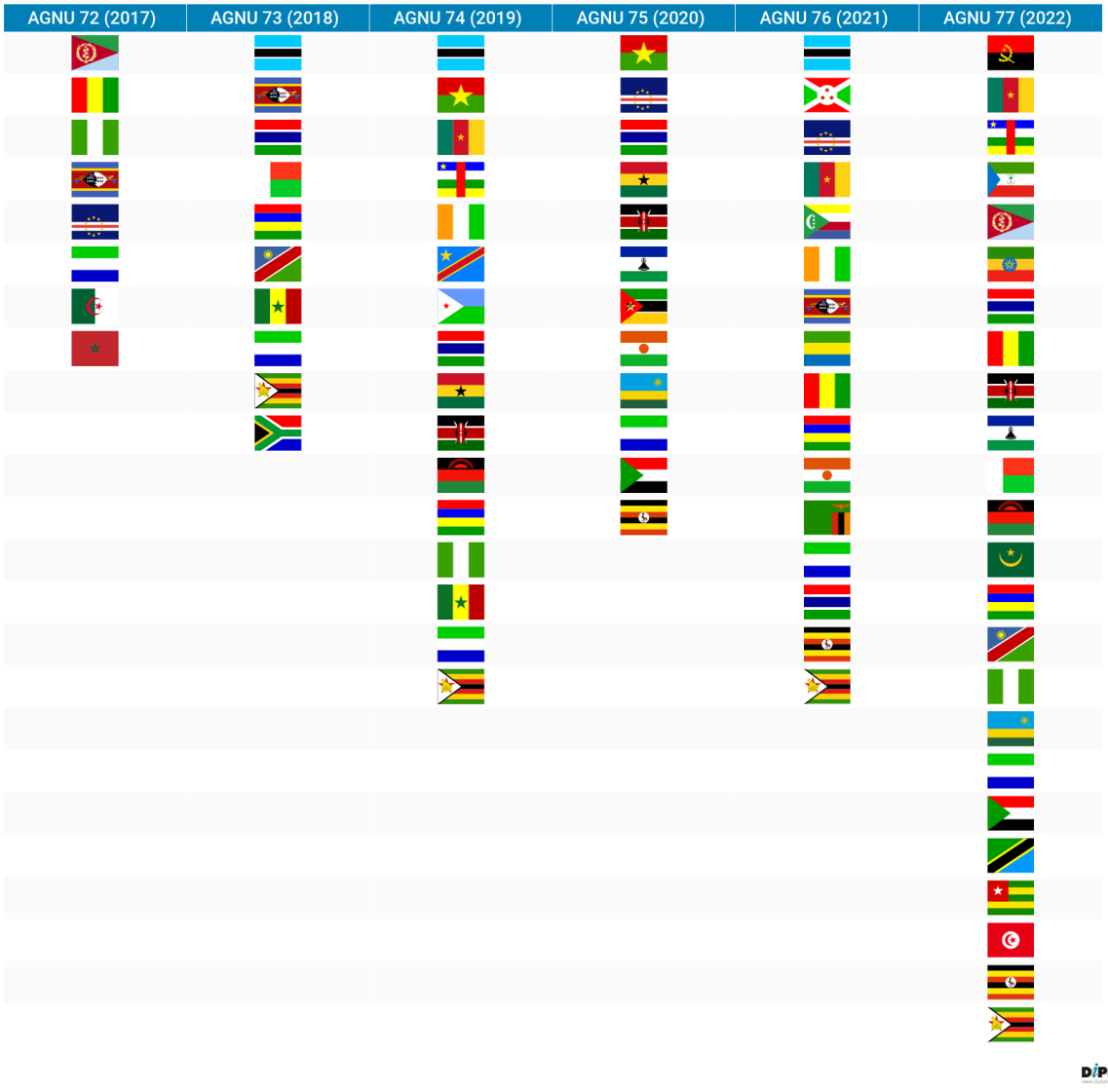


Figure 7. African countries whose leaders tackled digital topics in their UNGA General Debate statements.

As somewhat expected, most statements from Africa focused on the development aspects of digital, noting that digital technologies have the potential to accelerate the attainment of the SDGs; reduce inequality; and enable effective, reliable, and transparent services from banking and business, to education, healthcare, and agriculture, to name but a few. Other digital policy areas such as cybersecurity, the digital economy, and human rights online have also been tackled, although to a lesser extent.

	2017	2018	2019	2020	2021	2022
			Development		Cybersecurity	
			Development	Development		
			Economic and Development			Development, Infrastructure, Cybersecurity
		Economic and Development				Development
	Cybersecurity		Sociocultural			Human rights, Sociocultural
				Development		Economic, Development
		Legal				
		Development				

DIPLO

Figure 8. Digital topics covered by leaders of the focus countries in their UNGA General Debate statements.

Looking more closely at the focus countries, **development-related issues** are most represented, followed by economic and cybersecurity-related topics (Figure 8). **Ghana** noted that the application of technology leads to more prosperity, that access to ICT can bring quality education, and that technology can be employed to accelerate the provision of quality education to as many people as possible.

Similarly, **Côte d'Ivoire** addressed the role of ICTs in reducing social inequalities, in particular between genders. **Kenya**'s representative highlighted the role of technology in driving development, especially in the area of financial inclusion, citing the example of how taking advantage of mobile technology tripled financial inclusion in the country. At the 75th UNGA, the majority of development-related statements, including those of the focus countries, emphasised the importance and timeliness of the UN Secretary-General's *Roadmap for Digital Cooperation* and the need to leave no one behind, especially in times of crisis, such as the COVID-19 pandemic.

Bridging the digital divide and capacity development were at the heart of national statements by Kenya, Namibia, and Rwanda at the UNGA 77.[34] While **Namibia** committed to transformative leadership to ensure access to digital technologies, **Kenya** called for greater investment in the development of ICT infrastructure worldwide and for a global partnership to enhance ICT infrastructure in developing countries. **Rwanda** highlighted the importance of public-private partnerships for digital jobs creation, noting that high-quality digital jobs are a practical response to the underlying drivers of irregular migration.

Supporting the digital economy has been highlighted in several national statements focusing on the economic aspect of digital technologies. In 2019, **Kenya** underscored the country's aspiration to 'champion the growth of an African wide digital economy'. Technology is also seen as the main driver of economic growth and industrial development and as such can create vast opportunities and new jobs for the new generations. **Namibia** highlighted the importance of understanding the role of technology in an evolving job market.

On **cybersecurity**, Nigeria and Côte d'Ivoire highlighted the transnational nature of cybercrimes. **Côte d'Ivoire** pointed out that resolutely tackling cybercrime and other transnational threats will create a stable and resilient world, while **Nigeria** noted the importance of cooperation in this endeavour.

Declaration for the Future of the internet

In April 2022, over 60 countries and territories launched a *Declaration for the Future of the internet*, outlining their commitment to a free, open, interoperable, reliable, secure global internet and broader digital ecosystem. To sustain this vision, the signatories intend to uphold and promote several key principles: protect human rights and fundamental freedoms; maintain a global internet and refrain from actions such as internet shutdowns and blocking of access to lawful content; promote inclusive, affordable, and reliable access to the internet; and promote trust in the digital ecosystem. These principles are to be transposed into concrete policies and actions, as well as promoted within multistakeholder and multilateral processes while respecting the regulatory autonomy of partners.

The initiative was spearheaded by the USA and the EU. Cabo Verde and Niger were among the initial partners that signed the declaration.[35] **Kenya** was also listed among the partners, but an April 2022 letter from a government spokesperson noted that the country's inclusion in the list was 'erroneous'.[36]

[34] Geneva Internet Platform/DiploFoundation. (2022). *77th Session of the UN General Assembly (UNGA 77).* https://dig.watch/event/77th-session-of-the-un-general-assembly-unga-77

[35] US Department of State. (2022). *Declaration for the Future of the Internet.* https://www.state.gov/declaration-for-the-future-of-the-internet

[36] Kenya Government. (2022). *Press release: Declaration for the future of the internet*. https://ict.go.ke/wp-content/uploads/2022/04/DECLARATION-FOR-THE-FUTURE-OF-THE-INTERNET.pdf

UN Security Council: Digital topics

The UN Security Council is tasked with working to maintain international peace and security in accordance with the principles and purposes of the UN. The Council is composed of five permanent members (China, France, the Russian Federation, the UK, and the USA) and ten non-permanent members elected by the UNGA for two-year terms. There are three African countries currently serving on the Council: Gabon (2022–2023), **Ghana** (2022–2023), and **Kenya** (2021–2022).

Although not highly prominent, the Council inevitably addresses digital topics in its deliberations. Our analysis of records of meetings held between January 2020 and August 2022 reveals that such topics range from the misuse of digital communication tools for spreading misinformation and the abuse of digital technologies by terrorist groups to the need to strengthen cybersecurity capabilities at the national level and address gender-based online violence. What follows is an overview of the positions or main interests of several African countries that contributed to these discussions.[37]

In debates on maintaining international peace and security, **Kenya** stressed the need to **achieve a balance** between fostering digital innovation and addressing the malicious use of technology by both state and non-state actors. In Kenya's view, the **UN should support countries in their efforts to address the impact of the digital revolution on national stability**, and the Security Council should ensure that the UN has the expertise and capacity to play such a role. The country also argued that the UN and regional organisations should have a stronger voice in ensuring that militarised AI is developed ethically and in line with the principles of the UN Charter.

Ghana stressed the need for countries to build **national capacities to enhance cybersecurity**. Gabon noted that technology could help manage and prevent conflict, promote a better understanding of situations, ensure the safety of peacekeepers and civilians, allow for timely reactions, and minimise collateral damage. However, the country raised concerns about the increasing robotisation and digitalisation of battlefields and stressed the need for UN peacekeepers and national armed forces to be equipped with adequate technology to respond to emerging threats.

Not surprisingly, **the links between terrorist activities and digital technologies** were brought up in several Council discussions. **Kenya** noted the importance of ensuring that governments can combat the misuse of digital technologies by terrorist groups. **Ghana** added that vulnerable countries would benefit from international support in strengthening their digital capacities to address such challenges. The country also called for support for regional platforms for sharing intelligence and information (such as the Accra Initiative[38]), noting that they could contribute to enhancing the early detection of terrorist networks. Both Ghana and Tunisia noted that sustained efforts are needed to track and cut off terrorism financing mechanisms in the digital economy, in particular when it comes to the use of digital and cryptocurrencies.

Djibouti and Guinea referred to the need for sustainable financial support and technology transfer to support countries in need in their efforts to address terrorism and to leverage new technologies in the fight against it. Ethiopia added that strategies to combat terrorism and extremism need to be holistic, comprehensive, and address underlying causes as well. One such cause, the country noted, is the increasing social and political polarisation driven, among other elements, by the rise of intolerant speech and hate-filled narratives disseminated through the internet and social media.

South Africa, Niger, and Tunisia – together with all other members of the Security Council – voted in favour of the July 2020 *Resolution S/RES/2535* on maintaining international peace and security

[37] Identified based on records of meetings held by the Security Council between January 2020 and August 2022.

[38] The Accra Initiative, launched in 2017, brings together Benin, Burkina Faso, Côte d'Ivoire, Ghana, and Togo (with Mali and Niger as observers) with the goal to facilitate cooperation in addressing terrorism and transnational organised crime and violent extremism. In 2020, the member countries signed a memorandum of understanding on security and intelligence cooperation. Source: European Council on Foreign Relations. (n.d.). *Mapping African regional cooperation*. https://ecfr.eu/special/african-cooperation/accra-initiative/

which, among other provisions, encouraged member states to act cooperatively to prevent terrorists from exploiting technology, while respecting human rights and fundamental freedoms, and in compliance with international law.[39] This was reiterated in the December 2021 *Resolution S/RES/2617* on threats to international peace and security caused by terrorist attacks. The resolution stressed the need for member states to cooperate among themselves, and with the private sector and civil society, to develop and implement effective means to prevent and counter the use of the internet and other ICTs for terrorist purposes while respecting human rights and fundamental freedoms.[40] **Kenya**, Niger, and Tunisia were at the time on the Security Council and voted in favour of the resolution, together with all other members.

When discussions revolved around **women and peace and security**, countries brought up issues related to fostering digital inclusion and protecting women and girls in the digital space. Tunisia highlighted the role that modern technology and innovative solutions could play in empowering women and enhancing their full participation in the society and economy. It also called for more efforts to address the legal, social, and cultural barriers to gender equality.

South Africa called on public and private actors, as well as regional and international financial institutions, to invest in initiatives focused on enhancing women's access to digital technologies, developing their digital skills, and empowering them to become entrepreneurs in the digital economy. **Kenya** too noted that partnerships between local women entrepreneurs, peace and development agencies, and international and regional financial institutions could help strengthen the economic empowerment of women. It further stressed that ensuring women's economic and financial inclusion and participation is key to building peace and called for actions to enhance women's access to digital platforms. **Ghana** joined South Africa and Kenya in calling on developed countries and supranational institutions to provide funding and technical support for women's empowerment initiatives in developing countries and LDCs.

Kenya urged countries to increase the prosecution of perpetrators of online gender-based violence, harassment, and intimidation.

International instruments and regulatory frameworks related to digital topics were occasionally brought up in Council discussions. **Ghana** encouraged support for the implementation at the national level of policy instruments such as the Council of Europe (CoE) *Convention on Cybercrime (Budapest Convention)*[41] and the *AU Convention on Cybercrime and Personal Data Protection (Malabo Convention)*.[42] Noting that conversations are ongoing, in particular in the Global North, on the regulation of digital technologies, **Kenya** cautioned that the Global South is not sufficiently included. It further called for increased collaboration and partnerships between states, technology companies, and the UN in addressing cyber challenges such as fake news and encouraged companies to establish regional hubs to better support governments in such efforts. Such cooperation could also foster the development and deployment of early-warning tools to be used within peace operations.

It is worth noting that digital-related discussions at the Security Council tend to focus more on the impact of digitalisation and digital technologies on core security issues, and less on cybersecurity issues per se. For the upcoming period, we can expect digital topics to feature more and more often on the Council's agenda, including in relation to the misuse of digital technologies in the context of war and conflict, the potential of such technologies in peace operations, and the overall links between digital and national and international security.

---

39 UN Security Council. (2020). *Resolution S/RES/2535 (2020).* https://undocs.org/en/S/RES/2535%20(2020). Botswana, Burkina Faso, Cabo Verde, Djibouti, Kenya, Lesotho, Namibia, Niger, Nigeria, South Africa, and Tunisia were among the countries that submitted the draft resolution.

40 UN Security Council. (2021). *Resolution S/RES/2617 (2021)*. https://undocs.org/en/S/RES/2617%20(2021)

41 Council of Europe [CoE]. (2001). *Convention on Cybercrime (ETS No. 185).* https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

42 African Union [AU]. (2014). *African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

G-77 and Africa's digital diplomacy

In addition to member states' direct contributions, the position of African countries on digital policy topics discussed within the UN can also be inferred from statements of the Group of 77 (G-77).

G-77 describes itself as 'the largest intergovernmental organisation of developing countries in the United Nations which provides the means for the countries of the South to articulate and promote their collective economic interests and enhance their joint negotiating capacity on all major international economic issues within the United Nations System'.[43] African UN member states – all of which are part of the group – typically contribute to the formulation of G-77 unified positions.

For instance, G-77 has been particularly active in discussions and consultations following up to the UN Secretary-General's report entitled *Our Common Agenda*, which tackles issues related to digital cooperation. In a February 2022 statement, G-77 and China noted that advancing digital cooperation is particularly important when it comes to 'inclusive digital economy, access to digital networks and connectivity, technology transfer, investment in digital infrastructures, data protection, artificial intelligence, avoiding internet fragmentation, countering the proliferation of disinformation and misinformation, and outlining shared principles for a digital future for all to achieve the 2030 Agenda'. The statement also highlighted the need to 'avoid unnecessary politicization of technical issues to foster an open, fair, inclusive, and non-discriminatory environment for the development of digital technologies in developing countries'.[44]

Internet Governance Forum

Annual meetings of the IGF offer stakeholders from governments, businesses, the technical community, academia, civil society, and international organisations an opportunity to engage in open discussions on internet and digital policy topics they find relevant. While the IGF is not a decision-making body, forum discussions help inform decisions taken elsewhere.

IGF meetings are open to anyone interested. This, however, does not mean that anyone can indeed participate. Issues of capacities and costs tend to pose challenges to actors from developing countries and LDCs in particular, although the IGF itself and various organisations have put in place programmes to enhance participation from such actors (not only in terms of funding but also awareness raising and capacity development).

Participation in IGF meetings

An analysis of IGF participation data between 2016 and 2021 indicates that the participation of African actors was low in 2016, and considerably increased, but oscillated, between 2017 and 2021 (Figure 9). Venue matters and this is likely one of the reasons behind the low number of African participants in the IGF 2016 meeting. With the meeting held in Mexico, African stakeholders found it more difficult to attend (financial resources typically being a constraint preventing actors from developing countries and LDCs from participating in meetings taking place in remote locations). (The chart also reflects another IGF reality: The region where the physical meeting is hosted has the largest number of participants.)

When compared with participation from other regions,[45] Africa tends to occupy a middle position. The region ranked second in 2017, 2018, and 2019, and third in 2020 and 2021 (Figure

[43] G-77. (n.d.) *About the Group of 77*. https://www.g77.org/doc/

[44] G-77. (2022). *Statement of behalf of the Group of 77 and China by Ambassador Munir Akram, Permanent Representative of Pakistan to the United Nations, on thematic cluster-III, 'Frameworks for a peaceful world – Promoting peace, international law, and digital cooperation', at the informal thematic consultations as a follow-up to the report of the Secretary-General entitled 'Our Common Agenda' (New York, 21 February 2022).* http://www.g77.org/statement/getstatement.php?id=220221

[45] The IGF uses the following regional groups: Africa, Asia-Pacific, Eastern Europe, Latin America and the Caribbean (GRULAC), and Western Europe and Others (WEOG). Details on the composition of these groups are available at https://www.un.org/dgacm/en/content/regional-groups. Representatives of intergovernmental organisations (IGOs) are not

9).[46] Aggregated data for all six IGF meetings we have looked at place Africa as the third best-represented region, after the Western Europe and Others Group (WEOG) and Eastern Europe (and followed by Asia-Pacific and the Latin America and Caribbean Group (GRULAC)) (Figure 10).[47]

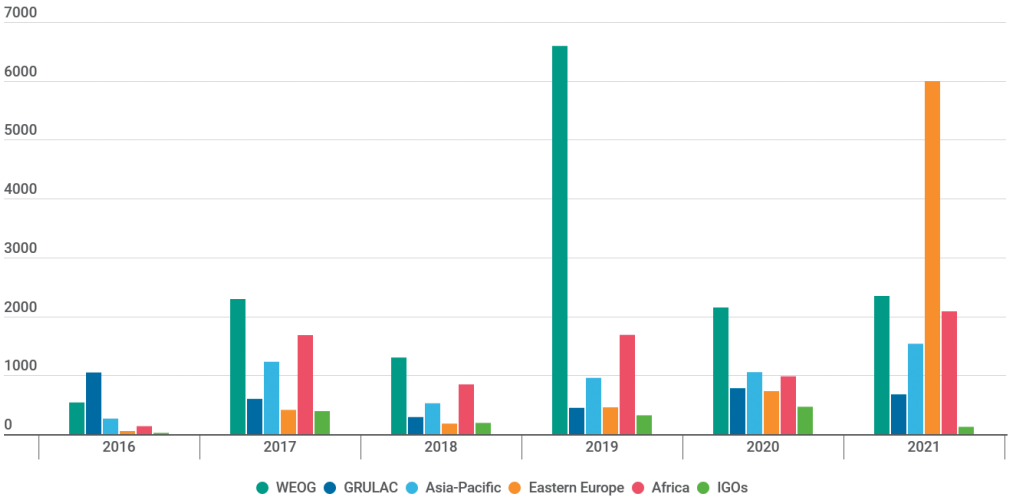


Figure 9. Participation in IGF meetings, by regional group (year-by-year data).

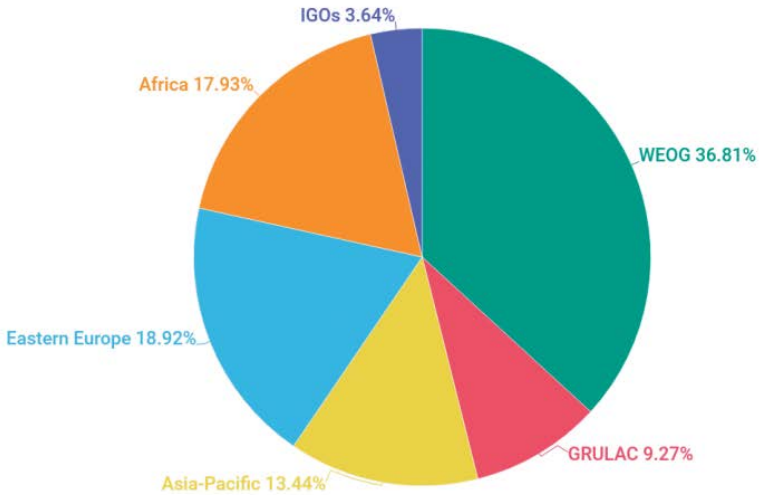


Figure 10. Participation in IGF meetings between 2016 and 2021, by regional group (aggregated data).

Looking at African participation only, civil society[48] has been the group with the highest representation among all stakeholder groups over the years (Figure 11). This is also consistent with overall IGF participation trends, which show that civil society is usually the group with the highest representation (Figure 12).

assigned to any regional group.

46 IGF-related statistics in this study are based on data provided by the IGF Secretariat.

47 Between 2016 and 2019, the IGF Secretariat collected data related to onsite participation; in 2020 the entire meeting was held completely online (so data refers to registered online participants), while in 2021 – when emphasis was put on hybrid participation modalities – information was collected for both onsite and online participants.

48 It is worth noting that the civil society group also includes academia and research communities.

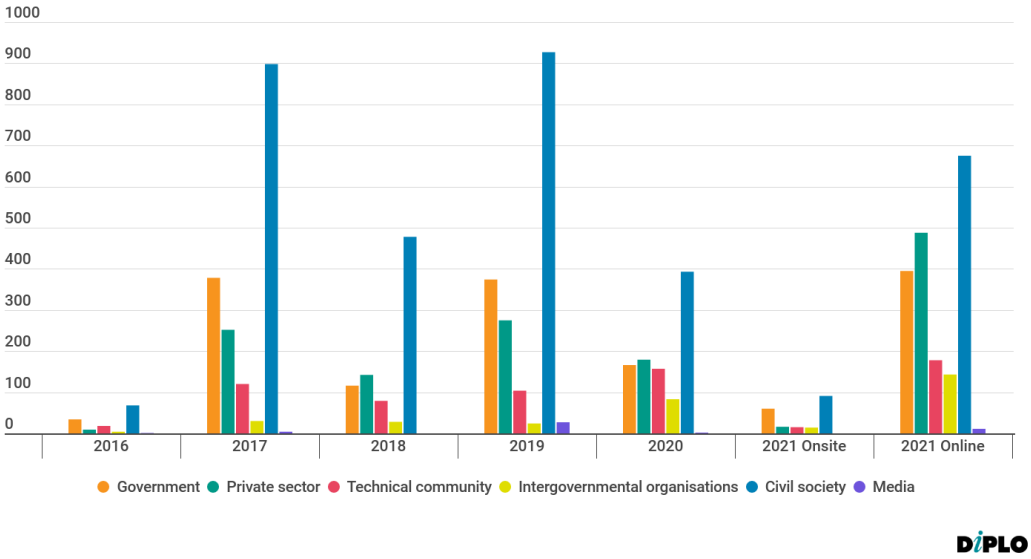


Figure 11. African participation in IGF meetings, by stakeholder group.

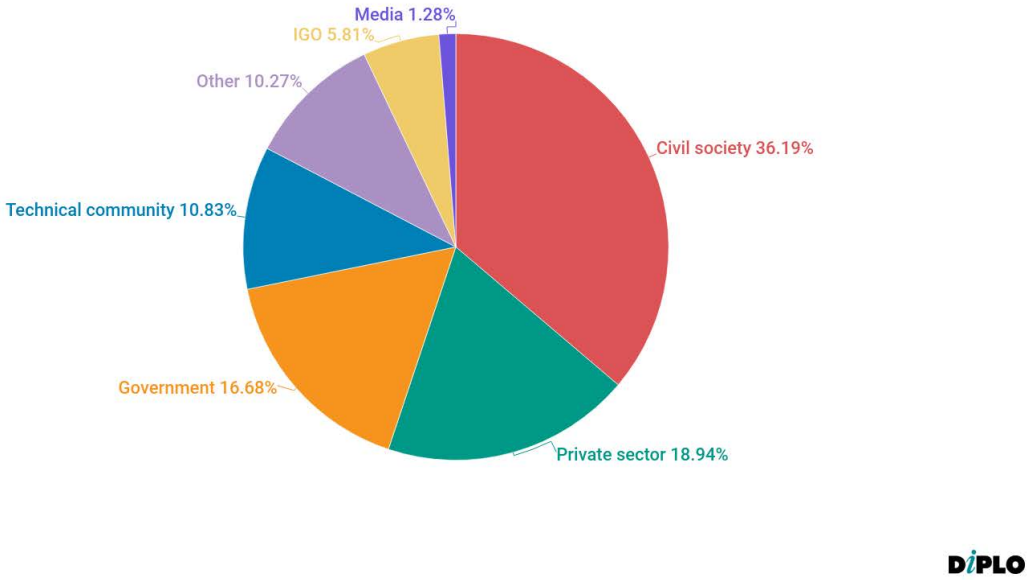


Figure 12. Participation in IGF meetings between 2016 and 2021, by stakeholder group (aggregated data).

Speakers in IGF meetings

Besides general IGF participation, we also looked at the involvement of African stakeholders in discussions, as speakers in IGF workshops. Between 2018 and 2021, the highest number of Africa-based speakers was recorded in 2018 (201) and the lowest in 2020 (35).

In a ranking of speakers by region, Africa positions itself only in third (2018, 2019, and 2021) and fourth place (2020) (Figure 13). Aggregated data for all four IGF meetings place the region as the third by number of speakers, after WEOG and Asia-Pacific, and ahead of GRULAC and Eastern Europe (Figure 14).

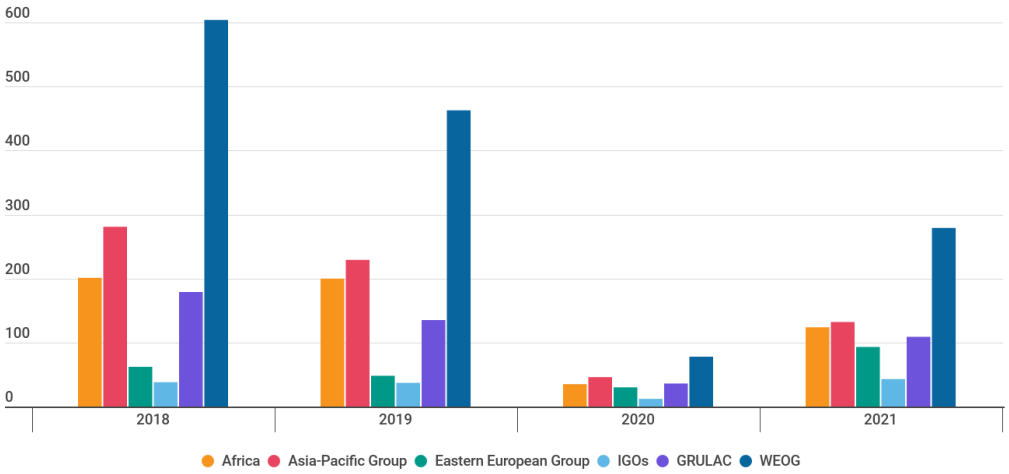


Figure 13. Distribution of IGF speakers by region (year-by-year data).

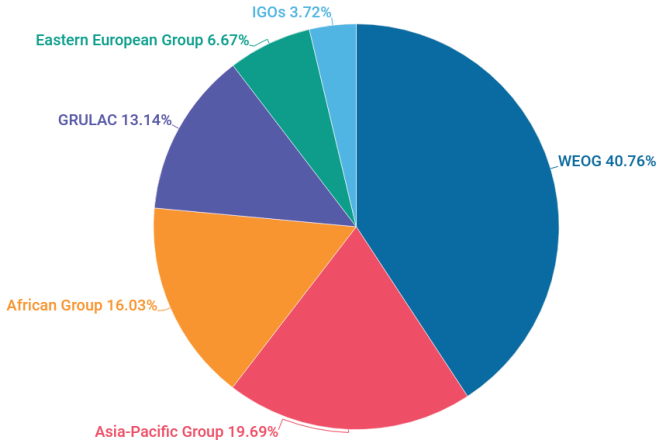


Figure 14. IGF speakers by region, IGF 2018–IGF 2021 (aggregated data).

In terms of distribution by stakeholder groups, civil society is again in the lead, as the group with the largest number of speakers from Africa (Figure 15). This too is consistent with overall IGF data: between 2018 and 2021, over 50% of speakers were civil society representatives (Figure 16).

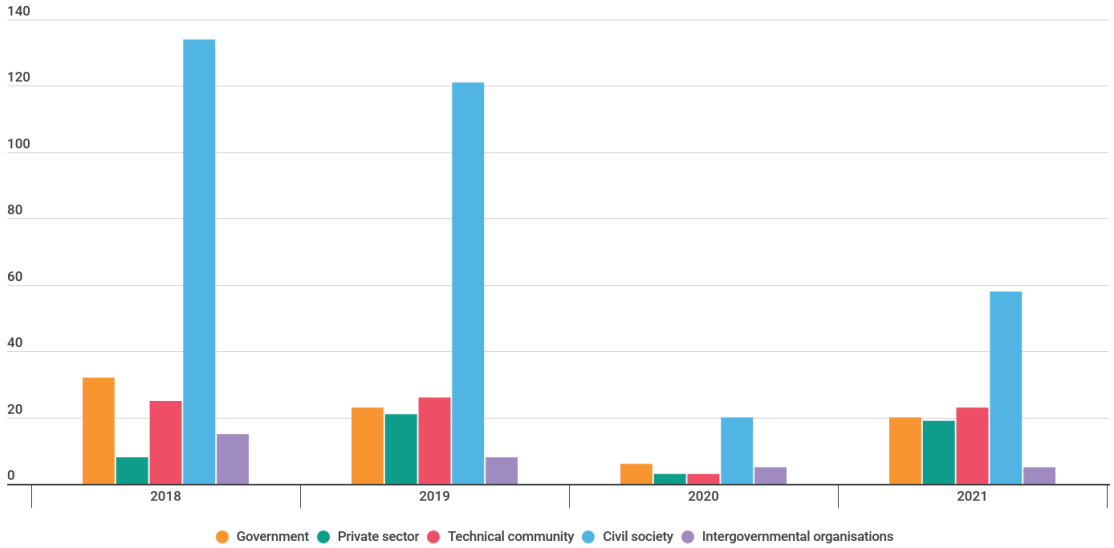


Figure 15. IGF speakers from Africa by stakeholder group, IGF 2018–IGF 2021 (year-by-year data).

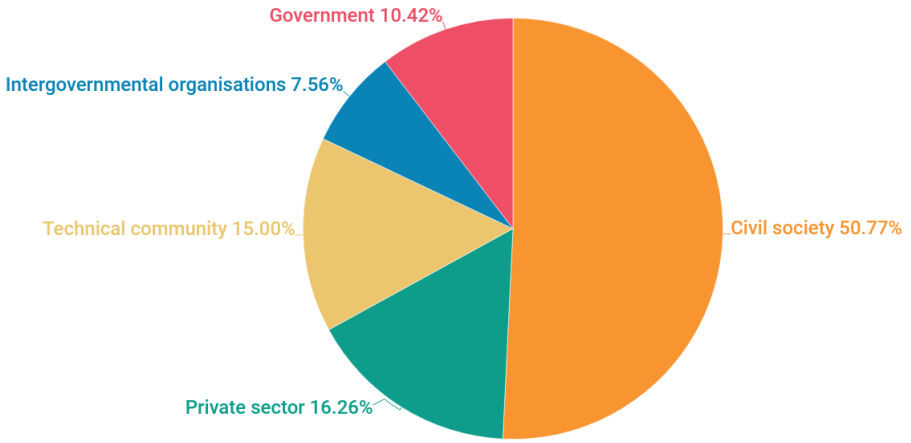


Figure 16. IGF speakers by stakeholder group, IGF 2018–IGF 2021 (aggregated data).

Actors organising sessions at the IGF

We also looked at the involvement of African actors in the organisation of workshops at annual IGF meetings between 2016 and 2021. Workshops form the largest part of IGF meetings and are selected by the Multistakeholder Advisory Group (MAG) from proposals submitted by stakeholders from all over the world. They are sometimes co-organised by two or more entities.

Compared with other regions, African actors are not particularly active when it comes to hosting IGF workshops (Figure 17). When they do host workshops, this is mostly done by civil society actors, followed by the technical community and the private sector (Figure 18). This too is consistent with overall IGF data, showing a higher involvement of civil society in the hosting of workshops (Figure 19).

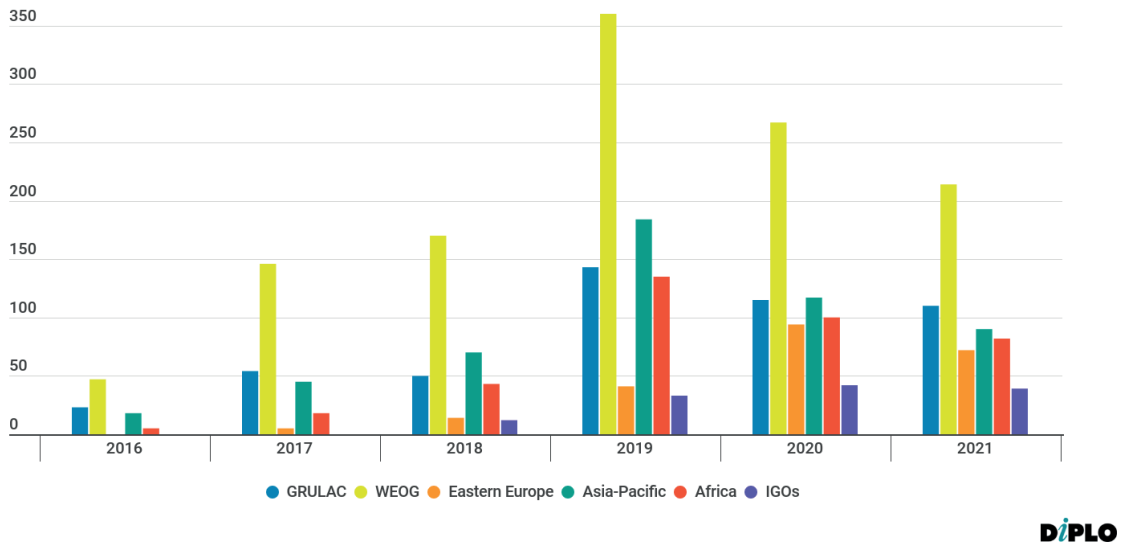


Figure 17. IGF workshop organisers by region, IGF 2016–IGF 2021 (year-by-year data).

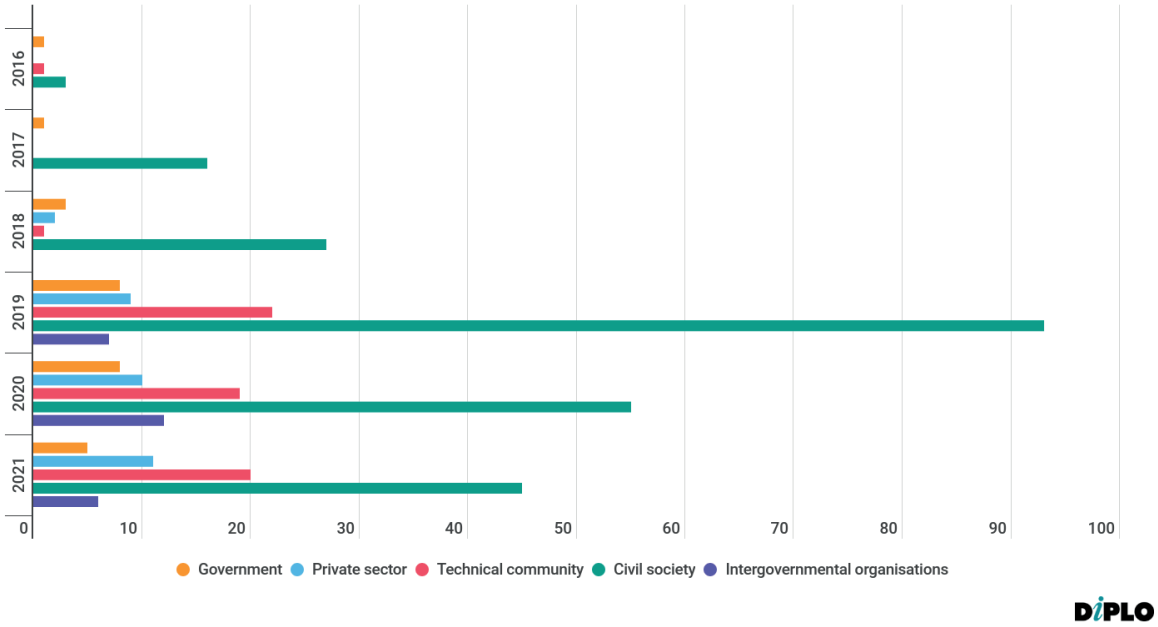


Figure 18. Workshop organisers from Africa by stakeholder group, IGF 2016–IGF 2021.

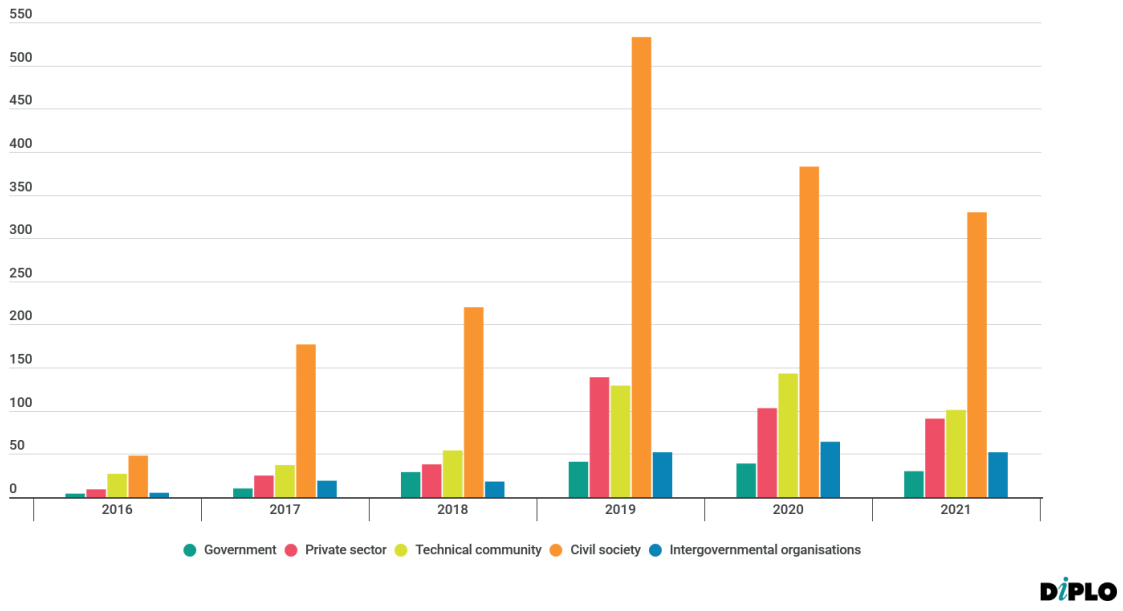


Figure 19. Workshop organisers by stakeholder group, IGF 2016–IGF 2021.

2. Digital infrastructure and standards

Section summary

Despite being a latecomer to digital transformation, Africa is a relatively fast adopter of technology. For instance, the percentage of individuals using the internet across the region has grown from 9.6% in 2010 to 33% in 2021. And improvements have been made at the level of internet infrastructure: more submarine cables connecting the region with the rest of the world and contributing to higher internet penetration rates; a slow, but continuous expansion of mobile networks (the African population largely relies on mobile devices to connect to the internet) and fibre optics; a growing number of Internet Exchange Points (IXPs); and increasing attention to the use of satellites to provide connectivity in particular in remote locations. However, challenges remain, from considerable digital divides between regions and communities to the affordability of access.

Objectives and measures to address such challenges and strengthen or expand internet infrastructures are outlined in various national, regional, and continental policies, some of which also include international dimensions. National broadband and 5G policies (e.g. in Kenya, Nigeria, Senegal, or South Africa), the AU's *Digital Transformation Strategy* and various initiatives across RECs talk about working with international partners/investors to boost infrastructure deployment, ensuring regional and international coordination on radio frequency matters, enhancing participation in relevant forums (e.g. ITU), and garnering support from international institutions to develop enabling policy environments.

All African countries have actors participating at ITU. In addition to specialised ministries or agencies, there is also participation from academic institutions, telecom operators, ISPs, and other private entities (this is the case for 34 countries). There are also several countries with actors engaged in leadership roles across several study groups of ITU Sectors (e.g. Algeria, Côte d'Ivoire, Egypt, Ghana, Morocco, Nigeria, Rwanda, Sudan, Tunisia), indicating their strong interest in being part of these international processes.

The adoption and enforcement of international technical standards and strengthened participation in relevant standardisation processes are also envisioned as goals in several domestic policies and strategies (e.g. Ghana, Kenya, Namibia, Nigeria, Senegal, and South Africa). While actors in several African countries participate in standardisation work at ITU, there is less involvement in other international standardisation processes such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Internet Engineering Task Force (IETF), and the 3rd Generation Partnership Project (3GPP). This can be explained by multiple factors, from limited awareness of the importance of being part of these processes to a lack of adequate resources (among governments, national standardisation bodies, and technical and business communities) to support such participation.

When it comes to the management of critical internet resources – particularly domain names and internet protocol addresses – African actors (governmental or non-governmental) tend to be engaged in relevant regional and international processes such as ICANN and the African Network Information Centre (AFRINIC). For instance, 44 governments participate in the work of ICANN's Governmental Advisory Committee (GAC), 39 operators of country-code top-level domains (ccTLDs) participate in the Country Code Names Supporting Organization (ccNSO), and business and civil society actors from at least 30 countries participate in the Generic Names Supporting Organization (GNSO) and the At-Large community.

Digital infrastructure and standards set the basis for future digital developments. They are also part of the critical infrastructure of modern society. Thus, countries need to, at least, follow policy developments and processes in this field and, at best, try to influence them in accordance with their national priorities related to access, security, and economic development. So far, Africa has been focusing on connectivity and access as a priority. This approach is understandable, considering that without reliable and meaningful connectivity, nothing else is possible within the digital realm.

2.1. Status of access and connectivity

Africa is a latecomer to digitalisation, but also a rather fast adopter of technology. Between 2010 and 2021, the internet penetration rate across the region grew from 9.6% to 33% (individuals using the internet).[49] Looking back to 2000, the growth rates are even more impressive, as illustrated in Figure 20.

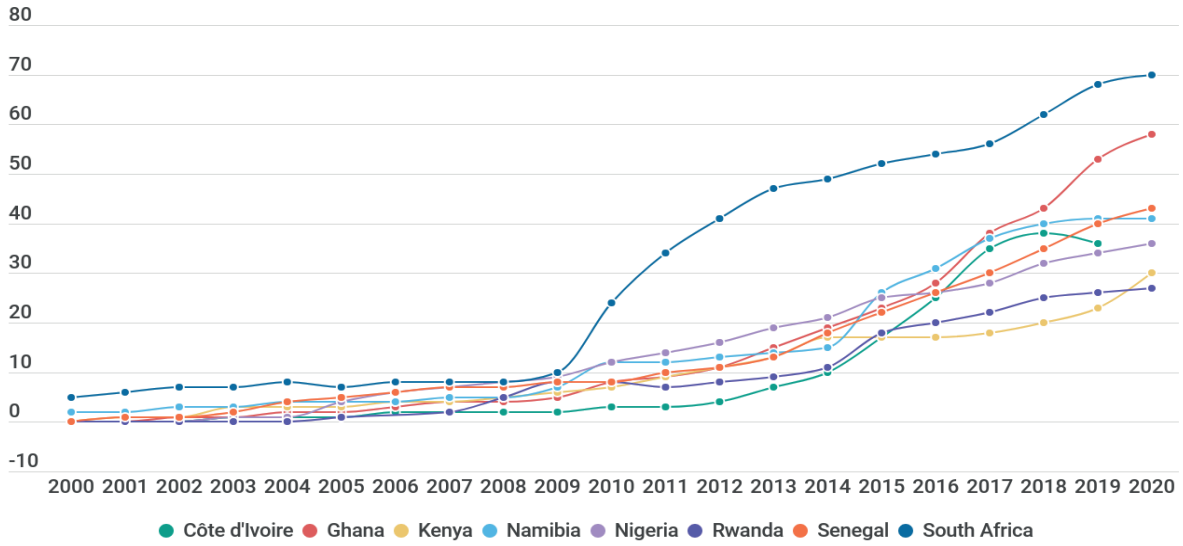


Figure 20. Evolution of internet penetration rates (% of population) in the focus countries[50]

As more Africans are getting online, there have also been improvements at the level of internet infrastructure. Tremendous shifts in terms of **submarine cable connections** have happened over the last 10–15 years: In 2008, only 16 African countries were connected to a submarine cable system. By the end of 2019, 37 countries had at least one submarine cable landing.[51] According to Telegeography, 71 cable systems connected to Africa are active or under construction in 2022.[52]

The number of cables connecting the region with other parts of the world keeps growing (Figure 21), and this contributes to higher internet penetration rates, reductions in the costs of internet services, stronger competition in the telecom market, and lowered risks of internet access disruptions.

For a long time, there has been a division between content providers such as tech companies Meta and Google, and providers of connectivity such as AT&T and British Telecom, the latter arguing that content providers take advantage of telecom infrastructures without financially contributing to deployment or maintenance. The situation is now changing, as tech platforms start investing in their own underwater cables connecting continents. Google, for instance, is deploying the Equiano cable connecting Europe and the West African coast (from Portugal to South Africa, with landings along the way, in places such as Togo and Nigeria).[53] The 2Africa cable system, built by Meta in partnership with several African and global operators, aims to be one of the largest subsea cables ever deployed, connecting 23 countries in Europe, Africa, and the Middle East.[54]

---

49 International Telecommunication Union [ITU]. (2021). *Measuring digital development: Facts and sigure 2021* and International Telecommunication Union [ITU]. (2010). *ICT Facts and Figures 2010*. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

50 Based on World Bank. (2022). *Individuals using the internet (% of population).* https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2020&start=2000&view=chart. Figure redrawn.

51 Submarine Cable Networks. (n.d.). *Submarine cables in Africa.* https://www.submarinenetworks.com/en/africa

52 TeleGeography. (2022). *Africa Telecom Map 2022*. https://africa-map-2022.telegeography.com

53 Francois, M. D., George, C., & Stowell, J. (2019, June 28). *Introducing Quioano, a subsea cable from Portugal to South Africa.* Google Cloud. https://cloud.google.com/blog/products/infrastructure/introducing-equiano-a-subsea-cable-from-portugal-to-south-africa

54 Ahmad, N. & Salvadori, K. (2020, May 13). *Building a transformative subsea cable to better connect Africa*. Engineering at

These developments could lead to altering current internet traffic practices and principles, as tech companies are likely to use their cables for their own traffic. Thus, the net neutrality principle – which guarantees equal treatment for all digital traffic – could be challenged, with an enormous impact on the core nature of the internet. Upholding net neutrality would therefore be a task for policymakers and regulators.

Moreover, although Africa mainly focuses on ensuring affordable connectivity – and having more cables contributes to achieving this goal – African stakeholders should envisage the possible risk of being faced with restrictions to access placed by any one tech company that provides vertically integrated services, from undersea cables to online services.[55]

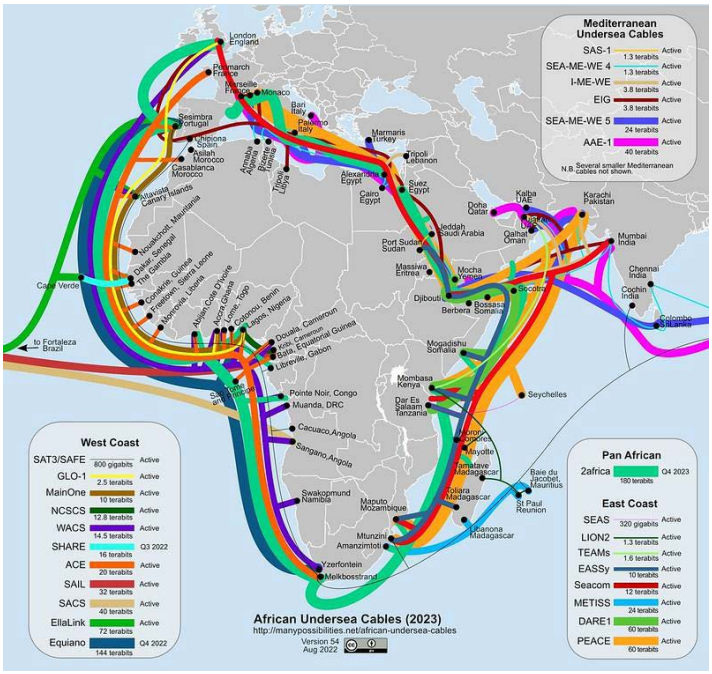


Figure 21. African undersea cables.[56]

Within the continent, internet access is made available – in varying degrees – through copper wires, fibre optic cables, mobile networks, and satellites. Because the region lacks an adequate network of copper telecom cables (as fixed telephony landlines or cable TV did not have a significant uptake), Africa's population has largely relied on mobile devices and networks for internet access.

ITU statistics for 2021 indicate that mobile broadband coverage – via 3G and 4G networks – was available to 82% of the population in Africa (49% for 4G and 33% for 3G).[57] And while many countries continue to invest in 4G networks, 5G is also being deployed. As of July 2022, 5G networks were being tested or widely deployed in 14 African countries (Figure 22).

Meta. https://engineering.fb.com/2020/05/13/connectivity/2africa/

55 Blum, B. & Baraka, C. (2022, May 10). *Sea change*. Rest of World. https://restofworld.org/2022/google-meta-underwater-cables/

56 Many Possibilities. (2022). *African undersea cables.* https://manypossibilities.net/african-undersea-cables/

57 International Telecommunication Union [ITU]. (2021). *Measuring digital development. Facts and figures 2021.* https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

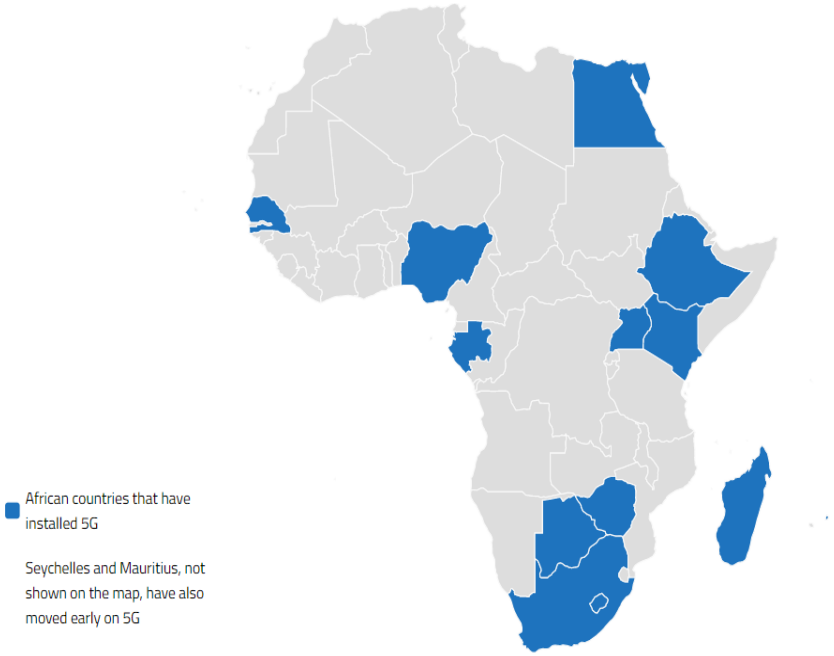


Figure 22. Countries that have deployed 5G networks (July 2022).[58]

The deployment of fibre optics has also taken up (Figure 23). Across the entire continent, the terrestrial network capacity (i.e. kilometres of fibre deployed) has more than tripled between 2010 and 2020, from 331,066 km in 2010 to 1,072,649 km in 2020.[59]

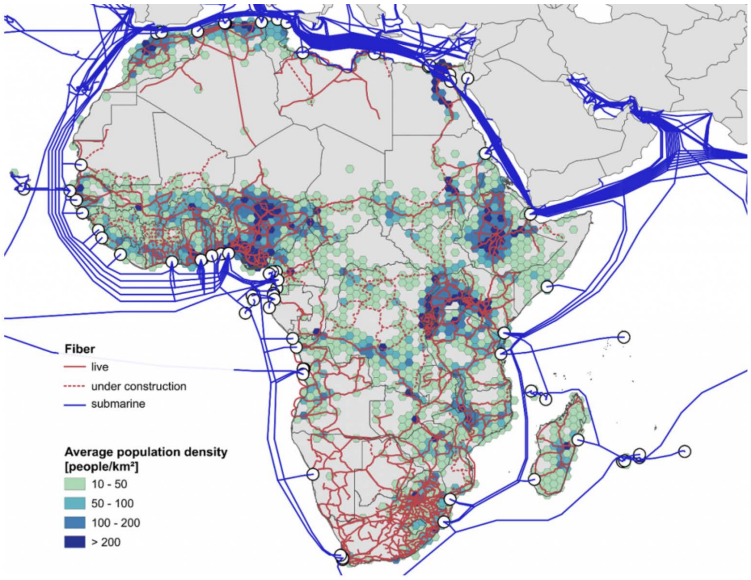


Figure 23. Fibre infrastructure in Africa.[60]

Africa also tries to maintain internet traffic locally by establishing IXPs. According to the African IXP Association, there are 49 active IXPs located in 45 cities across 35 countries in Africa (Figure 24).[61]

58 Based on Ngila, F. (2022, July 20). *Which countries have rolled out 5G in Africa?* Quartz Africa. https://qz.com/africa/2168658/which-countries-have-rolled-out-5g-in-africa/ Figure redrawn.

59 Hamilton Research. (2021). *Africa: Africa's International Bandwidth Reaches 15.289Tbps.* http://www.africabandwidth-maps.com/?p=6440

60 Ngari, L. & Petrack, S. A (2020). *Internet infrastructure in Africa*. https://empowerafrica.com/internet-infrastructure-in-africa/

61 African IXP Association. (2022). *List of active internet exchange points in Africa.* https://www.af-ix.net/ixps-list

Figure 24. IXPs across Africa (October 2022).

While terrestrial and mobile infrastructures represent the main gate to internet access across Africa, satellites are also increasingly used to enable connectivity, in particular in underserved and remote locations (Figure 25). In addition to governments launching operational geosynchronous equatorial orbit (GEO) satellites to provide internet connectivity (this is the case, for instance, with Algeria, Angola, Egypt, and **Nigeria**), there are also several GEO satellite companies (e.g. Eutelsat, Inmarsat, Intelsat) as well as an increasing number of low-Earth orbit (LEO) satellite operators (e.g. Globalstar, SES) providing access to broadband internet via satellites.[62]

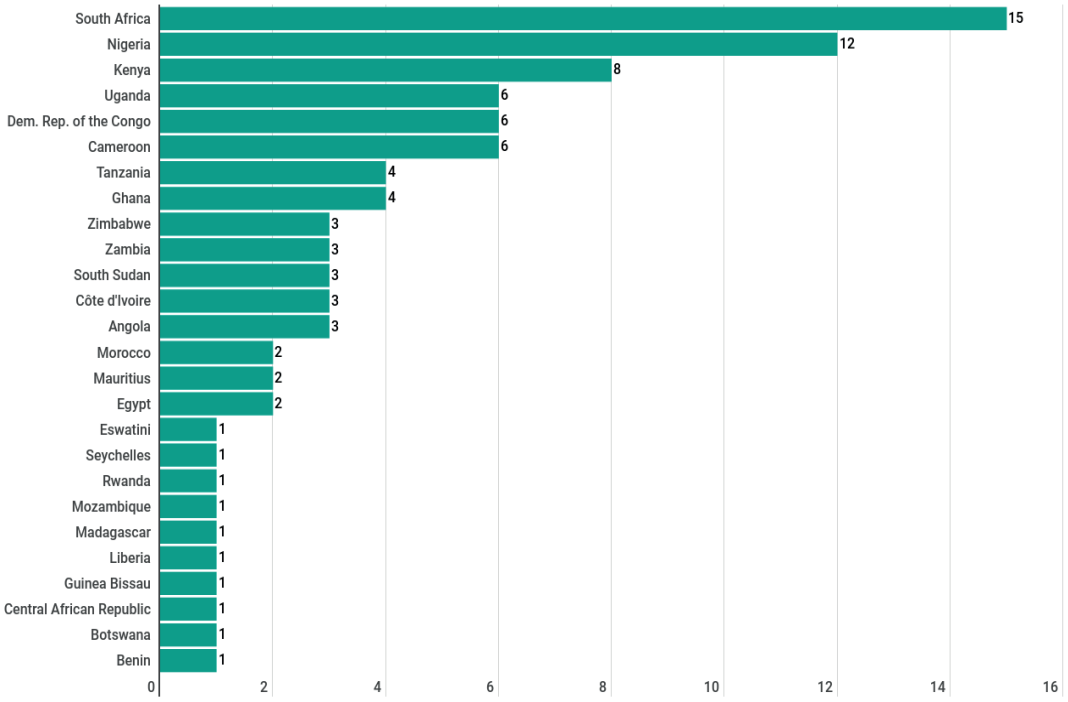


Figure 25. Number of GEO satellite internet providers in African countries (January 2022).[63]

[62] Space in Africa. (2022, January 18). *The state and future of LEO satellite internet connectivity in Africa*. Via Satellite. https://interactive.satellitetoday.com/via/january-february-2022/the-state-and-future-of-leo-satellite-internet-connectivity-in-africa/

[63] Space in Africa. (2022, January 18). *The state and future of LEO satellite internet connectivity in Africa*. Via Satellite. https://interactive.satellitetoday.com/via/january-february-2022/the-state-and-future-of-leo-satellite-internet-connectivity-in-africa/

A relatively new development in the digital connectivity space is Starlink's constellation of thousands of low-orbit satellites. Most of the satellites are aimed to serve remote areas, where the deployment of terrestrial or mobile connectivity would incur high costs. In 2022, Starlink announced it had received regulatory approvals to start operations in two African countries: **Nigeria** and Mozambique.[64] The service availability map on Starlink's website also lists Angola, Botswana, the Democratic Republic of the Congo, Egypt, Eswatini, **Kenya**, Malawi, Mauritania, Tanzania, and Zambia among the countries that are pending service coverage or regulatory approval in 2023.[65] Due to Africa's geographical size and the still weak terrestrial infrastructure, the company could play a prominent role in providing last-mile access to communities across the continent. But while it could contribute to solving the problem of access for local, remote communities, Starlink will likely also give rise to issues related to dependence on its services and risks associated with monopolies. And there is also the issue of affordability: a monthly residential subscription to Starlink could go up to USD$100, which is more often than not a prohibitive cost.

Across Africa, barriers to access are not only related to the availability of last-mile connectivity. In fact, affordable access to the internet remains the main challenge for the continent. In 2021, according to the Alliance for Affordable Internet (A4AI) and ITU, Africans had to pay, on average, 6.5% of their monthly income to get 2GB of mobile data which, for example, is used to watch four hours of low-quality video on Netflix. In comparison, users were spending, on average, 1.7% of their monthly income in Asia-Pacific and 0.5% in Europe.[66] Overall, the affordability of broadband connectivity remains the lowest across Africa, with fixed broadband (Figure 26) being less affordable than mobile broadband.

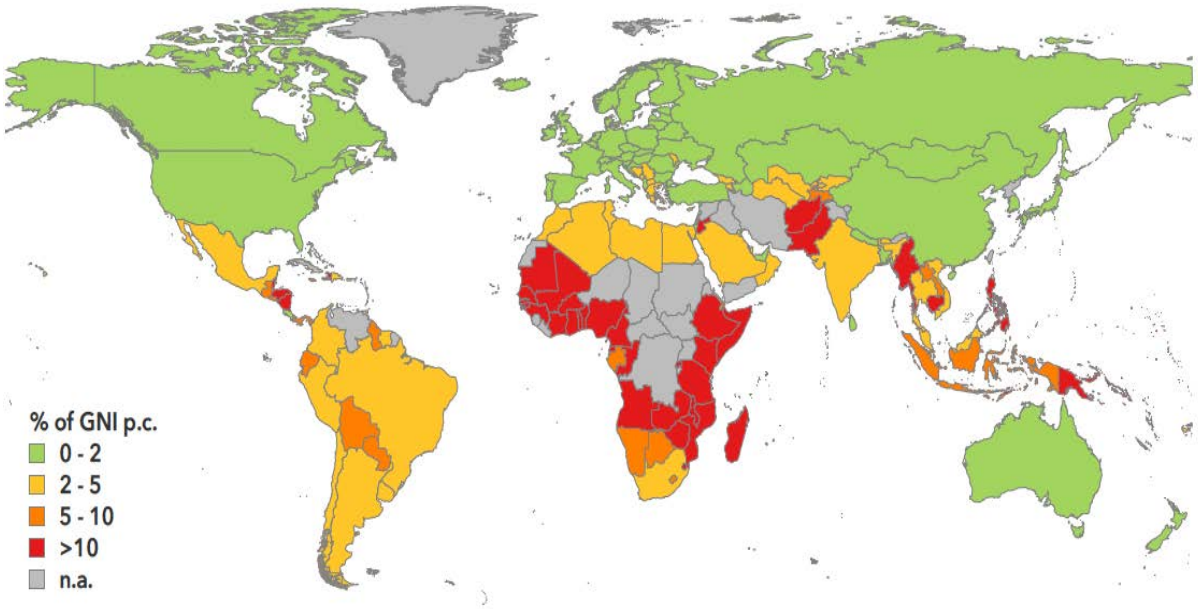


Figure 26. Affordability of fixed broadband, relative to monthly gross national income per capita (GNI p.c.).[67]

[64] Onukwue, A. (2022, May 31). *Starlink is coming to Africa, but who will use it?* Quartz Africa. https://qz.com/africa/2171730/starlink-is-coming-to-africa-but-who-will-use-it/

[65] Starlink. (n.d.). *Availability*. https://www.starlink.com/map

[66] International Telecommunication Union [ITU]. (2022). *Global Connectivity Report 2022*. https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/

[67] Ibid.

2.2. National priorities and elements of foreign policy

Across Africa, efforts are underway to **advance the deployment of digital infrastructures** that support meaningful internet connectivity. As A4AI explains, meaningful connectivity is about more than the mere availability of networks; it encompasses the ability to use the internet every day on an appropriate device with enough data and a fast connection.[68]

Countries are outlining goals and objectives related to expanding and strengthening their internet infrastructures in various policy documents. Out of the eight focus countries, seven have adopted national broadband strategies, policies, or plans.

Some of these documents include outward-looking elements, in particular when it comes to **identifying funding sources for financing broadband projects**. **Kenya**'s *National Broadband Strategy* refers to attracting an international investor to build a national backbone infrastructure and lists the World Bank, the Africa Development Bank, ITU, and the African Telecommunication Union (ATU) as potential international development partners that could contribute to financing infrastructure programmes.[69]

In **Nigeria**, the *National Broadband Plan* talks about accessing international funding sources 'where available' to support initiatives such as the creation of new landing points for international submarine cables.[70] **Senegal**'s *National Broadband Plan* identifies the World Bank, the French Development Agency, and the Asian Development Bank as potential funding sources for broadband deployment projects.[71]

The reliance on external sources (be they public or private) for funding digital infrastructure projects is a reality across most of Africa. This comes with a series of challenges related, for instance, to the availability of such funding and to the ability of countries to attract it. Strengthening capacities within public institutions to attract funding (e.g. capacities to prepare robust project proposals and to improve the implementation of such projects), putting in place business-friendly policies to attract private investors, and the coordination of policies and initiatives at the regional level (e.g. to identify investment priorities and reach out to donors/investors) could help countries address some of the challenges.[72]

When it comes to infrastructures for mobile communications, some national policies note the importance of promoting **coordination on radio frequency matters** and **harmonised usage of the spectrum at the regional and international levels**. To this end, ensuring that national frequency plans are in line with decisions taken at ITU World Radiocommunication Conference is specifically mentioned by **South Africa**, **Namibia**, and **Kenya**, which implies goals of participation in relevant ITU work.

Other policies outline the (potential) **contribution of broadband infrastructures to increasing the countries' competitiveness in international markets**. *South Africa Connect,* the country's broadband policy, notes that the goals and actions outlined in the document create 'a context

---

68 A4AI. (n.d.). *Meaningful connectivity – unlocking the full power of internet access*. https://a4ai.org/meaningful-connectivity/

69 Republic of Kenya. (2018). *National Broadband Strategy 2018–2023.* https://www.ict.go.ke/wp-content/uploads/2019/05/National-Broadband-Strategy-2023-FINAL.pdf

70 National Broadband Committee, Nigeria. (2020). *Nigerian National Broadband Plan 2020–2025*. https://www.ncc.gov.ng/documents/880-nigerian-national-broadband-plan-2020-2025/file

71 Ministry of Communications, Telecommunications, Post and Digital Economy, Republic of Senegal. (2018). *Plan National Haut Débit du Sénégal (National Broadband Plan).* http://www.numerique.gouv.sn/sites/default/files/Senegal_Plan_National_Haut_Debit_30062018.pdf

72 OECD Development Centre. (2021). *Improving public finance, boosting infrastructure. Three priority actions for Africa's sustainable development after COVID-19.* https://www.oecd.org/dev/africa/Financing-Summit-for-Africa_Background-paper.pdf

for the development of globally competitive niche ICT-related manufacturing industries' in **South Africa**.[73]

According to **Ghana**'s *Broadband Policy and Implementation Strategy*, broadband is 'a critical prerequisite to support innovators and entrepreneurs to re-assert their productive and market capabilities in the local and global IT sector'.[74] **Namibia**'s *Broadband Policy* notes that supporting the deployment of broadband will 'booth Namibia to increase [its] global competitive ranking',[75] while **Rwanda**'s *Broadband Policy* simply states that ubiquitous broadband networks can be viewed as a foundation for global competitiveness.[76]

(Strengthened) participation in international organisations is envisioned in 5G policies, which are emerging across Africa. **Kenya**'s in-the-making 5G strategy[77] notes the country's commitment to 'participate in international forums to contribute to the development of 5G technology and standards'. In **South Africa**, a multistakeholder 5G Forum was established by the Independent Communications Authority of South Africa (ICASA) in 2017 to, among other tasks, assist the authority in preparing contributions to ITU and other relevant standards bodies on 5G-related matters.[78] A report issued in 2021 by ICASA's 5G Council Committee recommends that the Forum strengthens its engagement with international bodies and 'countries that have moved further along the 5G road than South Africa'.[79] **Nigeria**'s *National Policy on 5G Networks* notes that the government will contribute to global processes focused on the development of 5G standards and will enable and encourage the participation of relevant stakeholders in ITU meetings and events, as well as in the development of national positions for such events.[80]

The **adoption and enforcement of international technical standards** (such as those adopted at ITU) appear as an action item across multiple policy documents. For **Kenya**, **South Africa, Ghana**, and **Namibia**, this is seen as essential for the development of high-quality, advanced, and reliable ICT products and services.

Namibia also wants its telecom service providers to ensure that the broadband systems they develop comply with international standards (*National Broadband Policy*).

Rwanda's broadband policy mandates the national ICT authority to issue guidelines that are based on international standards.

Kenya specifically intends to promote the development and use of open internet standards and to encourage adherence to globally accepted standards in innovation and the design of devices or software (*National Broadband Strategy*). In addition, its draft 5G strategy notes the importance of adopting international standards developed by ITU and 3GPP as a way to ensure the interoperability and security of mobile systems. Through the Communications Authority, Kenya also intends to continue its participation in regional and global forums 'to coordinate and harmonise technology standards'.

---

73 Department of Communications, South Africa. (2013). *South Africa Connect: Creating opportunities, ensuring inclusion. South Africa's Broadband Policy.* https://www.ellipsis.co.za/wp-content/uploads/2013/10/NBP-2013.pdf

74 Ministry of Communications, Republic of Ghana. (2012). *National Broadband Policy and Implementation Strategy.* https://moc.gov.gh/sites/default/files/downloads/GhanaBroadbandStrategyFinal.pdf

75 Ministry of Information and Communication Technology, Namibia. (2020). *National Broadband Policy.* https://gazettes.africa/archive/na/2020/na-government-gazette-dated-2020-08-14-no-7308.pdf

76 Republic of Rwanda. (2013). *National Broadband Policy for Rwanda.* https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/National_Broadband_Policy.pdf

77 The document was launched for public consultation in late 2021. At the date of writing this study, it is unclear whether the strategy has been formally approved. Communications Authority of Kenya. (2021). *Public Consultation on the Roadmap and Strategy for 5th Generation Mobile Communications in Kenya.* https://www.ca.go.ke/wp-content/uploads/2021/10/Public-Consultation-Paper-on-5G-Roadmap.pdf

78 Independent Communications Authority of South Africa. (2017). *Terms of Reference for the South Africans 5G Forum*. https://www.ellipsis.co.za/wp-content/uploads/2017/10/Terms-of-Reference-of-the-5G-Forum-08092016.pdf

79 Independent Communications Authority of South Africa's 5G Council Committee. (2021). *The state of 5G in South Africa. From readiness to recommendations*. https://www.icasa.org.za/uploads/files/ICASA-2021-5G-Annual-Report.pdf

80 Federal Executive Council, Nigeria. (2021). *National Policy on Fifth Generation (5G) Networks for Nigeria's Digital Economy.* https://www.ncc.gov.ng/accessible/documents/1019-national-policy-on-5g-networks-for-nigeria-s-digital-economy/file

Nigeria too wants to ensure that its 5G ecosystem embeds globally accepted standards and specifications. One objective of the government is to contribute to ITU and other global processes supporting the development of 5G standards and to leverage the expertise of the private sector to develop country positions for these processes. Encouraging the participation of 'relevant stakeholders' in ITU work is also specifically mentioned in the 5G policy.

Senegal's digital strategy outlines goals related to enhancing the country's participation in regional and international telecom and ICT forums that deal with standardisation issues, as well as with broader issues of digital governance.

When it comes to the **management of critical internet resources – particularly domain names and IP addresses** – African countries tend to be actively engaged in relevant regional and international processes such as ICANN and AFRINIC (see more in the sub-section 2.4. on international engagement), even if the national policies we have reviewed do not contain specific references to engagement in such processes. **Nigeria** may be an exception, as the country's broadband plan includes a goal of improving the global visibility of the .ng ccTLD.

Critical internet resources in Africa

In 2011, ICANN launched the so-called New gTLD Programme, opening up the domain name space for the registration of **new generic top-level domains** (gTLDs), beyond the 21 in existence at that point. From the total of 1,930 gTLD applications, only 17 came from Africa (the continent with the lowest number of submissions).[81] Among the 1,241 gTLDs delegated to the root zone up to September 2022, only one is managed by an entity based in Africa: **.africa**, sponsored by the ZA Central Registry.

African countries have their own **ccTLDs** (e.g. .ke for Kenya and .za for South Africa); some 40% of them are managed by national regulatory agencies.[82]

When it comes to the uptake of internet protocol version 6 (**IPv6**), Africa as a whole lags behind other regions, although some countries do better than others. Gabon, for instance, had a 28.3% IPv6 adoption rate in October 2022 (ranking 37th in an Akamai index of countries by the percentage of IPv6 connections from the country), **Kenya** was at 3.7% (102nd place), and **Senegal** at 0.2% (185th place).[83]

In March 2022, ICANN announced plans to install and manage two **ICANN Managed Root Server (IMRS) clusters** in Africa, one of them in **Kenya** (the second yet to be determined). IMRS is one of the 13 root server instances in the world (a root server performs key functions related to translating domain names into IP addresses, helping identify a website's IP address when someone looks for a domain name). IMRS itself has over 195 instances in 85 countries/territories.[84] The new IMRS clusters in Africa are expected to stimulate internet access and strengthen internet stability within the region. First, they will contribute to ensuring that DNS queries from Africa are answered within the region, thus reducing latency (i.e. the time for a website to load) and improving user experience. Second, they will reduce the risk of the internet going down in the eventuality of a massive cyberattack.[85]

81 Internet Corporation for Assigned Names and Numbers [ICANN]. (n.d.). *New generic top-level domains programme statistics*. https://newgtlds.icann.org/en/program-status/statistics

82 Internet Corporation for Assigned Names and Numbers [ICANN]. (2016). *The 2016 African Domain Name Market Study.* https://www.icann.org/en/system/files/files/africa-dns-market-study-final-06jun17-en.pdf

83 Akamai. (2022). *IPv6 adoption by country.* https://www.akamai.com/internet-station/cyber-attacks/state-of-the-internet-report/ipv6-adoption-visualization

84 Internet Corporation for Assigned Names and Numbers [ICANN]. (n.d.). *FAQ - ICANN Managed Root Server (IMRS).* https://www.icann.org/en/system/files/files/imrs-faq-28feb22-en.pdf

85 Internet Corporation for Assigned Names and Numbers [ICANN]. (2022). *ICANN-Managed Root Server clusters to strengthen Africa's internet infrastructure*. Press release, 28 February. https://www.icann.org/resources/press-material/release-2022-02-28-en

2.3. Continental and regional overview

At the continental level, one of the *Agenda 2063*'s goals is to connect Africa through world-class infrastructure. This includes financing and implementing major ICT infrastructure projects so that Africa is 'on equal footing with the rest of the world as an information society, an integrated e-economy where every government, business, and citizen has access to reliable and affordable ICT services'.[86]

Digital infrastructure is also one of the pillars of the AU's *Digital Transformation Strategy*, which outlines priorities and goals related, among other issues, to closing the digital infrastructure gap, achieving accessible, affordable, and secure broadband, and establishing and improving digital networks.

While many of the policy recommendations and actions proposed in the strategy relate to measures that governments should be taking at the national level, there are also references to international engagement and goals the region should be pursuing in its international relations.

For instance, one of the proposed actions is to **attract major equipment manufacturers** to install factories across the continent, as a way to 'generate added value in Africa and ensure the long-term viability of telecommunications infrastructures, which are still very precarious, given the lack of a balanced financing plan for their maintenance, development, and renewal'. AU countries are also called to **'work with international institutions, including the ITU,** to adopt rules on the evolution of technologies, and more particularly the standards on equipment to guarantee the technological interoperability of one generation of equipment to another'. **Working with international partners on boosting investment** in telecom infrastructure is also envisioned.[87]

[86] African Union [AU]. (n.d.). *Flagship projects of Agenda 2063*. https://au.int/en/agenda2063/flagship-projects

[87] African Union [AU]. (2020). *The Digital Transformation Strategy for Africa*. https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

Continental and regional infrastructure projects and programmes

Multiple projects and programmes are underway across Africa focused on the deployment/enhancement of infrastructure or the strengthening of related regulatory frameworks. These are some of them:

- **AU: Programme for Infrastructure Development in Africa (PIDA)**. Adopted by AU heads of states and government in 2012 as a reference programme for regional and continental infrastructure development in Africa, PIDA includes, among other elements, ICT projects that aim to strengthen digital connectivity across the continent.
- **SADC: Regional Infrastructure Development Master Plan**. To be implemented by 2027, the plan aims to improve the coverage, reliability, and security of ICT infrastructure and to strengthen the ICT policy and regulatory frameworks to make more efficient use of existing infrastructure (among other goals).
- **East African Community (EAC): EAC Broadband ICT Infrastructure Network.** The goal is to establish a cross-border broadband infrastructure network within the EAC.[88]
- **Intergovernmental Authority on Development (IGAD): Regional Infrastructure Master Plan (IRIMP)**. The plan is expected to help accelerate the region's growth and structural economic transformation. Narrowing digital divides is one of the envisioned goals.[89]
- **Common Market for Eastern and Southern Africa (COMESA): Master Plan 2021–2025**. Dedicated to advancing structural transformation and boosting overall economic development, the plan includes regional projects on terrestrial digital connectivity.[90]
- **ECOWAS: ICT Strategy 2018–2023.** One of the strategy's goals is to promote a harmonised and standardised ICT infrastructure across the region.
- **Arab Maghreb Union (UMA): Broadband Optical Fibre Telecommunication Network initiative**. Goals of this initiative include the deployment of broadband across the region and the harmonisation of regulatory frameworks.[91]
- **Smart Africa: Broadband Strategy Project**. A flagship project of Smart Africa, the initiative has as its final goal the development of a pan-African broadband strategy and a related action plan. (Smart Africa is an initiative bringing together 30 African countries, as well as various regional and international organisations and companies, to support the acceleration of sustainable development across the continent.)
- **AU: Policy and Regulatory Initiative for Digital Africa (PRIDA)**. A joint initiative of the AU, the EU, and ITU, the programme focuses on the creation of enabling regulatory frameworks to support, among other elements, the deployment of universally accessible and affordable broadband across the continent.

Across RECs, there are multiple policy initiatives and projects that cover matters related to digital infrastructure and standards; several of them contain elements of digital foreign policy. *SADC's Protocol on Transport, Communications and Meteorology* – which requires member states to develop harmonised telecom policies, infrastructure strategies, and technical standards – notes that states shall pursue their goals of achieving regional universal access to ICT infrastructure and services through **participating in regional and international telecommunications forums**. They will also promote international standards and **participate in the work of relevant international bodies** such as ITU and ISO. Moreover, member states agree to coordinate their positions on matters dealt with at all international telecommunications and other relevant forums.[92]

SADC's Development Plan for 2020–2030 has among its strategic objectives the establishment of quality, interconnected, integrated, and seamless infrastructure and networks. **Attracting**

88 EAC member states: Burundi, Democratic Republic of the Congo, Kenya, Rwanda, South Sudan, Uganda, and Tanzania.

89 IGAD member states: Djibouti, Eritrea, Ethiopia, Kenya, Somalia, South Sudan, Sudan, and Uganda.

90 COMESA member states: Burundi, Comoros, Democratic Republic of the Congo, Djibouti, Egypt, Eritrea, Eswatini, Ethiopia, Kenya, Libya, Madagascar, Malawi, Mauritius, Rwanda, Seychelles, Somalia, Sudan, Tunisia, Uganda, Zambia, Zimbabwe.

91 UMA member states: Algeria, Libya, Mauritania, Morocco, Tunisia.

92 Southern African Development Community [SADC]. (2006). *Protocol on Transport, Communications and Meteorology in the Southern African Development Community (SADC) Regio*n. https://www.sadc.int/files/7613/5292/8370/Protocol_on_Transport_Communications_and_Meteorology_1996.pdf

foreign investments in infrastructure and ensuring alignment between regional, tripartite, continental, and international agreements 'to ensure integrated approaches that optimise synergies for the development of infrastructure and services in the region' are among the plan's envisioned objectives.[93]

ECOWAS's Act on the management of radio frequency spectrum asks member states to coordinate spectrum use at regional and international levels, and to respect 'ITU international allocations' when managing radio frequencies. A regional committee is tasked with discussing matters of international relevance in the context of spectrum management.[94]

The fact that the importance of coordinating African positions to take in international processes is highlighted across these documents is encouraging. It signals that countries and the regional/continental organisations are acknowledging that speaking with one voice – as much as possible – at an international level offers them more chances to ensure that African interests are well represented and meaningfully considered. Actively encouraging such coordination and creating more opportunities for it to happen is a task that both RECs and the AU should pursue in a more consistent and sustained manner.

When it comes to standards, the African Organisation for Standardisation (ARSO) issued a *4th Industrial Revolution Standardization Strategy* in 2021 (in cooperation with the Institute of Electrical and Electronics Engineers – IEEE), with the overall goal of harnessing the potential of technical standards to implement the fourth industrial revolution across the continent. The strategy highlights the importance of **enhancing African representation in 'global standardisation and technology governance environments'** and calls for active participation of regional stakeholders in the definition and adoption of international standards; the taking of leadership positions within international standardisation organisations; and the establishment of partnerships with international standardisation organisations to support capacity building in the standardisation field for African countries.[95] The extent to which most of these recommendations could be put into practice very much depends on whether the national standardisation bodies have the capacity and resources not only to follow international standardisation work themselves, but also to coordinate national positions with domestic stakeholders, and to encourage such stakeholders to contribute themselves to international processes.

[93] Southern African Development Community [SADC]. (2020). *SADC Regional Indicative Strategic Development Plan 2020–2030*. https://www.sadc.int/files/4716/1434/6113/RISDP_2020-2030_F.pdf

[94] Economic Community of West African States [ECOWAS]. (2007). *Supplementary Act A/SA.5/01/07 on the management of the radio-frequency spectrum*. http://ecowas.akomantoso.com/_lang/fr/doc/_iri/akn/ecowas/statement/supplementaryAct/2007-01-19/A_SA.5_01_07/eng@/!main

[95] Institute of Electrical and Electronics Engineers [IEEE]/African Organisation for Standardisation [ARSO]. (2021). *Africa 4th Industrial Revolution Standardization Strategy (2021–2025).* https://www.arso-oran.org/wp-content/uploads/2021/12/IEEE_ARSO-Standardization-Strategy_FINAL.pdf

Promoting African interests through regional organisations

Besides the institutions covered (AU, RECs, ARSO), there are multiple other regional entities (of an intergovernmental, technical, or private sector nature) across Africa that work on issues related to digital infrastructure, standards, and critical internet resources. Many participate in various international organisations and processes (ITU, ICANN, IGF, etc.) and could thus be considered vectors of promoting African digital interests at the international level. Examples include:

- **African Electrotechnical Standardisation Commission (AFSEC)** – dedicated in particular to the harmonisation of electrotechnical standards across Africa.
- **Africa ICT Alliance (AfICTA)** – a private-sector-led association dedicated to promoting the ICT industry's contribution to economic growth and social development.
- **Africa Top Level Domain Organization (AfTLD)** – an association of African ccTLD managers.
- **African Network Information Centre (AFRINIC)** – the regional internet registry responsible for the distribution of internet number resources, such as IP addresses and autonomous system numbers, in Africa.
- **African Network Operators Group (AfNOG)** – an avenue for network operators to cooperate and exchange information.
- **African Telecommunications Union (ATU)** – facilitates cooperation between member states on telecommunications-related policies and strategies.
- Various **associations of telecom regulatory agencies**, such as the Communications Regulators' Association of Southern Africa (CRASA), the East African Communications Organisation (EACO), and the West Africa Telecommunications Regulators Assembly (WATRA).
- Local **Internet Society chapters**, often involved in projects and initiatives focused on supporting infrastructure deployment (in particular community networks).

2.4. International engagement

International Telecommunication Union

ITU membership and participation in Sectors

All African countries have participation at ITU. For 20 of them, this is done solely through specialised ministries (dealing with telecommunications/electronic communications, digitalisation, or ICT) and/or national agencies/authorities. For 34 countries, actors participating in ITU also include academic institutions, telecom operators (private or state-owned), internet services providers, and/or other private entities.

Among the eight focus countries, **South Africa** has the highest number of overall ITU members (11)[96] and is followed by **Cote d'Ivoire** (8), **Nigeria** (7), **Kenya** (6), **Ghana** (5), **Namibia**, **Rwanda**, and **Senegal** (3 each) (Figure 27). With the exception of Namibia, all other countries have at least one ITU member that is an academic institution, a national standards developing organisation (SDO), a telecom operator, an ISP, or other private entity (Figure 28). Namibia and Rwanda are the only two countries with no Sector members or associates involved in the work of ITU Sectors.[97]

[96] This is very low compared with the countries at the top of the ranking: USA (118) and China (86).

[97] ITU has three specialised Sectors: The Radiocommunication Sector (ITU-R) contributes to the global management of the radio frequency spectrum and satellite orbit resources and develops standards for radiocommunication systems; the Telecommunication Standardization Sector (ITU-T) develops international technical standards for ICTs; and the Development Sector (ITU-D) focuses on promoting access to telecommunications. In addition to member states, ITU Sectors are also open to participation from industry, academia, and NGOs, as well as regional and international organisations. These can join as Sector members – with the right to participate across all activities of the Sector, associates – which can participate in one study group, or academia.

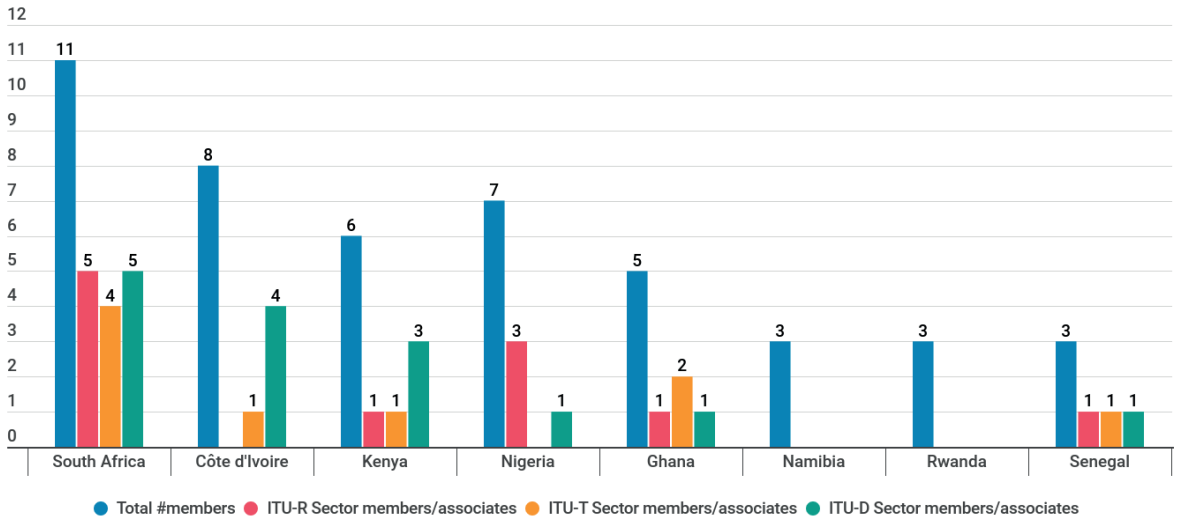


Figure 27. Number of ITU members by country (October 2022).

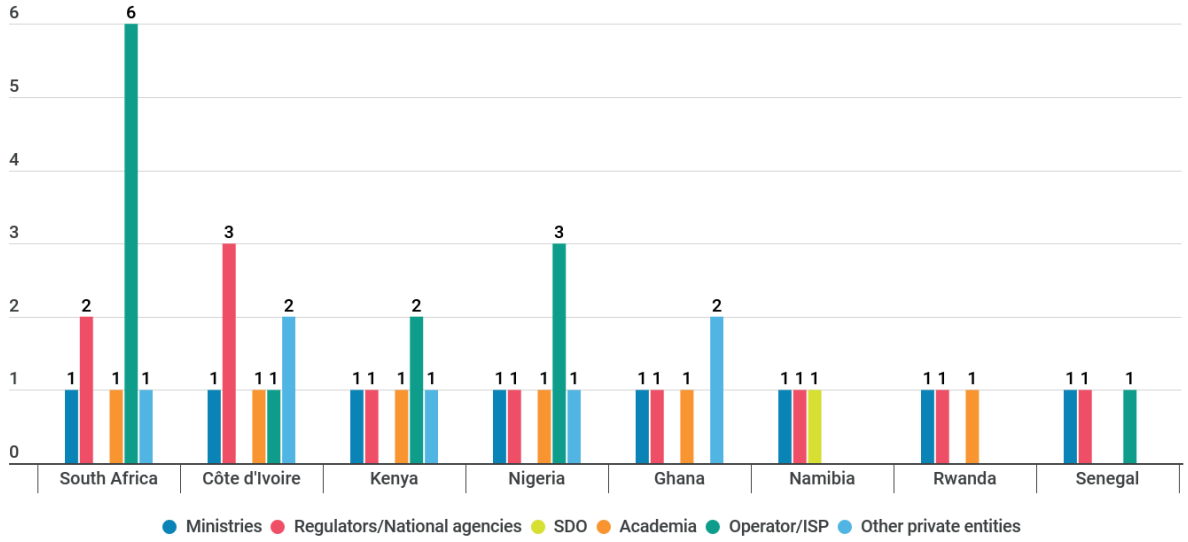


Figure 28. Type of ITU members by country (October 2022).

At ITU-T, standardisation work is carried out through study groups (SGs). Within the 11 SGs currently active, entities (in most cases ministries or regulators) from 11 African countries hold SG chair or vice-chair positions (Table 5). That these entities have put forward candidates for such positions reflects their interest in being involved in the development of international standards.

Table 5. Countries with entities holding leadership positions within ITU-T SGs (October 2022).

Country	SG	Entity holding SG leadership position
Algeria	SG13 – Future networks	[Vice-chair] Algerian Regulator of Post and Electronic Communication
	SG15 – Transport, access, and home	[Vice-chair] Algérie Télécom
	SG17 – Security	[Vice-chair] Algérie Télécom
	SG20 – IoT, smart cities, and communities	[Vice-chair] Ministry of Post and Telecommunications

Central African Republic	SG5 – Environment, EMF, and circular economy	[Vice-chair] Telecommunications Regulatory Agency
	SG9 – Broadband cable and TV	[Vice-chair] Ministry of Post, Telecommunications, and New Information and Communications Technologies
	SG15 – Transport, access, and home	[Vice-chair] Ministry of Post, Telecommunications, and New Information and Communications Technologies
	SG16 – Multimedia and digital technologies	[Vice-chair] Ministry of Post, Telecommunications, and New Information and Communications Technologies
Egypt	SG2 – Operational aspects	[Vice-chair] National Telecommunication Regulatory Authority
	SG3 – Economic and policy issues	[Chair] National Telecommunication Regulatory Authority
	SG5 – Environment, EMF, and circular economy	[Vice-chair] Ministry of Communications and Information Technology
	SG17 – Security	[Vice-chair] National Telecommunication Regulatory Authority
	SG20 – IoT, smart cities, and communities	[Vice-chair] National Telecommunication Regulatory Authority
Ghana	SG2 – Operational aspects	[Vice-chair] National Communications Authority
	SG3 – Economic and policy issues	[Vice-chair] National Communications Authority
	SG11 – Protocols, testing, and combating counterfeiting	[Vice-chair] National Communications Authority
	SG17 – Security	[Vice-chair] National Communications Authority
Nigeria	SG12 – Performance, QoS, and QoE	[Vice-chair] Nigerian Communications Commission
Rwanda	SG3 – Economic and policy issues	[Vice-chair] Rwanda Utilities Regulatory Authority
	SG12 – Performance, QoS, and QoE	[Vice-chair] Rwanda Utilities Regulatory Authority
	SG13 – Future networks	[Vice-chair] Rwanda Utilities Regulatory Authority
Senegal	SG3 – Economic and policy issues	[Vice-chair] Société Nationale des Télécommunications
	SG20 – IoT, smart cities, and communities	[Vice-chair] Ministry of Digital Economy and Telecommunications
Sudan	SG11 – Protocols, testing, and combating counterfeiting	[Vice-chair] Telecommunications and Post Regulatory Authority
	SG12 – Performance, QoS, and QoE	[Vice-chair] Telecommunication and Post Regulatory Authority

Tunisia	SG3 – Economic and policy issues	[Vice-chair] National Telecommunications Authority
	SG11 – Protocols, testing, and combating counterfeiting	[Vice-chair] Telecommunications Studies and Research Centre
	SG13 – Future networks	[Vice-chair] Tunisie Télécom
	SG16 – Multimedia and digital technologies	[Vice-chair] National Tunisian Broadcasting Office
	SG17 – Security	[Vice-chair] Ministry of Education
Tanzania	SG20 – IoT, smart cities, and communities	[Vice-chair] Tanzania Communications Regulatory Authority
Zambia	SG12 – Performance, QoS, and QoE	[Vice-chair] Zambia Information and Communication Technology Authority

At ITU-R, where there are 6 SGs focusing on radio communication matters (including, but not limited to standards), entities from 14 African countries hold vice-chair positions (Table 6).

Table 6. Countries with entities holding leadership positions within ITU-R SGs (October 2022).

Country	SG	Entity holding SG leadership position
Algeria	SG 4 – Satellite services	[Vice-chair] National Agency for Frequencies)
Burkina Faso	SG 4 – Satellite services	[Vice-chair] Regulatory Authority for Electronic Communications and Post
Côte d'Ivoire	SG 4 – Satellite services	[Vice-chair] Agency for Management of Radioelectric Frequencies
	SG 5 – Terrestrial services	[Vice-chair] Agency for Management of Radioelectric Frequencies
Egypt	SG 1 – Spectrum management	[Chair] National Telecommunication Regulatory Authority
	SG 5 – Terrestrial services	[Vice-chair] National Telecommunication Regulatory Authority
	SG 7 – Science services	[Vice-chair] National Telecommunication Regulatory Authority
Gabon	SG 7 – Science services	[Vice-chair] Ministry of Communications and Digital Economy
Ghana	SG 4 – Satellite services	[Vice-chair] National Communications Authority
Kenya	SG 1 – Spectrum management	[Vice-chair] Communications Authority
	SG 6 – Broadcasting service	[Vice-chair] Communications Authority
Mali	SG 1 – Spectrum management	[Vice-chair] Regulatory Authority for Telecommunications and Post

Morocco	SG 3 – Radiowave propagation	[Vice-chair] National Telecommunications Regulatory Agency
	SG 4 – Satellite services	[Vice-chair] National Telecommunications Regulatory Agency
	SG 5 – Terrestrial services	[Vice-chair] National Telecommunications Regulatory Agency
	SG 6 – Broadcasting service	[Vice-chair] National Telecommunications Regulatory Agency
	SG 7 – Science services	[Vice-chair] National Telecommunications Regulatory Agency
Nigeria	SG 6 – Broadcasting service	[Vice-chair] National Broadcasting Commission
	SG 7 – Science services	[Vice-chair] Nigerian Airspace Management Agency
Sudan	SG 5 – Terrestrial services	[Vice-chair] National Telecommunications Corporation
Tanzania	SG 6 – Broadcasting service	[Vice-chair] Communications Regulatory Authority
Togo	SG 3 – Radiowave propagation	[Vice-chair] Regulatory Authority for Post and Telecommunications
Tunisia	SG 5 – Terrestrial services	[Vice-chair] National Agency for Frequencies

ITU-D has only two SGs; entities from six African countries hold leadership positions within these groups (Table 7).

Table 7. Countries with entities holding leadership positions within ITU-D SGs (October 2022).

Country	SG	Entity holding SG leadership position
Côte d'Ivoire	SG 1 – Enabling environment for meaningful connectivity	[Chair] Regulatory Authority for Telecommunications
Egypt	SG 2 – ICT services and applications for the promotion of sustainable development	[Chair] National Telecommunication Regulatory Authority
Guinea	SG 2 – ICT services and applications for the promotion of sustainable development	[Vice-chair] National Regulatory Authority for Post and Telecommunications
Nigeria	SG 2 – ICT services and applications for the promotion of sustainable development	[Vice-chair] Nigerian Communications Commission
Togo	SG 1 – Enabling environment for meaningful connectivity	[Vice-chair] Regulatory Authority for Post and Telecommunications
Zimbabwe	SG1 – Enabling environment for meaningful connectivity	[Vice-chair] Postal and Telecommunications Regulatory Authority

Participation in the ITU Council

Besides participation in study groups, countries' interest in ITU work is also reflected by their **involvement in the ITU Council activities**. The Council acts as the Union's governing body in the interval between plenipotentiary conferences. For the period 2019–2022, the 13 seats on the Council allocated to the African region were held by Algeria, Burkina Faso, **Côte d'Ivoire**, Egypt, **Ghana**, **Kenya**, Morocco, **Nigeria**, **Rwanda**, **Senegal**, **South Africa**, Tunisia, and Uganda. Some of these countries also held leadership roles within ITU Council working groups and expert groups (Table 8). At the ITU Plenipotentiary Conference 2022 (PP-22), the following countries were elected

as Council members for the 2023–2026 period: Algeria, Egypt, **Ghana**, **Kenya**, Mauritius, Morocco, **Nigeria**, **Rwanda**, **Senegal**, **South Africa**, Tanzania, Tunisia, and Uganda.

Table 8. Countries' participation in the ITU Council and Council WGs and expert groups.

Country	Seat on Council (2019–2022)	Seat on Council (2023–2026)	Leadership roles within Council WGs and expert groups (2019–2022)[98]
Algeria	Yes	Yes	
Burkina Faso	Yes		
Côte d'Ivoire	Yes		[Vice-chair] Expert group on ITRs Regulatory Authority for Telecommunications/ICT
Egypt	Yes	Yes	[Vice-chair] Expert group on ITRs
			[Vice-chair] Expert group on Decision 482 National Telecommunication Regulatory Authority
Ghana	Yes	Yes	
Kenya	Yes	Yes	[Vice-chair] CWG for strategic and financial plans for 2024-2027 Communications Authority of Kenya
Mauritius		Yes	
Morocco	Yes	Yes	
Nigeria	Yes	Yes	[Vice-chair] CWG-Child online protection Nigeria Communications Commission
Rwanda	Yes	Yes	[Vice-chair] CWG-WSIS & SDGs Rwanda Utilities Regulatory Authority
Senegal	Yes	Yes	[Vice-chair] CWG on financial and human resources Regulatory Authority for Telecommunications and Post
South Africa	Yes	Yes	[Vice-chair] CWG-Internet Department of Communications and Digital Technologies
Tanzania		Yes	
Tunisia	Yes	Yes	[Chair] CWG on the use of the six official languages Ministry of Communications Technologies and Digital Economy
Uganda	Yes	Yes	
Zambia	No		[Chair] Expert group on ITRs Zambia Information and Communications Technology Authority

[98] At the date of writing this study, the leadership of Council WGs and expert groups for the 2023–2026 period had not been elected.

African contributions to ITU Plenipotentiary Conference 2022

In the context of ITU PP-22, African countries – through ATU – submitted 42 contributions, most of them being proposals for revising existing ITU resolutions or adopting new resolutions. Topics covered by such proposals range from AI to cybersecurity and from the use of ICTs to bridge the financial gap to outer space activities. For instance, a draft new resolution on AI suggested that ITU takes a more active role in AI-related issues through actions such as developing a toolkit to assist member states in establishing an AI ecosystem, as well as mechanisms to assist developing countries in mitigating AI-related risks. When it comes to the review of the International Telecommunication Regulations (ITRs) – an issue ITU member states have divergent opinions on – the view of African countries was that the ITRs should be completely revised, so as to harmonise their 1988 and 2012 versions and to keep them aligned with technological and market developments. In a draft new resolution on outer space, ATU members suggested that ITU should (a) foster international cooperation to ensure that the benefits of space are brought to everyone, and (b) engage in activities to strengthen the capacities of developing countries in space law.

International standards developing organisations

Digital standards are relevant not only from a technical point of view; they also have broader economic, social, and political implications. Standards support innovation and help develop and sustain competitiveness, thus being able to contribute to economic growth. They can also provide the context for promoting or abusing human rights. Moreover, standards can help achieve certain public policy objectives, such as protecting consumers' rights and promoting the safe development of technologies. More and more visible in recent years, standards also have geopolitical implications: Governments are increasingly aware that if a country's actors can influence standards in strategic industries, that country would likely obtain a significant advantage on the international stage.[99]

Given the borderless nature of the digital space, and the fact that digital standards are reflected in products and services used around the world, it is important that the development of standards integrates views and interests from as many stakeholders as possible.

In this section we look at African actors' participation in several key international SDOs (having already covered ITU-T): ISO, whose wide scope includes, among others, the development of standards for e-commerce, robotics, and security; IEC, which develops standards for electrical and electronic technologies; IETF, tasked with developing standards for the internet; the World Wide Web Consortium (W3C), dedicated to standards for the world wide web; and 3GPP, which focuses on standards for cellular (mobile) telecommunications technologies.

Forty-three African countries have **ISO membership** (be it full member, correspondent, or subscriber) through their national SDOs. Among them, **South Africa**, Egypt, and **Kenya** are involved in the largest number of technical committees (TCs), and only **South Africa** (11), **Kenya** (1), and Uganda (1) hold TC secretariat positions.[100]

Only 11 African countries have their national SDOs involved in the **IEC:** Algeria, Egypt, **Nigeria**, and **South Africa** as full members, and **Côte d'Ivoire**, Ethiopia, **Ghana**, **Kenya**, Morocco, Tunisia, and Uganda as associate members. Among them, only **South Africa** holds the secretariat position for one TC.

[99] Teleanu, S. (2021). *The geopolitics of digital standards: China's role in standard-setting organisations.* DiploFoundation. https://www.diplomacy.edu/resource/report-the-geopolitics-of-digital-standards-chinas-role-in-standard-setting-organisations/

[100] The statistics cover all ISO TCs, some of which are not necessarily working on standards related to digital technologies.

ISO and IEC have a **joint technical committee for information technology – JTC1**, which focuses on the development of standards related to issues such as cloud computing, biometrics, cybersecurity and privacy protection, internet of things and digital twins, and AI. Twenty-one African countries are engaged in at least one of the twenty-three JTC1 subcommittees (SCs), either as participating or observing members (Figure 29). In addition, Zimbabwe, Gabon, and Burundi participate as observers in the overall JTC1.

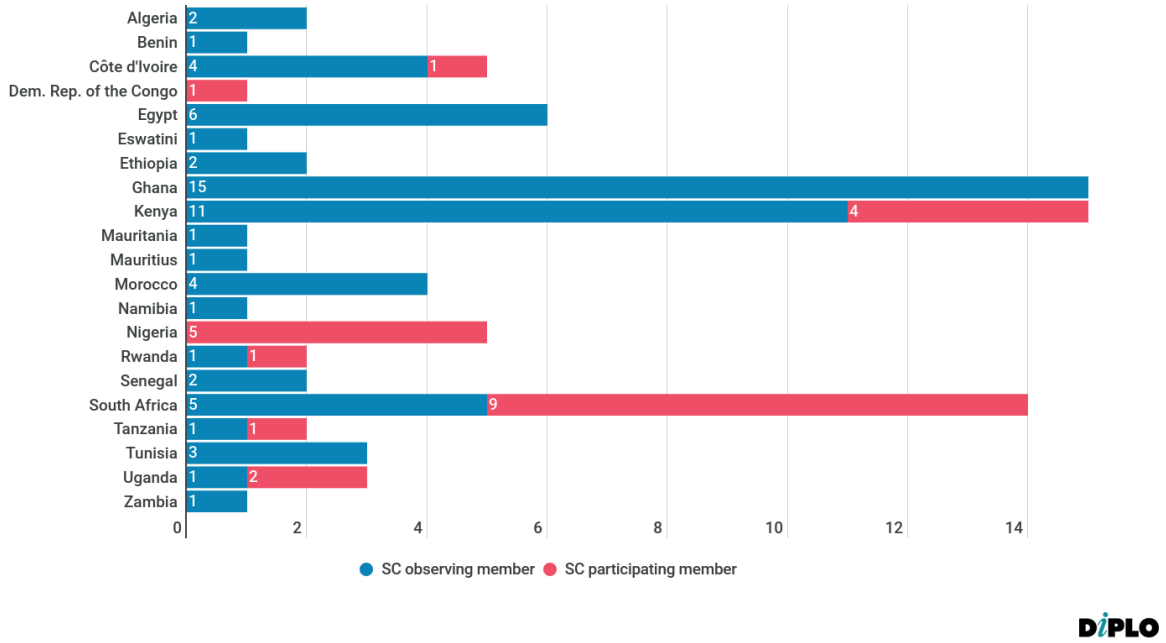


Figure 29. Countries with participation in JTC1 subcommittees (October 2022).

The **IETF** does not have a formal membership structure, and everyone interested is welcome to participate in the work. Data tracked by the organisation until 2021[101] shows that there have been very few individuals from African countries contributing to IETF work as document (draft/RFC) authors. Twelve countries are present in these statistics: Algeria (1 document author), Cameroon (1), Egypt (3), Gabon (1), Gambia (1), **Kenya** (2), Mauritius (4), Morocco (26), **Nigeria** (2), **South Africa** (9), Tunisia (1), and Uganda (3).

Historically, Africa is the continent with the least participation in IETF work (judging by the same metric). In 2000, for instance, there were 1,088 document authors from North America, 281 from Europe, 132 from Asia, 22 from Oceania, 4 from South America, and 3 from Africa. Twenty years later, in 2021, the number of authors from Africa remained the lowest (8), while recording significant shifts for the other continents: 567 from North America, 491 from Europe, 536 from Asia, 18 from South America, and 18 from Oceania.[102]

Botswana, Egypt, and **South Africa** are the only African countries with stakeholders involved in **3GPP**, the SDO responsible for, among other issues, the development of 5G-related standards. Botswana's Communications Regulatory Authority and South Africa's Telkom SA SOC Ltd are individual members of 3GPP, but via the European Telecommunications Standards Institute (ETSI), where they are both members (since participation in 3GPP is restricted to entities associated with 3GPP organisational partners,[103] and no African SDO has such a role). One Egypt-based entity – Open Valley – is a 3GPP guest.

[101] Internet Engineering Task Force [IETF]. (n.d.). *Draft/RFC statistics – Number of document authors per country.* https://datatracker.ietf.org/stats/document/author/country/

[102] Internet Engineering Task Force [IETF]. (n.d.). *Draft/RFC statistics – Number of document authors per continent.* https://datatracker.ietf.org/stats/document/yearly/continent/

[103] 3GPP's organisational partners are Japan's Association of Radio Industries and Businesses (ARIB) and Telecommunication Technology Committee (TTC), the US Alliance for Telecommunications Industry Solutions (ATIS), China Communications Standards Associations (CCSA), the European Telecommunications Standards Institute (ETSI), India's Telecommunications Standards Development Society (TSDS), and the Republic of Korea's Telecommunications Technology Association.

At the **W3C**, the only Africa-based members come from Morocco, Senegal, and South Africa. In the case of **South Africa**, it is a social media platform (Snake Nation) and a provider of identity and user identification services (Entersekt) that are W3C members, while the two members from **Senegal** and Morocco are academic institutions (École Supérieure Polytechnique de Dakar and École Mohammadia d'Ingénieurs Rabat).

The fact that there is little participation from African actors in international standardisation processes (besides ITU) could be explained by multiple factors, from limited awareness of the importance of being part of such processes, to lack of adequate resources (among governments, national standardisation bodies, technical and business communities) to support such participation. Faced with capacity constraints, some governmental entities also choose to engage through multilateral forums such as ITU, which they tend to be more comfortable with and to whom they confer legitimacy.

Internet Corporation for Assigned Names and Numbers

ICANN is the organisation responsible for coordinating the global internet's systems of unique identifiers and for ensuring their stable and secure operation. Its main responsibility is to coordinate the allocation of three sets of unique identifiers (or critical internet resources) – domain names, IP addresses and autonomous system numbers, and protocol port and parameter numbers – and to facilitate the coordination of the operation and evolution of the domain name system (DNS) root name server system.

Within ICANN's multistakeholder structure, the **GAC** is tasked with providing advice to the ICANN Board on matters pertaining to public policy. Forty-four African countries have representation on the GAC (Figure 30). The representation is typically ensured by ministries of ICT/digital economy or regulatory authorities. The AUC, the AU Development Agency (AUDA-NEPAD), the ATU, ECCAS, ECOWAS, NEPAD, and the West Africa Telecommunications Regulators Assembly also participate in GAC work as observers.

Figure 30. African countries with GAC membership (October 2022).

Besides governmental involvement in the GAC, there is also participation of other African stakeholders across other advisory committees and supporting organisations (Table 9). For instance, at the **ccNSO** – which brings together managers of ccTLDs to discuss issues of common interest and recommend policies for a limited set of ccTLD-related topics – there are 39 African

countries[104] participating through their ccTLD operators, including 7 of the focus countries: **Côte d'Ivoire, Kenya, Namibia, Nigeria, Rwanda, Senegal**, and **South Africa.**

The **GNSO** is the body in charge of developing policies for generic top-level domains (e.g. .com, .org) (which are eventually submitted to the ICANN Board for approval). Within the GNSO there are multiple stakeholder groups and constituencies representing the interests of various commercial and non-commercial stakeholders (be they organisations or individuals). A look at the membership of these groups and constituencies shows that there is some involvement from actors from at least 30 African countries,[105] including **Côte d'Ivoire, Ghana, Kenya, Nigeria, Rwanda, Senegal**, and **South Africa**.

Groups based in 31 African countries[106] – including **Côte d'Ivoire, Ghana, Kenya, Nigeria, Rwanda, Senegal**, and **South Africa** – are part of **ICANN's At-Large community,** which fosters the participation of individual internet users in ICANN policy development activities. These groups are known as At-Large Structures and are associated with the African Regional At-Large Organization (AFRALO). In addition to these structures, AFRALO also includes individual members from ten countries.[107]

The region's voice in the **Address Supporting Organization (ASO)**, which develops recommendations on internet protocol address policies (e.g. operation, assignments, management of IP addresses) is represented through AFRINIC. AFRINIC membership spans 54 African countries.

Table 9. Involvement of actors in the eight focus countries in selected ICANN advisory committees and supporting organisations (October 2022).

Country	GAC	GNSO[108]	ccNSO	At-Large Community	ASO/
Côte d'Ivoire	**Yes** Digital Economy Ministry & ICT Regulatory Authority	**Yes** – 2 companies within the Commercial Stakeholder Group (CSG) – 3 organisations (orgs) and 3 individuals within the Non-Commercial Stakeholder Group (NCSG)	**AFRINIC**	**Yes** – 5 orgs – 1 individual member	**Yes** 23 AFRINIC members
Ghana	**Yes** Ministry of Communications	**Yes** – 1 company and 1 ISP within the CSG – 8 orgs and 14 individual members within the NCSG		**Yes** 3 orgs	**Yes** 96 AFRINIC members

[104] The countries whose ccTLD operators participate in ccNSO work are Algeria, Benin, Botswana, Burkina Faso, Burundi, Cabo Verde, Cameroon, Chad, Comoros, Republic of the Congo, Côte d'Ivoire, Djibouti, Democratic Republic of the Congo, Egypt, Ethiopia, Gabon, Guinea-Bissau, Kenya, Lesotho, Libya, Madagascar, Malawi, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Nigeria, Rwanda, Senegal, Seychelles, Somalia, South Africa, Sudan, Tanzania, Tunisia, Uganda, Zambia, Zimbabwe.

[105] These are Algeria, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Chad, Republic of the Congo, Côte d'Ivoire, Democratic Republic of the Congo, Egypt, Ethiopia, Gambia, Ghana, Kenya, Liberia, Malawi, Mauritius, Morocco, Mozambique, Nigeria, Rwanda, Senegal, South Africa, Sudan, Togo, Tunisia, Uganda, Zambia, Zimbabwe.

[106] Groups based in the following countries participate in ICANN's At-Large community: Benin, Burkina Faso, Burundi, Cameroon, Chad, Comoros, Côte d'Ivoire, Democratic Republic of the Congo, Egypt, Gambia, Ghana, Kenya, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Nigeria, Rwanda, Senegal, Somalia, South Africa, Sudan, Tanzania, Togo, Tunisia, Uganda, Zimbabwe.

[107] These are Chad, Côte d'Ivoire, Egypt, Gabon, Guinea, Kenya, Nigeria, South Africa, Togo, and Tunisia.

[108] The statistics are based on information about membership collected from across GNSO groups and constituencies. The membership of one constituency – the Intellectual Property Constituency – is not included, as publicly available information on membership does not offer details about the members' countries.

Kenya	**Yes** Communications Authority	**Yes** – 1 company and 1 ISP within the CSG – 2 orgs and 13 individual members within the NCSG	**Yes**	**Yes** – 2 orgs – 2 individual members	**Yes** 150 AFRINIC members
Namibia	**Yes** Ministry of Information and Communication Technology		**Yes**		**Yes** 17 AFRINIC members
Nigeria	**Yes** Ministry of Communication Technology & Nigeria Communications Commission & National Information Technology Development Agency	**Yes** – 5 companies within the CSG – 1 registrar within the Registrars Stakeholder Group – 11 orgs and 15 individual members within the NCSG	**Yes**	**Yes** – 10 orgs – 5 individual members	**Yes** 235 AFRINIC members
Rwanda	**Yes** Rwanda Utilities Regulatory Authority	**Yes** – 1 individual member within the NCSG	**Yes**	**Yes** 1 org	**Yes** 17 AFRINIC members
Senegal	**Yes** Ministry of Digital Economy and Telecommunications & Telecommunications and Post Regulatory Authority	**Yes** – 1 org and 1 individual member within the NCSG	**Yes**	**Yes** 4 orgs	**Yes** 12 AFRINIC members
South Africa	**Yes** Department of Communications and Digital Technologies	**Yes** – 2 ISPs within the CSG – 2 registrars within the Registrars Stakeholder Group – 1 registry within the Registries Stakeholder Group – 5 orgs and 18 individual members within the NCSG	**Yes**	**Yes** – 1 org – 2 individual members	**Yes** 656 AFRINIC members

3. Human rights

Section summary

Across Africa, the growing uptake of digital technologies has led to calls for adequate legal frameworks to ensure the protection of privacy and personal data. Governments have accelerated the adoption of data protection laws, but differences between such laws create a complex and unharmonised framework (and the low adoption rate of the *Malabo Convention* further complicates issues). Coupled with law enforcement challenges, this puts countries at risk of exporting data outside of the continent without necessary protections. The Network of African Data Protection Authorities is working on supporting countries in preparing and updating data protection legislation.

The challenges the continent faces when it comes to human rights in the digital space are not only related to (the development of) legal frameworks. Reports indicate that over the past five years citizens in almost half of African countries have experienced some forms of internet restrictions (e.g. social media shutdowns, content throttling measures, or complete internet blackouts). In 2019, the ACHPR called on countries to refrain from measures involving removing, blocking, or filtering content, unless they are in compliance with international human rights law.

Civil society groups are particularly active on matters related to digital rights, as demonstrated by their leadership in the development of the *African Declaration on Internet Rights and Freedoms*. Many of them are also actively contributing to various international processes and initiatives such as the IGF and the HRC.

In recent years, some African countries have been involved in the submission of, and discussions on HRC resolutions covering digital-related topics. For instance, Botswana, Mali, South Africa, and Tunisia sponsored the 2021 *Resolution on the right to privacy in the digital age*, while Nigeria and Tunisia were among the initial sponsors of the 2021 *Resolution on the promotion, protection and enjoyment of human rights on the internet*. Overall HRC discussions on digital and human rights saw contributions from countries such as Egypt, Ghana, Namibia, Nigeria, South Africa, and Tunisia.

3.1. National overview

Laws and policies: Focus on privacy and data protection

Accelerated digital transformation processes and increasing cross-border trade within and beyond the African continent call for strengthened and harmonised legal frameworks to ensure adequate **protection of data and privacy**. Civil society organisations, for example, are concerned that a lack of such frameworks encourages extensive data mining and extraction of data for business without consideration for the human rights impacts.

Some governments share similar concerns: In its *National Digital Master Plan*, **Kenya** notes that one data-protection-related concern in need to be addressed is the mining of data by 'specific multinationals'.

Over the last few years, the drafting and coming into effect of data protection laws has been accelerated across Africa (Figure 31). A few examples include:

- **Algeria:** *Law on the Protection of Natural Persons in the Processing of Personal Data, 2018*
- **Egypt:** *Personal Data Protection Law, 2020*
- **Kenya**: *Data Protection Act*, 2019
- **Namibia**: Working on a draft for 2022
- **Nigeria**: *Nigerian Data Protection Regulation*, 2019
- **Rwanda**: *Law No. 058/2021 Relating to the Protection of Personal Data and Privacy*, 2021
- **South Africa**: *Protection of Personal Information Act*, 2013

Data protection laws in **Kenya**, **Rwanda**, and **South Africa** share some of the elements of the European Union's General Data Protection Regulation (GDPR). In particular, they adopt the extraterritorial approach. This means that entities outside of the country that handle citizens' data are subject to the law. Data protection frameworks of Benin, Cabo Verde, and Uganda also have extraterritorial provisions, and this appears to be the case for Egypt too.[109] It is also noteworthy that Kenya, Rwanda, and Zambia are among the countries with certain data localisation requirements.[110]

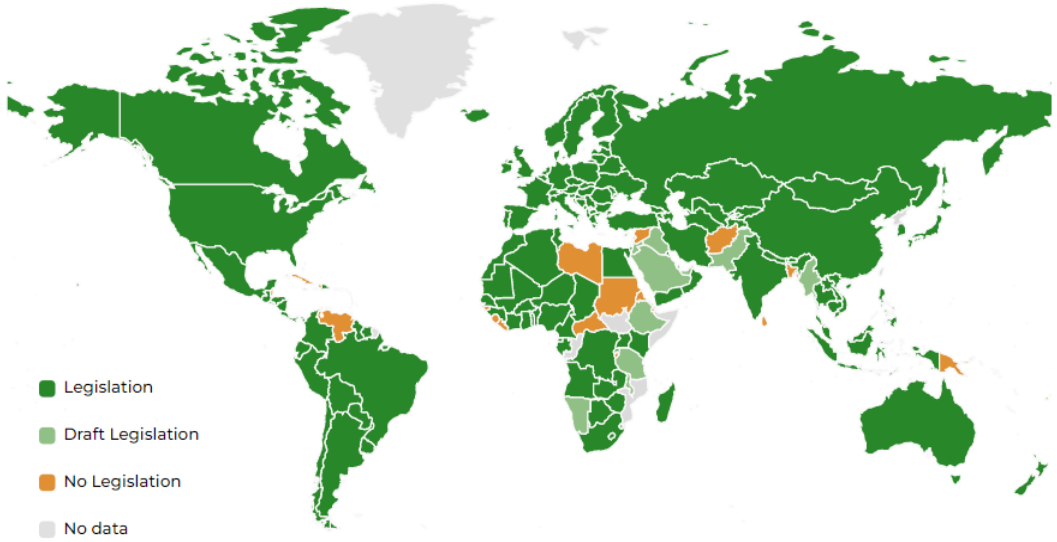


Figure 31. Data protection and privacy legislation (December 2021).[111]

[109] Rich, C. J. (2022, January 11). *Africa and the Near East: The region's privacy landscape facing rapid and dramatic changes.* Morrison and Foerster. https://www.mofo.com/resources/insights/220131-africa-and-the-near-east.html

[110] Ibid.

[111] Based on United Nations Conference on Trade and Development [UNCTAD]. (2021). *Data protection and privacy legisla-*

Despite these significant and fast-paced developments, some challenges remain. While more African countries are adopting data protection laws, enforcement of the law is a substantial task for the years to come. Where laws exist, there are sometimes significant differences in rules, and so far, only some provisions for mutual recognition of data laws. In addition, there is still no harmonised mechanism being consistently implemented to support human-rights-centric cross-border data flows, an issue that puts African states at risk of exporting their data outside the continent without necessary protections. **Kenya** acknowledges, for instance, that there are issues with data-sharing agreements concluded with countries: 'There is a provision for the data being processed, but no enforcement mechanism to ensure that data meant to remain local remains local' (*Digital Master Plan*). The AU Data Policy Framework (covered further in sub-section 5.2.) might help address some of these harmonisation challenges and empower countries to benefit from data-driven economies while ensuring adequate levels of data protection.

One illustrative example of harmonisation challenges relates to the low rate of adoption of the *Malabo Convention* (see Figure 38 in sub-section 4.2). Some countries acknowledge the shortcoming: **Nigeria**, for example, notes the importance of adopting the convention in its *National Digital Economy Policy and Strategy*.

Objectives related to the protection of human rights appear sporadically in some digital-related policies and strategies adopted at national level by some of the eight focus countries. **Kenya**'s *Digital Master Plan* has data protection (and cybersecurity management) as one of its cross-cutting themes. In addition to including several mentions of privacy (e.g. enacting effective legislation on privacy), the *National ICT Policy* notes that 'the government will seek to promote the right of the use of social media as an extension of the protection of freedom of expression'. It also highlights a series of commitments the government is making with a view to ensuring that persons with disabilities can benefit from digital products and services.

Nigeria's *Digital Economy Policy and Strategy* acknowledges the need to strengthen the regulatory instruments that govern data protection and privacy. **South Africa**'s *ICT and Digital Economy Master Plan* tackles briefly the need to ensure privacy and data protection/security in the context of the digital economy. **Namibia**'s *Overarching ICT Policy* notes that to ensure a proper regulation for the 'interface between technology and rights to privacy', the collection and protection of data will comply with international standards.

Cote d'Ivoire highlights, in its *National Digital Development Strategy*, the need to strengthen the implementation of national legislation on data protection and the plan to develop a strategy on data protection aimed at contributing to a safer cyberspace. The strategy also notes that the country has very little participation in international processes dealing with matters of personal data protection. **Senegal**'s *Digital Senegal Strategy* outlines as a priority the updating of legal frameworks on various digital issues, data protection being one of them.

State of internet freedoms

Beyond issues related to developing and implementing privacy and data protection legislation, there are also challenges across the continent when it comes to broader **internet/digital freedoms**. This is illustrated by Freedom House's *Freedom on the Net* report, which assesses the level of internet freedom by focusing on obstacles to internet access, limits on content (e.g. filtering, blocking, other forms of censorship), and violations of user rights (e.g. legal protections and restrictions on freedom of expression; surveillance and privacy; repercussions for online speech and activities).

For 2022, the report covered 17 African countries; among these, **South Africa** is the only one ranked as free. Partially free are **Kenya**, **Ghana**, Tunisia, Angola, Malawi, **Nigeria**, Zambia, Gambia, Morocco, Uganda, Libya, and Zimbabwe. **Rwanda**, Sudan, Ethiopia, and Egypt are ranked as not

tion worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Figure redrawn.

free (Figure 32).[112] Looking at the change in the internet freedom score from 2021 to 2022, we see an improvement for Egypt, Uganda, **Kenya**, and Zimbabwe, but a decline for several other countries such as **Nigeria**, **Rwanda**, and Sudan.[113]

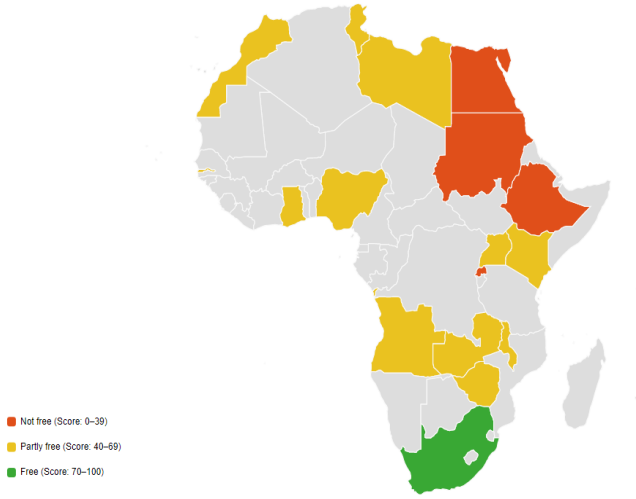


Figure 32. Internet freedom status in Africa.[114]

Consistent with Freedom House's findings, a Quartz report published in May 2022 indicates that between 2017 and 2022, citizens in almost half of African countries experienced some form of government-imposed internet restrictions (Figure 33).[115] Such restrictions come with economic implications. To illustrate, data collected by Top10VPN indicates that, in 2021 alone, internet shutdowns[116] across 11 African countries affected 171 million users and amounted to an overall cost of US$1.93 billion.[117]

Figure 33. African countries that have experienced forms of internet shutdowns between 2017 and 2022.[118]

[112] Freedom House. (2022). *Freedom on the Net 2022*. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

[113] Freedom House. (2022). *Change in internet freedom score*. https://freedomhouse.org/explore-the-map?type=fotn&year=2022&mapview=trend

[114] Based on Freedom House. (2022). *Internet freedom status*. https://freedomhouse.org/explore-the-map?type=fotn&year=2022. Figure redrawn.

[115] Ngila, F. (2022, May 13). *These are the African countries that censor the internet the most*. Quartz Africa. https://qz.com/africa/2165371/these-are-the-african-countries-that-censor-internet-the-most/

[116] Internet restrictions/shutdowns accounted for in the cited reports include complete internet blackouts, social media shutdowns, and severe throttling measures (e.g. speeds are reduced to the extent that they only allow SMS and voice calls only).

[117] Woodhams, S. & Migliano, S. (2022, January 4). *Government internet shutdowns cost $5.5 billion in 2021.* Top10VPN. https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/

[118] Based on Ngila, F. (2022, May 13). *These are the African countries that censor the internet the most.* Quartz Africa. https://

Using digital tech for surveillance

The capabilities of states to use digital technology for surveillance are increasing. The AI Global Surveillance (AIGS) Index, produced in 2019 by the Carnegie Endowment for International Peace[119] and updated in 2022,[120] gives an overview of the use of AI and big data surveillance tools (including smart city sensors, facial recognition, and smart policing) by state authorities in 179 countries around the world.

Eighteen African countries are included in the 2022 AIGS Index: Algeria, Angola, Botswana, Cameroon, **Côte d'Ivoire**, Egypt, **Ghana**, **Kenya**, Madagascar, Mauritius, Morocco, **Namibia**, **Nigeria**, **South Africa**, Tunisia, Uganda, Zambia, and Zimbabwe. The Index cannot differentiate between legitimate and illegitimate use of AI tools for surveillance by the state. So, the fact that these countries are listed on the AIGS Index does not indicate illegitimate use. Rather, as the author stresses, it shows 'how new surveillance capabilities are transforming the ability of governments to monitor and track individuals or groups'.[121]

The AIGS Index distinguishes between technology supplied by companies in China, the USA, and other countries. With the exception of Namibia (where a local company is used), the technology is supplied by Chinese companies only (in 14 countries) or Chinese and US/UK companies (in 3 countries).

3.2. Continental and regional overview

Besides the *Malabo Convention* (covered further in sub-section 4.2.), there are several other continental and regional frameworks and initiatives that cover issues related to the protection of human rights in the digital space.

A **Network of African Data Protection Authorities (NADPA)** – established in 2016 – brings together privacy and data protection authorities from 19 countries[122] to facilitate cooperation and the sharing of experience, support states in preparing legislation on privacy and data protection and establishing data protection agencies (DPAs), and promote the adoption and implementation of relevant African legal instruments.[123] The network is also cooperating with African and international bodies and associations (e.g. the Global Privacy Assembly and the Global Privacy Enforcement Network). In March 2022, the network signed a memorandum of understanding with the Smart Africa Alliance to work together on issues such as supporting the enforcement of data protection regulations, encouraging the creation of a harmonised framework for data protection policies and regulations across Africa, and supporting countries in preparing or updating legislation and establishing DPAs.[124]

Over the years, the **ACHPR** has developed several instruments and resources covering issues related to the protection of human rights and freedoms in the digital space. A *Resolution on the right to freedom of information and expression on the internet* (adopted in 2016) calls on countries to

qz.com/africa/2165371/these-are-the-african-countries-that-censor-internet-the-most/. Figure redrawn.

119 Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

120 Feldstein, S. (2022). *AI & Big Data Global Surveillance Index (2022 updated)*. Carnegie Endowment for International Peace. https://data.mendeley.com/datasets/gjhf5y4xjp/4

121 Ibid.

122 As of October 2022, NADPA membership includes DPAs from Angola, Benin, Burkina Faso, Cabo Verde, Chad, Côte d'Ivoire, Gabon, Ghana, Kenya, Mali, Mauritius, Morocco, Niger, Nigeria, Sao Tome and Principe, Senegal, South Africa, Tunisia, and Uganda.

123 Network of African Data Protection Authorities [NADPA]. (n.d.). *The Network's functions*. https://www.rapdp.org/en/missions-du-reseau

124 Smart Africa. (2022, March 10). *Smart Africa and NADPA signed an MOU to advance the enforcement and harmonisation of personal data protection laws in Africa*. Smart Africa blog. https://smartafrica.org/smart-africa-and-nadpa-signed-an-mou-to-advance-the-enforcement-and-harmonization-of-personal-data-protection-laws-in-africa/

guarantee, respect, and protect citizens' right to freedom of information and expression through access to internet services.[125]

In 2019, the Commission adopted a *Declaration of Principles on Freedom of Expression and Access to Information in Africa,* which highlights a series of principles related to internet access, freedom of expression online, the right to anonymity, and the right to privacy and data protection in the digital space. States are called, among others, to:

- Adopt laws, policies, and other measures to provide universal, equitable, affordable, and meaningful access to the internet without discrimination.
- Not to interfere with the right of individuals to seek, receive, and impart information through any means of communication and digital technologies. This means refraining from measures such as the removal, blocking, or filtering of content unless such interference is justifiable and compatible with international human rights law and standards.
- Not to engage in or support any disruption of access to the internet and other digital technologies for segments of the public or an entire population,
- Not to require internet intermediaries to proactively monitor content which they have not authored or otherwise modified.
- Not to adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows, and data localisation requirements unless such measures are justifiable and compatible with international human rights law and standards.
- To only engage in targeted communication surveillance that is authorised by law, conforms with international human rights law and standards, and is premised on the specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.[126]

A 2022 *Resolution on the protection of women against digital violence in Africa* calls on states to adopt or review legislation to combat digital violence against women and facilitate women's access to education in digital technology domains.[127]

Another Commission resource that touches briefly on digital issues is the set of *Guidelines on Access to Information and Elections in Africa.* It notes that regulatory bodies should refrain from shutting down the internet during electoral processes. In exceptional cases where shutdowns may be permissible under international law, such limitations need to be authorised by law, serve a legitimate aim, and be necessary and proportional in a democratic society.[128] Furthermore, in the *Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa*, the Commission stresses that, while the spread of terrorism may be intensified by the use of the internet and social media, these 'are tools which can be used to combat the spread of terrorism and should not be viewed as a threat in itself'.[129]

At a regional level, ECOWAS has an act on personal data protection (adopted in 2010), which requires member states to develop national legal frameworks for the protection of data and privacy and to establish data protection authorities.[130] There is also an ICT accessibility policy (endorsed in 2018), which calls on member states to ensure digital accessibility for all, including

[125] African Commission on Human and Peoples' Rights [ACHPR]. (2016). *Resolution on the right to freedom of information and expression on the internet in Africa – ACHPR/Res.362(LIX)2016*. https://www.achpr.org/sessions/resolutions?id=374

[126] African Commission on Human and Peoples' Rights [ACHPR]. (2019). *Declaration of Principles on Freedom of Expression and Access to Information in Africa*. https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf

[127] African Commission on Human and Peoples' Rights [ACHPR]. (2022). *Resolution on the protection of women against digital violence in Africa* – ACHPR/Res.522(LXXII)2022. https://www.achpr.org/sessions/resolutions?id=558

[128] African Commission on Human and Peoples' Rights [ACHPR]. (2017). *Guidelines on Access to Information and Elections in Africa*. https://www.achpr.org/legalinstruments/detail?id=61

[129] African Commission on Human and Peoples' Rights [ACHPR]. (2015). *Principles and Guidelines on Human and People's Rights while Countering Terrorism in Africa*. https://www.achpr.org/legalinstruments/detail?id=9

[130] Economic Community of West African States [ECOWAS]. (2010). *Supplementary Act A/SA.1/01/10 on personal data protection within ECOWAS*. http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf

persons with disabilities.[131] Within SADC, a model law on data protection was adopted in 2012 which outlines rights and obligations related to the protection of personal data.[132]

A significant pan-African initiative – spearheaded by civil society and later endorsed by multiple actors from across diverse stakeholder groups – is the *African Declaration on Internet Rights and Freedoms*. The declaration highlights 13 key principles to be promoted and respected in the digital space, from privacy and data protection to gender equality, and from freedom of expression to cultural and linguistic diversity.

The declaration calls on African governments to ratify and give effect to all relevant international and regional human rights treaties related to the protection of human rights on the internet, as well as to ensure that legal, regulatory, and policy frameworks for the protection of these rights are in full compliance with international standards and best practices. Civil society groups are encouraged to include identified abuses of internet rights and freedoms in their reports to international human rights bodies and mechanisms and to communicate with the Special Rapporteur on Freedom of Expression and Access to Information in Africa on measures to uphold freedom of expression in relation to the internet.[133] Technical communities are asked to ensure African participation in the development of open standards.[134]

As the adoption of the aforementioned declaration illustrates, civil society organisations, alliances and think tanks based in Africa are particularly active on matters related to the protection and promotion of digital rights. Among them are the African Digital Rights Network, the African Internet Rights Alliance, the Association for Progressive Communications (APC), Collaboration on International ICT Policy in East and Southern Africa (CIPESA), OpenNet Africa, Paradigm Initiative, and Research ICT Africa. These entities usually also participate in various international processes and initiatives such as the IGF, the RightsCon conference, and the HRC (making contributions to the Council and attending side events held on the margin of Council sessions). Governments can (and should) tap into the expertise of these organisations to strengthen their engagement in international processes dealing with such issues.

3.3. International engagement

UN Human Rights Council

Within the UN system, issues related to the promotion and protection of human rights in the digital space are more and more often finding their way on the agenda of the **HRC**.

By December 2022, 35 African countries will have served as members of the HRC (Figure 34).[135] The African countries with seats on the Council in 2022 are depicted in Table 10.

---

131 Economic Community of West African States [ECOWAS]. (2018). *ECOWAS moves to ensure digital accessibility in the region*. Press release, 15 December. https://ccdg.ecowas.int/wp-content/uploads/ECOWAS-MOVES-TO-ENSURE-DIGITAL-ACCESSIBILITY-IN-THE-REGION.pdf

132 Southern African Development Community [SADC]. (2012). *Model law on data protection*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

133 The mechanism of the Special Rapporteur on Freedom of Expression and Access to Information was established by the African Commission on Human and Peoples' Rights in 2004. The mandate includes, among others, monitoring compliance with freedom of expression standards and advising member states and submitting reports to the Commission on the status of the enjoyment of the right to freedom of expression in Africa.

134 African Internet Rights. (n.d.). *African Declaration of Internet Rights and Principles*. https://africaninternetrights.org/en/declaration

135 The Human Rights Council has 47 members elected by the UN General Assembly for a period of three years. Africa has 13 seats on the Council.

Figure 34. African countries to have served on the HRC by December 2022.

Table 10. African countries serving on the HRC in 2022.

Country	Term expires in
Benin	2024
Cameroon	2024
Côte d'Ivoire	2023
Eritrea	2024
Gabon	2023
Gambia	2024
Libya	2022
Malawi	2023
Mauritania	2022
Namibia	2022
Senegal	2023
Somalia	2024
Sudan	2022

In recent years, there has been some involvement of African countries in the submission of, and discussions on resolutions covering digital-related topics. For instance, Egypt was among the sponsors of the *Resolution on neurotechnology and human rights*. Adopted at the Council's 51st session (September–October 2022), the resolution calls on the HRC's Advisory Committee to prepare a study on the impact, opportunities, and challenges of neurotechnology with regard to the promotion and protection of human rights.[136]

[136] United Nations Human Rights Council [UNHRC]. (2022). *Resolution A/HRC/51/3 – Neurotechnology and human rights*. https://digitallibrary.un.org/record/3991860?ln=en

Namibia was among the sponsors of a *Resolution on freedom of opinion and expression* adopted at the Council's 50th session (June–July 2022). Among other provisions, the resolution calls on states to promote, protect, respect, and ensure the full enjoyment of the right to freedom of opinion and expression both online and offline, to address digital divides and promote digital literacy, and to refrain from imposing restrictions on the free flow of information.[137]

At the Council's 49th session (February–April 2022), Tunisia was one of the sponsors of the *Resolution on the role of states in countering the negative impact of disinformation and the enjoyment and realisation of human rights*, which raised issues related to the misuse of digital technologies to disseminate misinformation.[138]

For the Council's 48th session (September–October 2021), Tunisia was among the initial sponsors of the *Resolution on the right to privacy in the digital age.*[139] Botswana, Mali, and **South Africa** joined the sponsors after the resolution was adopted.

At the 47th session (June–July 2021), **Nigeria** and Tunisia were among the initial sponsors of the *Resolution on the promotion, protection and enjoyment of human rights on the Internet*.[140] Libya and Somalia joined the list of sponsors later on, with Botswana, **Ghana**, and Mali doing the same after the adoption of the resolution. When the resolution was put to vote, Cameroon abstained, while Burkina Faso, **Côte d'Ivoire,** Gabon, Libya, Malawi, Mauritania, Namibia, **Senegal**, Somalia, Sudan, and Togo voted in favour.

During the same session, a second resolution on digital issues was adopted – *Resolution on new and emerging digital technologies and human rights*.[141] Morocco, Somalia, and Tunisia were among the resolution's initial sponsors, and were subsequently joined by Libya. Botswana and Mali joined the resolution's sponsors after it was adopted. Burkina Faso, Cameroon, **Côte d'Ivoire**, Gabon, Libya, Malawi, Mauritania, **Namibia, Senegal**, Somalia, Sudan, and Togo voted in favour of the resolution, while Eritrea abstained.

The *Resolution on freedom of opinion and expression* – adopted at the HRC's 44th session (June–July 2020) – had **Namibia** and Tunisia among its initial co-sponsors. Botswana and **Ghana** joined the sponsors later on. The resolution reaffirms that the same rights that people have offline must also be protected online and calls on member states to facilitate and promote access to and use of communications and digital technologies.[142]

There has also been some level of engagement of African countries in overall discussions related to digital issues during HRC sessions, as the following examples illustrate.[143]

At the 50th session, during a discussion on the protection of human rights during and after the COVID-19 pandemic, **South Africa** highlighted the widening digital divides between and within countries and called for consideration of how to best use new technologies to strengthen good governance, promote and protect human rights, and support equitable and inclusive post-

[137] United Nations Human Rights Council [UNHRC]. (2022). *Resolution A/HRC/50/15 – Freedom of opinion and expression*. https://undocs.org/Home/Mobile?FinalSymbol=A%2Fhrc%2Fres%2F50%2F15&Language=E&DeviceType=Desktop&LangRequested=False

[138] United Nations Human Rights Council [UNHRC]. (2022). *Resolution A/HRC/49/21 – Role of states in countering the negative impact of disinformation on the enjoyment and realisation of human rights.* https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F49%2F21&Language=E&DeviceType=Desktop&LangRequested=False

[139] United Nations Human Rights Council [UNHRC]. (2021). *Resolution A/HRC/48/4 – Right to privacy in the digital age*. https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F48%2F4&Language=E&DeviceType=Desktop&LangRequested=False

[140] United Nations Human Rights Council [UNHRC]. (2021). *Resolution A/HRC/47/16 – The promotion, protection and enjoyment of human rights on the internet.* https://digitallibrary.un.org/record/3937534?ln=en

[141] United Nations Human Rights Council [UNHRC]. (2021). *Resolution* A/HRC/47/23 – *New and emerging digital technologies and human rights*. https://digitallibrary.un.org/record/3936036?ln=en

[142] United Nations Human Rights Council [UNHRC]. (2020). *Resolution* A/HRC/44/12 – *Freedom of opinion and expression*. https://digitallibrary.un.org/record/3877197?ln=en

[143] This overview is based on statements made during HRC discussions.

pandemic recovery efforts. Togo called for coordinated efforts at the regional and international levels to ensure that human rights are properly considered when it comes to governing and regulating digital technologies. In a debate on disinformation and human rights, Egypt expressed concerns over the use of electronic platforms to spread fake news and extremist and terrorist content, and called for strengthened cooperation between all stakeholders in developing codes of conduct to guarantee the exercise of the right to freedom of opinion and expression without infringing on the freedoms of others.

During the high-level segment of the Council's 49th session, **Nigeria** referred to the need to address the spread of fake news, hate speech, and incitement to hatred and violence. When the Council discussed children rights, Botswana, Cameroon, **Namibia,** and Tunisia spoke about the urgency of protecting children in the digital space – including with regard to online content related to child sexual exploitation and abuse.

During an interactive dialogue with the Special Rapporteur on the right to privacy, Togo called for strengthened mechanisms for privacy protection and information security, in the context of international cooperation, while Cameroon referred to legislation and capacity-building initiatives put in place at the national level to ensure privacy and data protection and address cybercrime-related challenges. Algeria expressed concern over practices involving the illegal use of spyware, noting that these constitute not only human rights violations, but also threats to peace, security, and international cooperation. The country suggested that consideration is given to the introduction of measures against such practices, including safeguards, effective monitoring and redress procedures, and codes of conduct. Egypt highlighted the importance of ensuring that the right to privacy extends to the digital space and called for adequate attention to be paid to the challenges posed by AI and other modern technologies.

At the 47th session, during the discussion on technical cooperation to advance the right to education and ensure inclusive and equitable quality education and life learning from all, the **African Group** (through a joint declaration) drew attention, among other issues, to the growing digital divide and its implications on the provision of educational services. The countries also called on international institutions to provide nations with technical assistance in their efforts to modernise their educational systems so that they respond to current and future needs driven by digital transformation processes.

When HRC members discussed the impacts, opportunities, and challenges of new and emerging digital technologies regarding the promotion and protection of human rights, at the 44th session, **Ghana** underscored the need for states to maintain and enforce individual rights and liberties when designing and deploying digital technologies for meeting public policy objectives. It also called on states to uphold international norms and principles in particular as they related to personal data protection and cybersecurity and invited countries to accede to key international instruments such as the Budapest and Malabo Conventions. The need for data governance rules was also highlighted: 'We need to consider putting in place data governance rules, ie, who owns the tons of data that we put online, how it is managed and used, who shares the benefits and of the monetisation and application of this data'.[144] Morocco spoke about the implications that new technologies could have at economic, cultural, and political levels, and highlighted the importance of ensuring that policymakers properly understand these technologies and their implications.

Nigeria and Tunisia (in a joint statement with Brazil and Sweden) called on states to respect all human rights online and offline, to enhance access to open, free and secure ICTs, and refrain from internet shutdowns and online surveillance and censorship measures. In a statement issued by the Non-Aligned Movement, African nations and their partners underlined the need to bridge digital divides, called for an end to the use of ICTs in contradiction with the norms and principles of international law ('including those related to sovereignty, sovereign equality, and

[144] Remarks by Ms Ursula Owusu-Ekuful, Minister for Communications of Ghana during the Panel Discussion on the impacts, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights, HRC 44th session, 8 July 2022. https://hrcmeetings.ohchr.org/HRCSessions/RegularSessions/44session/Pages/Statements.aspx?SessionId=35&MeetingDate=08/07/2020%2000%3a00%3a00

territorial integrity of the UN member states'), and noted the 'importance of international and multistakeholder cooperation in order to bridge the digital divides, benefit from opportunities and address the challenges arising from the rapid technological change which affects states in different ways due to their national realities, capacities and levels of development'.[145]

Other processes

Cabo Verde, Mauritius, Morocco, Senegal, and Tunisia have ratified the **Council of Europe's** Convention for the protection of individuals with regard to the processing of personal data (Convention 108), while Burkina Faso was invited to accede.[146] Among them, Mauritius has already ratified the 2018 protocol amending the convention (adopted with the aim to ensure that the convention is fit for purpose to deal with challenges resulting from the use of new technologies). The protocol was also signed by Tunisia.[147]

Ghana, **Kenya**, and Tunisia are the only African countries to have joined the **Freedom Online Coalition**, a group of 34 governments[148] committed to working together to support internet freedom and protect fundamental rights online.

[145] Statement delivered by Azerbaijan on behalf of the Non-Aligned Movement during the Panel Discussion on the impacts, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights, HRC 44th session, 8 July 2022. https://hrcmeetings.ohchr.org/HRCSessions/RegularSessions/44session/Pages/Statements.aspx?SessionId=35&MeetingDate=08/07/2020%2000%3a00%3a00

[146] Council of Europe [CoE]. (n.d.). *Details of Treaty No.108*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

[147] Council of Europe [CoE]. (n.d.). *Modernisation of Convention 108*. https://www.coe.int/en/web/data-protection/convention108/modernised

[148] As of October 2022. A list of members of the Freedom Online Coalition is available at https://freedomonlinecoalition.com/members/

4. Cybersecurity, cybercrime, and child online protection

Section summary

As digital transformation processes take off across Africa, the region faces considerable cybersecurity challenges. The 2020 Cybersecurity Exposure Index placed Africa as the region with the highest exposure rate to cyberattacks per country. Less than half of the countries across the continent have adopted or drafted cybersecurity strategies; among them are Côte d'Ivoire, Ghana, Kenya, Namibia, Nigeria, Rwanda, Senegal, and South Africa. Some have outlined cybersecurity-related objectives in other national strategies and plans. Most African countries have or are developing cybercrime laws. Some have also included issues of child online protection across various policies and strategies or developed dedicated frameworks (e.g. Rwanda's *Child Online Protection Policy*).

Generally, cybersecurity policies tend to focus on improving the country's cybersecurity posture, developing comprehensive governance frameworks, and building individual and institutional capacity. But they also include elements of foreign policy, as they highlight objectives related to greater international cooperation (bilateral, multilateral) in areas such as collaboration between computer emergency response teams (CERTs) / computer incident response teams (CIRTs), fostering capacity building and knowledge sharing on fighting cybercrime, upholding of international cybersecurity norms, and promoting the application of international law. Other objectives relate to involvement in regional and international fora dealing with cybersecurity and cybercrime issues, and compliance with relevant international frameworks.

Cybersecurity and cybercrime are also tackled in several initiatives at the AU level. The *Digital Transformation Strategy* outlines recommendations and actions for strengthening cybersecurity across the continent, while a Cybersecurity Expert Group is tasked, among others, with supporting member states on matters of international cooperation. At the core of AU's cybersecurity initiatives lies the 2014 *Convention on Cyber Security and Personal Data Protection* (*Malabo Convention*). Despite its ambitious goals, the convention is yet to come into force, having been ratified by only 13 countries to date. Meanwhile, twelve African countries are parties, signatories, or have been invited to join the *Convention on Cybercrime* (*Budapest Convention*, developed at the level of the CoE); four of them are party to both the Malabo and the Budapest Convention.

Within RECs, several strategies, policies, or model laws on cybersecurity, critical infrastructure protection, and cybercrime encourage countries to strengthen regional and international cooperation (including on judicial and digital evidence issues), harmonise protection measures, and exchange information on threats and risks.

When it comes to international processes, notable is the involvement of African countries in the work of the OEWG and the Cybercrime Ad Hoc Committee. For the OEWG, 16 African countries participated in the 2019–2021 group and 20 have so far contributed to the 2021–2025 group (including Côte d'Ivoire, Egypt, Ghana, Kenya, Morocco, Nigeria, and South Africa). Among the issues they raised are the need for a more consistent implementation of existing cyber norms; the importance of strengthening countries' capacities to detect, investigate, and counter cyberthreats; and the establishment of a global repository of confidence-building efforts. Nineteen African countries (including Algeria, Egypt, Ghana, Namibia, Nigeria, and South Africa) contributed to the first three substantive sessions of the Cybercrime Ad Hoc Committee, putting forward proposals for criminal offences to be included in a convention on cybercrime, noting that the convention should strengthen international cooperation, and stressing the need to ensure protection of human rights while fighting cybercrime.

Besides governmental involvement in UN processes, the African region also has some representation in multistakeholder initiatives. The Global Forum on Cyber Expertise has among its members 20 African governments, several regional and continental organisations, and multiple civil society groups and technical organisations. Eleven African governments and several other stakeholders from across the region have joined the Paris Call for Trust and Security in Cyberspace.

4.1. National overview

Cybersecurity is among the digital challenges that African countries need to address. In 2020, Africa ranked as the region with the highest exposure to cyberattacks per country, in the Cybersecurity Exposure Index.[149]

According to the ITU Global Cybersecurity Index, only 7 African countries – Mauritius, Egypt, Tanzania, **Ghana**, Tunisia, **Nigeria**, and Morocco – are among the top 50 countries with the highest cybersecurity indices.[150] The index maps countries' cybersecurity commitments across five pillars: legal measures, technical measures, organisational measures, capacity development measures, and cooperation measures. Morocco is the only African country that made it to the top 50 on the National Cybersecurity Index (October 2022) – which measures the preparedness of countries to prevent cyberthreats and manage cyber incidents (Table 11).[151]

Table 11. Ranking of focus countries in the Global Cybersecurity Index and National Cybersecurity Index.

Country	**Global Cybersecurity Index (2020)** Score (rank)	**National Cyber Security Index (October 2022)** Score (rank)
Côte d'Ivoire	67.82 (75)	31.17 (97)
Ghana	86.69 (43)	31.17 (98)
Kenya	81.7 (51)	41.56 (80)
Namibia	11.47 (155)	15.58 (131)
Nigeria	84.76 (47)	54.55 (61)
Rwanda	79.95 (57)	33.77 (92)
Senegal	35.85 (100)	19.48 (121)
South Africa	78.46 (59)	36.36 (89)

Cybersecurity strategies and elements of foreign policy

Many countries around the world have adopted national cybersecurity strategies (NCSs) establishing institutions, initiatives, and priorities, setting out roles and responsibilities, and outlining elements of international cooperation on cybersecurity issues.

Africa, however, is lagging behind in developing and implementing NCSs (Figure 35). All eight focus countries have approved or drafted NCSs. Besides dedicated strategies, cybersecurity-related aspects are sometimes also covered in other national strategies, policies, and plans.

[149] PasswordManagers. (2020). *Cybersecurity Exposure Index (CEI) 2020.* https://passwordmanagers.co/cybersecurity-exposure-index/#global

[150] International Telecommunication [ITU]. (2021). *Global Cybersecurity Index*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[151] eGovernance Academy Foundation. (2022). *National Cyber Security Index*. https://ncsi.ega.ee/ncsi-index/?order=rank

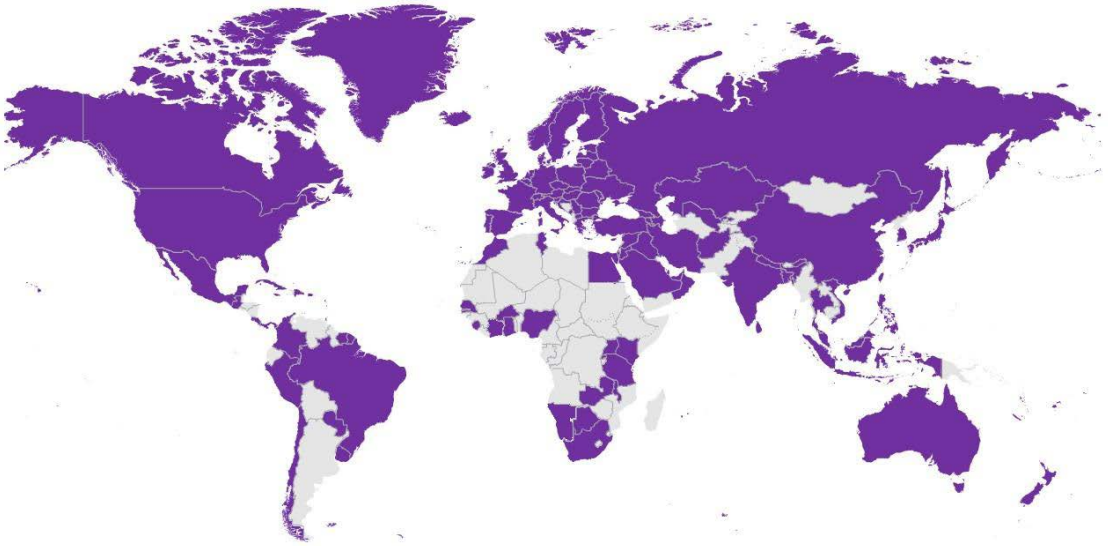


Figure 35. Countries with national cybersecurity strategies.[152]

Kenya's NCS has among its guiding principles the facilitation of international cooperation on cybersecurity matters. Noting that cyberthreats are cross-cutting and transnational, the strategy outlines the government's commitment to work with international partners to improve the country's cybersecurity posture. Kenya's participation in the development and implementation of international laws, agreements, treaties, policies, norms, and standards on cybersecurity is highlighted as an action line.[153] Enhancing international cooperation on matters of cybersecurity – at the regional and global levels – is also envisioned in *Kenya's Broadband Strategy* and *National Digital Master Plan*. Moreover, the broadband policy sets the country on a mission to 'build global alliances and promote the application of international law in cyberspace', while the master plan talks about Kenya's commitment to promoting a secure, stable and peaceful cyberspace, while upholding international cybersecurity norms. Concluding bilateral and multilateral agreements on sharing information on information security and collaborating with international CIRTs and threat intelligence research hubs are other goals outlined in the master plan.

The **Nigerian** NCS has an entire section dedicated to international cooperation, with goals and priorities ranging from accelerating efforts to cooperate in combatting cyberthreats to strengthening information sharing with global partners. The strategy highlights the country's commitment to cooperate with other countries and multinational organisations 'to garner consensus in cyber law enforcement, threat intelligence sharing, adoption of collective cyber norms and cybersecurity best practices, policy and strategy formulation and implementation, technology exchange and capacity development, including cyber defence'. It further talks about the importance of 'coordinating the responsibilities of domestic cybersecurity stakeholders within the countries to enhance international engagement'. To support such coordination efforts, the government will facilitate capacity development in the areas of international cyber law and cyber diplomacy. At a regional level, Nigeria intends to lead the creation of new initiatives, forums, and mechanisms to enhance regional cooperation in cybersecurity, including when it comes to developing capacity to improve cross-border law enforcement and enhancing information sharing.[154]

The importance of international cooperation on cybersecurity-related issues is also underscored by Nigeria's *National Digital Economy Policy and Strategy*.

---

[152] Based on International Telecommunication Union [ITU]. (2022). *National Cybersecurity Strategies Repository.* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx The repository includes approved and draft NCSs, be they in the form of a single or multiple documents, or as an integral part of a broader ICT or national security strategies.

[153] National Computer and Cybercrimes Coordination Committee Secretariat, Republic of Kenya. (2022). *National Cybersecurity Strategy*. https://ict.go.ke/wp-content/uploads/2022/10/KENYA-CYBERSECURITY-STRATEGY-2022.pdf

[154] Government of Nigeria. (2021). *National Cybersecurity Policy and Strategy*. https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

Similarly, involvement in regional and international cybersecurity work is stipulated as one of the strategic aims and priorities of **Senegal**'s NCS.[155] Sub-regional, regional, and international cooperation on cybersecurity issues is also envisioned in the *Digital Senegal Strategy*.

The national cybersecurity strategic plan of **Rwanda** defines the establishment of a National Cyber Security Agency which will, among other things, promote regional and international cooperation, R&D in the field of cybersecurity. Other strategic actions related to international cooperation include membership with regional and international CERTs, international cooperation in response to cybercrime, and international information sharing.[156]

Rwanda's *ICT Sector Strategic Plan* also outlines the objective of promoting regional and international cooperation, research, and development in the field of cybersecurity. It further talks about the importance of ensuring that ICT-related legal and regulatory frameworks comply with international cybersecurity standards and best practices. Establishing partnerships with international organisations for capacity building in cybersecurity is envisioned in the *ICT Hub Strategy.* Notable is the country's goal of becoming a regional hub for security, through building a sustainable cybersecurity industry (*ICT Sector Strategic Plan*) and ensuring a secure and resilient cyberspace (*Smart Rwanda Master Plan*).

The *National Cybersecurity Policy Framework* for **South Africa** is intended to provide a holistic approach to cybersecurity and sets out the promotion and strengthening of local and international cooperation on cybersecurity as one of the country's priorities. To this end, the document envisages South African participation in regional, AU, and international fora on cybersecurity-related matters to advance the country's position, establish bilateral and multilateral partnerships through various instruments, and join relevant international organisations to promote a coordinated response to cyberthreats and keep abreast of developments in the field of cybersecurity.[157] Aligning with global developments in the field of cybersecurity is highlighted as a goal in the country's broadband policy.

Ghana's *National Cyber Security Policy and Strategy* calls for the country's active participation in all relevant international cybersecurity bodies, panels, and multinational agencies.[158] In 2020, the Ghanaian parliament passed the *Cybersecurity Act* which includes several provisions related to international cooperation. The act mandates the Cybersecurity Authority of Ghana to implement and enforce international treaties on cybercrime and cybersecurity endorsed by the country, to cooperate with international agencies, and to establish a cybersecurity incident point of contact that would facilitate international cooperation on cybersecurity matters.[159]

Côte d'Ivoire's NCS was outlined in a communication adopted by the government in December 2021. The 2021–2025 strategy, whose overarching goal is to better secure cyberspace in support of the country's digital transformation efforts, also envisions a leadership role for Cote d'Ivoire in cybersecurity, at a continental level.[160] In addition, the *National Digital Development Strategy* outlines objectives related to reinforcing international cooperation on cybersecurity matters, together with specific action lines related to active participation in the FIRST network and in the ITU Cyberdrill initiative.

---

155 Ministry of Communications, Telecommunications, Post and the Digital Economy, Republic of Senegal. (2017). *Senegalese National Cybersecurity Strategy*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SNC2022-Senegal-NCS-Jan-2018_eng.pdf

156 Republic of Rwanda. (2015). National Cybersecurity Strategic Plan. https://www.risa.rw/fileadmin/user_upload/Others%20documents/National_Cyber_Security_Strategic_Plan_Rwanda.pdf

157 South Africa Government. (2015). *National Cybersecurity Policy Framework for South Africa*. https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

158 Ministry of Communications, Republic of Ghana. (2015). *National Cyber Security Policy and Strategy. Final draft*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf

159 Parliament of Ghana. (2020). *Cybersecurity Act*. https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf

160 Republic of Côte d'Ivoire. (2021). *Communique du Conseil des Ministres du Mercredi 22 Décembre 2021 (Communique of the Council of Ministers, Wednesday 22 Decembre 2021).* https://www.gouv.ci/doc/1640207049Communique-du-Conseil-des-Ministres-du-mercredi-22-decembre-2021.pdf

For **Namibia**, the *National Cybersecurity Strategy and Awareness Raising Plan 2022–2027* includes elements related to advancing international cooperation on cybersecurity-related issues.[161]

An overarching message that spans all the strategies and policies outlined relates to the importance of advancing international cooperation on cybersecurity-related issues. This sought-for cooperation is not only about sharing information and working together with partners to identify risks and mitigate threats but also about capacity development initiatives aimed to strengthen national cybersecurity capabilities. Developed countries and international organisations – especially those that look into strengthening their relations with African countries, including on digital topics – should respond to these calls and support African governments in their efforts to enhance their readiness to respond to cyberthreats.

Offensive cyber capabilities

Incidents of cybersabotage or cyberespionage have accelerated cyber armament. Some countries have declared 'cyber' to constitute the fifth military domain (after land, sea, air, and space). Many countries have established significant budgets for building military cyber capabilities – both offensive and defensive. A Geneva Internet Platform mapping of publicly available documents, such as national strategies, military doctrines, official statements, and credible media reports, presents evidence and indications that offensive cyber capabilities (OCCs)[162] exist or are being built in over 50 states (Figure 36).[163] Among them are four African countries: **Kenya**, **Nigeria**, **South Africa**, and Sierra Leone.

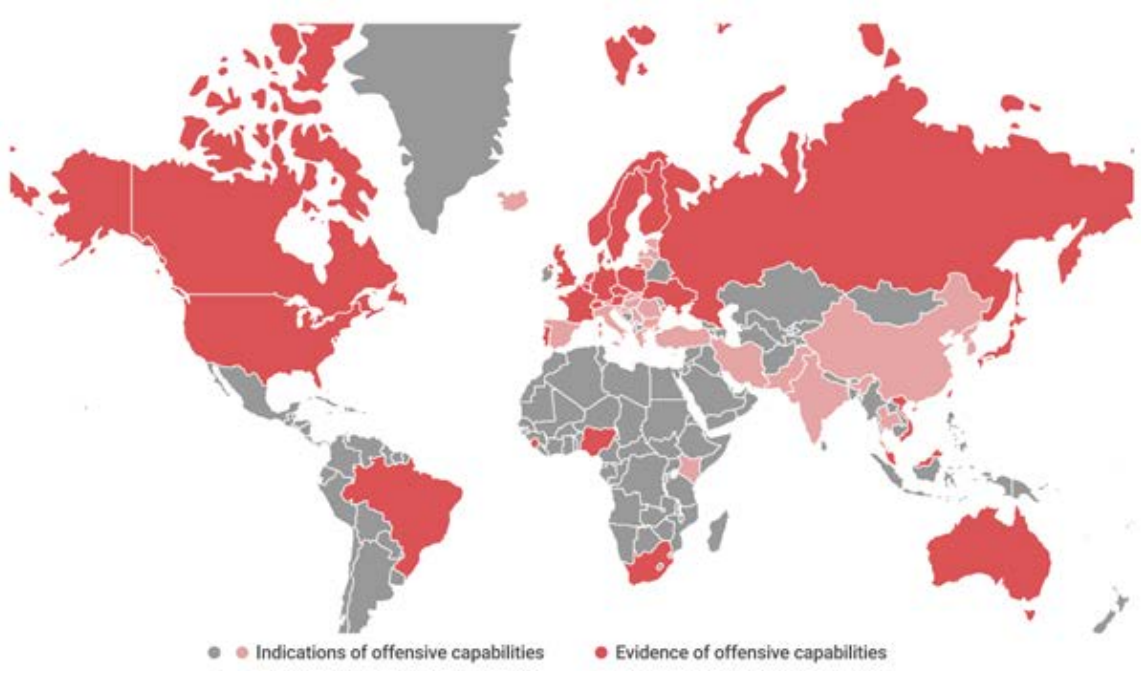


Figure 36. Offensive cyber capabilities.

[161] Namibia Media Trust. (2021). *Review of Namibia's National Cybersecurity Strategy & Awareness Raising Plan 2022–2027.* https://www.nmt.africa/uploads/614346b1d2ebb/NMTsubmision-ReviewofnationalcybersecuritystratA(22-27).pdf. Some sources note that the strategy was approved by the government in March 2022, while others indicate that, as of October 2022, the strategy was yet to be finalised.

[162] OCCs are understood as the capabilities of state institutions to conduct cyberattacks against the information security of other parties, including through access to or impact on, their digital systems, information and resources, or by making such systems unavailable.

[163] Geneva Internet Platform [GIP]. (n.d.). *Cyberconflict and warfare.* Digital Watch observatory. https://dig.watch/topics/cyberconflict

South Africa's Department of Defence has underscored the need to protect the country's cyber-domain through, inter alia, a comprehensive information warfare capability focused on six areas: network warfare; electronic warfare; psychological operations; information-based warfare; information infrastructure warfare; and command and control warfare. These are defined as follows:

- **Network warfare (Netwar)**: To exploit or use the information systems (offensive) of an adversary and to protect all defence information systems (defensive) to ensure use for own forces.
- **Electronic warfare**: To exploit or use electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum while retaining its friendly use.
- **Psychological operations**: To conduct planned psychological activities in peace, conflict, and war to create attitudes and behaviour favourable to the achievement of political and military objectives. These operations include psychological action and warfare activities designed to achieve the desired psychological effect.
- **Information-based warfare**: To enhance situational awareness at the operational and tactical levels as well as to degrade that of an adversary.
- **Information infrastructure warfare**: To protect its own information infrastructure and to attack or exploit an adversary's information infrastructure.
- **Command and control warfare:** To conduct information warfare on the battlefield by causing a disjuncture between an adversary's command structure and its commanded forces.[164]

The country also appears to have developed a Cyber Warfare Strategy covering offensive information warfare actions.[165]

In 2016, **Kenya**'s Cabinet Secretary for Information, Communication and Technology at that time was noting that the Kenyan government was committed to developing comprehensive and offensive cyber-capabilities.[166] In 2018, **Nigeria** appears to have commissioned a Nigerian Army Cyber Warfare Command with the goal 'to empower the Nigerian Army with the capabilities to protect its data and network against cyberattacks and hostile elements'.[167]

Sierra Leone's *National Cyber Security and Data Protection Strategy 2017–2022* states that the country 'shall have the means to respond to cyberattacks in the same way as we respond to any other attack, using whichever capability is most appropriate, including an offensive cyber capability'.[168]

Cybercrime policies: International dimensions

As Africa increasingly embraces digital transformation processes, the region is also becoming more and more vulnerable to cyberthreats. According to Interpol, the most prominent threats identified across Africa are online scams, digital extortion, business email compromise, ransomware, and botnets.[169] Research carried out by Kenya-based cybersecurity company Serianu indicates that the cost of cybercrime in Africa has increased from US$0.5 billion in 2015 to US$3 billion in 2020.[170]

---

164 Department of Defence, Republic of South Africa. (2015). *South African Defence Review.* https://static.pmg.org.za/170512review.pdf

165 Martin, G. (2017, September 26). *Department of Defence aims to beef up cyber security.* defenceWeb. https://www.defenceweb.co.za/cyber-defence/department-of-defence-aims-to-beef-up-cyber-security/?catid=111%3Asa-defence&Itemid=242

166 Korir, C .(2016, November 29). *Government to curb cyber crimes*. Ministry of ICT, Innovation and Youth Affairs. https://ict.go.ke/government-to-curb-cyber-crimes/

167 Erunke, J. (2018, October 16). *Army takes terror war to cyber space, launches command.* Vanguard. https://www.vanguardngr.com/2018/10/army-takes-terror-war-to-cyber-space-launches-command/

168 Government of Sierra Leone. (2017). *National Cyber Security and Data Protection Strategy 2017–2022*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00090_03_Sierra%20Leone%20national-cyber-security-strategy-2017-final-draft.pdf

169 Interpol. (2021). *African Cyberthreat Assessment Report. Interpol's key insight into cybercrime in Africa*. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa

170 Global Cyber Alliance. (2021.) *Serianu partners with the Global Cyber Alliance to reduce cost of cybersecurity*. https://www.

Many African countries – 39 in total, including **Côte d'Ivoire**, Egypt, **Ghana**, **Kenya**, Morocco, **Nigeria**, **Rwanda**, **Senegal**, and **South Africa** – have dedicated cybercrime laws (Figure 37), which typically outline elements related to international cooperation in tackling cybercrime. Cybercrime is sometimes also mentioned in legislation dealing with electronic transactions and data protection, as is the case with **Ghana**. In many cases, cybercrime is covered in broader cybersecurity strategies.

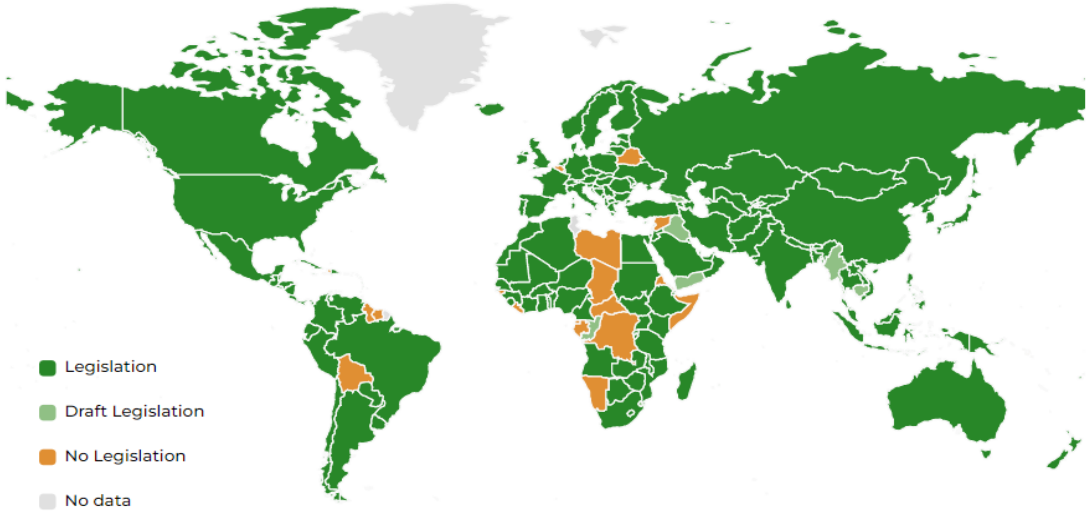


Figure 37. Cybercrime legislation worldwide (December 2021).[171]

One of the strategic goals stipulated in the national cybersecurity strategy of **Côte d'Ivoire** is to enhance international cooperation in two ways: by continuing its participation in international and regional initiatives, and by ratifying international conventions on cybercrime (Budapest and Malabo). Compliance with international laws and treaties is also mentioned in the cybersecurity strategies of **Senegal** and **Rwanda**.

International cooperation in dealing with cybercrime matters (e.g. in detecting and deterring cyberespionage and responding to cybercrime) is highlighted in national cybersecurity policies of **Rwanda** and **Nigeria**, as well as in **Kenya**'s cybersecurity law. An entire section of **Nigeria**'s *Cybercrime Act* is dedicated to international cooperation on jurisdictional issues and law enforcement.[172]

For international cooperation, the Cybersecurity Authority of **Ghana** should, according to the country's *Cybersecurity Act*, designate and maintain a 24/7 contact point to tackle cybercrime. The role of the contact point is to provide technical advice to other contact points, preserve data and evidence, provide information on the detection of suspects and related matters, as well as the immediate transmission of legal requests in accordance with applicable laws and treaties.

South Africa's *National Cybersecurity Policy Framework* highlights the need for participation in regional, continental, and international fora to advance the global cybersecurity agenda, combat cybercrime, and build confidence and trust in the secure use of ICTs.

International cooperation with respect to research and training also features in several policy documents. **Rwanda**'s cybersecurity policy mentions participation in international research projects and the exchange of experts in cybersecurity, whereas the **Nigerian** cybercrime act stresses the need to organise training and capacity development programmes for officers

globalcyberalliance.org/serianu-partners-with-the-global-cyber-alliance-to-reduce-cost-of-cybersecurity/

171 Based on United Nations Conference on Trade and Development [UNCTAD]. (2021). *Cybercrime legislation worldwide.* https://unctad.org/page/cybercrime-legislation-worldwide. Figure redrawn.

172 National Assembly, Nigeria. (2015). *Cybercrimes (prohibition, prevention, etc) Act*. https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

responsible for the prohibition, prevention, detection, investigation, and prosecution of cybercrimes. In addition, **Senegal**'s strategy encourages law enforcement authorities and courts to work with their partners bilaterally and multilaterally to strengthen their work in investigating, preventing, and prosecuting cybercrime.

Child online protection

The issue of child online protection (COP) appears across various national policy documents and strategies, both general and cybersecurity-related. **Kenya**'s *National ICT Policy* from 2019 calls for a global partnership on COP by, among others, developing a framework of engagement between local and international organisations and law enforcement authorities. The importance of international cooperation (with industry, criminal justice institutions, international organisations, etc.) is further highlighted in the country's *National Plan of Action to Tackle Online Child Sexual Exploitation and Abuse*, adopted in 2022.[173]

Global cooperation on COP is also mentioned in **Rwanda**'s dedicated *Child Online Protection Policy*, which calls, for instance, for the establishment of formal cooperation frameworks with regional and global COP communities. To strengthen domestic legal and regulatory frameworks related to COP, Rwanda needs to identify and ratify COP-related international treaties and protocols and strengthen and amend the relevant criminal laws in line with international standards and best practices.[174]

Compliance with international mechanisms such as ITU's *Industry Guidelines on Child Online Protection* is stipulated in **Kenya'**s draft *Industry Guidelines for Child Online Protection and Safety*.[175] The **Ghanaian** *Cybersecurity Act* has an entire section dedicated to COP. The country also has a dedicated COP policy.

4.2. Continental and regional overview

Cybersecurity features as a flagship programme under the AU's *Agenda 2063*, as 'a clear indication that Africa needs to not only incorporate in its development plans the rapid changes brought about by emerging technologies, but also to ensure that these technologies are used for the benefit of African individuals, institutions or nation states by ensuring data protection and safety online'.[176]

Cybersecurity and cybercrime are also given a prominent place in AU's *Digital Transformation Strategy*, which includes several policy recommendations and proposed actions in these two areas. While most of them are related to strengthening cybersecurity at the national and continental level, there are also a few elements related to international processes. One recommendation is for the AU and its member states to 'support the UN-led process for the establishment of the Global Cybersecurity Framework under the UN'.[177]

In 2018, the AU decided to establish a Cybersecurity Expert Group (AUCSEG) tasked with advising the AUC and policymakers on cybersecurity-related issues. The group, which started working

[173] Ministry of Public Service, Gender, Senior Citizens Affairs and Special Programmes, Republic of Kenya. (2022). *National Plan of Action to Tackle Online Child Sexual Exploitation and Abuse in Kenya, 2022–2026*. https://www.socialprotection.go.ke/wp-content/uploads/2022/06/National-Plan-of-Action-to-Tackle-Online-Child-Sexual-Exploitation-and-Abuse-in-Kenya-2022-2026.pdf

[174] Ministry of ICT and Innovation, Republic of Rwanda. (2019). *Rwanda Child Online Protection Policy*. https://rura.rw/fileadmin/Documents/ICT/Laws/Rwanda_Child_Online_Protection_Policy.pdf

[175] Communications Authority of Kenya. (2022). *Industry Guidelines for Child Online Protection and Safety*. https://www.ca.go.ke/wp-content/uploads/2022/03/Draft-Industry-Guidelines-for-Child-Online-Protection-COP-and-Safety-in-Kenya.pdf

[176] African Union [AU]. (n.d.). *Flagship projects of Agenda 2063*. https://au.int/en/agenda2063/flagship-projects

[177] African Union [AU]. (2020). *The Digital Transformation Strategy for Africa*. https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

in 2019, is also expected to support the AUC and member states on matters of international cooperation regarding cybersecurity, personal data protection, and combating cybercrime.[178]

At the core of AU's cybersecurity initiatives lies the 2014 Convention on Cyber Security and Personal Data Protection **(**Malabo Convention**).** The instrument covers more than cybersecurity and cybercrime and includes provisions on electronic transactions and personal data protection. This gives the *Malabo Convention* a unique and innovative character among cybersecurity-related regulations and policies. It is, however, also the reason for some of the challenges regarding its ratification.

The convention contains several provisions related to **international cooperation**. It encourages state parties to conclude agreements on mutual legal assistance in dealing with cybercrime and to enable the exchange of information on cyberthreats and vulnerability assessments through institutions such as CERTs. Countries are also mandated to use international cooperation mechanisms – be they based on private or public partnerships – when it comes to responding to cyberthreats, improving cybersecurity, and stimulating multistakeholder dialogue.

The convention has not come into effect yet. Out of 55 AU members, 14 have signed the convention, and 13 ratified it and deposited instruments of ratification with the AU (as of March 2022).[179] This falls short of the 15 instruments of ratification required for the convention to come into force.

Some observers underscore the fact that the *Malabo Convention* is an important instrument supporting continental e-commerce and urgently needs to be ratified, while others warn against over-regulation.[180] While the convention is significant given its scope, this lack of ratification takes away from its potential impact.[181] This rather slow pace of ratification may be explained by multiple reasons: from political ones (rooted in the region's political, cultural, and historical diversity),[182] to lengthy processes within countries, limited awareness among policymakers on the importance of cybersecurity and its relevance for national security, and limited capacity within the countries to take up and conclude the necessary processes.[183] It remains to be seen whether countries will overcome these and other challenges and follow up on the commitment they have taken at the March 2022 Cybersecurity Summit to sign and ratify the convention as an important step towards the 'development of a safe African cyberspace'.[184]

There is an **overlap in membership between the Malabo and Budapest Conventions**. The *Budapest Convention* is the *Convention on Cybercrime of the Council of Europe*, and it focuses on defining cybercrime, related legal provisions, and cross-border cooperation. Twelve African countries are parties, signatories, or have been invited to accede to the *Budapest Convention*: Cabo Verde, **Ghana**, Mauritius, Morocco, **Nigeria,** and **Senegal** are parties to the convention; **South**

[178] African Union [AU]. (n.d.). *African Union Cyber Security Expert Group – Terms of Reference.* https://au.int/sites/default/files/announcements/34922-annc-au_cyber_security_expertgroup_tors.pdf

[179] Countries that have ratified the convention: Angola, Cabo Verde, Republic of the Congo, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, Zambia. Countries that have signed the convention: Benin, Chad, Comoros, Republic of the Congo, Ghana, Guinea-Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome and Principe, Togo, Tunisia, Zambia. African Union [AU]. (2022). *List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf

[180] ITWeb. (2021, September 10). *African countries urged to ratify Malabo convention*. ITWeb blog. https://itweb.africa/content/GxwQD71ZJy4MlPVo

[181] Greenleaf, G. & Georges, M. (2015). *The African Union's Data Privacy Convention: A major step toward global consistency?* Privacy Laws & Business International Report 131, pp. 18-21. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546652

[182] Internet Governance Forum [IGF]. (2021). *IGF 2021 Workshop #18 Cyber diplomacy in Africa and digital transformation*. https://www.intgovforum.org/en/content/igf-2021-ws-18-cyber-diplomacy-in-africa-and-digital-transformation

[183] Amazouz, S. (2019). *International cyber security diplomatic negotiations: Role of Africa in inter-regional cooperation for a global approach on the security and stability of cyberspace*. Master thesis presented to the Faculty of Arts in the University of Malta. https://www.diplomacy.edu/wp-content/uploads/2021/06/141220191231-Amazouz_0.pdf

[184] Cybersecurity Summit – Lomé 2022. (2022, March 23–24). *The Lome Declaration on cybersecurity and fight against cybercrime*. https://www.uneca.org/sites/default/files/SROs/West-Africa/20220223-Déclaration%20de%20Lomé%20sur%20la%20cybersécurité%20et%20la%20lutte%20contre%20la%20cybercriminalité-EN%20%282%29.pdf

Africa signed the convention; while Benin, Burkina Faso, **Côte d'Ivoire**, Niger, and Tunisia were invited to accede.[185] Of these countries, Cabo Verde, **Ghana**, Mauritius, and **Senegal** have signed or ratified both the Malabo and the Budapest Conventions (Figure 38).

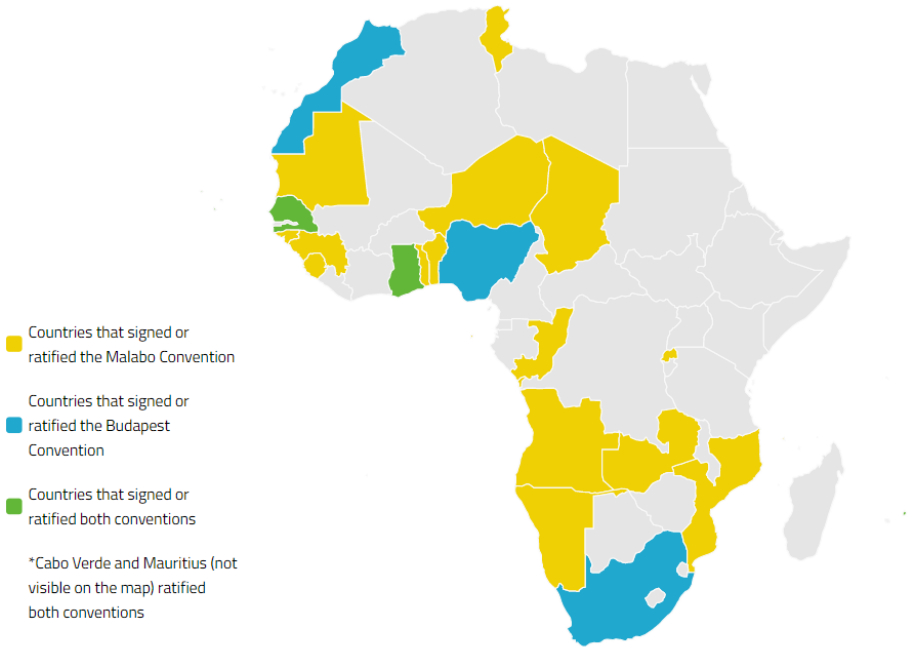


Figure 38. Malabo Convention and Budapest Convention across Africa (October 2022).

In August 2022, UN ECA and the Republic of Togo announced an agreement to jointly establish the African Center for Coordination and Research in Cybersecurity. The centre, to be based in Lomé, is intended as a regional hub for cybersecurity information and intelligence and to contribute to building capacities and frameworks at a national and regional level for assessing and mitigating cyberthreats.[186]

AU Peace and Security Council

Cybersecurity issues are also addressed by the AU Peace and Security Council (PSC). For instance, in May 2019, at a meeting on mitigating the threats of cybersecurity to peace and security in Africa, the PSC encouraged AU member states to 'enhance national, regional and continental harmonisation, among others, through harmonising and updating national cybersecurity strategies, cybersecurity emergency responses and policies'.[187] In August 2022, at a meeting on emerging technologies and new media, the PSC noted the importance of having the 'AU Commission and the member states develop a strategic approach to implement the UN norms on responsible state behaviour in cyberspace at regional and continental levels'.[188]

[185] Council of Europe [CoE]. (n.d.). *The Budapest Convention and its protocols*. https://www.coe.int/en/web/cybercrime/the-budapest-convention

[186] United Nations Economic Commission for Africa [UN ECA]. (2022, August 16). *Republic of Togo and the United Nations Economic Commission for Africa sign a memorandum of understanding to establish the African Cybersecurity Center.* https://www.uneca.org/stories/republic-of-togo-and-the-united-nations-economic-commission-for-africa-sign-a-memorandum-of

[187] African Union Peace and Security Council. (2019). *Communique: The 850th meeting of the AU Peace and Security Council on mitigating the threats of cybersecurity to peace and security in Africa*. https://www.peaceau.org/en/article/the-850th-meeting-of-the-au-peace-and-security-council-on-mitigating-the-threats-of-cyber-security-to-peace-and-security-in-africa

[188] African Union Peace and Security Council. (2022). *Communique of the 1097th meeting of the PSC held on 4 August 2022, on Emerging technologies and new media: impact on democratic governance, peace and security in Africa.* http://www.peaceau.org/en/article/communique-of-the-1097th-meeting-of-the-psc-held-on-4-august-2022-on-emerging-technologies-and-new-media-impact-on-democratic-governance-peace-and-security-in-africa

RECs have also initiated various cybersecurity-related policies and programmes. In 2021, ECOWAS adopted its *Regional Cybersecurity and Cybercrime Strategy*, outlining actions to be taken in particular at national level to strengthen cybersecurity and fight cybercrime (e.g. adoption of national cybersecurity strategies, establishing dedicated authorities, prioritising cybersecurity efforts in the area of critical infrastructures and essential services, enhancing cybersecurity skills development, and building capacity against cybercrime). When it comes to foreign policy issues, member states and the ECOWAS Commission are invited to promote and develop regional and international cooperation through actions such as sharing alerts and cybersecurity information (in particular between CERTs and similar institutions) and ensuring international judicial cooperation on cybercrime and transnational access to digital evidence.[189]

ECOWAS's *Regional Critical Infrastructure Protection Policy* proposes preventive, reactive, and proactive measures that countries could take to ensure the protection of their critical infrastructures and essential services. Noting that there are 'interdependencies between countries' in relation to telecommunication networks, internet connectivity, and other infrastructure and services, the policy calls on countries to cooperate in identifying transitional critical infrastructures and essential services, exchange information on threats and risks, and harmonise protection measures.[190]

ECOWAS also has a *Cybercrime Directive* (adopted in 2011); its objective is to ensure that the criminal law and criminal procedures of ECOWAS member states are adequately equipped to address cybercrime.[191]

EAC's *Model ICT Policy Framework* from 2015 encourages member states to establish mechanisms for regional and international cooperation on cybersecurity.[192]

Several RECs have adopted model laws and/or policies on cybercrime and cybersecurity. COMESA has a *Cyber Crime Model Bill* (2011),[193] as well as a model policy, a model bill, and an implementation roadmap for cybersecurity. ECCAS[194] has a model law on cybersecurity, while SADC has a *Model Law on Computer Crime and Cybercrime* (2012).[195]

Across the continent, cybersecurity and cybercrime issues are also addressed within several other settings:

- **AfricaCERT**. Focused on assisting African CERTs in improving cyber readiness and enhancing the resilience of ICT infrastructures, and fostering regional and international cooperation on related issues, the forum includes CERTs and CIRTs from 26 African countries; **Côte d'Ivoire**, **Ghana**, **Kenya**, **Nigeria**, **Rwanda**, and **South Africa** are among them.
- **African Union Mechanism for Police Cooperation** (AFRIPOL). Dedicated to fostering police cooperation at the continental level, AFRIPOL has among its objectives the development and implementation of a harmonised African approach to fight against cybercrime. To this aim, a strategy for the period 2020–2024 outlines four strategic priorities related to strengthening

189 Economic Community of West African States [ECOWAS]. (2021). *ECOWAS Regional Cybersecurity and Cybercrime Strategy*. https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf

190 Economic Community of West African States [ECOWAS]. (2021). *Regional Critical Infrastructure Protection Policy*. https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Critical-Infrastructure-Protection-Policy-EN.pdf

191 Economic Community of West African States [ECOWAS]. (2011). *Directive C/DIR.1/08/11 on Fighting Cyber Crime within ECOWAS*. http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf

192 East African Community [EAC]. (2015). *EAC Model ICT Policy Framework*. https://www.eaco.int/admin/docs/reports/Draft_Fodel_ICT_Policy_KGJ_March_2015.pdf

193 Common Market for Eastern and Southern Africa [COMESA]. (2011). *Cyber Crime Model Bill*. https://www.comesa.int/wp-content/uploads/2020/05/2011Gazette-Vol.-16.pdf

194 ECCAS member states: Angola, Burundi, Cameroon, Central African Republic, Chad, Democratic Republic of the Congo, Equatorial Guinea, Gabon, Republic of the Congo, and São Tomé and Príncipe.

195 Southern African Development Community [SADC]. (2012). *Model Law on Computer Crime and Cybercrime*. http://www.veritaszim.net/sites/veritas_d/files/SADC%20Model%20Law%20on%20Computer%20Crime%20and%20Cybercrime.pdf

the capacity of AFRIPOL's and member states' cybercrime teams, developing harmonious and coherent regulation, and ensuring constant threat assessment. The strategy also envisions the strengthening of cooperation frameworks at regional, continental, and international levels, participation in international bodies such as ITU and ICANN, and coordination on fighting cybercrime with bodies such as Interpol, the UN Office on Drugs and Crime (UNODC), and Europol.[196]

- **African Capacity Building Foundation (ACBF).** Advancing cybersecurity culture and skills and building capacities related to the development and implementation of cybersecurity policies are among the topics tackled by this AU specialised agency for capacity development.
- **Several civil society organisations** that work on raising awareness and building capacities on issues related to cybercrime, child online protection, and online safety and security. Examples include the Africa Cybersecurity and Digital Rights Organisation and the African Civil Society on the Information Society.

4.3. International engagement

Cybersecurity: UN GGE and OEWG

At the UN level, matters related to cybersecurity have been discussed within two groups of governmental experts, both falling under the First Committee of the UNGA.

The **UN Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (GGE)** (initially known as GGE on developments in the field of information and telecommunications in the context of international security) was convened six times: 2004–2005, 2009–2010, 2012–2013, 2014–2015, 2016–2017, and 2019–2021. The UN GGE can be credited with two major achievements: outlining the global agenda and introducing the principle that international law applies to digital space.[197] Eight African countries participated in GGE work over the years: Egypt in GGE 2012–2013, GGE 2014–2015, and GGE 2016-2017; **Ghana** in GGE 2014–2015; **Kenya** in GGE 2014–2015, GGE 2016–2017, and GGE 2019–2021; Mali in GGE 2004–2005; Mauritius in GGE 2019–2021; Morocco in GGE 2019–2021; **Senegal** in GGE 2016–2017, and **South Africa** in GGE 2004–2005, GGE 2009–2010, and GGE 2019–2021.

In 2018, the UNGA established an **Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security** (later renamed OEWG on security of and in the use of information and communications technologies), tasked with continuing to develop the rules, norms, and principles of responsible behaviour of states, discussing ways for their implementation, and studying the possibility of establishing regular institutional dialogue with broad participation under the auspices of the UN. Unlike the GGE, which was composed on the basis of 'equitable geographical distribution', the OEWG is open in the sense that all interested UN members can participate in its activities. The first OEWG concluded its work in March 2021 and was followed by a new OEWG for the period 2021–2025.

With the GGE concluded, we focus here on contributions to OEWG work.

[196] African Union Mechanism for Police Cooperation [AFRIPOL] (n.d.). *AFRIPOL Cybercrime Strategy.* https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/1680a30050

[197] Geneva Internet Platform [GIP]. (n.d.). *UN OEWG and GGE*. Digital Watch observatory. https://dig.watch/processes/un-gge

In the **OEWG 2019–2021**, 16 African countries participated: Algeria, Botswana, Cameroon, Côte D'Ivoire, Egypt, Ethiopia, Ghana, Kenya, Malawi, Mauritius, Morocco, Mozambique, Nigeria, South Africa, Uganda, Zimbabwe. These 16 countries made 69 interventions (out of 719 interventions). Out of the eight focus countries, the following have contributed to OEWG work: **Côte d'Ivoire, Ghana, Kenya, Nigeria,** and **South Africa**. These 5 countries made 27 interventions (out of 719 interventions). What follows is an overview of their positions/main interests.[198]

In discussions on **norms, rules, and principles, Ghana** and **Kenya** called for greater awareness, operationalisation, and implementation of the existing norms incorporated in the 2015 GGE report.

On **international law**, **Kenya** pointed out the need to clarify how these laws can be invoked and applied in relation to cyberthreats, including attribution challenges in cyberwarfare and proxy situations, as well as in the context of autonomous, automated, and AI cyber actors. According to Kenya, the interpretation and application of international law must be consistent and should not discriminate along the digital divide.

Ghana called for the establishment of a global repository of existing confidence-building efforts at regional and sub-regional levels, and of a global list of points of contact. The country suggested that the OEWG should become a repository for concrete and practical **confidence-building measures (CBMs)** on an effective response to threats to critical information infrastructures, and to reduce the risk of misperception and possible conflict and maintain a safe and secure cyberspace. It further suggested that national points of contact of focal institutions and networks should be created under the OEWG. **Kenya** similarly underlined that capacity building is a key CBM. CBMs cannot have the intended results if some countries lack the capability to detect, identify, investigate, defend, contain, or counter existing and potential cyberthreats.

When it comes to **capacity building, Ghana** noted that many developing countries lack enough capacity in cybersecurity, cybercrime, data protection and development, international security and cyber hygiene practices, incident response, and the overall protection of critical information infrastructure. However, the risks and challenges of cyberattacks are not confined to one country, group, or region. **Kenya** stressed the need for an evidence-based approach and metrics to ensure the effectiveness of capacity building initiatives and mentioned bridging the digital divide as a principle of capacity building and its primary task. According to Kenya, the UN is uniquely positioned to coordinate capacity building at a global level. The UN could start with initial coordination steps, such as creating a registry of existing capacity building measures and their contact points, and available lessons learned. This registry should then be used to determine a baseline for the measurement of the minimum cybersecurity level necessary for global security and allow countries to perform self-assessments.

In discussions on **regular institutional dialogue, Ghana** noted that the OEWG can best serve as a global platform to promote dialogue and exchanges of best practices, awareness raising, facilitate cooperation and consultation among states, and provide information on capacity building in cyberspace, which are essential constituents of CBMs. Ghana suggested that the OEWG become the repository of CBMs and points of contact.

In a joint contribution to OEWG work, the African Group reiterated support for the establishment of an action-oriented mechanism under the UN to promote the responsible use of ICTs by states, as well as for the development and implementation of norms and rules to govern global cyberspace. The group also highlighted its hope that the OEWG process would lead to the emergence of a legally binding and rules-based order regulating the use of ICT by spaces.

In the **OEWG 2021–2025**, 20 African countries have participated up to July 2022: Algeria, Botswana, Cameroon, Côte d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Ethiopia, Ghana,

[198] This overview is based on OEWG session reports produced by a team of GIP rapporteurs and transcripts produced by Diplo's AI and Data Lab.

Kenya, Malawi, Mauritius, Morocco, Nigeria, Senegal, Sierra Leone, South Africa, Tanzania, Togo, Uganda. These 20 countries made 79 interventions out of 894 interventions made at the OEWG 2021–2025 to date. Out of the eight focus countries, the following have contributed to OEWG work: **Côte d'Ivoire, Ghana, Kenya, Nigeria,** and **South Africa.** These five countries made 34 interventions out of 894 interventions made at the OEWG 2021–2025 so far. What follows is an overview of their positions/main interests.[199]

On matters related to **norms, rules, and principles, South Africa** agreed that the previous UN GGE and OEWG reports, including corresponding UNGA resolutions adopted by consensus, build an aquis for further discussions on the position, role, and implementation of the voluntary norms. South Africa would like the states to exchange their views on the need for further development of norms through evaluating, updating, and refinement of the existing non-binding norms, rules, and principles of state behaviour in cyberspace. South Africa also supports the use of the national survey of implementation of norms as proposed by Australia, Mexico, and other countries.[200]

Kenya suggested the creation of a working group to facilitate the sharing of best practices on how existing norms, rules, and principles can be contextualised and translated into national policies.

Nigeria underlined the need for legalising the already agreed-upon norms in order to ensure responsible behaviour. **Côte d'Ivoire** stressed that the application of optional and non-binding norms of responsible behaviour of state could contribute to increasing the safety and security of the use of ICTs and help prevent harmful uses of ICTs.

In discussions on **international law**, **Kenya** noted that it is important to consider how the normative framework will be effectively applied in future. The country called for additional efforts towards capacity building in the areas of international law and national legislation and policy in order to enable states to enhance the applicability of international law to the use of ICTs within their specific context.

South Africa noted that existing international law complemented by voluntary non-binding norms is sufficient for addressing issues related to state use of ICTs in the context of international peace and security. The country also suggested that the question of sharing national positions and exploring how international law applies in cyberspace should be referred to the International Court of Justice and the International Law Commission to establish their views on the matter.

Senegal stressed that all principles of international humanitarian law should apply to cyber-operations conducted in armed conflicts.

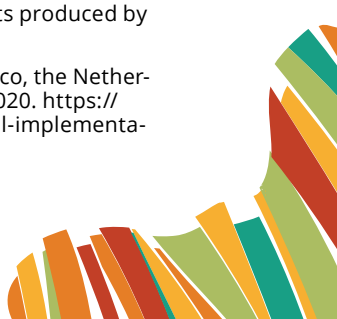
Côte d'Ivoire underlined the applicability of international law in cyberspace, including the UN Charter, international humanitarian law, and international human rights law.

Ghana highlighted that international cooperation and **CBMs** in the field of ICT are key to maintaining stability in cyberspace and achieving sustainable development. **Côte d'Ivoire** was in favour of appointing a national contact point to facilitate communication and exchange of information. On the issue of national points of contacts, **Senegal** called for consideration of the fact that some countries face difficulties in setting up such structures.

Kenya stressed that CBMs need to be inclusive of all relevant stakeholders involved in cyberspace, as a way to facilitate collaboration between state and non-state actors in devising and implementing strategies and policies to address challenges encountered in cyberspace.

[199] This overview is based on OEWG session reports produced by a team of GIP rapporteurs and transcripts produced by Diplo's AI and Data Lab.

[200] Joint Proposal by Argentina, Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member states, Poland, and South Africa to OEWG, 16 April 2020. https://www.internationalcybertech.gov.au/sites/default/files/2020-12/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf



According to **South Africa**, raising the general level of states' ICT capacities would also raise their overall resilience to cyberthreats. South Africa called for the OEWG to discuss appropriate institutional arrangement and special programmes for **capacity-building**. The country also suggested that the OEWG is used to achieve a common understanding of existing and potential threats in cyberspace, and to share practices and measures to combat them. **Côte d'Ivoire** underlined the importance of implementation of capacity building mechanisms for countries with assistance needs so they can address their vulnerabilities and guarantee safe use of digital technology.

Kenya drew attention to the important role that regional and sub-regional organisations (could) play in promoting responsible state behaviour and conducting related capacity building programmes. Both **Kenya** and **South Africa** made reference to the role of these organisations in supporting the implementation of norms of responsible behaviour.

In a contribution to OEWG's July 2022 session, the AU Cybersecurity Expert Group highlighted priority areas where capacity building is needed for Africa: governance, policymaking, technical tools and infrastructures, digital access, and research. The group noted that African actors need 'greater capacity' to be able to contribute effectively to UN processes such as the OEWG and other global cybersecurity initiatives. It also called for Africa not to be excluded from cybersecurity confidence-building initiatives.[201]

Cybercrime: UN Ad Hoc Committee

In 2019, the UNGA established the open-ended **Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes,** under the auspices of the Third Committee. The Ad Hoc Committee was proposed by the Russian Federation and 27 co-sponsors; among them there were 9 African countries: Algeria, Angola, Burundi, Egypt, Eritrea, Libya, Madagascar, Sudan, and Zimbabwe.[202]

After two sessions on organisational matters held in May 2021 and February 2022, the committee held three substantive sessions between February and September 2022. Nineteen African countries participated: Algeria, Angola, Burkina Faso, Burundi, Cameroon, Egypt, Eritrea, Ghana, Kenya, Madagascar, Mali, Morocco, Namibia, Niger, Nigeria, Senegal, Sierra Leone, South Africa, and Tanzania.

Of the eight focus countries, the following have contributed to the committee's work: **Ghana**, **Kenya**, **Namibia**, **Nigeria**, **Senegal**, and **South Africa**. What follows is an overview of some of their positions/main interests.[203]

Joint contributions by the African Group highlighted, among other issues, the need for the convention to have strong provisions on **international cooperation** and ensure that these provisions are aligned with existing international instruments. Individual countries, including **Kenya**, **Nigeria**, and **Senegal**, noted that **existing international and regional instruments** – such as the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the Malabo Convention, and the Budapest Convention – could be used as tools to assist in the development of the draft convention. **South Africa** further added that complementarity would need to be ensured between the new convention and other relevant instruments, while

[201] African Union Cybersecurity Experts Group. (2022). *Input on the occasion of the third substantive session of the Open-ended Working Groups on ICTs (OEWG) - 25 to 29 July 2022 at the United Nations Headquarters in New York.* https://documents.unoda.org/wp-content/uploads/2022/07/African-Union.pdf

[202] United Nations General Assembly [UNGA]. (2019). *Draft resolution on countering the use of information and communications technologies for criminal purposes*. https://digitallibrary.un.org/record/3835168?ln=en

[203] Identified based on written contributions and transcripts of discussions held during the committee's first three substantive sessions. The transcripts – where meeting recordings were available – were produced by Diplo's AI and Data Lab.

Ghana suggested that the convention should include provisions defining its relationship with other treaties, agreement, and arrangements.

One of the key questions in negotiations is **whether the convention should create new categories of cybercrime offences**, with states submitting their national positions on this issue and suggesting what new cybercrime offences can be added.

South Africa proposed the following criminal offences to be included in the convention:

- Offences against confidentiality, integrity, and availability of information systems (e.g. illegal access).
- Illegal interception of data.
- Illegal data interference.
- Illegal system interference.
- Cyberthreats.
- Fraud cyber forgery.
- Production and distribution of child abuse content.

For **Ghana**, some of the specific issues that the convention should tackle include:

- Conduct against confidentiality, integrity, and availability of computer systems.
- Cyber dependence crimes (such as hacking).
- Crimes against national information and infrastructure.
- Cyber enabled crimes against children, and online gender-based crimes such as revenge pornography.

Nigeria stated that the convention should also define substantive criminal law provisions with an emphasis on the cyber-enabled crimes, such as, among others:

- Cyber fraud forgery.
- Cyberbullying.
- Stalking.
- Online child sexual exploitation.

The African Group noted that **human rights** and principles of sovereignty and reciprocity should always be respected. This point was reinforced in contributions from individual states.

Kenya suggested that countries make commitments towards upholding international law and treaties on human rights, and ensure that such commitments are followed by action. **Nigeria** noted that data protection safeguards need to be provided for in the convention, whereas **South Africa** argued that requirements for protection of personal data and privacy are embedded in national law, and the convention should not duplicate this. **Senegal** called for express provisions to be included in the convention to ensure that international cooperation instruments respect individual rights and freedoms. A similar point was raised by **Ghana**, which noted that provisions are needed to establish appropriate conditions and safeguards to ensure the adequate protection of human rights and fundamental freedoms.

South Africa indicated that it does not support the inclusion of a specific provision on international cooperation for carrying out electronic surveillance and covert investigations techniques, as those are best to be left to domestic laws. **Namibia** had an opposing view, being in favour of such a provision.

Several countries reiterated the point made in contributions by the overall African Group that the convention should strengthen international cooperation and facilitate mutual legal assistance when it comes to combatting and prosecuting crimes across jurisdictions. Other **provisions on international cooperation** could cover issues such as law enforcement cooperation, joint investigations, confiscation, return and disposal of assets, as well as cooperation with service

providers (including across borders) (**Ghana**, **Kenya**, **Namibia**, **Nigeria**, **South Africa**, and **Senegal**). **Senegal** further suggested that it could be useful to create a mechanism for joint investigative teams.

Ghana, **Kenya**, **Namibia**, **Nigeria**, and **South Africa** noted that the convention should include a provision that establishes a 24/7 network of points of contacts to facilitate immediate assistance for investigations, proceedings, or the collection of evidence. **Nigeria** further noted that it would be useful to encourage synergies between such a network and existing networks.

The African Group noted that **building capacity** is a prerequisite to fighting cybercrime, and the convention should create a framework that enables the provision of long-term capacity building and training programmes to strengthen national capacities to detect and investigate cybercrime. The group also underscored the importance of predictable and stable funding for technical assistance for developing countries, and the need for an efficient utilisation of such resources to ensure sustainability in the implementation of the future convention. Individual countries listed several areas of capacity development, including (but not limited to) data collection, exchange of information, investigation techniques, law enforcement, and protection of human rights.

Kenya noted that the convention could make reference to cybercrime and cybersecurity-related education and awareness campaigns being collaboratively conducted by states party to the convention. **Senegal** pointed out that technical assistance and capacity building efforts should be guided by the principles of state sovereignty, confidence, transparency, and good governance. **South Africa** and **Nigeria** added that such capacity building and technical assistance should be demand-driven, context-specific, and tailor-made to meet the evolving needs of developing countries. **Ghana** proposed that a provision be included regarding the establishment of a conference of parties to be responsible for the development of mechanisms to improve the capacities of countries to counter the use of ICTs for criminal purposes. Such a conference of parties should tap into the expertise of civil society organisations, academia, and the private sector.

Kenya, **Senegal** and **South Africa** noted that the **private sector and civil society** are/could be important contributors to capacity building and resource mobilisation efforts. **South Africa** further pointed out that the ICT industry has insights that can be used to identify and analyse malicious activities. **Nigeria** stated that the convention should include flexible language encouraging member states to adopt whole-of-society approaches enabling public-private partnerships in tackling cybercrime.

Child online protection

When it comes to engagement in international forums on issues related to child online protection, 20 African countries participate in the multistakeholder WeProtect Global Alliance to develop policies and solutions to protect children from sexual exploitation and abuse online. These are Angola, Burundi, Central African Republic, Ethiopia, **Ghana**, Guinea, **Kenya**, Lesotho, Malawi, **Namibia**, **Nigeria**, **Rwanda**, **Senegal**, Sierra Leone, **South Africa**, Sudan, Tanzania, Uganda, Zambia, and Zimbabwe. The AU, as well as several NGOs based in Africa, are also part of the alliance.

In addition, between 2019 and 2022, **Nigeria** held a vice-chair position within the ITU Council Working Group on Child Online Protection. The group – which is open for participation to all ITU member states and Sector members – serves as a platform to discuss risks and vulnerabilities facing children and youth in cyberspace, provide recommendations, and seek to propose mechanisms for creating synergies among national, regional, and international efforts in this field.

International multistakeholder processes

Besides governmental involvement in UN processes, there is also some participation from Africa in multistakeholder processes and initiatives such as the GFCE and the Paris Call.

At the **GFCE**, established in 2015 to 'strengthen cyber capacity building and coordinate existing international efforts more effectively',[204] 20 African governments are members: Benin, Botswana, Cameroon, **Côte d'Ivoire**, Ethiopia, Gabon, Gambia, **Ghana**, **Kenya**, Lesotho, Liberia, Mauritius, Morocco, **Nigeria**, Republic of the Congo, **Rwanda**, **Senegal**, Somalia, Tanzania, and Tunisia.

Regional and continental organisations – including the AU, AUDA-NEPAD, AFRIPOL, ECCAS, ECOWAS – are also GFCE members. In addition, several civil society groups and technical organisations from across Africa contribute to GFCE work as partners; among them are African Civil Society on the Information Society, African Capacity Building Foundation, AfricaCERT, Africa Cybersecurity Resource Centre, Africa Cybersecurity and Digital Rights Organisation, AFRINIC, the Cybersecurity Capacity Centre for Southern Africa, Registry Africa Ltd, the West and Central African Research and Education Network, and .ZA Central Registry.

The Paris Call for Trust and Security in Cyberspace, launched in 2018, brings together state and non-state actors in a commitment to working together to adopt responsible behaviour and implement within cyberspace a series of key principles: protect individuals and infrastructure, protect the internet, defend electoral processes, defend intellectual property, non-proliferation of malicious software and practices intended to cause harm, lifecycle security, cyber hygiene, no private hack back, and promote international norms.[205] Eleven African governments and several other stakeholders from across the region had joined the call by August 2022 (Figure 39).

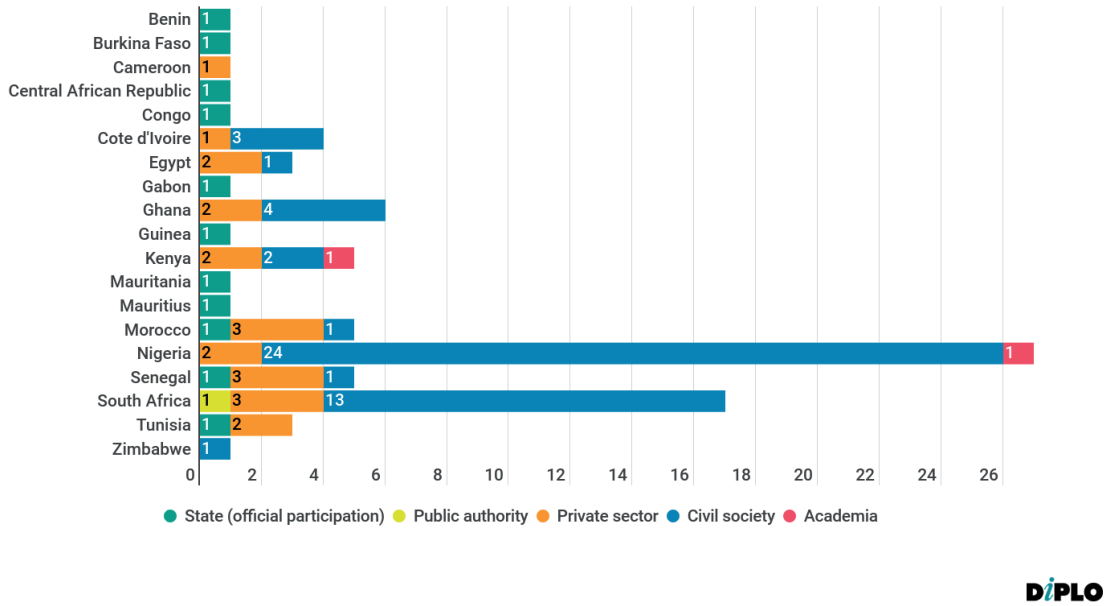


Figure 39. Supporters of Paris Call (August 2022).

[204] Global Forum on Cyber Expertise [GFCE]. (n.d.). *About the GFCE*. https://thegfce.org/about-the-gfce/

[205] Paris Call. (n.d.). *The 9 principles*. https://pariscall.international/en/principles

Strengthening cyber capacities

Several initiatives launched or supported by international partners focus on strengthening the cyber capacities of governments and other stakeholders across Africa. Examples include:

- **Africa Joint Operation against Cybercrime.** Funded by the UK (the Foreign, Commonwealth and Development Office) and implemented through Interpol's Africa Cybercrime Operation Desk, the project aims to drive coordinated actions against cybercrime in African countries.[206]
- **Enabling African countries to identify and address their cyber capacity needs.** A collaboration between the GFCE and the AUC, the project is dedicated to enabling African countries to prioritise and address their cyber capacity needs and fostering coordination between cyber capacity building efforts in Africa. The project is supported by the Bill & Melinda Gates Foundation.[207]
- **Global Action on Cybercrime Extended (GLACY+).** A joint initiative of the CoE and the EU, GLACY+ aims to strengthen the capacities of priority countries to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation. The project targets the following African countries: Benin, Burkina Faso, Cabo Verde, **Ghana**, Mauritius, Morocco, **Nigeria**, and **Senegal**.[208]
- **Cyber4Dev**. Funded by the EU, the project aims to strengthen cybersecurity policy and coordination frameworks, increase cybersecurity incident response capabilities, and foster networks of cyber expertise and cooperation. Botswana, Mauritius, and **Rwanda** are among the priority countries. Training has also been delivered in Gambia, Malawi, Mozambique, Republic of the Congo, and Seychelles.[209] In 2022, Cyber4Dev organised the African Cyber Resilience Conference, hosted by Mauritius (as the Cyber4Dev hub for Africa).[210]

[206] Interpol. (n.d.). *AFJOC – African Joint Operation against Cybercrime*. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

[207] Global Forum on Cyber Expertise [GFCE]. (2021). *AUC-GFCE Collaboration: Enabling African countries to identify and address their cyber capacity needs*. https://thegfce.org/auc-gfce-collaboration-enabling-african-countries-to-identify-and-address-their-cyber-capacity-needs/

[208] Council of Europe [CoE]. (n.d.). *Global Action on Cybercrime Extended (GLACY+)*. https://www.coe.int/en/web/cybercrime/glacyplus

[209] Cyber4Dev. (n.d.). *Project objectives*. https://cyber4dev.eu/project-activities/

[210] Cyber4Dev. (2022, May 2). *African Cyber Resilience Conference brings delegates from partner countries to Mauritius*. https://cyber4dev.eu/2022/05/02/african-cyber-resilience-conference-brings-delegates-from-partner-countries-to-mauritius

5. Digital economy

Section summary

Africa's digital economy is on a growing trend. This is a result of a combination of factors, from improved internet access and the presence of vibrant startup ecosystems to improvements in policy frameworks.

But there are disparities between countries. For instance, when it comes to e-commerce readiness, South Africa scored 56.5 points in UNCTAD's 2020 index, compared to only 5.6 for Niger. And the speed at which governments have adopted laws, policies, and regulations to foster the advancement of digital economies, as well as the focus of these frameworks, varies significantly. Only 28 African countries have consumer protection laws in place (although these are essential in fostering consumers' trust in e-commerce), while 33 have adopted e-transaction laws. Various types of digital service taxes have been introduced in recent years in several countries (e.g. Kenya, Nigeria, South Africa, Uganda).

There are also variations in policy and regulatory frameworks dealing with data flows. Some countries have introduced certain data localisation requirements or restrictions for the cross-border flow of data for either data protection or economic purposes. Rwanda, for instance, places the concept of data sovereignty at the core of its *National Data Revolution Policy*, noting that the country should retain 'exclusive sovereign rights on national data'. Nigeria has a set of guidelines according to which government data and consumer data held by telecom companies may not be transferred outside the country.

One policy area where some governments seem to be working towards a shared goal – advancing financial inclusion – is that related to digital payments and financial services. Ghana has several policies dedicated to fostering financial inclusion and creating a resilient and inclusive digital payments ecosystem while ensuring alignment with international standards and principles. Similar goals are also reflected in Kenya's payments strategy. AU's *Digital Transformation Strategy* also tackles issues related to digital financial services (DFS), calling for the harmonisation of rules, the interoperability of national projects, and the creation of a single African payments area.

Remarkable within the region is the adoption rate for cryptocurrencies and crypto assets. The 2022 Global Crypto Adoption Index placed Nigeria, Morocco, and Kenya among the top 20 countries worldwide by cryptocurrency adoption. Africa is becoming increasingly attractive for crypto companies, while the region's own companies are aiming to expand their presence in international markets. Regulatory initiatives are also taking off: Nigeria, for instance, requires digital assets offerings and custodians to register, while South Africa is looking into bringing crypto assets into the regulatory remit. And while countries such as Angola, Ghana, Botswana, Egypt, and Guinea have issued warnings outlining risks associated with cryptocurrency trading, the Central African Republic became the second country in the world to accept bitcoin and other cryptocurrencies as legal tender. Another notable development within the region relates to central bank digital currencies: Nigeria was the first African country to launch such a currency (eNaira), while Egypt, Ghana, Kenya, South Africa, Tunisia and several other African countries are exploring such options.

At the continental level, the most significant policy development has been the agreement on the African Continental Free Trade Area, expected to unleash the potential of a large single (digital) market. The RECs also have various policies and initiatives related to e-commerce and trade, including in the form of model laws aimed at harmonising national policies.

When it comes to engagement in international processes, seven African countries (Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Kenya, Mauritius, and Nigeria) participate in the Joint Statement Initiative (JSI) on e-commerce at the World Trade Organization (WTO). Here Nigeria has tabled a proposal on data flows, while Côte d'Ivoire advanced two proposals to enhance cooperation in e-commerce. On matters of taxation, 25 African countries joined the OECD-led agreement on new global corporate tax rules. Notably absent are Kenya and Nigeria, both of which have some forms of digital services tax in place. African countries joined other developing nations in the Group of 77 in putting forward a proposal for a UN resolution (adopted in December 2021), which 'recognises the importance of the consideration of international tax issues at the United Nations'.

5.1. State of the African digital economy

In 2012, Africa's digital economy was estimated at roughly 1.1%, or US$30 billion of its GDP.[211] In 2020, estimates indicated a contribution of 4.5%, or US$115 billion. This growth is expected to continue in the coming years. A 2020 study by Google and the International Finance Corporation (IFC) found that the digital economy could contribute US$180 billion (5.2%) to the continent's GDP by 2025, and US$712 (8.5%) billion by 2050 (Table 12). Reasons behind this estimated growth include better quality internet connectivity and improved access, vibrant startup ecosystems, growing tech talent pools, and improvements in policy and regulatory frameworks (including the launch of the African Continental Free Trade Area).[212]

Table 12. Contribution of the internet economy to African GDP (iGDP).[213]

Year	iGDP (billions)	iGDP as % of GDP	GDP (billions)
2019	US$100	3.9%	US$2,580
2020	US$115	4.5%	US$2,554
2025	US$180	5.2%	US$3,446
2050	US$712	8.5%	US$8,342

Some countries are on an especially rapid trajectory (Table 13). For example, by 2025, the share of the economy powered by the internet in **Kenya**, Morocco, **Senegal**, and **South Africa** will be between 7% and 9%.[214]

Table 13. Contribution of the internet economy to African GDP (iGDP) in some selected countries.[215]

Country	2020 (US$B)	2020 (%)	2025 (US$B)	2025 (%)	2050 (US$B)	2050 (%)
Kenya	7.42	7.70%	12.84	9.24%	51.07	15.17%
Morocco	7.80	6.82%	12.09	7.84%	48.06	12.88%
South Africa	21.55	6.51%	31.45	7.86%	125.08	12.92%
Senegal	1.51	6.22%	2.92	7.11%	11.61	11.68%
Nigeria	24.59	5.68%	36.53	6.86%	145.28	11.27%
Algeria	9.02	5.60%	11.92	6.16%	47.39	10.12%
Cameroon	2.06	5.39%	3.27	6.19%	13.00	10.16%
Côte d'Ivoire	3.18	5.27%	5.53	6.04%	21.98	9.92%
Egypt	15.41	4.98%	25.97	5.99%	103.29	9.83%
Rwanda	0.52	4.98%	0.97	5.96%	3.85	9.79%
Ghana	3.01	4.42%	5.01	5.31%	19.94	8.73%

[211] Kende, M. (2017). *Promoting the African Internet Economy.* https://www.internetsociety.org/wp-content/uploads/2017/11/AfricaInternetEconomy_111517.pdf

[212] Google and the International Finance Corporation [IFC]. (2020). *e-Conomy Africa 2020. Africa's $180 billion Internet economy future.* https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2

[213] GGoogle and the International Finance Corporation [IFC]. (2020). *e-Conomy Africa 2020. Africa's $180 billion Internet economy future.* https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2

[214] Accenture. (2022). *Tuning into Africa's digital transformation.* https://www.accenture.com/us-en/insights/software-platforms/africa-digital-transformation

[215] Google and the International Finance Corporation [IFC]. (2020). *e-Conomy Africa 2020. Africa's $180 billion Internet economy future.* https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2

Tanzania	2.57	3.98%	4.28	4.57%	17.03	7.50%
Uganda	1.36	3.82%	2.26	4.18%	8.97	6.87%
Mozambique	0.37	2.45%	0.67	2.81%	2.65	4.62%
Angola	2.02	2.17%	2.88	2.38%	11.44	3.91%
Ethiopia	1.26	1.27%	2.02	1.39%	8.03	2.28%
Rest of Africa	11.62	1.96%	18.55	2.16%	73.76	3.54%
Total	115	4.5%	180	5.2%	172	8.5%

E-commerce, fintech, healthtech, and media and entertainment are among the sectors that drive the growth of Africa's digital economy and the continent's overall digital transformation.[216]

The **e-commerce** picture across Africa is one full of contradictions. On the one hand, the e-commerce industry has grown considerably in the past decade, due to a combination of factors, such as growing internet penetration rates, the spread of mobile telephony and mobile money services, and increased use of credit cards and access to bank accounts. On the other hand, the average index of e-commerce readiness of African countries is still low compared to other developing regions and developed countries (Table 14).

Table 14. Regional values for the UNCTAD B2C E-commerce Index, 2020.[217]

Régions/économies	Valeur de l'indice 2020
Africa	30
East, South & Southeast Asia	57
Latina America and the Caribbean	49
Western Asia	58
Transition economies	62
Developed economies	86
World	55

There is also a significant disparity among countries when it comes to their participation in e-commerce. Table 15 provides a list of the top 10 developing countries and transition economies in the UNCTAD B2C E-commerce Index by region, showing the countries that have scored the highest in Africa in 2020. Within the overall index, the African countries that score the highest are Mauritius (58.4), **South Africa** (56.5), Tunisia (54.6), Algeria (52.2), and **Ghana** (51.9), while Burundi (8.3), Chad (7.1), and Niger (5.6) have the lowest scores.

[216] Google and the International Finance Corporation [IFC]. (2020). *e-Conomy Africa 2020. Africa's $180 billion Internet economy future.* https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2

[217] United Nations Conference on Trade and Development [UNCTAD]. (2021). *The UNCTAD B2C E-commerce Index 2020.* https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf. The index measures the readiness of countries to engage in online commerce. It is a composite indicator including four indicators: internet use penetration, secure servers per 1 million inhabitants, credit card penetration, and a postal reliability score.

Table 15. Top 10 developing and transition economies in the UNCTAD B2C E-commerce Index 2020, by region.[218]

Asie de l'Est, du Sud et du Sud-Est	Asie occidentale	Afrique	Amérique latine et Caraïbes	Économies en transition
Singapore	UAE	Mauritius	Costa Rica	Belarus
China, Hong Kong SAR	Saudi Arabia	South Africa	Chile	Russian Federation
Korea, Republic of		Tunisia	Brazil	Serbia
Malaysia	Qatar	Algeria	Dominican Republic	Georgia
Thailand	Oman	Ghana	Colombia	Ukraine
Iran (Islamic Republic of)	Turkey	Libya	Uruguay	North Macedonia
China	Kuwait	Kenya	Jamaica	Republic of Moldova
Mongolia	Lebanon	Nigeria	Trinidad and Tobago	Kazakhstan
Viet Nam	Bahrain	Morocco	Peru	Azerbaijan
India	Jordan	Senegal	Argentina	Bosnia and Herzegovina
	Iraq			

In 2020, Africa had over 600 unique business-to-consumer online marketplaces for physical goods. Only 10 marketplaces attracted 84% of the overall web traffic to such platforms. The top 10 countries with the largest number of marketplaces were **South Africa**, Morocco, Tunisia, Egypt, Algeria, **Kenya**, **Senegal**, **Nigeria**, **Ghana**, and **Côte d'Ivoire**. Most marketplaces were not open to sellers from foreign countries: Only 20% of the marketplaces were operating in multiple African countries or worldwide, but they represented almost 75% of all marketplace websites in Africa.[219]

There are several challenges for African countries to take advantage of e-commerce. These can be found across three layers: a) the digital society considered broadly, which encompasses challenges related to access to infrastructure, cybersecurity, and capacity development on digital issues, for example; b) the digital economy, which depends on the provision of services, such as electronic payments, digital signatures, and cloud computing; c) e-commerce more specifically, which encompasses issues related to trade facilitation, access to markets, and the observance of basic principles, such as transparency and non-discrimination (Figure 40).

The regulatory framework also shows some important gaps at the national and regional levels. The speed with which African governments have adopted laws, policies, and regulations to foster e-commerce and the advancement of the digital economy varies significantly.[220]

[218] United Nations Conference on Trade and Development [UNCTAD]. (2021). *The UNCTAD B2C E-commerce Index 2020.* https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf

[219] International Trade Centre [ITC]. (2021). *African Marketplace Explorer*. https://ecomconnect.org/page/african-market-place-explorer

[220] United Nations Conference on Trade and Development [UNCTAD]. (2020). *Member States of the WAEMU eTrade Readiness Assessment*. https://unctad.org/system/files/official-document/dtlstict2020d10_en.pdf

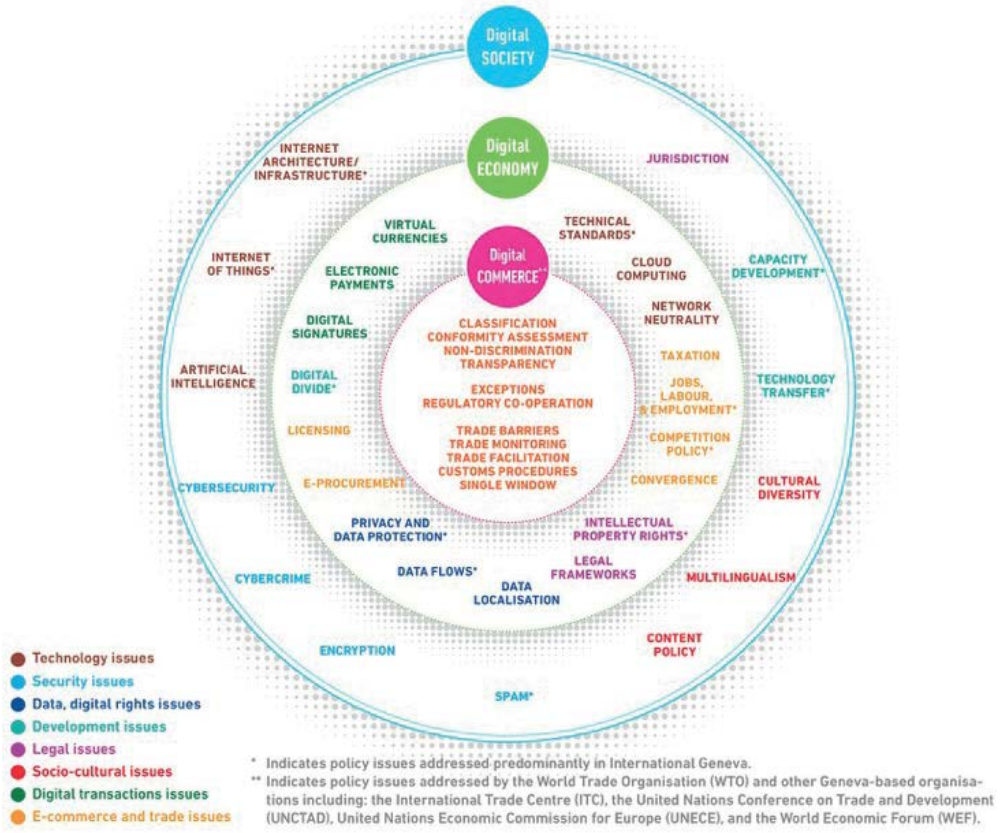


Figure 40. The interplay between e-commerce issues and wider digital policy issues.

Support from international organisations and development cooperation bodies

The support of international organisations and development cooperation bodies has been important for the continent's digital transformation. For example, the ECOWAS e-commerce strategy is being developed with the support of UNCTAD's E-commerce and Digital Economy Programme, with funds from the government of the Netherlands. The German Federal Ministry for Economic Cooperation and Development has supported the development of the e-commerce strategy for the EAC, by means of the Pan-African e-Commerce Initiative.[221]

International support has also been relevant to the development of frameworks at the national level. For example, the World Bank has sponsored the e-Transform project, which has assisted **Ghana** with digitising its economy, especially e-government service delivery, e-commerce and e-payments. This initiative is being undertaken to promote efficiency in areas such as education, health, and judicial and parliamentary services, through the use of ICTs.

Digitalisation is at the forefront of the EU's geopolitical strategy towards Africa, as a way to promote sustainable development and economic growth. This has been reflected in development cooperation efforts and in the intervention of international financial institutions throughout the years. More recently, in February 2022, the EU announced a plan to invest up to €150 billion in Africa over the next seven years, in five priority areas, including accelerating the digital transition.

The European Investment Bank (EIB) has been providing overall support to Africa's transition to a digital economy, articulating around six complementary areas of intervention: universal access to affordable connectivity, digital services, financial inclusion, entrepreneurship, cybersecurity and green power alternatives.[222]

[221] German Cooperation. (n.d.). *Pan-African e-Commerce Initiative*. https://www.eacgermany.org/storage/app/uploads/public/609/d22/91b/609d2291bd91d576209309.pdf

[222] European Investment Bank [EIB]. (2021). *The rise of Africa's digital economy. The European Investment Bank's activities to support Africa's transition to a digital economy.* https://www.eib.org/attachments/thematic/study_the_rise_of_africa_s_digital_economy_en.pdf

5.2. National policy and regulatory frameworks and foreign policy elements

E-commerce, e-transactions, and consumer protection

Growing consensus is emerging on the need to adopt **e-commerce-enhancing policies** in the context of national development strategies and plans. The existence of e-commerce strategies has been deemed particularly relevant, not only because they help to articulate the application of other norms in the specific context of online trade, but also because they provide strategic vision, which may help to enhance governmental coordination. In some cases, the process leading to the formulation of a national e-commerce strategy has been instrumental to fostering greater public-private cooperation and coordination.[223] National e-commerce strategies also provide a useful blueprint for diplomats engaging in international negotiations or seeking to establish international cooperation in areas related to e-commerce.

The first sketches of e-commerce policy in the African continent find their roots in national plans for the development of the digital economy. For example, in 2016 **Côte d'Ivoire** expressed the desire to promote the development of the digital economy and e-commerce through its *2016–2020 National Development Plan*.[224] **Kenya**'s *Digital Economy Blueprint* outlines the need for e-commerce to expand beyond national boundaries and posits that integrating Africa into a single digital market will create economies of scale and opportunities to grow the local and regional economies. Furthermore, one of the measures proposed in the country's *National ICT Policy* is to support the growth of local e-commerce platforms with global reach.

Senegal has outlined goals related to promoting e-commerce and DFS in its *Digital Senegal Strategy* – the national strategy for the digital economy. The government also adopted a *National Strategy for the Development of E-commerce*, in 2019.

Across African countries, there is a strong demand on the part of online buyers and vendors for more tailored laws and regulations that would provide greater protection for online operations. Despite this, only 28 countries in Africa (or 52%) had **consumer protection laws** in place at the end of 2021 (Figure 41).

[223] United Nations Conference on Trade and Development [UNCTAD]. (2020). *Fast-tracking implementation of eTrade Readiness Assessments*. https://unctad.org/system/files/official-document/dtlstict2020d9_en.pdf

[224] Republic of Côte d'Ivoire. (2016). *Plan National de Développement (National Development Plan).* https://scorecard.prb.org/wp-content/uploads/2018/05/Plan-National-de-Développement-2016-2020.-Côte-d'Ivoire.pdf

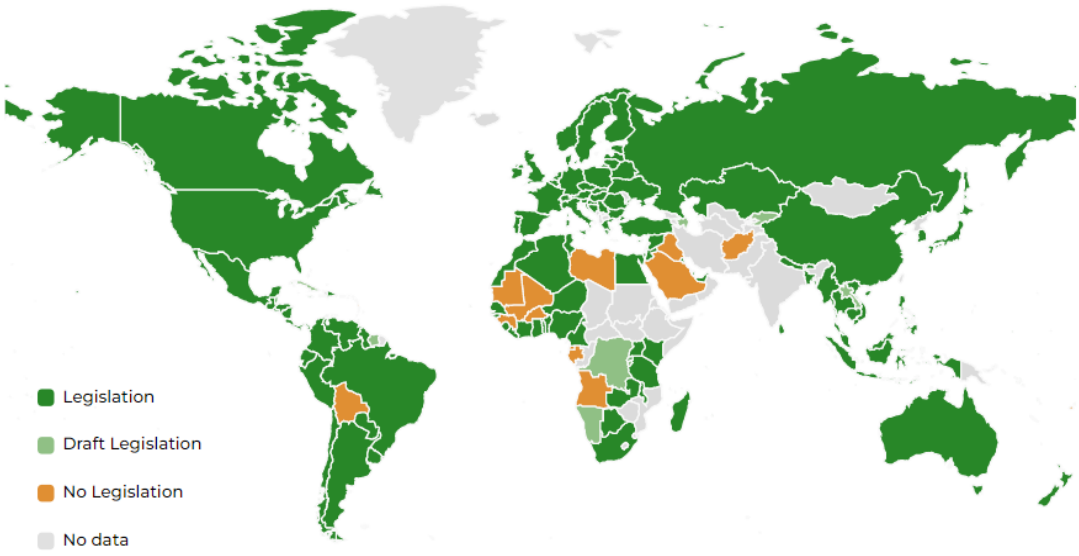


Figure 41. Online consumer protection legislation worldwide (December 2021).[225]

The landscape is slightly better when it comes to **e-transaction laws** that recognise the legal equivalence between paper-based and electronic forms of exchange. At the end of 2021, 33 African countries (61%) had legislation on this issue (Figure 42).

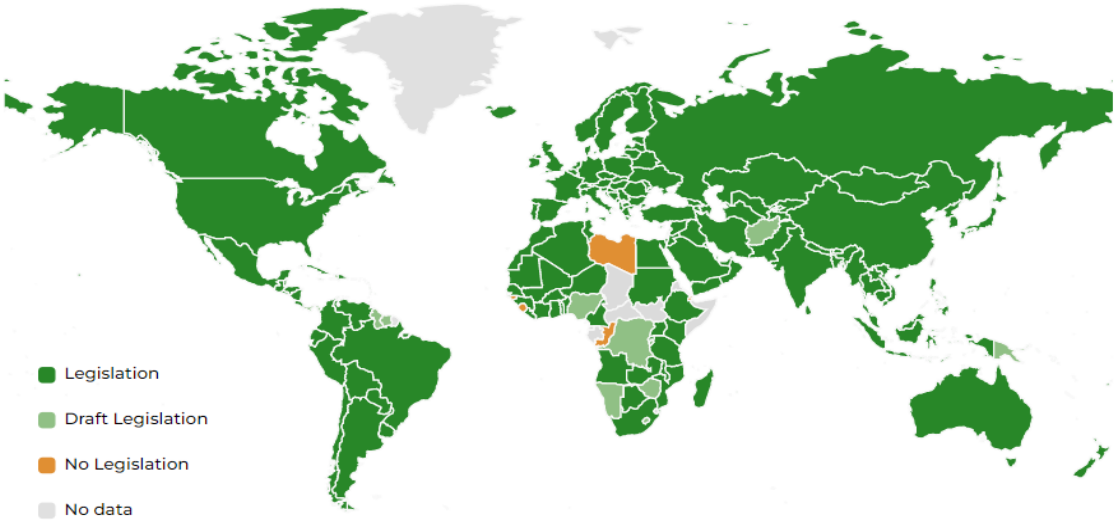


Figure 42. E-transactions legislation worldwide (December 2021).[226]

[225] Based on United Nations Conference on Trade and Development [UNCTAD]. (2021). *Online Consumer Protection Legislation Worldwide*. https://unctad.org/page/online-consumer-protection-legislation-worldwide. Figure redrawn.

[226] Based on United Nations Conference on Trade and Development [UNCTAD]. (2021). *E-transactions Legislation Worldwide*. https://unctad.org/page/e-transactions-legislation-worldwide. Figure redrawn.

Data flows

Cross-border data flows are essential elements of a well-functioning global digital economy. Data from Smart Africa (cited by GSMA) indicates that, in 2021, 26 African countries had no cross-border data flow restrictions, while 26 had adopted conditional flow regimes (i.e. they permit cross-border data flows subject to contractual safeguards, prior authorisation, or adequacy decisions by authorities).[227]

Some African countries have adopted data localisation requirements for **data protection purposes**. Section 50 of the *Data Protection Act* of 2019 in **Kenya** provides that the Cabinet Secretary may determine certain types of processing which may only be conducted through a server or data centre located in Kenya on the basis of strategic interests of the state or for the protection of revenue.[228] Moreover, there is a requirement that health data should not be stored outside Kenyan territory. The implementing *Data Protection (General) Regulations* (2021) clarify that entities which process personal data for the purpose of strategic interest of the state (such as administering the civil registration and legal identity management systems, overseeing systems for administering public finances, offering certain education services, or providing secondary health care) must process such data through a server and data centre located in Kenya, or at least store one serving copy of the concerned personal data in a data centre in Kenya. There is also the possibility that entities which process personal data outside of Kenya and suffer data breaches or violate the act may be required to comply with data localisation requirements.[229]

In **Rwanda**, the concept of data sovereignty has been at the core of the government's *National Data Revolution Policy* and requires that national data be hosted locally: 'Rwanda shall retain exclusive sovereign rights on her national data with control and power over own data.' The policy mentions, however, the importance of collaborating with regional and international stakeholders in building a data industry, and notes that the government will work on attracting investors in the data industry.[230] The 2021 *Law relating to the Protection of Personal Data and Privacy* includes requirements for data localisation: Entities may only store personal data in Rwanda, unless they are authorised by the regulator to store such data outside the country.[231]

In **South Africa**, the *Protection of Personal Information Act* regulates the transfer of personal information about a data subject to a third party in a foreign country under a number of conditions.

Some African countries use **economic development justifications** to introduce data flow restrictions. One such justification is that keeping data locally would contribute to job creation by enabling the growth of the domestic data processing industry.[232] **Nigeria** is one illustrative example: According to the *Guidelines for Nigerian Content Development in ICTs* established by Nigeria's National Information Technology Development Agency (NITDA), telecommunication and networking service companies should host all subscriber and consumer data within the country. Data and information management companies are also expected to host 'all sovereign data'

---

227 GSM Association [GSMA]. (2021). *Africa's data opportunity. Cross border data flows and IoT.* https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Africas-Data-Opportunity-Cross-Border-Data-Flows-and-IoT-Webinar-Slides.pdf

228 Republic of Kenya. (2019). *The Data Protection Act no.24 of 2019.* http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

229 Kenya Gazette. (2021). *The Data Protection (General) Regulations, 2021.* https://www.odpc.go.ke/wp-content/uploads/2021/06/L.N-263-265-THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021FIN....pdf

230 Ministry of Youth and ICT, Republic of Rwanda. (2017). *National Data Revolution Policy.* https://statistics.gov.rw/file/5410/download?token=r0nXaTAv

231 Official Gazette of Rwanda. (2021). *Law no 058/2021 relating to the Protection of Personal Data and Privacy.* https://www.risa.rw/fileadmin/user_upload/Others%20documents/Law_relating_to_the_protection_of_personal_data_and_privacy.pdf

232 Kugler, K. (2021). *The impact of data localisation laws on trade in Africa.* https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB%2008%20Data%20localisation%20laws%20and%20trade.pdf

locally, unless an approval to store such data outside the country is granted by NITDA. Moreover, ministries, departments, and agencies of the federal governments should ensure that all sovereign data is hosted locally on servers within Nigeria.[233]

In April 2021, **South Africa** published its draft *National Policy on Data and Cloud* of 2021 for comment.[234] In this policy, the South African government seeks to adopt strict data localisation requirements for economic development objectives.

As these examples indicate, the data governance landscape across the continent is rather fragmented and there is a wide diversity of rules in place when it comes to cross-border data flows. While ensuring an adequate level of data protection (in particular when it comes to personal data) is a commendable policy objective, strict restrictions to data flows pose challenges for cross-border digital trade. And while goals related to the strengthening of national economies can be seen as reasonable, there is a risk that these may turn into protectionist policies, with negative consequences for the functioning of regional and global digital economies. Governments, as well as regional and continental institutions, have the difficult task of trying to foster more harmonisation of data flows policies across the continent, while balancing these various policy interests (protecting data, strengthening national economies, enabling cross-border digital commerce/trade, etc.).

The AU Data Policy Framework, endorsed in February 2022 by the AU Executive Council, is expected to address some of these challenges. The framework is intended to contribute to the harmonisation of data governance policies across Africa and the establishment of adequate data-sharing mechanisms and frameworks that encourage cross-border data flows while safeguarding people's rights and fostering innovative data-driven businesses and solutions. Moreover, one of the recommendations outlined in the framework is for the AUC, RECs, and regional institutions to 'strengthen links with other regions and coordinate Africa's common positions on data-related international negotiations'. Another recommendation is for member states to 'foster a coordinated, comprehensive and harmonised regional approach to global governance challenges associated with the global data-driven digital economy'.[235]

Digital payments and financial services

Many countries in Africa are experiencing a significant transformation of their financial sectors as they extend financial inclusion and move to DFS. There has been an unprecedented increase in the number of people enjoying access to formal financial services in the continent, which is home to more DFS deployments than any other region in the world.[236]

Over the past decade, **financial technologies (fintech)** have become a significant driving force in the African internet economy, contributing directly to GDP growth while also enabling various other sectors. Fintech startups tend to be the top destination for funding, receiving almost 50% of all tech startup investment in 2021.[237]

The DFS sector is growing in Africa to serve the population that is currently unbanked and financially excluded. The sector is enabling African countries to leapfrog from physical retail banking to online payments. Paired with rising mobile connectivity, individuals living in rural areas with poor

[233] National Information Technology Development Agency, Nigeria. (2019). *Guidelines for Nigerian Content Development in Information and Communication Technology.* https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf

[234] South Africa Ministry of Communications and Digital Technologies. (2021). *Invitation to submit written submission on the proposed National Data and Cloud Policy.* ttps://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

[235] African Union [AU]. (2022). *AU Data Policy Framework*. https://au.int/en/documents/20220728/au-data-policy-framework

[236] International Finance Corporation [IFC]. (2018). *Digital access: The future of financial inclusion in Africa*. https://www.ifc.org/wps/wcm/connect/region__ext_content/ifc_external_corporate_site/sub-saharan+africa/resources/201805_report_digital-access-africa

[237] Jackson, T. (2022, February 8). 50% of African tech's $2bn funding pot went to fintech startups in 2021. *Disrupt Africa.* https://disrupt-africa.com/2022/02/08/50-of-african-techs-2bn-funding-pot-went-to-fintech-startups-in-2021/

physical banking infrastructure and limited access to fixed-line internet access are increasingly able to use mobile devices for financial transactions.[238]

The COVID-19 pandemic further accelerated the shift to digital finance in many economies. In Africa, governments have enacted regulations to support the adoption of DFS, used them as a way to enable emergency cash transfer programmes, and encouraged the use of cashless and contactless modes of payment to reduce the risk of virus spread, while customers increasingly used phones to pay merchants.

Compared to other policy areas, the level of development and policy coherence when it comes to frameworks for digital payments and financial services is remarkable in some countries in the African continent.

Ghana has been one of the countries to set forth a comprehensive set of policy initiatives designed to deepen financial inclusion and accelerate the shift to digital payments, based on three key instruments. The *National Financial Inclusion and Development Strategy*, developed in collaboration with the World Bank, aims at increasing financial inclusion to 85% of the population by 2023, helping create economic opportunities and reducing poverty. The strategy also outlines goals related to the alignment of national policies and regulations with international standards and principles.[239]

The *Digital Financial Services Policy* aims to create a resilient, inclusive, and innovative digital ecosystem.[240] The *Cash-Lite Roadmap*, designed in collaboration with the UN-based Better Than Cash Alliance, puts forward concrete steps to build an inclusive digital payments ecosystem. This includes better access to financial services, enabling regulation and oversight, and promoting consumer protection.[241]

The **Kenyan** *National Payments Strategy 2022–2025* sets a forward looking approach, aiming to 'support a payments system that meets the diverse needs of customers, especially with respect to financial inclusion and shared prosperity'.[242] Another goal of the strategy is to foster a supportive policy, legal, and regulatory framework that is robustly enforced across existing and emerging players in the payments ecosystem.

The strategy also notes the need to ensure alignment to relevant international standards and global best practices and outlines the central bank's commitment to engage in dialogue with regional and global stakeholders to ensure that the payment framework remains adaptive and relevant in the view of emerging trends and regulatory debates.

Taxing digital services

Several African countries have introduced various types of digital service taxes (DSTs). For instance, since January 2021, **Kenya** applies a 1.5% DST for income derived or accrued in the country from services offered through a digital marketplace.[243] **Nigeria** requires companies that offer digital services in the country (resident or non-resident) to pay a tax of 6% of the annual turnover of their

[238] Motobi, O. & Grzybowski, L. (2017). Infrastructure deficiencies and adoption of mobile money in sub-Saharan Africa. *Information Economics and Policy 40.* https://editorialexpress.com/cgi-bin/conference/download.cgi?db_name=CSAE2017&paper_id=105

[239] Republic of Ghana. (2018). *National Financial Inclusion and Development Strategy.* https://mofep.gov.gh/sites/default/files/acts/NFIDs_Report.pdf

[240] Ministry of Finance, Ghana. (2020.) *Digital Financial Services Policy.* https://mofep.gov.gh/sites/default/files/acts/Ghana_DFS_Policy.pdf

[241] Republic of Ghana. (2020). *Towards a cash-lite Ghana. Building an inclusive digital payments ecosystem*. https://mofep.gov.gh/sites/default/files/acts/Ghana_Cashlite_Roadmap.pdf

[242] Central Bank of Kenya. (2022). *National Payments Strategy 2022–2025*. https://www.centralbank.go.ke/wp-content/uploads/2022/02/National-Payments-Strategy-2022-2025.pdf

[243] Kenya Revenue Authority. (n.d.). *Introducing Digital Service Tax.* https://kra.go.ke/images/publications/Brochure-Digital-Service-Tax-Website.pdf

business in Nigeria.[244] In 2020, Tunisia introduced a 3% tax on the turnover generated by non-residents from the sale of computer applications and the provision of digital services.[245] Starting in 2022, **Ghana** has a levy of 1.5% on electronic transactions, targeting in particular mobile money transfers.[246]

In **South Africa**, income earned by non-resident providers of electronic services is subject to value added tax (VAT).[247] VAT on digital services is imposed in a few other countries, including **Côte d'Ivoire,** Egypt, **Ghana**, **Kenya**, **Nigeria**, **Rwanda**, and Tunisia.[248] Uganda at a point imposed a tax on social media websites, which was later replaced with a tax on data packages.[249]

In 2020, the African Tax Administration Forum (ATAF) published a *Suggested Approach to Drafting Legislation on Digital Sales Tax Services*. The document was 'intended to provide African countries with a suggested structure and content for their [DST] legislation', taking into account various DST frameworks in place in other jurisdictions, but adapted to local realities and needs.[250]

Cryptocurrencies

The adoption rate for cryptocurrencies and crypto assets is high and steady growing across Africa. Local businesses are developing a strong network of payments and services using blockchain technology and digital tokens. The 2022 Global Crypto Adoption Index placed **Nigeria**, Morocco, and **Kenya** among the top 20 countries worldwide by cryptocurrency adoption.[251]

One of the main reasons behind the high adoption rate of crypto services is related to the high cost of remittance under traditional financial services. Data for the fourth quarter of 2021 indicates that Africa is the region with the highest average remittance costs (7.83% of the sent amount).[252] By contrast, blockchain-based payments tend to be seen as a cheaper way to send money from abroad to families and communities.

Apart from remittances, cryptocurrencies are often also used for peer-to-peer (P2P) financial transactions. The aforementioned Crypto Adoption Index places **Kenya** in fifth place in a ranking of countries by P2P exchange trade volumes, with **Nigeria** and Morocco also among the top 25 countries worldwide.

While Africa's cryptocurrency market is the smallest among all world's regions, the continent is recording a fast and significant growth: US$105.6 billion worth of crypto assets between July 2020 and June 2021, accounting for 1,200% crypto value growth.[253] This makes the region quite attractive for international firms: In 2020 and 2021, some of the biggest names associated with cryptocurrency, online payments, and blockchain technology (e.g. Binance, Stripe) announced that

---

244 Oyeniyi, A. (2022, March 4). *Nigeria captures foreign tech firms in its tax net.* Quartz Africa. https://qz.com/africa/2137660/google-meta-and-others-raise-nigeria-prices-due-to-digital-tax/

245 Asquith, R. (2021, November 25.) *Tunisia VAT on foreign digital services.* VATCalc. https://www.vatcalc.com/tunisia/tunisia-vat-on-foreign-digital-services/

246 Ghana Revenue Authority. (2022). *Electronic transfer levy.* https://gra.gov.gh/e-levy/

247 South African Revenue Service. (2019). *FAQs: Supplies of Electronic Services.* https://www.sars.gov.za/wp-content/uploads/Ops/Guides/LAPD-VAT-G16-VAT-FAQs-Supplies-of-electronic-services.pdf

248 Asquith, R. (n.d.). *Global VAT & GST on digital services to consumers.* VATCalc. https://www.vatcalc.com/global/global-vat-and-gst-on-digital-services-to-consumers/

249 Kafeero, S. (2021, July 3). *To control speech, Uganda is taxing internet usage by 30%*. Quartz Africa. https://qz.com/africa/2028653/uganda-replaces-ott-social-media-tax-with-tax-on-internet-bundles/

250 African Tax Administration Forum [ATAF]. (2020). *ATAF publishes an approach to taxing the digital economy.* https://www.ataftax.org/ataf-publishes-an-approach-to-taxing-the-digital-economy

251 Chainalysis. (2022, September 14). The 2022 Global Crypto Adoption Index. *Chainalysis.* https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/

252 International Fund for Agricultural Development. (2022). *MobileRemit Africa.* https://gfrid.org/whats-on/mobileremit-africa-report/

253 Fries, T. (2021, September 23). *Africa's crypto market has grown by $105.6 billion in the last year.* World Economic Forum. https://www.weforum.org/agenda/2021/09/what-are-the-implications-of-widespread-cryptocurrency-adoption-in-africa/

they will place development centres in Africa or otherwise become more present in the region. At the same time, the region's own companies are aiming to expand their presence in international markets. One example is Luno, Africa's largest cryptocurrency exchange, which in early 2022 was looking into establishing a legal presence in the USA.[254]

Several countries have started looking into regulatory issues surrounding crypto markets. In **Nigeria** – where 33% of the population either owns or uses cryptocurrencies[255] – the central bank issued a statement in 2021 directing commercial banks and other regulated financial institutions not to deal, trade, or facilitate the use of cryptocurrencies.[256] However, in May 2022, the Securities and Exchange Commission published a set of *Rules on Issuance, Offering Platforms and Custody of Digital Assets*, outlining registration requirements for digital assets offerings and custodians, among other provisions.[257]

In **South Africa**, a report issued in 2021 by the Crypto Assets Regulatory Working Group indicates the country's intention to bring crypto assets into the regulatory remit 'in a phased and structured approach' across three main areas: anti-money laundering and combating the financing of terrorism, cross-border financial flows, and application of financial sector laws.[258] In 2022, both the South African Reserve Bank and the Financial Sector Conduct Authority indicated that work was ongoing on developing a regulatory framework for the cryptocurrency industry.[259]

Kenya's central bank issued a warning in 2015 about the risks associated with the use of unregulated digital currencies.[260] Over the years, the bank has also warned financial institutions against conducting crypto-transactions.[261] Central financial institutions in countries such as Angola, **Ghana**, Botswana, Egypt, and Guinea have also issued warnings outlining risks associated with cryptocurrency trading and stressing the need to ensure full compliance with anti-money-laundering and other regulations.

While many financial authorities across Africa took a cautionary approach in relation to cryptocurrencies (in line with what could be described as a global trend), in May 2022 the Central African Republic became the second country in the world (after El Salvador) to accept bitcoin and other cryptocurrencies as legal tender along with the national fiat currency (CFA franc). A bill to this effect was passed by the parliament and signed into law by the country's president regulating the use of cryptocurrencies in online trade and electronic transactions and stipulating that such exchanges are not subject to tax.[262] The Bank of Central African States (BEAC), the Banking Commission of Central Africa, the International Monetary Fund, and the World Bank raised concerns over the decision.

---

254 Changole, A. & Prinsloo, L. (2022, February 4). *Biggest crypto exchange in Africa sets sights on U.S. expansion*. Bloomberg. https://www.bloomberg.com/news/articles/2022-02-04/biggest-crypto-exchange-in-africa-sets-sights-on-u-s-expansion

255 Buchholz, K. (2021, February 18). *These are the countries where cryptocurrency use is the most common*. World Economic Forum. https://www.weforum.org/agenda/2021/02/how-common-is-cryptocurrency

256 Central Bank of Nigeria. (2021). *Letter to all deposit money banks, non-bank financial institutions and other financial institutions.* https://www.cbn.gov.ng/out/2021/ccd/letter%20on%20crypto.pdf

257 Security and Exchange Commission, Nigeria. (2022). *New rules on issuance, offering platforms and custody of digital assets*. https://sec.gov.ng/regulation/rules-codes/

258 Crypto Assets Regulatory Working Group, South Africa. (2021). *Position Paper on Crypto Assets.* https://www.resbank.co.za/content/dam/sarb/publications/media-releases/2021/fintech/IFWG%20CAR%20WG%20Position%20paper%20on%20crypto%20assets.pdf

259 Malinga, S. (2022, August 22). *FSCA sets ball rolling on crypto regulation in SA.* ITWeb. https://www.itweb.co.za/content/GxwQDM1DA8Q7lPVo

260 Central Bank of Kenya. (2015). *Caution to the public on virtual currencies such as bitcoin*. https://www.centralbank.go.ke/images/docs/media/Public_Notice_on_virtual_currencies_such_as_Bitcoin.pdf

261 Kitimo, A. (2022, March 22). *Kenya's central bank warns of risks in crypto.* The East African. https://www.theeastafrican.co.ke/tea/business/kenya-s-central-bank-warns-of-risks-in-cryptos-3756272

262 Jackson, K. (2022, April 11). *Central African Republic passes bill to make bitcoin legal tender.* CNET. https://www.cnet.com/personal-finance/crypto/central-african-republic-passes-bill-to-make-bitcoin-legal-tender/#ftag=CAD590a51e

Central bank digital currencies

In October 2021, **Nigeria** became the first African country to launch a central bank digital currency (CBDC) pilot: eNaira, issued by the Central Bank of Nigeria. Simply described by the bank as 'the digital equivalent of the cash Naira', eNaira is expected to contribute to encouraging financial inclusion, supporting a resilient payment system, facilitating diaspora remittances, and reducing the cost and improving the efficiency of cross-border payments.[263]

In **South Africa**, the Reserve Bank has been experimenting with a wholesale CBDC (wCBDC), but remains cautious about the policy and regulatory implications of such a currency and is of the view that further reflection and analysis are needed to unpack the legal status of a wCBDC and the treatment of wCBDC wallets as accounts with the central bank, among other issues.[264]

The Bank of **Ghana** announced in August 2021 that it is piloting a CBDC, with the overall goal of promoting diverse digital payments, while ensuring a secure and robust payment infrastructure in the country.[265]

Kenya's *National Payments Strategy 2022–2025* tackles the possibility of Kenya issuing a CBDC and notes that the central bank would 'need to carefully examine a number of important issues such as current legal, regulatory and supervisory frameworks, existing infrastructure, governance and risk management, central bank resources, and the core central bank legislation'. Issues of trust, safety and security, consumer protection, and regional cooperation and global convergence would also have to be considered.

Several other countries have announced that they are exploring the launch of their own CBDCs: Egypt, Eswanti, Madagascar, Mauritius, Morocco, **Namibia**, **Rwanda**, Tanzania, Tunisia, Uganda, Zambia, Zimbabwe (Figure 43). BEAC might also start exploring the introduction of a CBDC for its six member states (Cameroon, Central African Republic, Chad, Equatorial Guinea, Gabon, and Republic of the Congo), as encouraged by its Board.[266]

Digital currencies come with both challenges and opportunities. They could pose challenges to financial stability and raise privacy and security risks. But CBDCs could also facilitate a broader take-up of digital payments and contribute to more inclusive and convenient financial services and systems. This makes digital currencies particularly attractive for African countries, supporting their efforts towards inclusive finance, and allowing them to bring innovation in their financial systems and better adapt to the realities of the expanding digital economy.

[263] Central Bank of Nigeria. (n.d.). *Design Paper for the eNaira*. https://enaira.com/download/eNaira_Design_Paper.pdf

[264] South African Reserve Bank. (2022). *Project Khokha 2. Exploring the implications of tokenisation in financial markets.* https://www.resbank.co.za/content/dam/sarb/publications/media-releases/2022/project-khokha-2/Project%20Khokha%202%20Full%20Report%206%20April%202022.pdf

[265] Bank of Ghana. (2021). *Bank of Ghana partners with Giesecke+Devrient to pilot first general purpose Central Bank Digital Currency in Africa.* https://www.bog.gov.gh/wp-content/uploads/2021/08/CBDC-Joint-Press-Release-BoG-GD-3.pdf

[266] Mieu, B. & Hoije, K. (2022, July 22). *Central African regional bank seeks common digital currency.* Bloomberg. https://www.bloomberg.com/news/articles/2022-07-22/central-african-regional-bank-seeks-common-digital-currency

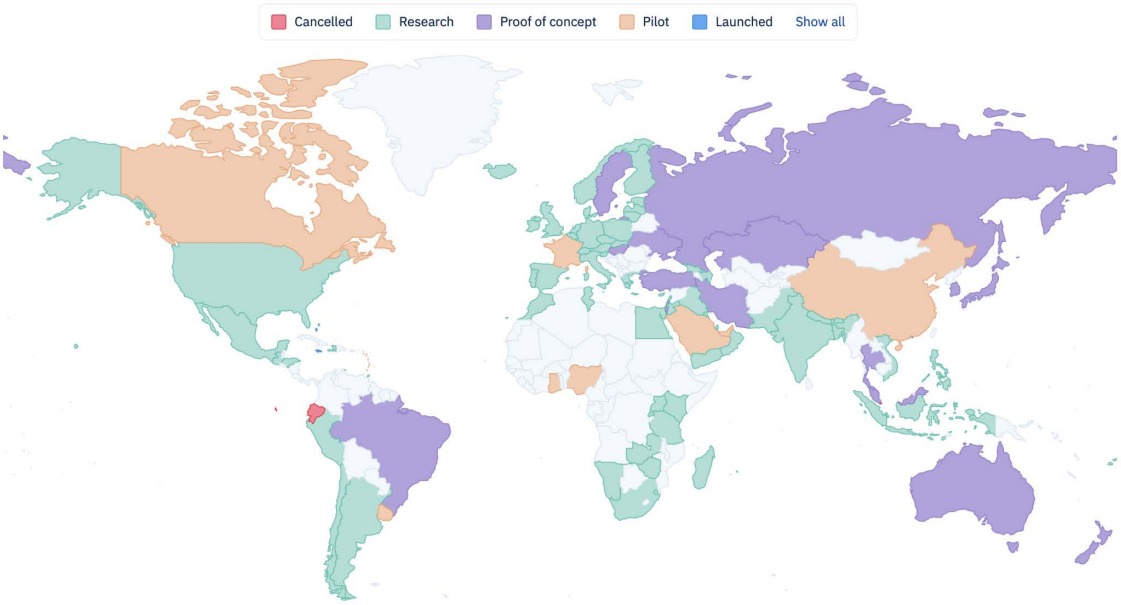


Figure 43. CBDCs' status (October 2022).[267]

Digital businesses across Africa: Success stories

Africa is the home of several successful digital businesses, such as:

- **Cellulant**. A pan-African payment solutions company providing local and global payment solutions integrating mobile money, local and international cards, and banks.
- **Jumia**. Founded in 2012 in Nigeria, Jumia evolved into Africa's leading e-commerce platform.
- **Luno**. The cryptocurrency exchange with hubs in South Africa and Lagos, Luno has over 10 million customers in more than 40 countries.
- **M-PESA**. Launched in 2007 by Kenya-based Safaricom and Vodafone, the mobile phone-based money transfer service is now available across multiple African countries, as well as beyond the continent, in countries such as Germany, China, and the UAE.
- **Paystack**. The financial payments company became one of Nigeria's most successful startups when it was acquired for over US$200 million by Stripe.
- **Wave**. Based in Senegal and the USA, this mobile money provider became the first unicorn in Francophone Africa in 2021.
- **Yellow Card**. One of the biggest fintech companies in Africa, Yellow Card operates as an online payments company and a cryptocurrency exchange.

[267] CBDC Tracker. (2022). *Today's Central Bank Digital Currencies Status*. https://cbdctracker.org

5.2. Continental and regional overview

African Continental Free Trade Area

The recognition of the importance of e-commerce for national and regional development in Africa has been present in political documents for some years, but there was a lack of regional pan-African vision for e-commerce and for the development of the digital economy. This is starting to change with the approval of the African Continental Free Trade Area (AfCFTA).

The agreement was signed in March 2018 and entered into force on 30 May 2019 after attaining the threshold ratification of 24 countries. As at May 2022, 54 AU members have signed the AfCTA agreement and 43 have both signed and deposited their instruments of AfCFTA ratification with the AUC Chairperson (Figure 44).

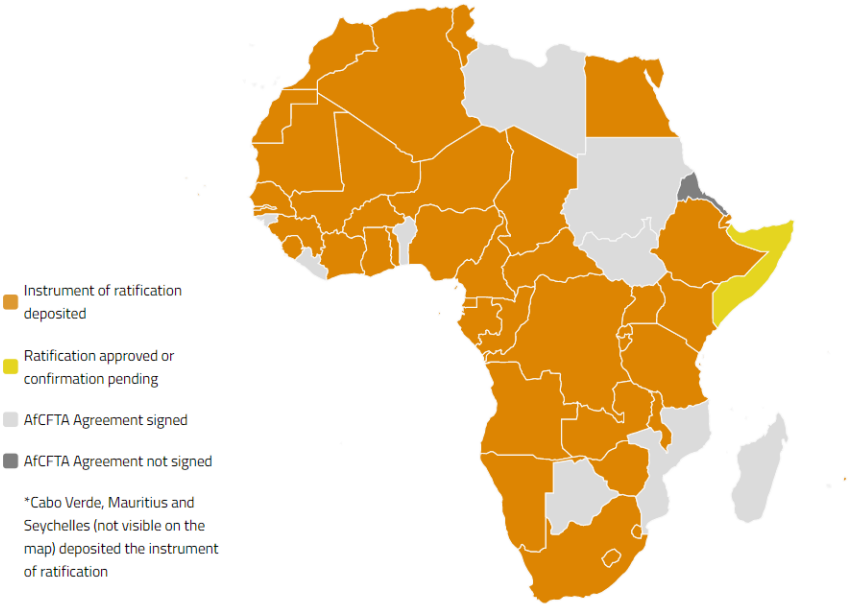


Figure 44. Countries that have ratified or signed AfCFTA.[268]

Overall, AfCFTA can be seen as a diplomatic success given the ambitious goals for free trade and the diversity of member states. The agreement raises hopes to 'unleash the potential of a large single market'[269] of 1.3 billion people. Key AfCFTA provisions include removing 90% of tariffs of goods, progressive trade liberalisation in services, and addressing other non-tariff barriers. In this way AfCFTA seeks to address three areas of obstacles to increased intra-African trade:

- Low complementarity of regional trade due to low economic diversification and weak productive capacities.
- Tariff-related trade costs associated with the slow implementation of the tariff liberalisation schedules underpinning free trade agreements.
- High non-tariff trade costs that hamper both the movement of goods and services and the competitiveness of firms in Africa.[270]

AfCFTA sees the RECs' free trade areas as its building blocks. Rather than replacing regional integration, the treaty builds on the existing structure of the RECs. Therefore, in a first step,

[268] Based on TRALAC Trade Law Centre. (2022). *African Continental Free Trade Area (AfCFTA) legal texts and policy documents*. https://www.tralac.org/resources/by-region/cfta.html#ratification. Figure redrawn.

[269] African Development Bank Group. (2021). *African Economic Outlook 2021*. https://www.afdb.org/en/documents/african-economic-outlook-2021

[270] United Nations Conference on Trade and Development [UNCTAD]. (2021). *Reaping the potential benefits of the African Continental Free Trade Area for inclusive growth*. https://unctad.org/system/files/official-document/aldcafrica2021_en.pdf

AfCFTA is likely to increase trade between regions. As mentioned previously, there is considerable diversity among the RECs. Differences in regional integration and, for example, levels of trade liberalisation between various RECs will complicate agreeing on further details under AfCFTA. Overlapping memberships will add further challenges. Smaller countries are also concerned about the potential dominance of economic powerhouses such as Côte d'Ivoire, Kenya, Senegal, and South Africa.[271]

AfCFTA offers great potential, but a lot of work needs to be done before the free trade area can become a reality. Much will depend on how further negotiations are progressing and how provisions will be implemented.

Further considerations in the context of digital foreign policy include:

- Digitalisation will play an important part in the success of AfCFTA and enable businesses to truly benefit from increased integration. The uneven rates of digital development across the continent will, however, be a challenge. Increasing digital infrastructure developments across regions will be an important factor in AfCFTA's success.
- As part of AfCFTA Phase III an e-commerce protocol is being negotiated. This offers the chance for Africa to increase its share in global e-commerce by 'expan[ding] market space for e-commerce players on the continent through coordinating initiatives and rules (data protection, payment integration, trust, etc.).'[272]
- Overall, AfCFTA will be important for harmonising intra-African trade. It might also contribute to, or even necessitate, the development of an African position regarding e-commerce and trade in digital services, thus supporting future bilateral and multilateral negotiations in this area.[273]

Other continental and regional initiatives

Over the years, the RECs have worked on various policies and initiatives related to **e-commerce and trade**. COMESA, for instance, which approaches digitalisation from a trade perspective, has created frameworks related to ease of doing business, digital trade, and harmonisation of regulations. In 2020, it adopted a model law on electronic transactions and guide to enactment. In 2017, COMESA launched a plan for a digital free trade area. While it has not been adopted, aspects of it, for example e-commerce, have been integrated by member states in their regulatory frameworks. COMESA's 2020 annual report recognises the urgency to 'complete the regulatory (e-commerce) agenda for digital transition'.[274]

ECOWAS has an *Act on Electronic Transactions* (2010), aimed at establishing a harmonised framework for the regulation of electronic transactions within the region.[275] In addition to its *Model Law on Electronic Transactions and Electronic Commerce*, SADC also approved a regional e-commerce strategic framework as early as 2012, with the goal of promoting an enabling legal and regulatory environment for e-commerce, facilitating intra-regional e-trade, and strengthening e-commerce infrastructures at the national and regional level.[276]

---

[271] Schmieg, E. (2020). The African Continental Free Trade Area. *SWP Comment*. https://www.swp-berlin.org/publikation/the-african-continental-free-trade-area

[272] Gillwald, A. (2020). *Readiness for the Digital Economy in Africa?* UNCTAD Intergovernmental Group of Experts on E-commerce and the Digital Economy (IGE) 2020. https://unctad.org/system/files/non-official-document/tdb_ede4_2020_p03_AlisonGillwald_en.pdf

[273] Abimbola, O., Aggad, F., & Ndzendze, B. (2021, September 23) *What is Africa's Digital Agenda?* APRI Policy Brief. https://afripoli.org/what-is-africas-digital-agenda#

[274] Common Market for Eastern and Southern Africa [COMESA]. (2020) *Annual Report*. https://www.comesa.int/wp-content/uploads/2021/10/COMESA-Annual-Report-2020-English.pdf

[275] Economic Community of West African States [ECOWAS]. (2010) *Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS.* http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Electronic-Transaction-Act.pdf

[276] United Nations Economic Commission for Africa [UN ECA]. (2012). *SADC eCommerce Strategy approved by ICT ministers*. https://repository.uneca.org/handle/10855/32193

EAC announced a similar strategy in 2021 focused on improving overall conditions for cross-border e-commerce in the region.[277] In ECOWAS, an e-commerce strategy is currently under development.[278] In May 2022, a meeting took place with the goal to kick off the strategy formulation process, with the participation of representatives of the ECOWAS Commission and two national focal points from each ECOWAS member states, representing trade and ICT ministries.[279]

Within the AU, an e-commerce strategy is to be developed by the AUC, as requested by the AU Executive Council in February 2022.[280]

Monitoring and ensuring competition in digital markets is also becoming a topic for regional cooperation. In February 2022, competition authorities in Egypt, **Kenya**, Mauritius, **Nigeria**, and **South Africa** launched the Africa Heads of Competition Dialogue as a framework for cooperation on issues such as ensuring fair regulation and enforcement, researching barriers to competition, and assessing mergers and acquisitions in digital markets.[281]

When it comes to **e-money and other DFS**, the AU's *Digital Transformation Strategy* calls for the creation of a conducive environment for the development and uptake of such services. Measures in this regard would include harmonising relevant rules across member states, deploying national and regional interoperability projects for e-money and other DFS solutions, fostering greater competitiveness, and encouraging the creation of a single African payments area to bolster cross-border trade and investments.

Across the continent, the African Digital Financial Inclusion Facility (ADFI) works to accelerate financial inclusion through investments in and support for (a) national and regional DFS-related infrastructures; (b) regulatory frameworks and policies that foster innovation and inclusion; (c) sustainable digital products and innovations; and (d) awareness raising and skills development across the digital finance ecosystem. AFDI is an initiative of the African Development Bank in partnership with the Bill & Melinda Gates Foundation, the French Development Agency, the Ministry of the Economy and Finance of France, and the Ministry of Finance of Luxembourg.[282]

At the regional level, the Central African Economic and Monetary Community's (CEMAC's) BEAC[283] introduced a set of regulations on mobile money interoperability in April 2020.[284] In 2022, BEAC's Banking Commission issued an official statement that cryptocurrency use should be restricted in the CEMAC region.[285]

One of the main challenges to cross-border trade across Africa has been related to the absence of mechanisms to ensure cost-effective and straightforward cross-border payment systems. Several initiatives have been put in place in recent years to address such challenges. RECs have worked on regional payment systems such as the COMESA Regional Payment and Settlement System, the East African Payments Systems, and the SADC Integrated Regional Electronic Settlement System.[286]

---

277 EAC-GIZ. (2021). *Regional EAC e-Commerce Strategy set to be implemented in 2022*. https://www.eacgermany.org/news/regional-eac-e-commerce-strategy-set-be-implemented-2022#:~:text=In%202021%2C%20the%20Pan%2DAfrican,e%2DCommerce%20in%20the%20region

278 United Nations Conference on Trade and Development [UNCTAD]. (n.d.). *Regional e-commerce strategy development for the Economic Community of West African States*. https://unctad.org/project/regional-ecommerce-strategy-for-ecowas

279 United Nations Conference on Trade and Development [UNCTAD]. (2022). *Third Regional Meeting on the Development of an ECOWAS E-commerce Strategy*. https://unctad.org/meeting/third-regional-meeting-development-ecowas-e-commerce-strategy

280 African Union Executive Council. (2022). *Decision 1144 (XL) on the reports of the specialized technical committees (STCs) and other ministerial meetings*. https://au.int/sites/default/files/decisions/41584-EX_CL_Dec_1143-1167_XL_E.pdf

281 Africa Heads of Competition Dialogue. (2022). *Joint Statement of the Heads of Competition Authorities Dialogue on Regulation of Digital Markets*. https://competitioncommission.mu/wp-content/uploads/2022/02/Joint-Statement-Final-18_02_final-version.pdf

282 African Digital Financial Inclusion Facility [ADFI]. (n.d.). *AFDI overview.* https://www.adfi.org/about-us/overview

283 CEMAC is made up of Gabon, Cameroon, Central African Republic, Chad, Republic of the Congo, and Equatorial Guinea.

284 Atabong, A.B. (2020, April 21). *Central African cements mobile money interoperability*. ITWeb. https://itweb.africa/content/PmxVEMKlNjOqQY85

285 Zimwara, T. (2022, May 15). *Report: Central African banking regulator says crypto ban still effective*. Bitcoin.com. https://news.bitcoin.com/report-central-african-banking-regulator-says-crypto-ban-still-effective/

286 United Nations Conference on Trade and Development [UNCTAD]. (2022). *Economic development in Africa report 2022:*

At the continental level, the Pan-African Payments and Settlement System (PAPSS) – an initiative spearheaded by the African Export-Import Bank (Afreximbank) and supported by the AU – is expected to facilitate the efficient and secure flow of money across African borders and contribute to financial integration across the regions, in conjunction with the implementation of AfCFTA.[287] In February 2022, the AU Assembly directed the AfCFTA Secretariat and the Afreximbank, in consultation with member states and central bank governors, to 'deploy the system to cover the entire continent and finalise the regulatory frameworks'.[288]

5.3. International engagement

Participation in the WTO Joint Statement Initiative on e-commerce

As the key policy player in modern global trade, the WTO has established a system of agreements which provides the legal architecture for the liberalisation of international trade. At the WTO, discussions on e-commerce are taking place in two parallel tracks: the *WTO Work Program on Electronic Commerce* (WPEC), launched in 1998 with a non-negotiating and exploratory nature,[289] and the *Joint Statement Initiative (JSI) on e-commerce*, which aims to produce a binding agreement among its members.[290] The JSI on e-commerce encompasses both traditional trade topics (e.g. trade facilitation) and several digital policy issues, such as cross-border data flows and data localisation, online consumer protection and privacy, and network neutrality.

Currently, the total number of WTO members formally participating in the e-commerce JSI negotiations is 87. They account for slightly more than half of all WTO members and 90% of global trade. With regards to the participation of developing countries, some regions remain notably underrepresented. There are six WTO members from Africa participating in JSI work (from a total of 43 African WTO members): Benin, Burkina Faso, Cameroon, **Côte d'Ivoire, Kenya**, Mauritius, and **Nigeria**. Africa is, in fact, among the least represented regions in JSI, together with the Caribbean.[291]

Reasons for this limited participation of African countries are diverse. Countries argue, for instance, that the JSI's plurilateral approach may undermine multilateralism and would prefer work on potential e-commerce rules to take place within the WTO's overall multilateral processes. They are also concerned that the approach and the resulting rules may ignore their development interests, pose challenges to Africa's integration agenda, and marginalise them and expose them to the risk of having to accept what others decide. Other concerns are related to the issues under discussion, African countries being in favour of having development topics – such as bridging the digital divide, developing digital infrastructure, and facilitating technology transfers – tackled more prominently. Because e-commerce policy frameworks and infrastructures are still under development across many countries, some governments feel they are not properly equipped to adequately participate in the discussions and defend their interests.[292]

Rethinking the foundations of export diversification in Africa: The catalytic role of business and financial services. https://unctad.org/system/files/official-document/aldcafrica2022_en.pdf

[287] Pan-African Payments and Settlement System [PAPSS]. (n.d.). *About PAPSS*. https://papss.com/about-us/

[288] African Union Assembly of Heads of State and Government. (2022). *Decision 831(XXXV) on the African Continental Free Trade Area (AfCFTA)*. https://au.int/sites/default/files/decisions/41583-Assembly_AU_Dec_813-838_XXXV_E.pdf

[289] World Trade Organization [WTO]. (n.d.). *Work programme on electronic commerce*. https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm

[290] World Trade Organization [WTO]. (2019). *Joint statement on electronic commerce*. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/1056.pdf&Open=True

[291] World Trade Organization [WTO]. (n.d.). *Joint Initiative on E-commerce.* https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm#participation

[292] Tigere Pittet, F. (2022). African Participation in WTO E-Commerce Negotiations: Policy Positions and Development Issues. *South African Institute of International Affairs, Policy Insights 131, June*. https://saiia.org.za/research/african-participation-in-wto-e-commerce-negotiations-policy-positions-and-development-issues/

The JSI's negotiating agenda is broad, encompassing issues such as spam, electronic signatures and authentication, consumer protection, and open government data. One of the issues considered key to achieving a high-level, meaningful agreement in the JSI is **data flows**. Nevertheless, this has been an issue in which obstacles are significant.

No developing countries had tabled text proposals on data flows until June 2021, when a proposal from **Nigeria** was introduced. Nigeria is now one of the few developing countries that have presented text proposals on data flows in the JSI. Most proposals so far have been made by developed countries (Table 16).

Table 16. Countries that have made text proposals on cross-border data flows and location of computer facilities in the JSI e-commerce.

	Brazil	Canada	Chinese Taipei	EU	Japan	Nigeria	South Korea	Singapore	UK	USA	Ukraine
Flow of information											
Cross-border data flows	X	X	X	X	X	X	X	X	X	X	
Location of computer facilities		X			X	X	X	X	X	X	X

X	Exceptions related to achieving 'legitimate public policy objective'
X	Exceptions related to achieving 'legitimate public policy objective' and security exceptions
X	Specific rules on cross-border data transfer may apply to personal data
X	Exceptions related to special and differential treatment to developing countries and LDCs
X	Text proposal without clear exceptions

The proposal from Nigeria introduces a special and differentiated treatment to developing countries and least developed countries (LDCs), which would allow them to adopt any measures regulating cross-border data flows that the country considers appropriate. Some important points make Nigeria's proposal unique.

First, no specific exception on cross-border data flows aiming to benefit developing countries and LDCs had been introduced before in the context of the JSI. Second, the proposal goes beyond the main policy justifications that usually motivate exceptions to free data flows – legitimate public policy objectives, privacy, security – by allowing developing countries and LDCs to adopt any measures they consider necessary. Finally, the proposal innovates by introducing a self-judging exception[293] to free data flows, which is not common in the context of data flows provisions.

Côte d'Ivoire has advanced two proposals seeking to **enhance cooperation** within the field of e-commerce among members of the JSI. The proposals call for concrete commitments from developed members, as well as developing countries with the capacity, to provide the assistance and technical support developing countries need to be able to engage in the negotiations, implement the forthcoming agreement, and bridge their digital divide.

It is important to recognise that due to their limited capacities, developing countries and LDCs make fewer submissions than developed and more advanced developing economies. They would

[293] In the context of self-judging clauses, states retain their right to escape or derogate from an international obligation based on unilateral considerations and based on their subjective appreciation of whether to make use of and invoke the clause *vis-à-vis* other states or international organisations.

greatly benefit from drafting support in JSI negotiations to crystallise, articulate, and present their interests and concerns on the issues being negotiated, bringing more balance to the negotiations and a more balanced outcome.[294]

OECD tax rules

In October 2021, 136 jurisdictions approved a set of new global corporate tax rules, developed under the umbrella of the OECD. The so-called *Statement on the Two-Pillar Solution to Address the Tax Challenges Arising from Digitalisation of the Economy with a Detailed Implementation Plan*[295] covers two tracks/pillars:

Pillar One will ensure that profits from companies generating more than €20 billion in revenues are distributed more fairly among countries entitled to tax them.

Pillar Two will ensure healthier tax competition among countries by capping the minimum corporate tax rate at 15%.

As of November 2021, 25 African countries had joined the agreement (Figure 45).[296] Standing out among those not joining are **Kenya** and **Nigeria**. They have decided not to support the agreement, although they are part (together with the other 25 African countries) of the OECD/G20 Inclusive Framework on Base Erosion and Profit Sharing (BEPS). Under this framework, 141 countries and jurisdictions had agreed to implement several actions to tackle tax avoidance, improve the coherence of international tax rules, ensure a more transparent tax environment, and address tax challenges arising from the digitalisation of the economy.[297]

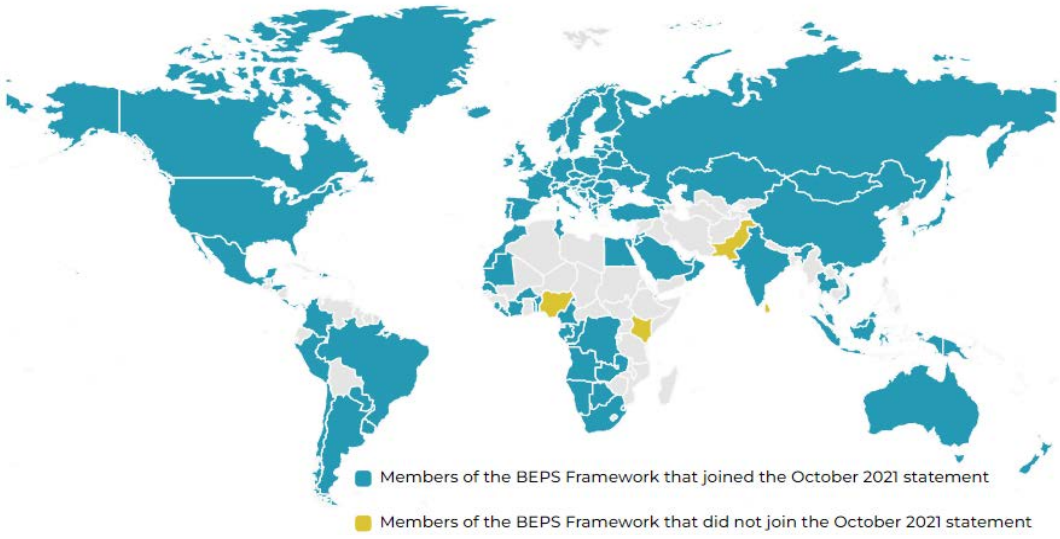


Figure 45. Members of the OECD/G20 Inclusive Framework on BEPS that joined and did not join the October 2021 statement.

294 Ismail, Y. (2022). *Cooperation, capacity building, and implementation considerations of developing countries in the E-commerce Joint Statement Initiative: Status and the way forward*. https://www.iisd.org/system/files/2022-04/developing-countries-e-commerce-joint-statement-initiative.pdf

295 Organisation for Economic Co-operation and Development [OECD]. (2021). *Statement on the Two-Pillar Solution to Address the Tax Challenges Arising from Digitalisation of the Economy with a Detailed Implementation Plan*. https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf

296 Organisation for Economic Co-operation and Development [OECD]. (2021). *Members of the OECD/G20 Inclusive Framework on BEPS joining the October 2021 Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy as of 4 November 2021*. https://www.oecd.org/tax/beps/oecd-g20-inclusive-framework-members-joining-statement-on-two-pillar-solution-to-address-tax-challenges-arising-from-digitalisation-october-2021.pdf

297 Organisation for Economic Co-operation and Development [OECD]. (n.d.) *International collaboration to end tax avoidance*. https://www.oecd.org/tax/beps/

With less than half of Africa supporting the new taxation rules, questions arise as to why this is the case. One reason is related to countries being concerned that, by joining the agreement, they might give up part of their sovereignty on taxation issues. The agreement includes a mandatory and binding arbitration mechanism for dispute resolution, whose applicability may mean that 'taxing countries lose their sovereignty by having tax issues resolved in the home countries of the corporations'.[298] Then, several countries across the continent have or are planning their own digital service tax, but the OECD agreement would have them drop such national, unilateral measures.[299]

As **Kenya**'s revenue authority explained, the deal only covers certain multinationals, whereas national taxes typically apply to a broader range of companies. In Kenya alone, 11 companies would fit the OECD requirements, whereas the country's DST applies to over 80 companies.[300] Dropping national taxes in favour of the OECD deal would therefore mean that countries agree to lower the amounts they collect from taxes. There is also an overall concern that the agreement tends to favour developed countries.

Discontent with the OECD deal is leading to **calls for discussions on tax reforms to happen within the UN framework**. In 2021, Guinea – on behalf of G-77 (which includes all African UN member states) and China – put forward a draft resolution at the UNGA on combating illicit financial flows. Adopted by the Assembly in December 2021, the resolution takes note of the OECD framework, but also 'recognises the importance of the consideration of international tax issues at the United Nations'. It also calls on all countries 'to work together to eliminate base erosion and profit shifting and to ensure that all companies, including multinationals, pay taxes to the governments of countries where economic activity occurs and value is created, in accordance with national and international laws and policies'.[301]

[298] Mureithi, C. (2021, November 9). *Why Kenya and Nigeria haven't agreed to a historic global corporate tax deal.* Quartz Africa. https://qz.com/africa/2082754/why-kenya-and-nigeria-havent-agreed-to-global-corporate-tax-deal/

[299] Ehl, D. (2021, October 29). *Why African nationals doubt OECD tax plan.* DW. https://www.dw.com/en/why-african-nations-doubt-oecd-tax-plan/a-59653146

[300] Mureithi, C. (2021, November 9). *Why Kenya and Nigeria haven't agreed to a historic global corporate tax deal.* Quartz Africa. https://qz.com/africa/2082754/why-kenya-and-nigeria-havent-agreed-to-global-corporate-tax-deal/

[301] United Nations General Assembly [UNGA]. (2021). *Resolution A/RES/76/196: Promotion of International Cooperation to Combat Illicit Financial Flows and Strengthen Good Practices on Assets Return to Foster Sustainable Development*. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/409/49/PDF/N2140949.pdf?OpenElement

Alliance for Financial Inclusion

Almost all African countries participate – either directly or through RECs institutions – in the work of the Alliance for Financial Inclusion (AFI), a network composed of central banks and other financial regulatory institutions from more than 80 developing countries, where the majority of the world's unbanked reside (Figure 46).

An example of a platform for peer learning, AFI has facilitated dialogue among African regulators and with the private sector and provided capacity building to advance digital financial innovation. Between 2016 and 2018, over 160 financial inclusion policies and regulations were implemented by African policymakers through engagement in AFI.[302]

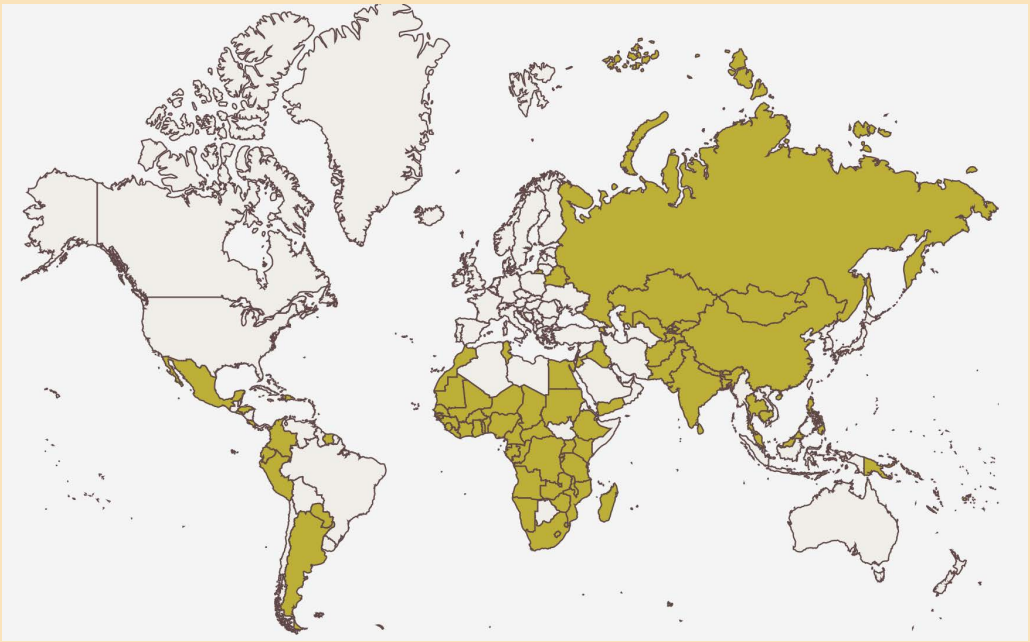


Figure 46. Members of the Alliance for Financial Inclusion (June 2022).[303]

[302] Alliance for Financial Inclusion [AFI]. (2019). *Cybersecurity and Financial Inclusion: Framework & Risk Guide*. https://www.afi-global.org/sites/default/files/publications/2019-11/AFI_GN37_DFS_AW_digital_0.pdf

[303] Alliance for Financial Inclusion [AFI]. (2022). *Member institutions*. https://www.afi-global.org/members/

6. Frontier technologies: Focus on artificial intelligence

Section summary

As with other digital technologies, Africa is making steps towards a faster uptake of AI, and AI-related investments and innovation are advancing. South Africa and Tunisia, for instance, were labelled as 'waking up' nations in terms of AI investment, innovation, and implementation in the Global AI Index, while Egypt, Nigeria, and Kenya are 'nascent'.

While governments around the world are increasingly adopting AI strategies, this is not yet the case across most of the African region. Notable exceptions are Mauritius and Egypt, which published such a strategy in 2018 and 2021, respectively. Kenya is looking into developing a master plan to foster the research, development, and deployment of AI, while Ethiopia, Ghana, Morocco, Rwanda, South Africa, Tunisia, and Uganda are also taking steps towards defining AI policies. Two priorities that most of these countries share are related to developing AI-related capacities and skills at the national level and encouraging AI research. Within the AU, there are attempts to develop a pan-African AI strategy. Meanwhile, major tech companies such as Google, IBM, and Meta are already tapping into the region's AI research potential.

The implications of AI for human rights have been on the ACHPR's agenda; it has called on governments, regional bodies, and the AU to put in place legal, regulatory, and ethical framework to ensure that AI and other frontier technologies respond to the needs of people.

A few African governments contributed to the discussions taking place within UNESCO on the *Recommendation on the Ethics of AI*. Experts from Cameroon, Egypt, Ghana, Morocco, Rwanda, and South Africa were part of the group which prepared the text of the recommendation. There has also been some involvement of African countries – either individually (e.g. South Africa, Mauritius) or through the Non-Aligned Movement – in discussions on lethal autonomous weapons systems.

6.1. National overview

Generally speaking, Africa has been slow in the uptake of AI technologies, for a variety of reasons, from infrastructure challenges to limited financial resources. The Global AI Index, for instance, places the African countries it analyses among 'waking up' and 'nascent' nations in terms of AI investment, innovation, and implementation: Egypt, **Nigeria**, and **Kenya** are nascent, while Morocco, **South Africa,** and Tunisia are waking up (Figure 47).

But there are expectations that AI can be a significant contributor to the region's digital transformation and economic growth. The AI industry is growing across Africa – with over 2,400 companies specialising in AI, 41% of which are startups (Figure 48) – and estimates indicate that the technology could contribute US$1.5 billion to the continent's GDP by 2030.[304]

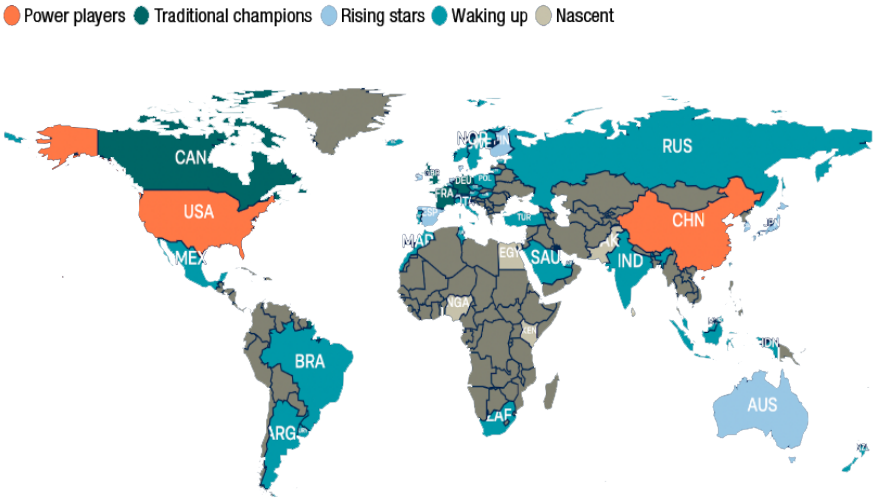


Figure 47. Global AI Index.[305]

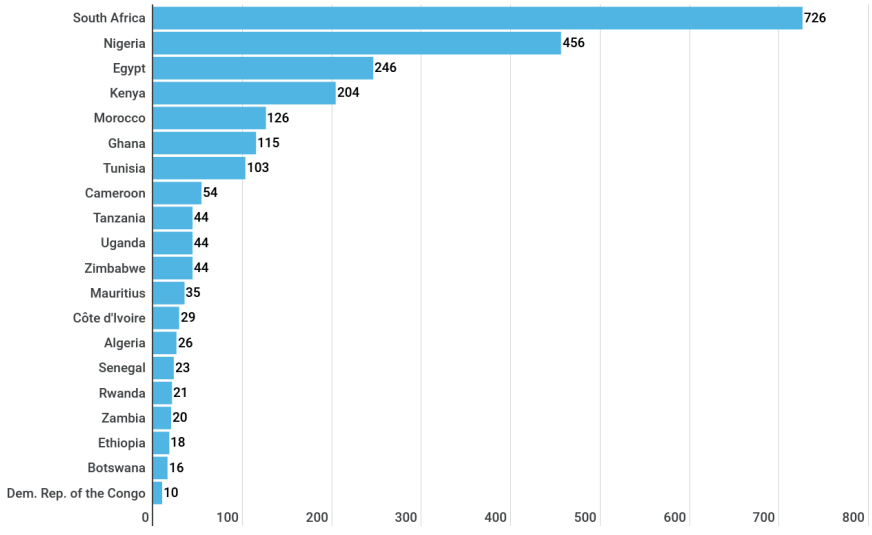


Figure 48. Number of companies specialised in AI, by country.[306]

[304] Ngila, F. (2022, June 23). *Africa is joining the global AI revolution.* Quartz Africa. https://qz.com/africa/2180864/africa-does-not-want-to-be-left-behind-in-the-ai-revolution/

[305] Tortoise. (2022). *The Global AI Index*. https://www.tortoisemedia.com/intelligence/global-ai/

[306] Based on Ngila, F. (2022, June 23). *Africa is joining the global AI revolution.* Quartz Africa. https://qz.com/africa/2180864/africa-does-not-want-to-be-left-behind-in-the-ai-revolution/. Figure redrawn.

More and more governments around the world are publishing national AI strategies outlining goals and action lines for ensuring that the countries can take advantage of the opportunities offered by the technology while mitigating the associated challenges (Figure 49). Some of these strategies also outline a desire for AI leadership, from China's goal of becoming a world leader in AI theories, technologies, and applications by 2030,[307] to Germany's intention of achieving and maintaining leading global excellence in the research, development, and application of AI.[308]

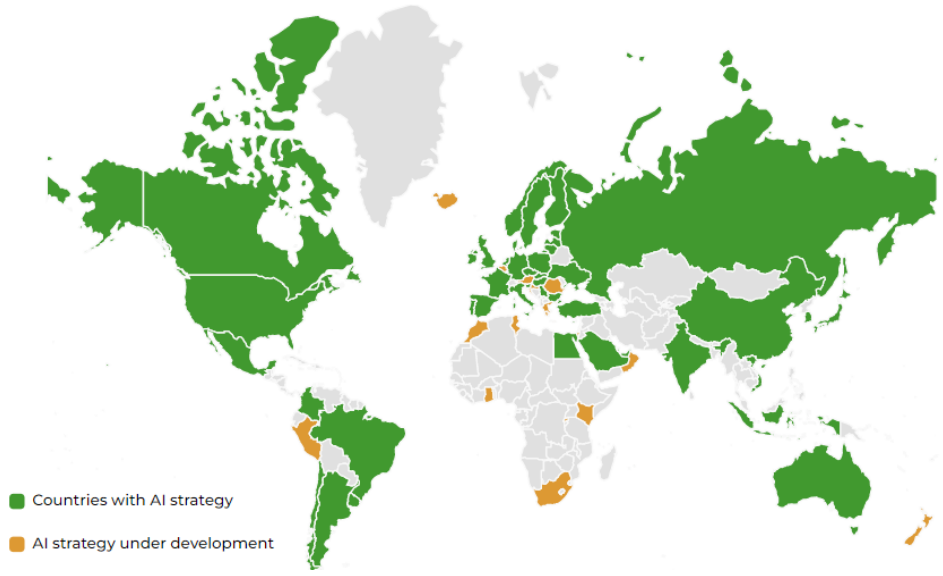


Figure 49. National AI strategies (June 2022).[309]

Three African countries have made efforts to advance policy documents dedicated specifically to AI: Mauritius, Egypt, and Kenya.

Mauritius's AI strategy, published in 2018, describes AI and other emerging technologies as having the potential to address, in part, the country's social and financial issues and as 'an important vector of revival of the traditional sectors of the economy as well as for creating a new pillar for the development of our nation in the next decade and beyond'. Areas of focus suggested in the strategy include manufacturing, healthcare, fintech, agriculture, and smart ports and maritime traffic management.[310]

Egypt has a national AI strategy (2021) built around a two-fold vision: exploiting AI technologies to support the achievement of SDGs, and establishing Egypt both as a key actor in facilitating regional cooperation on AI and as an active international player. The strategy focuses on four pillars: AI for government, AI for development, capacity building, and international activities. Egypt's goal to foster bilateral, regional, and international cooperation on AI is to be achieved through activities such as active participation in relevant international initiatives and forums, launching regional initiatives to unify voices and promote cooperation, promoting AI for development as a priority across regional and international forums, and initiating projects with partner countries.[311]

Kenya's government started exploring the potential of AI in 2018 when it created the Distributed Ledgers Technology and AI Task Force to develop a roadmap for how the country can take full advantage of these technologies. The report the task force published in 2019 notes that AI and other

[307] Webster, G., Creemers, R., Triolo, P., & Kania, E. (2017, August 1). Full translation: China's 'New Generation Artificial Intelligence Development Plan'. *New America* blog. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

[308] German Federal Government. (2018). *Artificial Intelligence Strategy.* https://www.ki-strategie-deutschland.de/home.html

[309] Geneva Internet Platform [GIP]. (n.d.). *AI Governmental Initiatives*. Digital Watch observatory. https://dig.watch/trends/ai-gov-initiatives

[310] Working Group on Artificial Intelligence, Mauritius. (2018). *Mauritius Artificial Intelligence Strategy*. https://cib.govmu.org/Documents/Strategies/Mauritius%20AI%20Strategy%20(7).pdf

[311] National Council for Artificial Intelligence, Egypt. (2021). *Egypt National Artificial Intelligence Strategy.* https://mcit.gov.eg/Upcont/Documents/Publications_672021000_Egypt-National-AI-Strategy-English.pdf

frontier technologies can increase national competitiveness and accelerate the rate of innovation, 'propelling the country forward and positioning [it] as a regional and international leader in the ICT domain'. As actions that could help achieve this goal, the report recommends investments in infrastructure and skills development and the development of 'effective regulations to balance citizen protection and private sector innovation'.[312]

The *2022–2032 Digital Master Plan* contains extensive references to AI. It starts from acknowledging that 'AI technologies and capabilities will be the in thing in the next 5–10 years and Kenya cannot afford to be left behind or to be the late laggards' and sets as an objective the development of an AI master plan to encourage the research, development, and deployment of AI solutions 'to solve local problems while exporting the same capabilities to other countries'. The plan also envisioned strengthened international partnerships with leading R&D actors in the emerging technologies space, to facilitate technology transfers and attract foreign direct investments.

Ethiopia, **Ghana**, Morocco, **Rwanda**, **South Africa**, Tunisia, and Uganda are also taking steps towards defining AI policies. **Ghana** and Uganda have been part of the *Ethical Policy Frameworks for Artificial Intelligence in the Global South*, a pilot project conducted in 2019 by UN Global Pulse and the German Federal Ministry for Economic Cooperation and Development, and dedicated to supporting the development of local policy frameworks for AI.[313] **Ghana** continues to work with UN Global Pulse to conduct a mapping of its AI ecosystem and to complete a blueprint for its national AI strategy.

Rwanda intends to develop a national AI policy focused on the ethical use of AI in support of social and economic development.[314] Ethiopia has set up an AI institute – the Ethiopian Artificial Intelligence Institute – which has among its tasks the formulation of national AI-related policies, legislation, and regulatory frameworks.[315]

In **South Africa**, a report issued in 2020 by the Presidential Commission on the Fourth Industrial Revolution acknowledged that AI is one of the high-technology industries in which the country is 'seriously underperforming', but notes that it also has 'a unique opportunity to take stock of [its] vast potential in the form of human capacity, identify opportunities consistent with promoting a human centred, Africa-centric strategy for the future'.[316]

Government AI readiness

The 2021 Government AI Readiness Index indicates significant differences among African countries when it comes to how prepared governments are to use AI. Within the region, Mauritius (52.71), Egypt (49.75), and **South Africa** (48.24) have the highest scores, consistent with the fact that they are also among the most developed African economies. At the opposite end are the Democratic Republic of the Congo (23.32), Angola (22.87), and the Central African Republic (20.73). No African country is ranked among the top 50 in the global ranking of 160 countries (Mauritius occupies the 58th position).[317]

The use of such rankings to place the region in context comes with two caveats. First, there is a limited availability of official data, exacerbated by capacity and governance challenges. Second, the index consists of several measures on which African countries score low due to existing inequalities (such as infrastructure). In other words, a low ranking is not surprising and is compounded by existing gaps.

[312] Ministry of Information, Communications and Technology, Kenya. (2019). *Emerging Digital Technologies for Kenya*. https://www.ict.go.ke/blockchain.pdf

[313] German Agency for International Cooperation [GIZ]. (2019). *Background paper on Open Forum to present Ethical Policy Frameworks for Artificial Intelligence in the Global South*. https://www.intgovforum.org/multilingual/sites/default/files/webform/open_forum_on_ethical_policy_frameworks_for_artificial_intelligence_in_the_global_south.pdf

[314] Smart Africa. (2021). *Blueprint: Artificial Intelligence for Africa*. https://smart.africa/board/login/uploads/70029-eng_ai-for-africa-blueprint.pdf

[315] Ethiopian Artificial Intelligence Institute. (n.d.). *Powers and duties*. https://aic.et/web/guest/powers-and-duties

[316] South Africa Presidential Commission on the Fourth Industrial Revolution. (2020). *Summary Report and Recommendations*. https://www.gov.za/sites/default/files/gcis_document/202010/43834gen591.pdf

[317] Oxford Insights. (2022). *Government AI Readiness Index 2021*. https://www.oxfordinsights.com/government-ai-readiness-index2021

Overall, AI is discussed in African countries in the context of public sector reform, education and research, national competitiveness, and partnerships with tech companies. Countries with the relevant capacities focus on skills, talent, and capacity development to build local and regional expertise. **Kenya**, for example, has adjusted its national curriculum to this effect: In 2022 the government approved the introduction of coding in curricula for primary and secondary schools. In **South Africa**, private associations host conferences and other events – such as the Deep Learning Indaba conference – to support the development of local capacities in AI and related technologies. Similar private-sector-led initiatives that focus on the development of AI skills at the local level are encouraged by the government of **Ghana**, in the context of the *National Entrepreneurship and Innovation Plan*.[318]

In **Nigeria**, a National Centre for AI and Robotics (NCAIR) – established under the National Information Technology Development Agency – works to promote R&D in AI, robotics, drones, and related technologies and create 'a thriving ecosystem for innovation-driven entrepreneurship, job creation and national development'.[319] In Egypt, an AI Centre of Excellence works to educate AI professionals, accelerate the deployment of AI, and produce standards and guidelines on the safe and responsible use of AI.

A pan-African programme is the *African Master of Machine Intelligence (AMMI)*, supported by Meta and Google,[320] while several South African Universities offer programmes in the area of AI.

South Africa hosts the Centre for AI Research (CAIR) – a research network, as well as a Centre for the Fourth Industrial Revolution (C4IR South Africa) – an initiative of the Department of Science and Innovation, connected with the World Economic Forum's (WEF's) networks of centres for the 4IR. One of C4IR's goals is to transition South Africa towards a data-based digital economy to improve its competitiveness and become a relevant global player. **Rwanda** too has opened a Centre for the Fourth Industrial Revolution (C4IR Rwanda) in cooperation with the WEF. And the Republic of the Congo is hosting the African Centre for Research on AI, an initiative launched in February 2022 with the support of UN ECA and dedicated to advancing AI-related capacity development and research across the continent.

Multinational tech companies are also becoming more and more active within the African AI ecosystem. IBM, for example, supports research labs in **Kenya** and **South Africa**. Google does the same in Ethiopia, **Ghana**, **Kenya**, and **South Africa**.[321] In **Ghana**, the company has a dedicated African AI research centre (opened in 2018), while **Kenya** is hosting a product development centre (announced in 2022).

Besides these developments, growing concerns about data and AI neocolonialism are being raised, in particular among civil society and academia. The overall argument is that 'the AI invasion of Africa echoes colonial era exploitation'.[322] AI solutions developed in the West – in accordance with Western perspectives, values, and interests – are being imported into Africa without truly reflecting the needs and interests of the local communities. This also leaves little room for the development of local AI solutions. Another criticism is that the AI industry is both exploiting cheap labour and harvesting data from consumers in Africa while giving little (if anything) back to these communities.[323] Initiatives such as Masakhane – an academia-led organisation working to build a

[318] World Bank. (2021). *Harnessing artificial intelligence for development in the post-Covid-19 era: A review of national AI strategies and policies*. https://openknowledge.worldbank.org/handle/10986/35619

[319] Nigeria's National Information Technology Development Agency. (n.d.). *National Center for Artificial Intelligence and Robotics*. https://nitda.gov.ng/ncair/

[320] AIMS. (n.d.). *About*. https://aimsammi.org/about-ammi-2/

[321] Saslow, K. (2019). Foreign Policy Engagement with African Artificial Intelligence. *Stiftung Neue Verantwortung*. https://www.stiftung-nv.de/sites/default/files/snv_memo_african-ai_final.pdf

[322] Birhane, A. (2020). Algorithmic colonization of Africa. *Scripted*, Volume 17, Issues 2, August 2020. https://script-ed.org/article/algorithmic-colonization-of-africa/

[323] Hao, K. (2022, April 19). *Artificial intelligence is creating a new colonial world order.* MIT Technology Review. https://www.technologyreview.com/2022/04/19/1049592/artificial-intelligence-colonialism/

natural language processing corpus in African languages, for Africans – are taking off across the continent in reaction to such concerns.

6.2. Continental and regional overview

AI is making it on the agenda of regional processes across the African continent. In 2019, AU country ministers in charge of ICT called for the establishment of a working group tasked with developing a common African stance on AI, developing a capacity-building framework, and establishing an AI think tank.[324] The group, chaired by Egypt, held its first meeting in February 2021.[325] Meanwhile, the AU Executive Council – at its February 2022 meeting – requested the AUC to pursue the development of a continental AI strategy.[326] And in May 2022, the AU High-Level Panel on Emerging Technologies[327] reiterated the need for a continental AI strategy that 'would enable African countries to enhance policymaking and implementation and improve stakeholder engagement on AI-related challenges and opportunities'.[328]

Within Smart Africa, an AI initiative spearheaded by **South Africa** in collaboration with the German Agency for International Cooperation (GIZ) and the Smart Africa Secretariat aims to work on strengthening technical know-how on AI, removing entry barriers to AI, and developing policy frameworks for AI.[329]

In 2021, a blueprint was published in the framework of this initiative which outlines recommendations for the development of AI strategies and legal frameworks in Africa. One recommendation is for national AI guidelines and regulations to be based on international best practices. The blueprint also highlights the importance of ensuring that Africa is part of global processes where AI-related governance and regulatory challenges are being discussed. But, more importantly, the document notes that Africa needs a smart strategy to allow it to 'find a profitable niche in the global environment of fierce [AI] competition. A focus on intra-African, home-grown AI development is a promising way forward. Local AI avoids dependencies from international platform monopolies in the field of data provision, data processing and AI solutions'.[330]

The ACHPR has been paying attention to issues at the intersection between AI and human rights. In its 2019 *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, the Commission calls on states to ensure that the 'development, use and application of AI, algorithms and other similar technologies by internet intermediaries are compatible with international human rights law and standards, and do not infringe on the rights to freedom of expression, access to information and other human rights'.[331]

In 2021, the Commission adopted a resolution specifically on AI and human rights, urging governments to 'work towards a comprehensive legal and ethical governance framework for AI

[324] African Union [AU]. (2019). *African Digital Transformation Strategy and African Union Communication and Advocacy Strategy among Major AU Initiatives in Final Declaration of STCCICT3*. https://au.int/sites/default/files/pressreleases/37592-pr-stc_pr-1-5.pdf

[325] Ministry of Communications and Information Technology, Egypt. (2021, February 25). *Egypt chairs AU Working Group on AI.* https://mcit.gov.eg/en/Media_Center/Latest_News/News/58203

[326] African Union Executive Council. (2022). *Decision 1144 (XL) on the reports of the specialized technical committees (STCs) and other ministerial meetings.* https://au.int/sites/default/files/decisions/41584-EX_CL_Dec_1143-1167_XL_E.pdf

[327] The AU High-Level Panel on Emerging Technologies is a multistakeholder group tasked with advising the AU and its member states on how to harness innovation and emerging technologies for socio-economic development.

[328] AUDA-NEPAD. (2022, May 30). *The African Union Artificial Intelligence Continental Strategy for Africa.* https://www.nepad.org/news/african-union-artificial-intelligence-continental-strategy-africa

[329] Smart Africa. (n.d.). *Artificial intelligence*. https://smartafrica.org/sas-project/artificial-intelligence/

[330] Smart Africa. (2021). *Blueprint: Artificial Intelligence for Africa*. https://smart.africa/board/login/uploads/70029-eng_ai-for-africa-blueprint.pdf

[331] African Commission on Human and Peoples' Rights [ACHPR]. (2019). *Declaration of Principles on Freedom of Expression and Access to Information in Africa*. https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf

technologies, robotics and other new and emerging technologies', and stressing the need for the AU and regional bodies to 'develop a regional regulatory framework that ensured that these technologies respond to the needs of the people of the continent'. Furthermore, the Commission committed to 'undertake a study in order to further develop guidelines and norms that address issues relating to AI technologies, robotics and other new and emerging technologies and their impact on human rights in Africa working together with an African Group of Experts on AI and new technologies'.[332]

6.3. International engagement

UNESCO Recommendation on the Ethics of AI

In November 2021, UNESCO member states adopted a *Recommendation on the Ethics of AI* outlining a series of values, principles, and actions to guide countries in the formulation of legislation, policies, and other instruments related to AI.[333] As the recommendation was adopted in unanimity, all African member states are considered to have endorsed it. The 24-member expert group appointed by UNESCO's Director-General to prepare the text of the recommendation included experts from six African countries: Cameroon, Egypt, **Ghana**, Morocco, **Rwanda**, and **South Africa**.

Algeria, Mali, Morocco, **Nigeria**, and Tunisia were the African countries that contributed comments on the first draft of the recommendation.

Algeria's contribution focused on AI and education, noting that while the education sector could benefit from AI, the role of teachers and human contact should not be underestimated. Morocco suggested that the recommendation should invite member states to use AI 'to serve the interest of humans', as well as to encourage the uptake of the technology by enterprises. Mali expressed support for all principles outlined in the draft recommendation and offered some additional observations. For instance, it called for the final text to strongly highlight that the developers and users of AI systems maintain full responsibility for the actions of AI systems, and to underscore the importance of encouraging and supporting the development of AI systems at the local level, so as to reflect local culture and traditions.

Nigeria called for the introduction of a recommendation for UNESCO to 'support the domestication of the recommendations by developing legislations for ethical oversight and accountability as AI is applied to human endeavours'. Tunisia highlighted the importance of promoting human-centred, ethical, and trustworthy AI. It also called for international cooperation on establishing 'recommendations and standards of good practice or even regulations in order to benefit globally from this new technology and avoid technological divides'.[334]

When the final text of the recommendation was put for debate at the Commission on Social and Human Sciences during the 41st Session of UNESCO's General Conference,

the Democratic Republic of the Congo, **Kenya**, **Côte d'Ivoire**, Ethiopia, Uganda, Mali, Djibouti, Morocco, Zambia, Cameroon, **Namibia**, Tunisia, Equatorial Guinea, and Burkina Faso were among the 68 member states that took the floor.

---

[332] African Commission on Human and Peoples' Rights [ACHPR]. (2021). *ACHPR/Res.473 (EXT.OS/XXXI) 2021 – Resolution on the Need to Undertake a Study on Human and Peoples' Rights and Artificial Intelligence, Robotics and other New and Emerging Technologies in Africa.* https://www.achpr.org/sessions/resolutions?id=504

[333] United Nations Educational, Scientific and Cultural Organization [UNESCO]. (2021). *Recommendation on the ethics of AI*. https://unesdoc.unesco.org/ark:/48223/pf0000379920.page=14

[334] United Nations Educational, Scientific and Cultural Organization [UNESCO]. (2021). *Compilation of comments received from member states on the first draft of the recommendation, Intergovernmental meeting of experts (category II) related to a draft recommendation of the ethics of artificial intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000376747

OECD and G20 AI Principles

Although the *OECD Recommendation on AI*[335] is open for adherence to non-OECD countries, Egypt is the only African government that had adhered to it by October 2022. **South Africa**, as a G20 member, has endorsed the *G20 AI Principles*,[336] which are based on the OECD Recommendation.

UN discussions on lethal autonomous weapon systems

African diplomats are involved in discussions on lethal autonomous weapons systems (LAWS) at the level of the UN, and some countries have clear positions regarding this topic. Algeria, Djibouti, Egypt, **Ghana**, Morocco, **Namibia**, Uganda, and Zimbabwe are among some 30 states that have called for a ban on lethal autonomous weapons – including their development and production.[337,338]

Several African countries have participated in the meetings of the Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS) – a group created in the framework of the Convention on Certain Conventional Weapons (CCW) with the goal of examining issues related to emerging technologies in the areas of LAWS in the context of the objectives and purposes of CCW.

In 2019, the GGE adopted a set of guiding principles (later endorsed by the CCW Meeting of the High Contracting Parties) outlining issues such as the applicability of international humanitarian law in the context of the potential development and use of LAWS and retaining human responsibility for decisions on the use of weapons systems.[339] The following African countries participated in the work of the group throughout the year: Algeria, Djibouti, Morocco, **South Africa**, Uganda (high contracting parties to the CCW); Egypt and Sudan (signatory states to the CCW); and Mozambique (state not party to the CCW).

In 2020, Mauritius and **South Africa** were among the countries that submitted written contributions to feed into the group's work. Mauritius expressed a preference for an instrument or treaty on LAWS which would, among others, oblige member states to (a) divulge their research programmes in the field of AI and robotics in weapons systems, (b) divulge the number of autonomous weapons systems (AWS) produced yearly, (c) ensure that AWS abide with humanitarian laws, and (d) inform before LAWS are used.

South Africa's contribution highlighted the country's view that the 2019 principles were developed solely to guide the work of the GGE and not for operationalising at the national level. The country also noted that both the design and use of LAWS need to be taken into account when considering a ban or restriction on the production and use of such systems.[340]

In 2021, the following African countries participated in the GGE work: Algeria, Angola, Burkina Faso, Burundi, **Côte d'Ivoire**, Egypt, Madagascar, Morocco, **Nigeria**, Sierra Leone, and **South Africa**.

---

335 Organization for Economic Co-operation and Development [OECD]. (2019). *Recommendation of the Council on Artificial Intelligence*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

336 G20. (2019). *G20 AI Principles*. https://www.g20-insights.org/wp-content/uploads/2019/07/G20-Japan-AI-Principles.pdf

337 Human Rights Watch. (2020). *Stopping killer robots. Country positions on banning fully autonomous weapons and retaining human control*. https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and

338 Congressional Research Service. (2021). *International discussions concerning Lethal Autonomous Weapon Systems*. https://sgp.fas.org/crs/weapons/IF11294.pdf

339 Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. (2019). *Report of the 2019 session*. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/285/69/PDF/G1928569.pdf?OpenElement

340 Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. (2021). *Chairperson's Summary*. https://documents.unoda.org/wp-content/uploads/2020/07/CCW_GGE1_2020_WP_7-ADVANCE.pdf

In 2022, the list of participating countries included Algeria, **Côte d'Ivoire**, Djibouti, Madagascar, **Nigeria**, Sierra Leone, **South Africa**, and Tunisia. **Nigeria** joined several other countries in submitting a contribution to GGE 2022 which suggested, among other things, that the next GGE be given a mandate to initiate open-ended negotiations on a legally binding instrument on autonomous weapon systems.[341]

Over the years, African countries have also joined others in the Non-Aligned Movement in the issuance of working papers and other contributions to GGE work. Their 2021 statements, for instance, underscore the 'urgent need to pursue a legally binding instrument under the Convention that will contain prohibitions and regulations for addressing the humanitarian and international security challenges' posed by LAWS. They also called for a new mandate for the GGE, one that would focus on developing a legally binding instrument to cover emerging technologies in the area of LAWS.[342],[343]

[341] Argentina, Costa Rica, Guatemala, Kazakhstan, Nigeria, Panama, the Philippines, Sierra Leone, State of Palestine and Uruguay. (2022). *Proposal: Roadmap Towards New Protocol on Autonomous Weapons Systems.* https://meetings.unoda.org/section/ccw-gge-2022_documents_18542_proposals_19869/

[342] Non-Aligned Movement. (2021). *Statement on behalf of the Non-Aligned Movement (NAM) and Other States Parties to the Convention on Certain Conventional Weapons (CCW) by the Delegation of the Bolivarian Republic of Venezuela to the United Nations Office in Geneva, First session of the 2021 CCW Group of Governmental Experts on emerging technologies in the area of LAWS*. https://documents.unoda.org/wp-content/uploads/2021/12/NAM.pdf

[343] Non-Aligned Movement. (2021). *Statement on behalf of the Non-Aligned Movement (NAM) and Other States Parties to the Convention on Certain Conventional Weapons (CCW) by the Delegation of the Bolivarian Republic of Venezuela to the United Nations Office in Geneva, Second session of the 2021 CCW Group of Governmental Experts on emerging technologies in the area of LAWS*. https://documents.unoda.org/wp-content/uploads/2021/12/Closing-Statement-NAM-agenda-item-6.pdf

7. Sociocultural issues

Section summary

African governments are increasingly implementing or exploring the implementation of digital identity solutions, sometimes with the support of international donors. While digital IDs are expected to help ensure that more people have access to legal identification and encourage the use of digital services, they also raise concerns about privacy and security. As both governments and regional institutions are advancing digital ID initiatives, there are calls to foster interoperability and develop a continental concept for digital identity.

Advancing gender equality and addressing gender digital divides are among the policy priorities of many African countries. Some, like Namibia and Rwanda, are making remarkable progress, although Africa remains one of the regions with the widest digital gender gaps. Several continental and regional initiatives – such as the *AU Strategy for Gender Equality and Women's Empowerment* – also underscore the need to facilitate women's access to digital technologies, ensure the protection of women and girls in the digital space, and empower them to take advantage of opportunities associated with the digital economy.

Most digital-related policies and strategies adopted by African governments outline goals related to digital capacity development. Some, like Rwanda and South Africa, have specific policies detailing objectives and measures related to advancing digital skills, including through cooperation with international bodies.

Governments acknowledge that advanced digital skills are essential in building sustainable digital societies and competitive digital economies. Some, like Kenya, Ghana, Rwanda, and South Africa, aspire to leverage their human talent to become regional or even global leaders in certain digital areas. Nigeria aspires to become a global outsourcing destination for digital jobs.

There are also multiple capacity development initiatives conducted throughout Africa with the engagement of regional and international organisations, as well as the technical community and civil society. These relate not only to the development of skills for using or developing digital technologies but also for building individuals' capacities to contribute to digital policy processes.

7.1. Digital identification

National developments

In an attempt to address a pressing challenge of more than 500 million people in Africa lacking any form of legal identification, policymakers have begun to deploy digital solutions – biometric digital identification (ID) systems. This has also coincided with the surge in the use of mobile technology across the continent, and the need to facilitate registration to access those services.

The increasing popularity of digital identities is owing to their efficacy, low cost, and convenience compared to more analogue systems.[344] However, these systems also increase the potential for citizen surveillance and can undermine privacy. This was recognised, for instance, by **Nigeria**'s Data Protection Bureau when it called in the National Identity Management Commission to set high standards for privacy and data protection as a way to strengthen the country's digital ID system.[345]

While some countries are making use of the growing digital infrastructure and developing national digital ID systems, many countries are lagging due to the uneven pace of digital transformation across Africa. Furthermore, lack of trust in governments and concerns about data privacy breaches, cyberattacks, and cyber fraud are also cited as the main challenges to the implementation of digital ID systems. There are also concerns that digital ID projects are sometimes promoted – for instance in the context of some development assistance programmes – without ensuring that the tech and policy solutions are indeed necessary, relevant to the local context (not merely replicating foreign examples), and properly tested from the perspective of their potential implications for citizens and communities.

So far, countries that have introduced or are working on introducing national IDs with electronic components – such as microchips or machine-readable barcodes – include Algeria, Angola, Cameroon, Egypt, **Ghana**, **Kenya**, Lesotho, Mauritius, Morocco, **Nigeria**, **Senegal**, Seychelles, **Rwanda**, **South Africa**, Tanzania, Uganda, and Zimbabwe.[346, 347, 348, 349] Among them, **Nigeria** is benefiting from funding from the EIB to support the development of an eID infrastructure and the supply of biometric identity to all citizens.[350]

[344] van der Spuy, A. (2021). *Digital Identity in Ghana: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. https://researchictafrica.net/publication/digital-identity-in-ghana-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/

[345] Macdonald, A. (2022, April 19). *New Nigerian data protection body calls for stronger privacy standards to drive digital ID.* Biometric Update. https://www.biometricupdate.com/202204/new-nigerian-data-protection-body-calls-for-stronger-privacy-standards-to-drive-digital-id

[346] Barasa, H. (2022). *Digital government in sub-Saharan Africa: Evolving fast, lacking frameworks.* Tony Blair Institute for Global Change. https://institute.global/policy/digital-government-sub-saharan-africa-evolving-fast-lacking-frameworks

[347] van der Spuy, A. (2021, November 9). *RIA releases 10 country reports on digital ID frameworks.* Research ICT Africa. https://researchictafrica.net/2021/11/09/ria-releases-10-country-reports-on-digital-id-framework/

[348] IDEMIA. (2022). *The Kingdom of Morocco introduces a national digital ID program.* https://www.idemia.com/wp-content/uploads/2022/06/idemia-national-digital-id-program-kingdom-morocco-case-study-202206.pdf

[349] Thales. (2021, December 29). *Digital identity trends – 5 forces that are shaping 2022.* https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/trends

[350] European Investment Bank [EIB]. (2018). *Nigeria Digital ID*. https://www.eib.org/en/projects/pipelines/all/20180298

World Bank's ID4D initiative

The World Bank is currently supporting 49 countries through its Identification for Development (ID4D) initiative. **Rwanda**, **Nigeria** and Tunisia are among the beneficiaries. The Rwanda Digital Acceleration Project was approved in 2021 and will see investments in the modernisation of the national ID system, for example, the introduction of a digital ID for online transactions and the digitisation of civil registration records. In Nigeria, the Digital ID for Development project was approved in February 2020, while in 2021, technical assistance was provided for the implementation of the project, focusing among other things on strengthening legal frameworks, introducing data protection safeguards, and improving cybersecurity. Tunisia has benefited from technical assistance for the development of a roadmap for digital IDs. Support is also provided for the development of models for digital authentication and the operationalisation of a unique citizen identifier.[351]

Regional frameworks and initiatives

The AU's *Digital Transformation Strategy* sees digital IDs as one of the main cross-cutting areas to support the digital ecosystem and as a key mechanism for promoting the UN concept of 'legal identity for all' and attaining SDGs and Agenda 2063.

In West Africa, the regional ECOWAS National Biometric Identity Card (ENBIC) was approved in 2015, to facilitate free movement for the 320 million citizens of the ECOWAS zone. The card will make it possible for the citizens of member states to move around the ECOWAS area, serving as a residency permit, a passport, and proof of identity. It is expected that further functionalities, such as identification for e-commerce, will be added. **Senegal** was the first country to fully implement the scheme,[352] while **Ghana** and **Nigeria** are among those following suit.

In addition, the West Africa Unique Identification for Regional Integration and Inclusion (WURI) programme, as part of the ECOWAS-World Bank partnership, started in 2018 with **Côte d'Ivoire** and Guinea to facilitate access to services for millions of people in the ECOWAS member states, irrespective of nationality, citizenship, or legal status. Consisting of the three components, the project aims to strengthen the legal and institutional framework, establish robust and inclusive foundational ID systems, and facilitate access to services through IDs.[353] Later expanded to Benin, Burkina Faso, Niger, and Togo, WURI also intends to help improve access to services, including safety nets, social registries, health and pension programmes, financial and digital inclusion, women and girls' empowerment, and labour mobility.[354] During the May 2022 meeting of the ECOWAS Directorate of Free Movement and Migration and the World Bank, the importance of **avoiding multitudes of regional ID cards was stressed**, given the existence of ENBIC, and the need to link the two initiatives.[355]

Within Smart Africa, a flagship project is dedicated to developing a continental concept for digital identity. A blueprint was proposed to assist both public and private actors with the design and implementation of digital ID systems that are trusted by all stakeholders.[356] These systems should be based on shared standards and rules to facilitate mutual recognition of respective ID systems.

---

[351] World Bank. (2021). *ID4D 2021 Annual Report*. https://documents1.worldbank.org/curated/en/436051643089705385/pdf/Identification-for-Development-ID4D-and-Digitalizing-G2P-Payments-G2Px-2021-Annual-Report.pdf

[352] Presidency of Senegal. (2016). *ECOWAS Biometric ID Card: the 10 facts you need to know.* https://www.presidence.sn/en/newsroom/ecowas-biometric-id-card-the-10-facts-you-need-to-know_1118

[353] World Bank. (n.d.). *West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program*. https://projects.worldbank.org/en/projects-operations/project-detail/P161329

[354] World Bank. (2020). *Togo, Benin, Burkina Faso and Niger join West Africa regional identification program to help millions of people access services*. https://www.worldbank.org/en/news/press-release/2020/04/28/togo-benin-burkina-faso-and-niger-join-west-africa-regional-identification-program-to-help-millions-of-people-access-services

[355] Economic Community of West African States [ECOWAS]. (2022). *The ECOWAS Commission and the World Bank Exchange on the West Africa Unique Identification for Regional Integration and Inclusion (WURI) project*. https://ecowas.int/?p=55284

[356] Smart Africa. (2020). *Blueprint: Smart Africa Alliance - Digital Identity*. https://smartafrica.org/wp-content/

The challenges of diverse digital ID systems across the continent were also recognised by the AU, which developed an *Interoperability Framework for Digital ID*, in cooperation with GIZ, the World Bank, Smart Africa, and UN ECA. Endorsed by the AU Executive Council in early 2022, the framework is intended to contribute to defining common requirements, minimum technical standards, governance mechanisms, and alignment among legal frameworks across the continent.

7.2. Gender equality

Gender equality and gender digital divides

In 2022, Namibia and Rwanda were ranked among world's top 10 gender equal societies. **Namibia** has made significant progress in bridging the gender gap as it moved up from the 12th place in the *Global Gender Gap Index 2020*[357] to 8th place in the latest report.[358] Similarly, **Rwanda** has advanced from the 9th to 6th place. According to the 2022 report, Namibia has closed 80.7% of the gender gap, while Rwanda has closed 81.1%.

Across Africa in particular, digital gender equality has been driven among other things by increased access to mobile money. The prevalence of fintech across the region should help reduce the barriers faced by women who are frequently excluded from the formal financial sector. The use of mobile money is found to be associated with a higher likelihood of self-employment and entrepreneurship among women.[359]

Still, there is a wide digital gender gap. Not only is internet penetration the lowest in Africa, but the difference between men and women using the internet is among the highest in the African region (Figure 50).

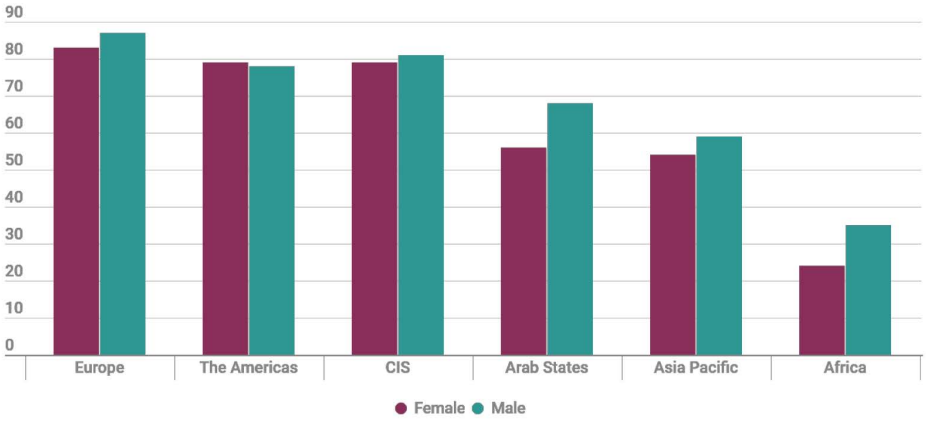


Figure 50. Internet usage rate worldwide in 2020, by gender and region.[360]

The gender internet divide seems to be narrowing at a very slow pace. Figure 51 shows that the gender parity score (the proportion of women who use the internet divided by the proportion of men) in Africa has only grown from 0.58 to 0.67 between 2018 and 2020.

uploads/2020/12/BLUEPRINT-SMART-AFRICA-ALLIANCE-%E2%80%93-DIGITAL-IDENTITY-LayoutY.pdf

[357] World Economic Forum [WEF]. (2020). *Global Gender Gap Report 2020*. https://www3.weforum.org/docs/WEF_GGGR_2020.pdf

[358] World Economic Forum [WEF]. (2022). *Global Gender Gap Report 2022*. https://www3.weforum.org/docs/WEF_GGGR_2022.pdf

[359] Kedir, A. & Kouame, E. (2022). FinTech and women's entrepreneurship in Africa: The case of Burkina Faso and Cameroon. *Journal of Cultural Economy*, DOI: 10.1080/17530350.2022.2041463

[360] Based on International Telecommunication Union [ITU]. (2021). *The gender digital divide*. https://www.itu.int/itu-d/reports/statistics/2021/11/15/the-gender-digital-divide/

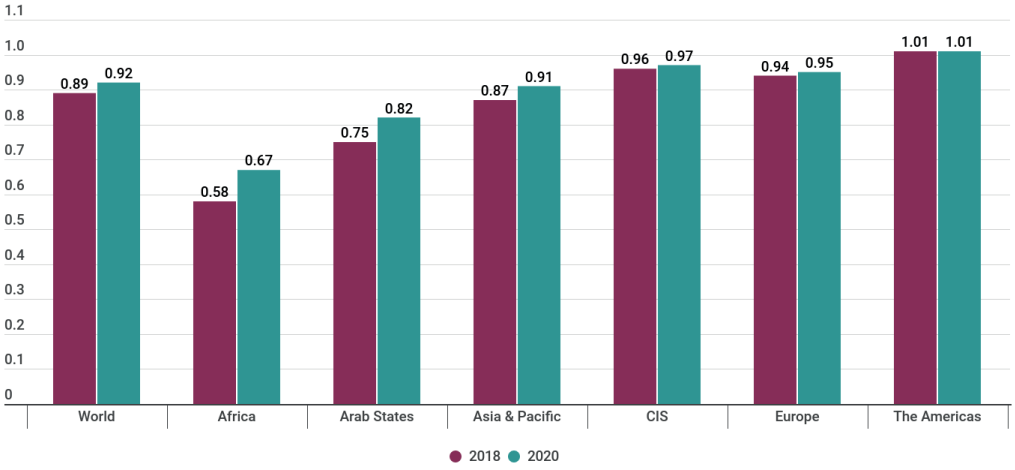


Figure 51. The internet user gender parity score, 2018 and 2020.[361]

Women are also less likely than men to own mobile devices. But the gender gap in mobile ownership tends to be smaller than the gender gap in mobile internet use. This is illustrated in GSMA's Mobile Gender Gap Report covering Egypt, **Kenya**, **Nigeria**, and **Senegal** (Figure 52).

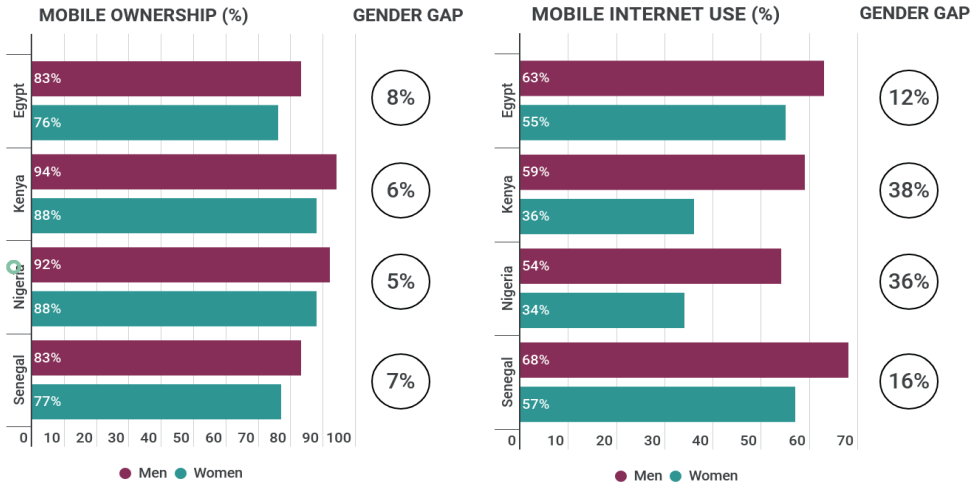


Figure 52. Mobile ownership and mobile internet use by men and women.[362]

The two main barriers to mobile ownership and mobile internet use are affordability (in particular handset costs) and functional literacy and digital skills. According to GMSA, difficulties with reading and writing, as well as not knowing how to access the internet on a mobile device tend to be greater barriers for women than men. Safety and security issues are also reported as significant barriers when it comes to internet use.[363]

There are numerous international and regional initiatives aimed at addressing the gender digital divide and one of the most impactful is the *African Girls Can Code* initiative implemented by UN Women, in partnership with the AUC and ITU, which trains African girls in coding and tech skills. During the first phase of the initiative, 600 girls were trained; a guide on mainstreaming ICT, gender, and coding in national curricula across the continent was developed; an eLearning platform was

[361] Based on International Telecommunication Union [ITU]. (2021). *The gender digital divide*. https://www.itu.int/itu-d/reports/statistics/2021/11/15/the-gender-digital-divide/

[362] GSM Association [GSMA]. (2022). *The Mobile Gender Gap Report 2022.* https://www.gsma.com/r/wp-content/uploads/2022/06/The-Mobile-Gender-Gap-Report-2022.pdf

[363] GSM Association [GSMA]. (2022). *The Mobile Gender Gap Report 2022.* https://www.gsma.com/r/wp-content/uploads/2022/06/The-Mobile-Gender-Gap-Report-2022.pdf

launched; and a series of webinars were held during the pandemic.[364] The second phase was launched in May 2022.[365]

Continental and regional initiatives

The *Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa* (2003), also known as the Maputo Protocol, provides a legal framework for promoting and upholding civil and political, economic, social, cultural as well as environmental rights for all African women. Among other things, it urges member states to 'promote research and investment in new and renewable energy sources and appropriate technologies, including information technologies and facilitate women's access to, and participation in their control'.[366]

The *Solemn Declaration on Gender Equality in Africa* from 2004, recognising the growing digital divide between genders and the role of digital technologies in the advancement of gender equality, called on member states to sign and ratify the Protocol and take specific actions to ensure the protection of human rights and capacity development of African girls and women.[367]

The protocol entered into force in November 2005, after having been ratified by the required 15 AU members. As of June 2022, 43 of the 55 AU members had ratified the protocol, and 9 had signed but not ratified it.[368] However, its full implementation and domestication still face challenges, in particular because several countries have placed reservations on some of its provisions.[369]

In 2009, the AU developed a gender policy to guide its commitments towards gender mainstreaming and women empowerment across the continent. The policy aims to mainstream gender equality and women's empowerment into all the institutional arrangements at policy and programming levels to address a series of issues affecting women, including that of enabling 'equal access to ICT infrastructure and applications, global alliance for IT development and building a sustainable e-future'.[370]

Ten years later, the *AU Strategy for Gender Equality and Women's Empowerment 2018–2028* was launched with the overall aim to mitigate, if not eliminate, the major setbacks to gender equality so that women and girls can fully participate in economic, social, and political endeavours. The strategy is composed of four pillars, one of them dedicated to digital empowerment:

- Pillar 1: Maximising (economic) outcomes, opportunities and tech e-dividends, which calls for an equal access to quality education for girls and women and control over productive resources.
- Pillar 2: Dignity, human security, and resilience, which are critical for the achievement of gender equality.
- Pillar 3: Effective laws, policies and institutions, which address, among others, a gap between the written provisions for gender equality, and the daily reality.

---

364 UN Women. (2021). *Addressing the digital gender divide in Africa through the African Girls Can Code Initiative*. https://unwomen.org.au/addressing-the-digital-gender-divide-in-africa-through-the-african-girls-can-code-initiative/

365 African Union [AU] et al. (2022). *African girls can code initiative (AGCCI), Second phase launch and TOT*. https://africa.unwomen.org/sites/default/files/2022-06/Final-%20Final-AGCCI%202nd%20phase%20launch%20report-May%202022_0.pdf

366 African Union [AU]. (2003) *Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa* https://au.int/sites/default/files/treaties/37077-treaty-charter_on_rights_of_women_in_africa.pdf

367 African Union [AU]. (2004). *Solemn Declaration on Gender Equality in Africa.* https://au.int/en/documents/20200708/solemn-declaration-gender-equality-africa

368 SOAWR. (n.d.). *Protocol watch*. https://soawr.org/protocol-watch/

369 Equality Now. (2021). *The Maputo Protocol turns 18 today. But what does this mean for women and girls in Africa.* https://www.equalitynow.org/news_and_insights/maputo_protocol_turns_18/

370 African Union [AU]. (2009). *African Union Gender Policy*. https://www.un.org/shestandsforpeace/sites/www.un.org.shestandsforpeace/files/african_union_gender_policy_2009.pdf

- Pillar 4: Policies and institutions leadership, voice, and visibility, which address the need for women to be equally represented in decision making.[371]

In the area of digital empowerment, the strategy stipulates that the AU will endorse digital solutions and platforms that advance gender equality and women's empowerment. It will advocate for tech firms and financial institutions to provide funds for start-ups and innovation hubs that promote gendered solutions and women's equal participation in technology development.

The AU's Women, Gender, Development and Youth Directorate (WGDY) is responsible for coordinating the AU's efforts on gender equality and promoting women's and youth's empowerment.[372] The mission of the Directorate is to ensure the implementation of the AU Strategy on Gender Equality and Women's Empowerment. The Directorate is tasked with designing programmes and projects based on the policies and frameworks adopted by AU members. It also oversees the development and harmonisation of gender and youth policies, defines strategies for gender and youth mainstreaming across the continent, and supports capacity building by providing training on gender and youth policies and instruments.

7.3. Digital skills and capacity development

National priorities and policies

A few African countries have dedicated national policies on digital capacity development, while most of them address issues pertaining to capacity development – such as workforce upskilling and digital literacy in primary and higher education – in their various general ICT or sectoral strategies.

Rwanda and South Africa are among the countries that developed dedicated policy and strategy documents. **South Africa**'s *National Digital and Future Skills Strategy* also has an international component. It notes that international collaboration with other higher education institutions, research entities, the private sector, and international bodies such as ITU and the International Labour Organization (ILO) is essential to build research capacity and ensure that the country is up-to-date when it comes to global developments in digital R&D. The strategy also notes that international best practices, as valuable as they may be, are not always appropriate or applicable to the national context and may not adequately inform national strategy. Therefore, in-depth research and case study analysis is needed for greater accuracy in initiatives to enhance digital skills in South Africa.[373]

The international component of **Rwanda**'s *National Talent Policy* is reflected in the country's objective to transform Rwanda 'from a consumer/importer to a producer/exporter of ICTs to the region and global scene' by setting up an elite IT corps. Other policy objectives include achieving digital literacy for all – both students and the general population – by enhancing digital literacy across all levels of society; building a digitally savvy workforce, through upskilling programmes; and coordination of digital literacy initiatives by formulating standards and providing relevant coordination mechanisms.[374]

[371] African Union [AU]. (2019). *AU Strategy for Gender Equality and Women's Empowerment.* https://au.int/sites/default/files/documents/36195-doc-au_strategy_for_gender_equality_womens_empowerment_2018-2028_report.pdf

[372] African Union [AU]. (n.d.). *Women, Gender, and Youth Directorate (WGDY).* https://au.int/en/directorates/women-gender-and-development-wgdd

[373] Department of Communications and Digital Technologies, South Africa. (2020). *National Digital and Future Skills Strategy.* https://www.gov.za/sites/default/files/gcis_document/202009/43730gen513.pdf

[374] Ministry of Youth and ICT, Republic of Rwanda. (2016). *National Digital Talent Policy.* https://rwandatrade.rw/media/2016%20MINICT%20Digital%20Talent%20Policy.pdf

As mentioned earlier, the topic of digital capacity development features high in various digital policies and strategies of the African countries. According to **Namibia**'s *National Broadband Policy*, access to ICT and the development of ICT-related skills in the younger population are national imperatives in enabling the country's participation in a competitive global economy.

Kenya's *National Broadband Strategy* is premised on several areas, including capacity building and innovations. Building technical and user capacity, education, and R&D are among the key principles of the strategy and crucial components of a robust digital society. Digital skills are also among the four main pillars of the country's *National Digital Master Plan*. The document recognises the shortage of digitally skilled workforce not only in Kenya but also the rest of the region, noting that a country with an excess of these skills has the advantage of supplying the region with the required human capital. The plan is therefore for Kenya to 'export, in the future, this skilled workforce to serve the region'. The government has also recently launched a programme to train 20 million Kenyans in digital skills.[375] The Kenyan *National ICT Policy* also reflects the country's ICT leadership aspiration, by noting the desire of the Kenyans to be 'leaders and innovators in the fourth industrial revolution and so we want to attract and create the best educational institutions in the world'.

ICT leadership cuts across most countries' digital policy documents. For instance, one of **South Africa** broadband policy's objectives is to develop a strong national skills base so that the country can be a globally competitive knowledge economy, while Ghana *Beyond Aid* outlines plans to leverage the nation's abundant human talent to become a leader, at least in Africa, in the digital economy by 2028. The *Smart Rwanda Master Plan* aims to position **Rwanda** as a regional ICT hub, enhancing the country's international position as a knowledge-based middle-income nation.

Nigeria's *National Digital Economy Policy and Strategy* aims to make Nigeria a global outsourcing destination for digital jobs. The strategy also emphasises the need to partner with relevant institutions to promote globally competitive training that focuses on digital technologies. The country's collaboration with IBM is a practical example of this.[376] Similarly, **Ghana**'s *ICT for Accelerated Development (ICT4AD) Policy* aims to encourage collaboration between local and international educational institutions to facilitate educational exchange and the promotion of ICT education and training, transfer of technology, and collaboration on R&D. The *Smart Rwanda Masterplan* mentions the establishment of ICT R&D centres in collaboration with international ICT companies as one of its focus areas.

The *Digital Senegal Strategy 2025* sees 'human capital' as one of the three fundamental prerequisites for a digital **Senegal**, along with adequate legal and institutional frameworks and digital trust. Digital skills are also among the seven fundamental pillars of **Côte d'Ivoire**'s *National Digital Development Strategy* by 2025. The objective of enhancing digital skills is to be achieved through strengthening professional training and introducing digital technologies in curricula and its generalisation in higher education.

Continental and regional initiatives

At the continental level, the AU's *Digital Transformation Strategy* proposes the following actions in the area of capacity development:

- Build capacity among officials on digital development.
- Promote the uptake and usage of digital tools.
- Strengthen cross-border and regional cooperation on digital infrastructure.

[375] Ng'ang'a, J. (2022, June 8). *ICT Ministry to train 20 million Kenyans on digital skills*. Kenya News Agency. https://www.kenyanews.go.ke/ict-ministry-to-train-20-million-kenyans-on-digital-skills/

[376] Udegbunam, O. (2020, January 18). *Nigerian government signs agreement for digital skills development.* Premium Times. https://www.premiumtimesng.com/news/more-news/373187-nigerian-government-signs-agreement-for-digital-skills-development.html

- Provide training for citizens and communities.

Building inclusive digital skills and human capacity across different sectors such as judiciary and education is one of the main objectives of the strategy. In addition, the AU aims to put in place a massive online e-skills development programme to provide basic knowledge and skills in online security and privacy to 300 million Africans per year by 2025.

Numerous capacity development projects supported by international organisations, the private sector, the technical community, and civil society organisations are being conducted throughout Africa. One of them is *Digital government capacity for Africa*, supported by the World Bank, with the aim of strengthening the capacity of the AUC and participating countries to provide public services through adoption of selected digital public sector platforms.[377]

The African technical community is also very active in the field of digital capacity development at the continental, regional, and national levels. It adopts different approaches, such as face-to-face and online activities, policy immersion, and other types of support. Some of the most prominent actors are AFRINIC and AfNOG, which promote activities aimed at building individual, institutional, and systemic capacities.[378]

Lastly, schools on internet governance play an important role in capacity development in Africa. Training is typically offered once a year and most schools take place in parallel with the regional or national IGFs. In some cases, the schools are convened by the same groups convening the IGFs. For instance, the West Africa School on Internet Governance (WASIG) is organised by the Secretariat for the West Africa Internet Governance Forum (WAIGF) and ECOWAS. Schools can also be convened by civil society organisations as is the case with the Ghana SIG, organised by the E-Governance and Internet Governance Foundation for Africa (EGIGFA).[379]

At the continental level, the African School on Internet Governance (AfriSIG) takes place once a year with the aim of creating a pool of leaders from diverse sectors to participate in local and international internet governance structures and shape the future of the African internet landscape.[380]

[377] World Bank. (n.d.). *Digital Government Capacity for Africa.* https://projects.worldbank.org/en/projects-operations/project-detail/P172935

[378] Maciel, M. (2020). *Sustainable capacity building: Internet governance in Africa – An action plan.* https://www.diplomacy.edu/resource/sustainable-capacity-building-internet-governance-in-africa-an-action-plan/

[379] Ibid.

[380] https://afrisig.org/

III
Africa in digital geopolitics and geoeconomics

Chapter summary

In recent years, digital issues have started becoming increasingly prominent in the relations between Africa and its partners. But in the-fast changing digital geopolitics environment, African countries tend to avoid being strategically aligned with the major actors, and instead focus on taking advantage of various partnerships to diversify their technological base and strengthen digital governance.

The EU and USA are both wooing African nations to support their value-driven digital governance approach (outlined, for instance by the *Declaration for the Future of the Internet*). China aims to garner African support for two key digital governance initiatives: the *Initiative on Jointly Building a Community with a Shared Future in Cyberspace* and the *Global Initiative on Data Security.* All three actors aim to play an important role in the development of digital infrastructure across the continent: The G7's Partnership for Global Infrastructure, spearheaded by the USA, China's Digital Silk Road (DSR), and the EU's Global Gateway are illustrative in this respect.

The US-Africa Leaders' Summit and the new Africa strategy are expected to further shape US policy towards Africa, including on digital matters. Noteworthy is the growing focus on placing digital competition with China in the African context.

While China's involvement in Africa's digital transformation has been a topic of controversy (e.g. concerns about Chinese companies' dominance over the deployment of mobile networks or their growing presence in other digital sectors such as smart cities), there are suggestions that neither the USA nor the EU can compete alone with China's commitment and investments in the digital sphere across the continent. And a China-Africa Project analysis indicates that African countries are not likely, for instance, to follow anti-Huawei narratives largely for practical reasons: cheaper product reliability and easy access to credit. Moreover, some actors argue that China's own experience in development is particularly useful for Africa and the continent should take advantage of it. Overall, China's approach towards Africa is evolving from a focus on infrastructure towards more digital governance issues, including e-commerce and the digital economy, cybersecurity, education, and capacity development.

The EU is putting significant resources into strengthening its relations with Africa, and the digital field is among the priority areas. On a strategic level, several convergences between Africa and Europe could shape future cooperation in the digital realm: a shared concern about the enormous power of big tech companies; another shared concern about data as a personal and economic asset; a priority for multilateral solutions to protect core digital interests; a drive towards digital/cyber/tech sovereignty; and the centrality of the human-centric approach. Meanwhile, initiatives such as the AU-EU Digital Economy Task Force, the AU-EU Digital for Development Hub, and the Global Gateway are in place to strengthen digital relations between EU and African nations. The EU regulatory framework on digital issues is also increasingly serving as a blueprint and inspiration for national and regional approaches.

India has also placed digital as a priority for its cooperation with Africa, in particular in areas such as digital health, e-government, and digital IDs. On broader issues of digital cooperation and cybersecurity, India has concluded cooperation agreements with several African nations.

Digital geopolitics and geoeconomics follow the overall trend of a growing interest of foreign actors in Africa. This is illustrated, for example, by the increasing number of embassies opened on the African continent over the past ten years (Figure 53).

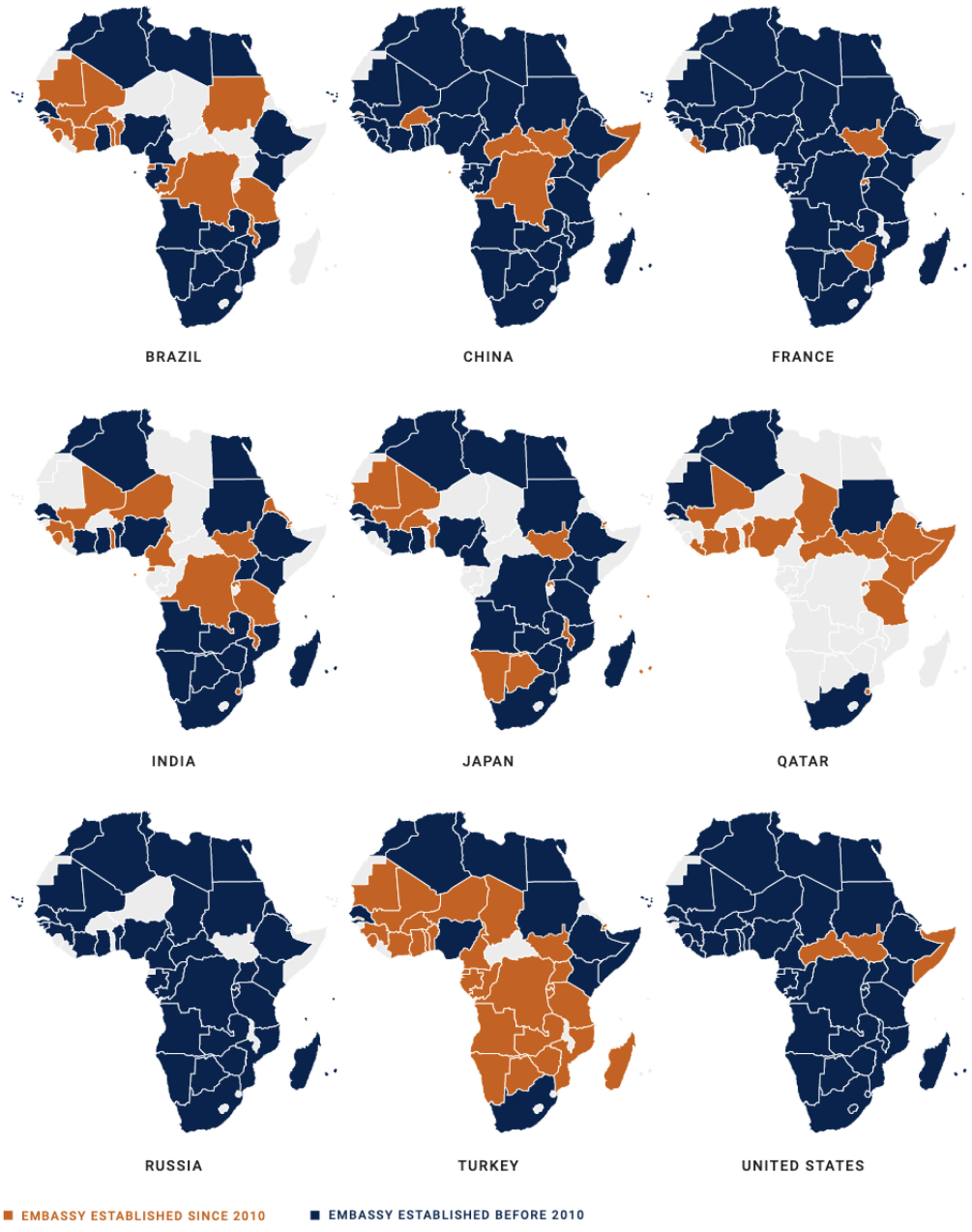


Figure 53. Embassies across Africa, by guest country.[1]

Africa is on the eve of a further acceleration of its already fast digital growth and overall modernisation. Against this backdrop, digital geopolitics and geoeconomics will be framed around two main coordinates: (a) development cooperation and investment, and (b) digital governance.

Over the last few years, there has been a clear shift towards a greater focus on digital governance issues in the relations between Africa and other actors. The EU, for instance, wants to pursue, together with African countries, 'a vision of an inclusive digital economy and society that is based on common principles'.[2] Both the EU and the USA have outlined their value-driven digital

1 Africa Growth Initiative at Brookings. (2022). *Foresight Africa. Top priorities for the continent in 2022*. https://www.brookings.edu/wp-content/uploads/2022/01/foresightafrica2022_fullreport.pdf

2 Council of the European Union. (2020). *Council conclusions on Africa*. https://www.consilium.europa.eu/media/44788/

governance approach in the recently adopted *Declaration for the Future of the Internet*. The same shift towards digital governance issues can be noticed in the relations between China and Africa. The *Dakar Action Plan (2022–2024)* on China-Africa cooperation includes clear references to African support for two key Chinese governance initiatives: the *Initiative on Jointly Building a Community with a Shared Future in Cyberspace* and the *Global Initiative on Data Security.*[3]

Having in mind the strategic priorities of the main digital actors, Africa's approaches to digital governance will be shaped around the following two extreme scenarios and various variations between them:

- **Integrated internet.** This scenario would follow the current internet architecture, which enables the free flow of data across national and corporate borders.
- **Fragmented internet.** This scenario would lead towards creating national and corporate networks that could coexist or be in conflict.

In the search for their position in the fast-changing digital geopolitics, African countries aim to follow their priorities and avoid taking sides, for instance in the USA-China digital competition. The first glimpse of this pressure to make strategic choices was the Trump administration's request for countries worldwide not to use Huawei technologies for their 5G networks. Most African countries do not want to be strategically aligned with major digital political powers. They are more interested in diversifying their technological base and strengthening digital governance by making tactical decisions based upon technology's affordability and impact on society's social and economic growth.

The following analysis of positions of the main digital actors should help navigate emerging digital geopolitics and geoeconomics in Africa.

1. USA

The USA was a key actor in Africa's digital growth. US companies and the tech community played an important role in providing the first computers and building the first networks in Africa. At that time, parts of Africa's technical community received support from US-based technical community organisations, such as ICANN, the Internet Society, and the IETF. For decades, US digital actors worked with the European technology community to support the development of African ccTLDs, Internet exchange points, and other areas of digital infrastructure.

The dynamics of these early days of rather undisputed US influence started changing with the growing presence of China in Africa's digital development over the last two decades. Since the Trump administration, there has been a shift towards 'Chinese containment' in US foreign policy, putting digital competition with China on the African continent into a sharper focus.

As a recent analysis from the Atlantic Council argues, the USA cannot compete alone with China's investment and commitment in the digital field.[4] The US is increasingly coordinating its digital approach towards Africa with the EU and its member states. For example, Finland and the USA announced in late 2021 a 'deeper cooperation on digital empowerment in developing countries'.[5]

st_9265_2020_init_en.pdf

3 Forum on China-Africa Cooperation. (2021). *China-Africa Cooperation Dakar Action Plan (2022–2024).* http://www.focac.org/eng/zywx_1/zywj/202201/t20220124_10632444.htm

4 Gadzala Tirziu, A. (2021). *Partnering for Africa's digital future: Opportunities for the United States, South Korea, and India*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/partnering-for-africas-digital-future-opportunities-for-the-united-states-south-korea-and-india/

5 Ministry for Foreign Affairs Finland. (2021, October 19). *Finland and United States announce deeper cooperation on digital empowerment in developing countries*. Press release. https://um.fi/press-releases/-/asset_publisher/ued5t2wDmr1C/content/suomi-ja-yhdysvallat-tiivistavat-yhteistyotaan-kehittyvien-maiden-digitaalisaation-edistamisessa

On the formal side, the first US–Africa Leaders' Summit took place in 2014. Digital topics were not one of the main areas of focus. The business forum accompanying the summit, however, stressed the relevance of digital infrastructure. A second US–Africa Leaders' Summit is planned for late 2022.[6]

The *U.S. Strategy toward sub-Saharan Africa* published in August 2022 outlines a commitment to 'drive digital transformation' across the region and 'foster a digital ecosystem built on an open, reliable, interoperable, and secure internet'. Focus areas for US actions and initiatives in the region include affordable internet access, digital skills and capacity development (in particular for youth), digital democracy, disinformation, gender-based online harassment and abuse, and standards for responsible conduct in cyberspace. Overall, the strategy puts emphasis on democracy and human rights, and countering Chinese and Russian influence.[7]

In the US digital policy towards Africa, the Partnership for Global Infrastructure and Investment (PGII) will play a central role in developing digital infrastructures. Launched as a G7 initiative in June 2022, the partnership is expected to mobilise US$600 billion by 2027 in global infrastructure investments to 'close the infrastructure gap in developing countries [and] strengthen the global economy and supply chains', including through developing and deploying secure ICT networks and infrastructures. The USA has already committed grants of US$200 billion in the next five years to support PGII goals.[8] On governance issues, the US policy will be shaped by the *Declaration on the Future of the Internet*.

2. China

China is one of the most important economic partners for many African countries and the largest single country trader with the continent.[9] Despite the global economic impact of the COVID-19 pandemic, Chinese direct investment in African countries has grown in 2020, according to the China–Africa Economic and Trade Relationship Annual Report 2021.[10]

Observers have suggested that in light of recovery from the COVID-19 pandemic, the Africa–China relationship, especially in economic terms, will become even more important. There are, however, also suggestions that a new Chinese policy of 'Dual Circulation', which describes a re-focusing of capital and investment inwards, might lead to reduced Chinese foreign direct investment and lending in Africa.[11]

China's role in Africa is a topic of controversy. Some authors have suggested that China's own experience in development is a source of mutual understanding and cooperation and that China's focus on infrastructure investment has laid the foundation for further economic growth in Africa.[12] Others have warned that China is taking on the role of a new colonial power in Africa. More recently, there are indications that some African countries are increasingly rethinking their

6 US White House. (2022). *Statement by President Biden on the U.S.-Africa Leaders Summit*. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/07/20/statement-by-president-biden-on-the-u-s-africa-leaders-summit/

7 US White House. (2022). *U.S. Strategy toward sub-Saharan Africa*. https://www.whitehouse.gov/wp-content/uploads/2022/08/U.S.-Strategy-Toward-Sub-Saharan-Africa-FINAL.pdf

8 US White House. (2022). *Fact Sheet: President Biden and G7 leaders formally launch the Partnership for Global Infrastructure and Investment*. https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment/

9 Mureithi, C. (2022, February 8). *Trade between Africa and China reached an all-time high in 2021*. Quartz Africa. https://qz.com/africa/2123474/china-africa-trade-reached-an-all-time-high-in-2021/

10 Chinese Academy of International Trade and Economic Cooperation and China-Africa Economic and Trade Promotion Council. (2021). *China-Africa Economic and Trade Relationship Annual Report 2021*. https://caidev.org.cn/news/1153

11 Paduano, S. (2021). Can China pull back? A balance-of-payments assessment of the decline in China's overseas investment. In: *LSE Ideas. FOCAC at 21: Future Trajectories of China-Africa Relations*, pp. 7–10. https://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-FOCAC-at-21.pdf

12 Brautigam, D. (2011). *The dragon's gift. The real story of China in Africa*. Oxford University Press.

relationship with Chinese infrastructure investments and are scrutinising or suspending contracts with Chinese companies.[13]

The growing involvement of China in Africa's digital transformation is at the centre of debates on digital geopolitics in Africa. For a long time, China has been boosting its digital presence in Africa from the bottom up, mainly through the development of telecommunication infrastructure. The presence of Huawei in Africa can be traced back to 1996. Most of the hardware infrastructure is financed by China's Eximbank, with 50 deals between Huawei and African governments.[14] As of 2021, Chinese companies dominate Africa's mobile infrastructure. Huawei and ZTE cover nearly 80% of Africa's 3G mobile networks, 70% of 4G networks,[15] and continue to lead the deployment of 5G networks.

The Digital Silk Road (DSR) represents the major international framework for China's foreign digital cooperation. The DSR is part of the Belt and Road Initiative (BRI) and benefits from BRI's infrastructural projects. This means that support for the deployment of digital infrastructure will follow major infrastructural projects of building roads, railways, and pipelines. The more recent Global Development Initiative, announced in September 2021, also has connectivity and digital economy among its priorities, although the overall goal seems to be about focusing less on building infrastructure (as it has been the case with the BRI) and more on broader development initiatives aligned with the SDGs.

In digital geopolitics, the Chinese market dominance over the deployment of 5G networks is a key concern. The first main pushback against Chinese market leadership, mainly around Huawei technology, was the Clean Network initiative of the Trump administration. However, no African country joined this initiative to ban the use of Huawei 5G technology (Figure 54). A 2020 China-Africa Project analysis argues that anti-Huawei narratives are not likely to succeed in Africa for the following reasons: cheaper product reliability and easy access to credit.[16] The Boston University Global Development Policy Center estimates that, between 2000 and 2020, Chinese lenders (banks, government entities, companies, etc.) signed 1,188 loan commitments with US$160 billion with 49 African governments, their state-owned enterprise and 5 regional organisations. In 2020, the ICT sector received the second largest amount of funding (after transport), worth US$569 million.[17]

Satellite technology is another area that contributes to the growth of China's role in Africa. The StarTimes brand has spread across Africa to hundreds of rural areas, in the framework of a Chinese initiative dedicated to delivering satellite TV to 10,000 villages in Africa. In 2020, China completed the BeiDou-3 constellation, becoming the third country, after the USA and Russia, to have a satellite navigation system with global coverage. The BeiDou-3 Navigation Satellite System (BDS-3) is used in the context of projects under the BRI in more than 120 countries and regions by some 100 million users.[18] China's satellite diplomacy is particularly active, through the first overseas BeiDou applications research centre located in Tunisia, and the delivery of training in Egypt, Algeria, and Morocco.

---

13 International Institute for Sustainable Development. (2021, October 25). Chinese Investment in Africa Rises as Project Values and Bilateral Trade Decline. *IISD News*. https://www.iisd.org/articles/chinese-investment-africa-bilateral-trade-decline

14 Hart, M. & Link, J. (2020). *There Is a solution to the Huawei challenge*. Center for American Progress. https://www.americanprogress.org/article/solution-huawei-challenge/

15 Gadzala Tirziu, A. (2021). *Partnering for Africa's digital future: Opportunities for the United States, South Korea, and India*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/partnering-for-africas-digital-future-opportunities-for-the-united-states-south-korea-and-india/

16 Oander, E. (2020). *Why the US campaign against Huawei will fail in Africa*. The China-Africa Project. https://chinaafricaproject.com/analysis/why-the-u-s-campaign-against-huawei-will-fail-in-africa/

17 Boston University Global Development Policy Center. (2022). *Chinese loans to Africa database*. https://www.bu.edu/gdp/chinese-loans-to-africa-database/

18 CGTN. (2022, August 1). *More than 120 countries, region use China's BeiDou-3 Navigation Satellite System.* https://news.cgtn.com/news/2022-08-01/More-than-120-countries-regions-use-China-s-BDS-3-system-1c9cMyX4NJ6/index.html

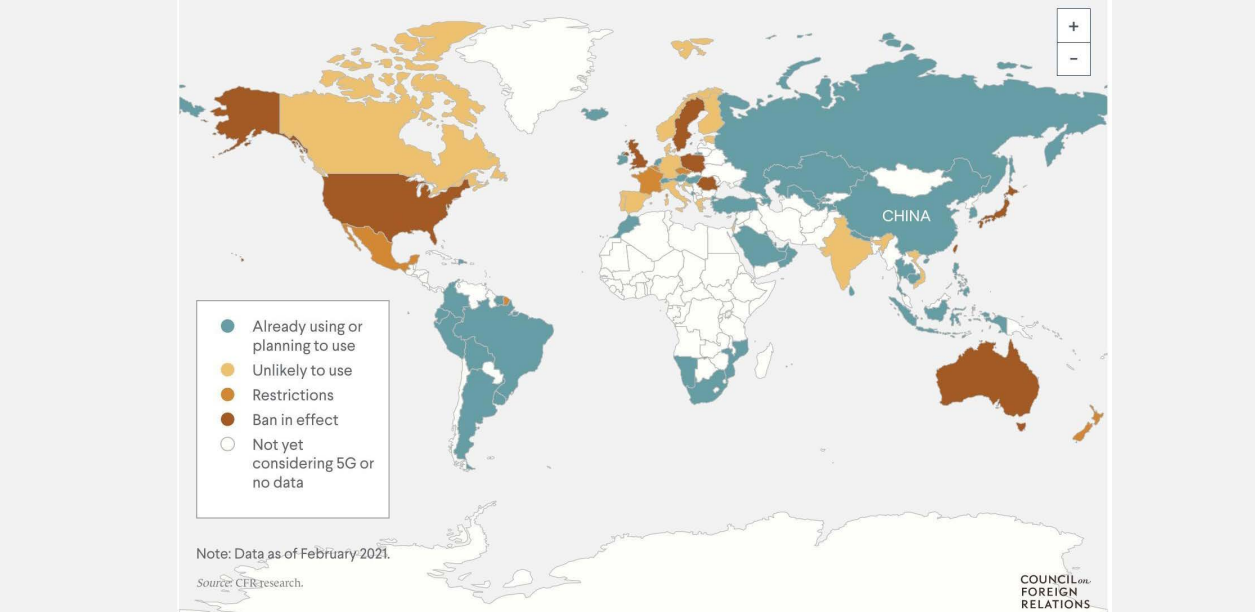


Figure 54. Use of Huawei 5G equipment (February 2021).[19]

Over the last decade, China's focus has gradually evolved from building networks towards knowledge transfer, cloud computing, AI solutions, and smart city projects.[20]

Chinese companies – Huawei in particular – are promoting the concept of smart cities, which have data at their centre. Cameras, sensors, and other tools collect massive amounts of data that is processed and used as input for public administration, transport management, fire-fighting, emergency management, etc. In this way, Huawei creates a holistic approach by combining 5G, data centres, and smart cities. Two projects follow this approach where data centres are linked to smart cities: Kenya's Konza Technology City[21] and the Zamengoe Data Center in Cameroon.[22],[23] In another significant development, Huawei provided equipment and technical support for the development of Senegal's Diamniadio National Data Centre; the centre, which is expected to host data from all government agencies and state-owned companies, was financed with a Chinese loan.[24]

Although China dominates the telecommunications infrastructure and has an increasing role in the data field, China's impact on content consumption is relatively limited. For example, according to *The Economist,* in April 2022 only 9% of Tanzanians watched China's flagship news channel compared to 73% following the BBC.[25]

19 Sacks, D. (2021, March 29). *Winning the 5G race. Here's what the United States should do to respond.* Council on Foreign Relations. https://www.cfr.org/blog/china-huawei-5g

20 Calzati, S. (2022). 'Data sovereignty' or 'Data colonialism'? Exploring the Chinese involvement in Africa's ICTs: a document review on Kenya. *Journal of Contemporary African Studies*, 40:2, 270-285. https://www.tandfonline.com/doi/pdf/10.1080/02589001.2022.2027351?needAccess=true

21 Moss, S. (2019, April 30). *Huawei to build Konza Data Center and Smart City in Kenya, with Chinese concessional loan*. Data City Dynamics. https://www.datacenterdynamics.com/en/news/huawei-build-konza-data-center-and-smart-city-kenya-chinese-concessional-loan

22 Alley, A. (2020, July 20). *Huawei equips Cameroon Gov't Data Center, helps Rain's South Africa 5G project.* Data Center Dynamics. https://www.datacenterdynamics.com/en/news/huawei-equips-cameroon-govt-data-center-helps-rains-south-africa-5g-project/

23 ASPI International Cyber Policy Centre. (n.d.). *Mapping China's tech giants: Cameroon Tier III (Design) Data Center*. https://chinatechmap.aspi.org.au/#/map/marker-2548

24 O'Grady V. (2021, June 24). *Senegal announces big plans for new data centre*. Developing telecoms. https://developingtelecoms.com/telecom-technology/data-centres-networks/11392-senegal-announces-big-plans-for-new-data-centre.html

25 *The Economist.* (2022, May 20). *China, meet Fourth Estate*. https://www.economist.com/special-report/2022/05/20/china-meet-fourth-estate

Formal processes and official diplomacy between China and Africa

China's shifting focus from technical infrastructure to data and applications is reflected in policy initiatives. In 2021, during the Dakar Summit of the Forum on China-Africa Cooperation (FOCAC), China-Africa digital cooperation was put in the wider governance context.

On digital governance, the *Dakar Declaration* indicates a broader ambition to jointly shape the global governance of the digital space. The same paragraph that outlines Chinese support for African digital development also hints at African support for China's *Global Initiative on Data Security*, launched in 2020.[26] The initiative calls for an 'open, secure and stable supply chain of global ICT products and services' and takes a stand against states impairing critical infrastructure, using mass surveillance against other states, and including backdoors in digital products and services.[27] Upon its launch, the Chinese initiative was largely interpreted as a response to the USA's Clean Network Initiative.[28]

The *Dakar Action Plan* (2022–2024) further fleshes out points of cooperation. Noteworthy in the context of digital foreign policy, it includes:

- Infrastructure development (including the Pan-African E-network, cybersecurity projects, optical fibre cable backbone networks, cross-border connectivity, international undersea cable, new-generation mobile networks, and data centres).
- E-commerce support (including Silk Road e-commerce cooperation, ten digital economy assistance projects for Africa, and a joint cooperation mechanism on e-commerce for trade facilitation).
- Cybersecurity support and collaboration.
- Active support for African capacity building in various areas related to digital and ICT.
- Expanding practical cooperation in the internet domain.

The action plan also fleshes out further cooperation on global digital governance, such as:

- Strengthening dialogue and exchanges on internet laws and regulations.
- Supporting the UN Cybercrime Ad Hoc Committee.
- African support for the Chinese initiative of *Jointly Building a Community with a Shared Future in Cyberspace* and the aforementioned *Global Initiative on Data Security.*
- Suggestions regarding political support in multilateral forums (e.g. to 'coordinate [...] positions [...] in the [ITU's] World Radio Communication Conference').[29]

Comparing the *Dakar Declaration* with its predecessor, the *Forum on China–Africa Cooperation Beijing Action Plan* (2019–2021), the shift towards a greater and more detailed emphasis on digital governance is significant.[30]

This evolution from purely technical towards more digital governance issues was further shaped in August 2021, during the Forum hosted by the China Cyberspace Administration, when China's Assistant Foreign Minister Deng Li outlined the *China-Africa Digital Innovation Partnership Program,*[31] with the following main pillars for future cooperation:

---

26 Ministry of Foreign Affairs of the People's Republic of China (PRC). (2020, September 8). *Global Initiative on Data Security.* https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t20200908_599773.html

27 Embassy of the PRC in the USA. (2020). *Global Initiative on Data Security*. https://www.mfa.gov.cn/ce/ceus//eng/zgyw/t1812951.htm

28 Ray, S. (2020, September 8). China launches own global data security initiative, targets U.S. 'Clean Network'. *Forbes*. https://www.forbes.com/sites/siladityaray/2020/09/08/china-launches-own-global-data-security-initiative-targets-us-clean-network/

29 Forum on China-Africa Cooperation [FOCAC]. (2021). *Forum on China-Africa Cooperation Dakar Action Plan (2022-2024).* http://focac.org.cn/focacdakar/eng/hyqk_1/202112/t20211222_10474206.htm

30 Forum on China-Africa Cooperation [FOCAC]. (2018). *Forum on China-Africa Cooperation Beijing Action Plan (2019-2021).* http://www.focac.org/eng/zywx_1/zywj/201809/t20180912_7933578.htm

31 The Partnership was announced at the "China-Africa Internet Development and Cooperation Forum" held on August 24, 2021. https://www.mfa.gov.cn/ce/cebw//chn/zfgx/t1901528.htm

- Strengthening digital infrastructure, including fibre-optic backbone networks, cross-border interconnection, and new-generation mobile communication networks. The main focus will be on access in remote areas and 'last mile' of digital connectivity.
- Developing the digital economy through the use of cloud computing, AI, IoT, and mobile payment to promote Africa's industrialisation process. This initiative should accelerate the integration of African information and industrial chains through cross-border e-commerce.
- Supporting education and vocational training aiming particularly at youth. Concrete projects include China–Africa distance education cooperation and support for African talents by Chinese companies.
- Fostering digital inclusion aimed at ordinary people in Africa. Here the main focus is on the use of digital technology for transportation, medical care and finance, smart cities, e-government, and e-payment.
- Advancing digital security and governance. China invites Africa to participate in the *Initiative on Building a Community with a Shared Future in Cyberspace* and the *Global Data Security Initiative*. China envisages cooperation in cybersecurity emergency response, internet laws and regulations, and formulating global digital governance rules.
- Establishing a high-level dialogue platform for China–Africa digital cooperation and strengthening communication and exchanges with African governments and organisations such as Smart Africa.

3. European Union

The digital relations between the EU and Africa follow the overall economic, educational, and political relations between the two continents. The EU is one of the most important partners for African countries and the AU. Based on data from 2020, the EU as a whole is Africa's main trading partner, accounting for 33% of exports from Africa and 31% of imports.[32] The EU is the source of the largest foreign direct investment in Africa and the largest provider of development assistance.[33]

In her 2019 *A Union that Strives for More* agenda, EU Commission President Ursula von der Leyen announced a 'comprehensive strategy on Africa'[34] and her first trip outside of the EU took her to the AU headquarters.[35] Since 2020, the EU has pursued a path of strengthening its relationship with Africa. Reflecting this, the EU Council's joint communication *Towards a comprehensive strategy with Africa* of June 2020 expresses the aim 'to initiate a new ambitious partnership with Africa'. In this document, digital is listed as one of the 'ambitious priority' areas for 'the next phase of the EU partnership with Africa'.

The joint communication mentions 'cyber security and democratic integrity, closing the digital divide, fighting data poverty, participating in digital trade, promoting digital for development, enhancing digital skills and protecting human rights and fundamental freedoms online', and stresses the importance of a multistakeholder approach.[36] At the end of 2020, the EU agreed on a new financing instrument as part of its external action, which has earmarked €29 billion for Africa over the period 2021–2027.[37]

---

32 Eurostat (2022). *Africa-EU – international trade in goods statistics.* https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Africa-EU_-_international_trade_in_goods_statistics#Africa.E2.80.99s_main_trade_in_goods_partner_is_the_EU

33 Reliefweb. (2021). *Team Europe mobilises to support African economies*. https://reliefweb.int/report/world/team-europe-mobilises-support-african-economies

34 Von der Leyen, U. (2019). *A Union that Strives for More. My Agenda for Europe*. https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en.pdf

35 Herszenhorn, D.M. (2019, December 8). *Von der Leyen ventures to the heart of Africa*. Politico. https://www.politico.eu/article/european-commission-president-ursula-von-der-leyen-ventures-to-the-heart-of-africa-ethiopia-african-union/

36 Council of the European Union. (2020). *Council Conclusions on Africa*. https://www.consilium.europa.eu/media/44788/st_9265_2020_init_en.pdf

37 European Commission. (2020). *European Commission welcomes political agreement on future €79.5 billion for a new instru-*

In the digital realm, there are many interdependencies between Africa and Europe. Most of the data from Africa travels via underwater cables to the rest of the internet via landing points in Europe (Figure 55). European universities and technical organisations have trained some of the African technical experts. Africa may also choose to tap into the EU's regulatory and governance experience and see to what extent it could adapt such experiences within the continent, as it advances with the implementation of its continental free trade area, with a strong digital market component.

But some actors in Europe are concerned that the region has not realised all of this potential and left the space for faster growth of China's digital role in Africa. This concern has been shaping the EU's recent initiatives and activities on digitalisation and Africa.

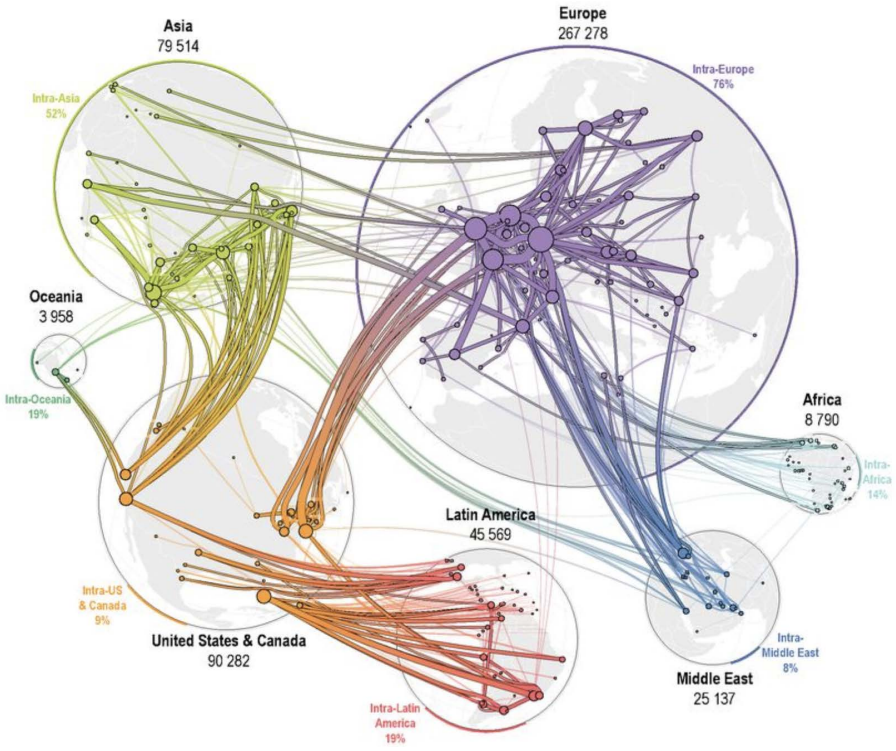


Figure 55. Global internet map.[38]

Strategic convergences between EU and Africa

On a strategic level, there are a few convergences between the EU and Africa that could form the basis for future cooperation in the digital realm.

The first is a shared **concern about the enormous power of big tech companies** based in the USA and China. The EU has been using anti-monopoly, data, and competition regulations to ensure that big tech platforms do not distort the EU's market. Africa is following this 'battle' in Brussels and may choose to take inspiration from EU regulations and approaches and adapt them to regional contexts.

The second common concern is about **data as a personal and economic asset.** More and more African countries are trying to introduce regulations to protect data. In the search for an optimal balance between free data flows and justified protection of data, African countries may rely on the EU's regulatory experience developed around the GDPR.

ment to finance the EU external action. https://ec.europa.eu/commission/presscorner/detail/ro/IP_20_2453

38 Telegeography. (2018). *Global internet map 2018.* https://global-internet-map-2018.telegeography.com

The third shared point of convergence between EU and Africa is **a priority for multilateral solutions,** which would protect core digital interests of nation states and shield them from bilateral pressure exercised by the major digital powers. The digital multilateral approach fits well in the overall focus of multilateralism as embedded in the new agreement replacing the 2000 Cotonou Agreement on the relationship between the EU and African, Caribbean, and Pacific (ACP) countries. This post-Cotonou agreement places 'stronger emphasis on cooperation in international fora and on building alliances on the global scenes'.[39] The relationship between the EU and ACP countries is also seen in the context of broader multilateralism, and their working together at the UN.[40] There are some differences, however, when it comes to multistakeholder methods. African countries are more inclined to the traditional intergovernmental method, partly because they lack the institutional and human resources required to follow multiple multistakeholder processes on digital policy.

The fourth common element is **a drive towards digital/cyber/tech sovereignty** by both EU and African countries. As many actors are in search of an optimal formula of digital sovereignty which will ensure integration in the global market while protecting certain national priorities, EU and African actors can share experiences in striking right balances and trade-offs around the question of digital sovereignty.

The fifth area of convergence is **the centrality of human-centric approach** as often promoted by Europe and increasingly by Africa. The approach wants to put technology in the service of people, protect fundamental rights, and 'harness the power of technology to find real solutions to the challenges our societies face, fighting poverty in an inclusive way that leaves no one behind'.[41] The human-centric approach to technology is perhaps best-defined in the area of AI and introduced in the EU's *Ethical Guidelines for Trustworthy AI*, and has since become an important point of reference for discussions on the impact and use of (emerging) digital technology.

In the next section, we analyse policy spaces and concrete initiatives that could convert the above listed strategic convergence into political and diplomatic realities.

AU-EU summits

From the perspective of traditional diplomacy, the AU-EU Summits are some of the most important arenas for shaping relationships, clarifying priorities, and agreeing on concrete measures. After meetings in 2000, 2007, 2010, 2014, and 2017, the 6th AU-EU summit took place in February 2022.

While the declaration of the first summit (2000) remained silent on digital issues, the second summit (2007) adopted the *Joint Africa-EU Strategy* and led to the establishment of the *Africa-EU Partnership*, both of which address digital issues. The strategy focuses on bridging the digital divide through harmonisation of policy and regulatory frameworks, investment in broadband infrastructure, and support for non-commercial e-services.[42] The strategic plan originating from the third summit (2010) further fleshes out the joint strategy and, in particular, concretises aims in the area of ICT. Here, ICT is put in the context of socio-economic growth and sustainable development. Digital infrastructure is the main focus and the digital economy and digital literacy and skills development are mentioned as part of the priority action to support the development of an inclusive information society in Africa.[43]

---

39 European Commission. (2021). *Questions and Answers on the new EU/Africa-Caribbean-Pacific Partnership Agreement*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1553

40 European Commission. (2020). *Q&A: Political deal EU new Partnership with OACPS.* https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2303

41 Vestager, M. (2020, February 28). *Africa and Europe – partners for a human-centric digital transformatio*n. Strathmore College, Nairobi. https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/africa-and-europe-partners-human-centric-digital-transformation_en

42 EU-Africa Summit. (2007). *The Africa-EU Strategic Partnership: A Joint Africa-Eu Strategy*. https://africa-eu-partnership.org/sites/default/files/documents/eas2007_joint_strategy_en.pdf

43 Africa-EU Summit. (2010). *Joint Africa EU Strategy Action Plan 2011-2013*. https://africa-eu-partnership.org/sites/default/files/documents/03-jeas_action_plan_en.pdf

The declaration of the fourth summit mentions digital infrastructure and ICT in the context of development, growth, and human rights.[44] The main angle of approach, as detailed in the summit's roadmap, is through digital infrastructure, and also includes aims towards (a) 'harmonisation and alignment of the appropriate aspects of e-communications policies and regulatory frameworks between Africa and the EU, including cybersecurity'; (b) connection of research and education networks through e-infrastructures; and (c) enhancement of ICT capacities.[45]

The joint declaration of the fifth summit in 2017 shows a shift of focus towards discussing digital through the lens of technological development and the digital economy. The realisation of opportunities in this area is envisioned through 'exchanging on measurable ICT policy, legal and regulatory frameworks including cyber-security and biometrics', investment in infrastructure, and mainstreaming digitalisation.[46]

In preparation for the sixth AU-EU summit, an AU-EU ministerial meeting took place in October 2021. After 2017, this was the second meeting at ministerial level. In relation to digital, the meeting agreed on facilitating investment and advancing 'safe, sustainable, and inclusive digital transformation'.[47] This meeting was followed by the joint AU-EU-ITU event *Towards Digital Africa*, which emphasised digital as a key pillar of the relationship between the AU and the EU.[48]

The sixth AU-EU summit in February 2022 saw the launch of an Africa-Europe Investment Package of €150 billion dedicated to helping 'build more diversified, inclusive, sustainable and resilient economies'. Support for digital transformation efforts is envisioned as a key pillar of the package, with a focus on investments in infrastructure for 'trusted connectivity', affordable access to the digital and data economy, and boosting digital entrepreneurship and skills.[49]

DETF and D4D Hub

The **AU–EU Digital Economy Task Force (DETF),** initiated in 2018, marked a practical step in formulating digital strategic relations between the EU and Africa. DETF was created to provide a platform for cooperation between the private sector, donors, international organisations, financial institutions, and civil society. The task force's 2019 report makes a number of policy recommendations: acceleration of the achievement of universal broadband access, digital skills training, supporting digital entrepreneurship through improved access to finance and business support services, and accelerated adoption of e-services.[50] These recommendations are integrated into the EIB's approach to financing.[51]

The **AU–EU Digital for Development (D4D) Hub** was initiated in 2020 as part of a wider initiative to improve coordination among member states and EU institutions. It focuses on providing

44 EU-Africa Summit. (2014). *Fourth EU-Africa Summit. Declaration*. https://africa-eu-partnership.org/sites/default/files/userfiles/2014_04_01_declaration_4th_eu-africa_summit_en.pdf

45 EU-Africa Summit. (2014). *Fourth EU-Africa Summit. Roadmap 2014-2017*. https://www.consilium.europa.eu/media/21520/142094.pdf

46 AU-EU Summit. (2017). *Investing in Youth for Accelerated Inclusive Growth and Sustainable Development. Declaration*. https://www.consilium.europa.eu/media/31991/33454-pr-final_declaration_au_eu_summit.pdf

47 African Union [AU]. (2021). *Joint Press Statement Second AU-EU Ministerial Meeting*. https://au.int/en/pressreleases/20211028/joint-press-statement-second-au-eu-ministerial-meeting

48 Delegation of the European Union to the Council of Europe. (2021). *Towards digital Africa: Accelerating the achievement of the sustainable development goals*. https://eeas.europa.eu/delegations/council-europe/106908/towards-digital-africa-accelerating-achievement-sustainable-development-goals

49 Sixth AU-EU Summit. (2022). *A Joint Vision for 2030*. https://www.consilium.europa.eu/media/54412/final_declaration-en.pdf

50 European Commission. (2019). *New Africa-Europe Digital Economy Partnership. Accelerating the Achievement of the SDGs*. https://digital-strategy.ec.europa.eu/en/library/new-africa-europe-digital-economy-partnership-report-eu-au-digital-economy-task-force

51 European Investment Bank [EIB]. (2021). *The rise of Africa's digital economy. The European Investment Bank's activities to support Africa's transition to a digital economy*. https://www.eib.org/attachments/thematic/study_the_rise_of_africa_s_digital_economy_en.pdf

capacity building for institutions to develop appropriate policies and development plans, facilitating knowledge sharing between stakeholders, and promoting dialogues between various stakeholders within the digital sector.[52] The main challenge for the hub is to find the way to fit with other activities and funding under the EU's Neighbourhood, Development and International Cooperation Instrument - Global Europe (NDICI-Global Europe).

So far, the main focus of the hub has been on digital regulation and governance especially in the data field. However, there are doubts over the effectiveness of hub's activities in competing with the influence of China and the USA, mainly due to slow decision-making process, procurement rules, and lack of priorities.[53] Some of these weaknesses are addressed by member states taking their lead in specific areas including Germany on data, France on connectivity/infrastructure, Belgium on development, Estonia on e-commerce, and Luxembourg on cybersecurity.

Related projects are the *African European Digital Innovation Bridge* (AEDIB) and the *EU–AU Data Flagship*. The latter will work towards a joint and non-binding data framework based on common principles, in particular with the creation of the African Single Digital Market in mind.[54] Personal data protection and interoperability are key themes.

While these and other partnership and cooperation initiatives continue to be implemented, it will take time for them to be assessed from the perspective of their effectiveness and overall acceptance by African stakeholders.

Cooperation in infrastructure and connectivity: Global Gateway Africa-Europe Investment Package

In 2021, the European Commission announced the Global Gateway strategy dedicated to supporting infrastructure development around the world. Within the Global Gateway, the *Africa–Europe Investment Package* was launched in 2022 to support Africa's 'strong, inclusive, green and digital recovery and transformation'.[55] Investments are envisioned in initiatives such as the deployment of a EurAfrica Gateway submarine fibre cable connecting the two continents, the construction of networks of fibre cables across Africa, and the consolidation of the Africa Europe Digital Innovation Bridge to support countries in strengthening their digital and innovation ecosystem and promote intercontinental cooperation.[56]

Worth noting is that the Global Gateway infrastructure investments are meant to be coupled with assistance for partner countries to ensure 'the protection of personal data, cybersecurity and the right to privacy, trustworthy AI, as well as fair and open digital markets'. Moreover, the investments are to be aligned with 'standards and protocols that support network infrastructure and resilience, interoperability, and an open, plural and secure internet'.[57]

---

52 D4D. (n.d.). *Supporting Africa's digital transformation*. https://d4dhub.eu/au-eu-project

53 Teevan, C. (2021). *Building strategic European digital cooperation with Africa*, Briefing note 134 by The European Centre for Development Policy Management (ECDPM) Maastricht. https://ecdpm.org/publications/building-strategic-european-digital-cooperation-with-africa/

54 D4D. (n.d.). *Eight innovative projects*. https://d4dhub.eu/projects

55 European Commission. (n.d.). *EU-Africa: Global Gateway Investment Package*. https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en#accelerating-the-digital-transition

56 European Commission. (2022). *EU-Africa: Global Gateway Investment Package - Digital transition.* https://ec.europa.eu/commission/presscorner/detail/en/fs_22_1117

57 European Commission. (2021). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank – The Global Gateway.* https://ec.europa.eu/info/sites/default/files/joint_communication_global_gateway.pdf

Initiatives in digital governance

Through the so-called Brussels effect, the EU is shaping global digital governance and regulation. The most prominent example has been the GDPR, which has influenced data governance worldwide, including in Africa. The GDPR serves as a blueprint and inspiration for national and regional data regulation. In addition, the regulation is also introduced in EU's foreign and development agreements such as EU-ACP agreement. EU's data rules are also supplemented by regulations on industrial and other non-personal data. Some aspects of the recently adopted *Digital Service Act* and *Digital Markets Act* relate to data protection as well.

In addition to data, digital governance cooperation can be further developed in the field of cybersecurity (the EU's new network and information security directive), AI (the EU's AI Act) and other regulatory areas where the EU has expertise and experience: competition policy, e-commerce, and standardisation.

4. India

Among the major actors, India is probably the closest to become a role-model for Africa's digital development. In supporting this point, the *Financial Times* indicates similarity in the young population under the age of 25 (India – 50%; Africa – 60%). Another analogy is the growing gap between digitally savvy mega cities and vast rural areas.[58]

Thus, it is not surprising that digital has a high relevance among the priorities of the Indian government for cooperation with Africa. Digital health and telemedicine are areas where India is concentrating efforts in Africa. They build on an overall interest of African players for healthcare in India. For example, the number of Africans visiting India for so-called health tourism increased from 5.4% of the total health tourist visit in 2010 to 15.4% in 2019.[59] Digital health initiatives focus on joint ventures in clinical research and educational programmes.

On e-government, one priority across Africa is to provide citizens with a digital identity as the basis for their full access to digital services. But digital identification is also a highly controversial issue, given the risks they pose for privacy protection and misuses of digital identification systems. Aadhar, India's biometric digital identification system, is of particular interest for African countries. Experience from deploying Aadhar in India is relevant due to similar challenges that Africa faces, for instance in providing identity to rural populations often without digital skills and expertise.

Africa's share in India's foreign investment between 2017 and 2019 was 15%. It is interesting to note that 82% of this investment was routed via Mauritius due to its favourable tax regime.[60]

India signed memoranda of understanding on cybersecurity and digital cooperation with the following African countries: Morocco, Egypt, Seychelles, South Africa, Kenya, and Mauritius.

[58] Hruby, A. (2019, November 4). Africa should look to India for digital inspiration. *Financial Times*. https://www.ft.com/content/5237edd3-2763-4ac7-a16a-8bec17b58167

[59] Karingi, S. & Naliaka, L.N. (2022, February 25). *The future of India-Africa relations: Opportunities abound.* Brookings. https://www.brookings.edu/blog/africa-in-focus/2022/02/25/the-future-of-india-africa-relations-opportunities-abound/

[60] Ibid.

IV
Recommendations

This study started with acknowledging the reality that African countries do not have ready-made digital foreign policies. There is no specific written framework solely focused on outlining digital-policy-related goals and objectives countries should be pursuing in their international relations. However, African actors are not completely absent from international digital governance, as they participate in various technical, economic, and legal policy processes and initiatives.

As the various sections of this study reveal, countries integrate certain elements of foreign policy in various documents and strategies dealing with digital issues (digital economy, cybersecurity, broadband, skills, etc.). Policies and frameworks devised by continental and regional organisations also include international aspects. Several countries actively follow digital agenda in the work of international organisations such as ITU and the HRC. Moreover, actors from the business, technical, civil society, and academic communities can be seen as actors of foreign policy, as they advance regional and national interests through their participation in international processes such as the IGF and ICANN.

Governments and continental and regional initiatives should build on these realities to ensure that African voices are indeed stronger in international digital processes, and that these processes meaningfully consider the region's interests and needs. The active participation of African actors in global digital policy is not only about advancing their interests, but also the key for building an inclusive, safe, secure, and sustainable digital future for humanity. To this aim, actions that could be undertaken by African governments and regional and continental organisations include:

Ensure digital priorities are clearly reflected in foreign policies/international relations

- As it shapes its path towards sustainable digital development, Africa has multiple priorities to focus on, from expanding access, connectivity, and digital skills, to supporting innovation and the growth of the digital economy. Advancing these priorities requires first and foremost adequate enabling environments, in the form of policies, regulation, legislation, and institutions capable of fostering digital transformation processes that respond to the region's needs and interests. At the same time, clearly reflecting these priorities in the foreign policies and international relations of countries and continental and regional institutions would be beneficial for the continent and contribute to ensuring that African perspectives on digital issues are more strongly articulated at the international level.
- Integrating digital issues into foreign policies could be done through several approaches. Countries and institutions should analyse the various options; assess them against the backdrop of their own contexts, priorities, and resources; and choose the model that works best for them.
    - Embedding digital issues into general foreign policy strategies.
    - Including elements of foreign policy in digital-related strategies and policies dealing with issues such as overall digital transformation, cybersecurity, digital economy, and infrastructure (an approach several countries have already started implementing). Where such elements are reflected in various policy documents, there needs to be consistency across these documents and coordination in their implementation.
    - Developing dedicated digital foreign policy strategies. While such strategies could be inspired by those of countries that have put in place similar initiatives, they would need to be strongly anchored in local realities and needs in order to be effective and efficient.

Prioritise engagement in specific international digital governance processes

- In the short to medium term, countries should strengthen their engagement in those international processes that reflect their digital policy priorities. This is not to say that other digital processes should be ignored, or left aside, but should be seen rather as a matter of prioritising the allocation of the usually limited resources (human, financial) countries have at their disposal.

Strengthen participation in International Geneva

- Most digital issues of high relevance for Africa are addressed in International Geneva, from commercial to development and humanitarian ones, from ITU that deals with infrastructure and standards and the WTO that handles e-commerce, to the World Health Organization (WHO) and the World Intellectual Property Organization (WIPO). Countries' permanent missions at the UN in Geneva need to be properly equipped to engage with international organisations in digital policy processes and link these processes to digital activities in their home countries.

Continue to prioritise economic and development considerations in bilateral and multilateral relations

- Africa is emerging in the centre of competition between major powers for shaping future digital governance models and for asserting dominance over networks, data, and digital markets. In the fast-changing digital geopolitical ecosystem, situations arise when one actor or another tries to push African countries into picking one side (e.g. choose between US and Chinese technology, support initiatives that are usually framed – more or less explicitly – in opposition to one governance model or another). When faced with such choices, African countries need to continue to prioritise their economic and development considerations related to digital issues over geopolitical ones, in line with their national priorities and interests.

Strengthen the whole-of-government approach

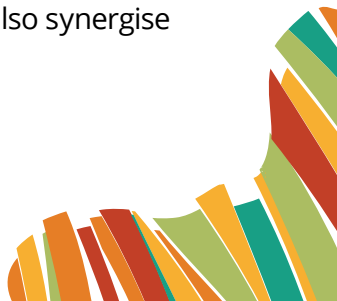
- Countries should ensure that digital governance reflects horizontally the impact of digitalisation and that the various ministries, agencies, and other public institutions dealing with trade, economic, security, cultural, and other issues integrate digital aspects in their work. To this aim, capacity development and experience sharing with international partners should be leveraged to conduct policy research, training, and immersion across governmental bodies.

Facilitate the whole-of-society approach

- Countries should support the involvement of the tech community, businesses, and civil society in digital governance processes on all levels from national to global. They should then galvanise existing capacities within these communities – which already participate in various processes such as ICANN and the IGF – to enhance participation in international digital policy spaces. Activating the diaspora, academia, local communities, youth, and other African actors should also be considered.
- Countries could also benefit from supporting the strengthening of national and regional IGF initiatives and encouraging them to more actively contribute to the global IGF, as a way to better reflect African voices and positions in global debates. At the same time, they can leverage the multistakeholder nature of IGF initiatives across the region to consult – formally or informally – actors on regional and national priorities to advance and positions to take in international digital governance processes.

Foster coordinated positions in international digital governance

- Notwithstanding the economic, cultural, social, and political diversity across Africa, countries could benefit from having coordinated positions on matters discussed in international processes and organisations. The AU and RECs could be leveraged as frameworks to coordinate and harmonise – where possible and relevant – African positions to be advocated for in international processes. Where feasible, individual governments could also synergise directly with their counterparts.



Devise long-term approaches for building academic, research, and digital policy capacities of the next generation of African diplomats and policymakers

Such approaches would include:

- Developing research capacities and academic programmes in the field of digital foreign policy and diplomacy.
- Developing individual and institutional capacities within MFAs to follow digital issues.

Annex I:
Analysis of eight focus countries

This section contains an analysis of digital diplomacy and foreign policy elements of eight African countries.

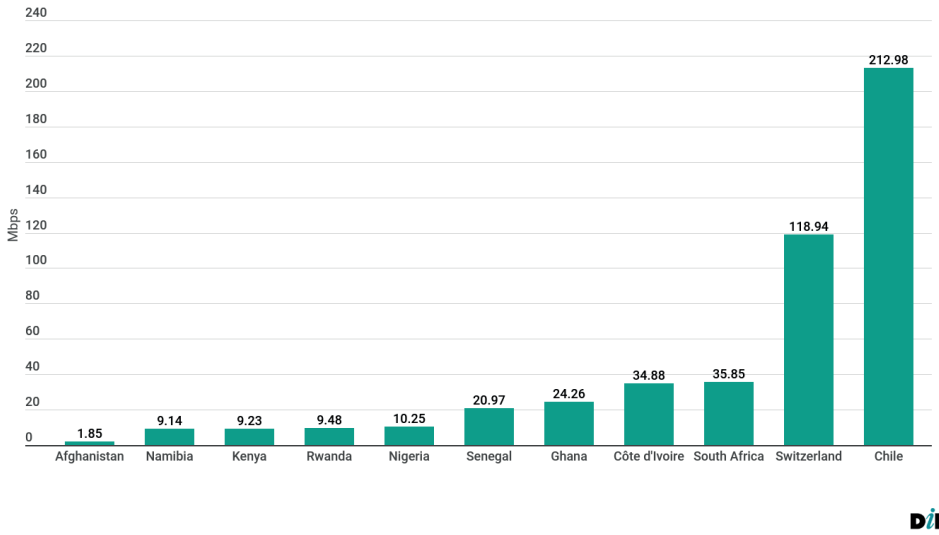
Ghana	Côte d' Ivoire
Kenya	Namibia
Nigeria	Rwanda
South Africa	Senegal

The first part sets the stage by providing an illustrated comparative analysis of these eight countries, which differ in digital developments, priorities, and involvement in international activities.

The second part includes a digital profile for each country with statistics and rankings, national strategies and legislations, and the involvement levels of respective countries in global digital policy.

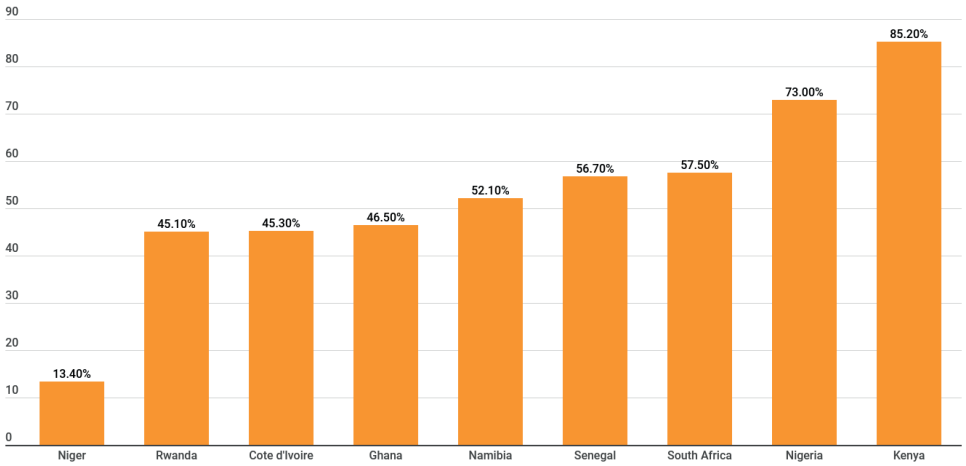
1. Comparative survey

Average speed of internet access (fixed broadband) from the slowest (Afghanistan) to the fastest (Chile), with the eight focus countries in between.[1]



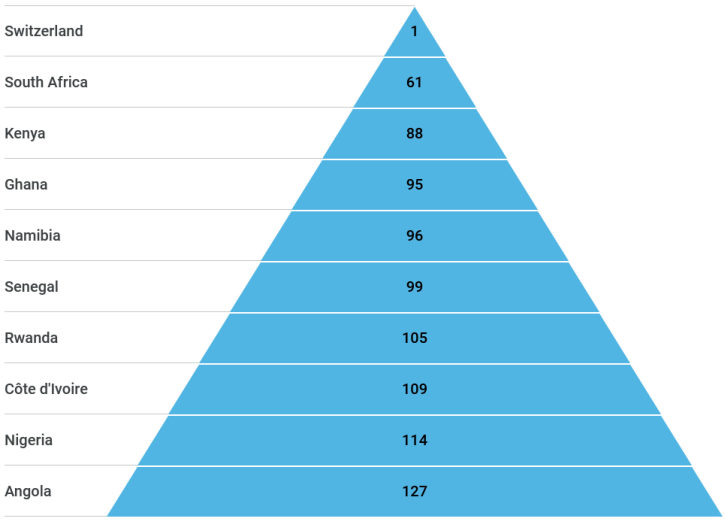
[1] Ookla. (2022). *Speedtest Global Index (July 2022).* https://www.speedtest.net/global-index

Internet penetration (percentage of population) rate, from the lowest in Niger with 13.40% to the highest in Kenya with 85.20%.[2]



DiPLO

The **global innovation index** is a complex calculation that involves a wide range of data from internet access to publications in scientific journals. Countries are ranked according to their positions, and relative to the holders of the first (Switzerland) and last (Angola) positions.[3]



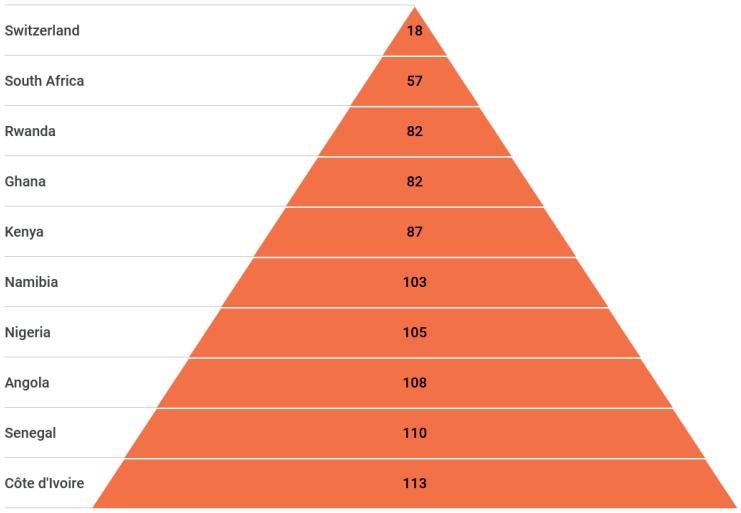
DiPLO

The **e-participation index** focuses on government use of online services in providing information to citizens (e-information sharing), interacting with stakeholders (e-consultation), and engaging in decision-making processes (e-decision-making). Countries are ranked according to their position in the index, from a high e-participation level (Switzerland) to a low level (Côte d'Ivoire).[4]

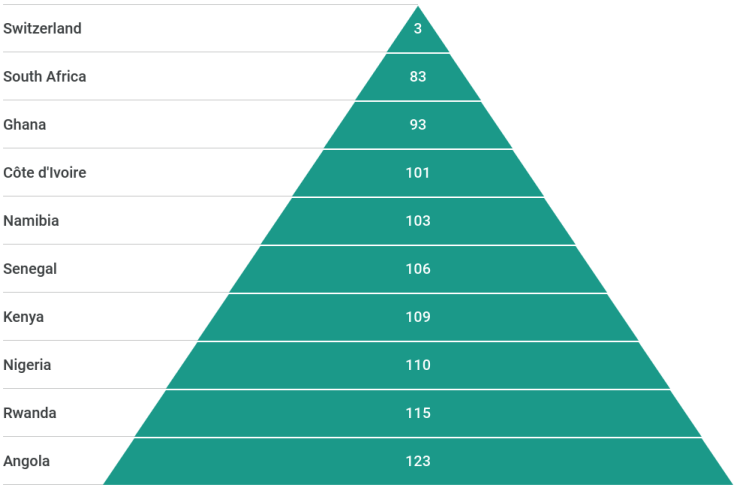
2 Statista. (2022). *Internet users statistics for Africa.* https://www.internetworldstats.com/stats1.htm

3 World Intellectual Property Organization [WIPO]. (2022). *Global Innovation Index 2022. What is the future of innovation-driven growth?* https://www.wipo.int/publications/en/details.jsp?id=4622

4 Ibid. The index is derived as a supplementary index to the UN E-Government Survey: United Nations Department of Economic and Social Affairs [UN DESA]. (2020). *United Nations E-Government Survey 2020.* https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020. Data year: 2020.

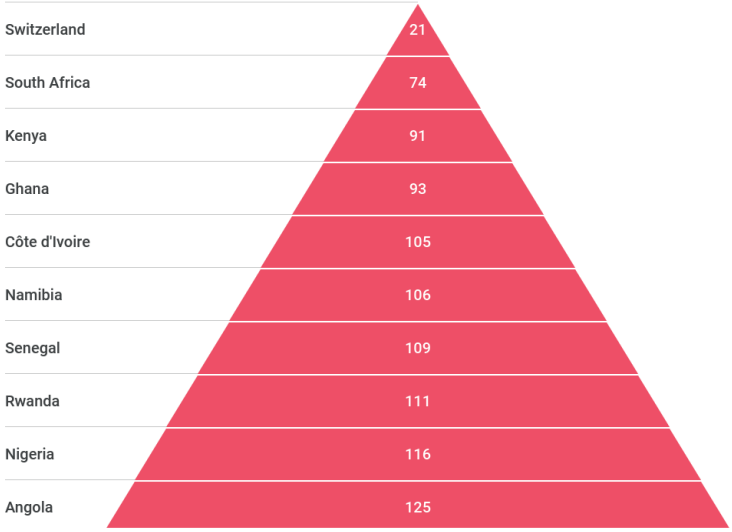


ICT use is a composite index that measures four ICT indicators (25% each): (a) percentage of individuals using the internet; (b) fixed (wired) broadband internet subscriptions per 100 inhabitants; (c) active mobile broadband subscriptions per 100 inhabitants; and (d) mobile broadband internet traffic (gigabytes/subscriptions). Countries are ranked according to their position in the index, from the highest rate of ICT use (Switzerland) to the lowest (Angola).[5]



5 World Intellectual Property Organization [WIPO]. (2022). *Global Innovation Index 2022. What is the future of innovation-driven growth?* https://www.wipo.int/publications/en/details.jsp?id=4622 The calculations are based on data from WIPO and the World Telecommunication/ICT Indicators Database (February 2022 edition). Data year: 2020.

ICT access is a composite index that weights four ICT indicators (25% each): (a) percentage of population covered by mobile networks (at least 3G); (b) mobile cellular telephone subscriptions per 100 inhabitants; (c) international internet bandwidth (bit/s) per internet user; and (d) percentage of households with internet access. Countries are ranked according to their position in the index.[6]



[6] World Intellectual Property Organization [WIPO]. (2022). Global Innovation Index 2022. *What is the future of innovation-driven growth?* https://www.wipo.int/publications/en/details.jsp?id=4622. The calculations are based on data from WIPO and the World Telecommunication/ICT Indicators Database (February 2022 edition). Data year: 2020.

2. Digital profiles of eight focus countries

Ghana

Digital profile

Population 2022, estimate	**Internet penetration** Dec. 2021	**Internet users** Dec. 2021	**Internet growth** (2000–2021)	**Facebook subscribers** Apr. 2022	**Number of data centres** 2022[7]
32,154,245	45.9%	14,767,818	49,126%	9,163,200	5

Signatory of

- CoE Convention on Cybercrime (Budapest Convention)
- AU Convention on Cyber Security and Personal Data Protection (Malabo Convention))

Ranking (out of 132 countries)

Source: Global Innovation Index 2022[8]

Global Innovation Ranking	ICT access	ICT use	E-participation	Citable documents H-index[9]	Country-code TLDs/th pop. 15-69[10]	High-tech manufacturing %[11]
95	93	93	82	83	124	86

Key policies and strategies

- *National ICT for Accelerated Development Policy*
- *Broadband Policy and Implementation Strategy*
- *National Cybersecurity Policy and Strategy*
- *Ghana Beyond Aid*
- *National Financial Inclusion and Development Strategy*
- *Digital Financial Services Policy*
- *Cash-Lite Roadmap*

Ghana is a vibrant digital economy with a clear link to international developments. All major strategic documents the country has developed have highlighted the need for international cooperation.

7 Statistics on population, internet penetration, internet users, internet growth, and Facebook subscribers are based on Miniwatts Marketing Group. (2022). *Internet users statistics for Africa.* https://www.internetworldstats.com/stats1.htm. Statistics on data centres are based on Data Center Map. (2022). *Data Centres.* https://www.datacentermap.com/datacenters.html

8 World Intellectual Property Organization [WIPO]. (2022). *Global Innovation Index 2022. What is the future of innovation-driven growth?* https://www.wipo.int/publications/en/details.jsp?id=4622

9 The H-index (2021) is the countries' number of published articles (H) that have received at least H citations.

10 The total number of registered domain names under the country's ccTLD, per thousand population, 15–69 years old (December 2021).

11 High-technology and medium-high-technology output as a percentage of total manufacturing output (2019).

Digital economy. The *National ICT for Accelerated Development Policy* lists the development of a 'dynamic export-led and globally competitive ICT industry' and 'securing a place for Ghana in the international economic system' as priorities.[12] These goals are reinforced in the *Ghana Beyond Aid* policy, which foresees that by 2028 the country 'would have leveraged its abundant human talent to become a leader (at least in Africa) in the digital economy'.[13]

Ghana is among the African countries that have introduced VAT on digital services.

Cybersecurity. The fast rise in ranking of the Global Cybersecurity Index (GCI) illustrates Ghana's success in developing cybersecurity infrastructure. In the 2020 GCI, Ghana rose to the 43rd position with an 86.69% score, significantly higher compared to previous years – 32.6% in 2017 and 43.7% in 2018.

Ghana's *National Cyber Security Policy and Strategy* calls for the country's active participation in all relevant international cybersecurity bodies, panels, and multinational agencies.[14] This approach was reiterated in 2020 when the Ghanaian parliament passed the *Cybersecurity Act* with provisions related to international cooperation. The act mandates the Cybersecurity Authority of Ghana to implement and enforce international treaties on cybercrime and cybersecurity endorsed by the country; to cooperate with international agencies; and to establish a cybersecurity incident point of contact which would facilitate international cooperation on cybersecurity matters.[15]

These strategic priorities are not only written in policy documents, but also put into practice, making Ghana one of the most active African countries in international cybersecurity and cybercrime processes. Ghana has ratified both the Budapest and Malabo conventions. It has also been very active in – and supportive of – the OEWG, where it has advanced several proposals aimed at establishing the OEWG as a global platform for cybersecurity, dedicated to promoting dialogue and exchanges of best practices, raising awareness, facilitating consultation among states, and providing information on capacity building. Ghana further proposed the establishment of a global repository of existing confidence-building efforts at regional and sub-regional levels on effective responses to threats to critical information infrastructure. It also suggested that national points of contact of focal institutions networks be created under the OEWG.

Cybercrime. The *Cybersecurity Act*, among other provisions, mandated the establishment of a 24/7 contact point to tackle cybercrime. As an indication of an advanced regulatory approach, Ghana approaches cybercrime regulation in a cross-cutting manner, by including provisions on cybercrime in electronic transactions and data protection legislation.

Digital skills. The *Ghana Beyond Aid* strategy outlines plans to leverage the country's abundant human talent to become a leader, at least in Africa, in the digital economy by 2028.[16] On the development of AI skills, the *National Entrepreneurship and Innovation Plan* calls for cooperation with private-sector-led initiatives.[17]

The Ghana-India Kofi Annan Centre of Excellence in ICT (AITI-KACE) was established in 2003 as the ICT Capacity Development Agency under the Ministry of Communications and Digitalisation.

---

12 Republic of Ghana. (2003). *The Ghana ICT for Accelerated Development (ICT4D) Policy.* https://nita.gov.gh/theevooc/2017/12/Ghana-ICT4AD-Policy.pdf

13 Ghana Beyond Aid Committee. (2019). *Ghana beyond Aid Charter and Strategy Document*. http://osm.gov.gh/assets/downloads/ghana_beyond_aid_charter.pdf

14 Ministry of Communications, Republic of Ghana. (2015). *National Cyber Security Policy and Strategy. Final draft*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf

15 Parliament of Ghana. (2020). *Cybersecurity Act*. https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf

16 Ghana Beyond Aid Committee. (2019). *Ghana Beyond Aid Charter and Strategy Document*. http://osm.gov.gh/assets/downloads/ghana_beyond_aid_charter.pdf

17 World Bank. (2021). *Harnessing artificial intelligence for development in the post-Covid-19 era: A review of national AI strategies and policies*. https://openknowledge.worldbank.org/handle/10986/35619

The centre promotes individual and institutional capacity building; research and innovation; consultancy and advisory services in ICT; and e-governance solutions in Ghana and Africa.

Ghana's *National ICT for Accelerated Development Policy* calls for cooperation with international educational institutions to facilitate educational exchange and the promotion of ICT education and training, transfer of technology, and collaboration on research and development (R&D).[18] In science diplomacy, there is a call to promote partnerships between local R&D institutions and foreign and international centres of excellence.

Digital finance. The *National Financial Inclusion and Development Strategy* aims to increase financial inclusion to cover 85% of the population by 2023, helping create economic opportunities and reducing poverty. The strategy also outlines goals related to the alignment of national policies and regulations with international standards and principles.[19] The *Digital Financial Services Policy* aims to create a resilient, inclusive, and innovative digital ecosystem.[20] The *Cash-Lite Roadmap* puts forward concrete steps to build an inclusive digital payments ecosystem. This includes better access to financial services, enabling regulation and oversight, and promoting consumer protection.[21]

Ghana has introduced a national ID system with electronic components, seen by the government as an important element towards inclusive finance.[22]

Digital infrastructure. Enabling fast and reliable internet connectivity is among Ghana's digital policy priorities. The *Broadband Policy and Implementation Strategy* describes broadband as 'a critical prerequisite to support innovators and entrepreneurs to re-assert their productive and market capabilities in the local and global IT sector'.[23] The country is also committed to adopting and enforcing international technical standards; to this aim, it participates in international standardisation work at ITU, ISO, and IEC. Actors from Ghana are also actively involved in ICANN's work, in particular within the constituencies representing civil society and the business community.

[18] Republic of Ghana. (2003). *The Ghana ICT for Accelerated Development (ICT4D) Policy.* https://nita.gov.gh/theevooc/2017/12/Ghana-ICT4AD-Policy.pdf

[19] Republic of Ghana. (2018). *National Financial Inclusion and Development Strategy.* https://mofep.gov.gh/sites/default/files/acts/NFIDs_Report.pdf

[20] Ministry of Finance, Ghana. (2020). *Digital Financial Services Policy.* https://mofep.gov.gh/sites/default/files/acts/Ghana_DFS_Policy.pdf

[21] Republic of Ghana. (2020). *Towards a Cash-Lite Ghana. Building an Inclusive Digital Payments Ecosystem*. https://mofep.gov.gh/sites/default/files/acts/Ghana_Cashlite_Roadmap.pdf

[22] Barasa, H. (2022). *Digital government in sub-Saharan Africa: Evolving fast, lacking frameworks.* Tony Blair Institute for Global Change. https://institute.global/policy/digital-government-sub-saharan-africa-evolving-fast-lacking-frameworks

[23] Ministry of Communications, Republic of Ghana. (2012). *National Broadband Policy and Implementation Strategy.* https://moc.gov.gh/sites/default/files/downloads/GhanaBroadbandStrategyFinal.pdf

Kenya

Digital profile

Population 2022, estimate	**Internet penetration** Dec. 2021	**Internet users** Dec. 2021	**Internet growth** (2000–2021)	**Facebook subscribers** Apr. 2022	**Number of data centres** 2022
55,752,020	85.2%	46,870,422	23,335%	12,445,700	9

Signatory of

- CoE Convention on Cybercrime (Budapest Convention)
- AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)

Ranking (out of 132 countries)

Source: Global Innovation Index 2022

Global Innovation Ranking	ICT access	ICT use	E-participation	Citable documents H-index	Country-code TLDs/th pop. 15-69	High-tech manufacturing %
88	91	109	87	52	92	83

Key policies and strategies

- *National Digital Master Plan*
- *Digital Economy Blueprint*
- *National ICT Policy*
- *National Broadband Strategy*
- *National Cybersecurity Strategy*

Kenya is among the most vibrant digital economies on the African continent. This has been achieved due to a combination of factors, including an energetic private sector, smart regulation, and a comprehensive engagement with international actors.

M-Pesa is an example of how Kenya's digital footprint expands regionally and internationally: The mobile phone-based money transfer service was launched in 2007 by Safaricom and Vodafone in Kenya and became one of the global symbols of financial inclusion. It is now operational across multiple African countries, as well as beyond the continent, in countries such as Germany, China, and the UAE. M-Pesa is also an inspirational example of how enabling policy environments – created through cross-cutting cooperation between electronic communications, financial, and competition regulators – can drive digital growth.

Digital developments are guided by the *National Digital Master Plan* (2022–2032), whose overall aim is to develop a 'robust, secure, affordable, accessible and reliable digital ecosystem which benefits the public and private sector, and improved quality of life'.[24] Such a digital ecosystem would have a strong digital economy at its core, well integrated into the international ecosystem.

[24] Ministry of ICT, Innovation and Youth Affairs, Kenya. (2021). *The Kenya National Digital Master Plan.* https://repository.

Digital economy. One of the master plan's specific objectives is to position Kenya as a 'globally competitive digital economy' by creating a 'globally attractive legal, regulatory, and policy ecosystem that provides adequate support to start-ups'. The plan further envisions Kenya as 'a leader in emerging technology adoption, localisation, and utilisation for development', as well as in global discourses and discussions on issues related to emerging technologies.

Similar goals appear in the country's *Digital Economy Blueprint*, which notes that the digital economy offers Kenya a leapfrogging opportunity for economic development, and outlines objectives and actions to help the country 'become a regional and global innovation leader driving a strong sustainable economy and a better society'.[25] The blueprint also outlines the importance of integrating Kenya's digital economy into Africa's single market, as a way to create economies of scale and enable further growth of local and regional economies.

Likewise, the *National ICT Policy* wants Kenya to 'gain global recognition for innovation', develop an innovation and start-up ecosystem that can lead globally, and 'become a more prosperous participant in the global economy'.[26] Another measure proposed in the policy is to support the growth of local e-commerce platforms with global reach. The document also reflects the country's ICT leadership aspiration, by noting the desire of Kenyans to be 'leaders and innovators in the fourth industrial revolution and so we want to attract and create the best educational institutions in the world'.

International partnerships and cooperation are overarching themes across Kenya's digital policies and strategies. The country intends to foster links with, and seek support (technical, material, financial, capacity development) from international development partners to implement elements of its *National Digital Master Plan* and other ICT and digitalisation policies. As stated in its *National ICT Policy*, it also wants to 'leverage regional and international cooperation and engagement to ensure that [it] is able to harness global opportunities'.

Digital finance. Advancing financial inclusion features prominently in Kenya's digital strategies; the focus is placed on financial inclusion through mobile technology, as has been vividly shown by the M-Pesa payment system's success. The fact that the country has included financial inclusion among its priorities is also an attractive element for companies: Visa opened its first innovation hub in Africa in April 2022.[27]

On cryptocurrencies, the 2022 Global Crypto Adoption Index placed Kenya among the top 20 countries by cryptocurrency adoption.[28]

Kenya is among the first countries to regulate digital credit services; providers are required, among others, to have a local presence and obtain a licence from the Central Bank of Kenya (CBK). CBK published the *Digital Credit Providers Regulations* in March 2022, giving lenders six months to comply with the rules.[29]

Digital taxation. Kenya's digital service tax – which currently applies to over 80 companies – is challenged by the 2021 OECD agreement on new international tax rules.[30] Kenya has not joined

kippra.or.ke/bitstream/handle/123456789/3580/Kenya%20-%20Digital%20Master%20Plan.pdf

25 Republic of Kenya. (2019). *Digital Economy Blueprint*. https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf

26 Ministry of Information, Communications and Technology of Kenya. (2019). *National Information, Communications and Technology Policy*. https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf

27 Njanja, A. (2022, April 6). *Visa unveils its first innovation hub in Africa to drive product development.* TechCrunch. https://techcrunch.com/2022/04/06/visa-unveils-first-innovation-hub-in-africa-to-drive-product-development/

28 Chainalysis. (2022, September 14). The 2022 Global Crypto Adoption Index. *Chainalysis*. https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/

29 Central Bank of Kenya. (2022). *Digital Credit Providers Regulations*. https://www.centralbank.go.ke/2022/03/21/central-bank-of-kenya-digital-credit-providers-regulations-2022/

30 Organisation for Economic Co-operation and Development [OECD]. (2021). *Statement on the two-pillar solution to address the tax challenges arising from digitalisation of the economy with a detailed implementation plan*. https://www.oecd.org/

the agreement yet, one of the country's concerns being that a new taxing regime, compliant with the new international framework – may reduce the number of taxable companies to 11.[31] Dropping national taxes in favour of the OECD deal would therefore mean that countries agree to lower the tax amounts they collect. There is also an overall concern that the agreement tends to favour developed countries.

Cybersecurity. The *National Cybersecurity Strategy* outlines the government's commitment to work with international partners to improve the country's cybersecurity posture. Also highlighted as an action line is Kenya's participation in the development and implementation of international laws, agreements, treaties, policies, norms, and standards on cybersecurity.[32] Enhancing international cooperation on matters of cybersecurity – at the regional and global levels – is also envisioned in *Kenya's Broadband Strategy* and its *National Digital Master Plan*. Moreover, the *National Broadband Strategy*[33] sets the country on a mission to 'build global alliances and promote the application of international law in cyberspace', while the master plan talks about Kenya's commitment to promoting a secure, stable and peaceful cyberspace, while upholding international cybersecurity norms.

Protecting the security and stability of the country's digital infrastructures is another national priority. One that requires the development of comprehensive and offensive cyber capabilities, as Kenya's Cabinet Secretary for Information, Communication and Technology noted in 2016.[34]

Kenya is an active participant in discussions at the OEWG, where it has called for a central role for the UN in coordinating cyber capacity building. The UN could start with initial coordination steps, such as creating a registry of existing capacity building measures and their contact points, and available lessons learned. This registry should then be used to determine a baseline for the measurement of the minimum cybersecurity level necessary for global security and allow countries to perform self-assessments.

Data governance. Kenya has put in place certain data localisation requirements: Section 50 of the *Data Protection Act* of 2019 has a provision according to which 'the Cabinet Secretary may determine certain types of processing which may only be conducted through a server or data centre located in Kenya on the basis of strategic interests of the State or for the protection of revenue'.[35] Moreover, there is a requirement that health data should not be stored outside Kenyan territory. The country also acknowledges that there are issues with data sharing agreements concluded with third countries: 'there is a provision for the data being processed, but no enforcement mechanism to ensure that data meant to remain local remains local' (*National Digital Master Plan*).

Digital skills. The *Kenya National Digital Master Plan* recognises the shortage of digitally skilled workforce not only in Kenya but also the rest of the region, noting that a country with an excess of these skills has the advantage of supplying the region with the required human capital. The plan is therefore for Kenya to 'export, in the future, this skilled workforce to serve the region'. The government has also recently launched a programme to train 20 million Kenyans in digital skills.[36]

---

tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf

31 Mureithi, C. (2021, November 9). *Why Kenya and Nigeria haven't agreed to a historic global corporate tax deal.* Quartz Africa https://qz.com/africa/2082754/why-kenya-and-nigeria-havent-agreed-to-global-corporate-tax-deal/

32 National Computer and Cybercrimes Coordination Committee Secretariat, Republic of Kenya. (2022). *National Cybersecurity Strategy.* https://ict.go.ke/wp-content/uploads/2022/10/KENYA-CYBERSECURITY-STRATEGY-2022.pdf

33 Republic of Kenya. (2018). *National Broadband Strategy 2018–2023.* https://www.ict.go.ke/wp-content/uploads/2019/05/National-Broadband-Strategy-2023-FINAL.pdf

34 Korir, C. (2016, November 29). *Government to curb cyber crimes*. Ministry of ICT, Innovation and Youth Affairs. https://ict.go.ke/government-to-curb-cyber-crimes/

35 Republic of Kenya. (2019). *The Data Protection Act no.24 of 2019.* http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

36 Ng'ang'a, J. (2022, June 8). *ICT Ministry to train 20 million Kenyans on digital skills*. Kenya News Agency. https://www.kenyanews.go.ke/ict-ministry-to-train-20-million-kenyans-on-digital-skills/

Digital infrastructure. Kenya's *National Broadband Strategy* makes reference to attracting an international investor to build a national backbone infrastructure, and lists the World Bank, the Africa Development Bank, ITU, and the ATU as potential international development partners that could contribute to financing infrastructure programmes. International aspects are also indicated in the country's in-the-making 5G strategy,[37] with a commitment to 'participate in international forums to contribute to the development of 5G technology and standards'.

At the national level, Kenya tries to diversify the links through which it connects to the internet. In March 2022, the Pakistan & East Africa Connecting Europe (PEACE) submarine cable system was launched in Kenya, becoming the sixth submarine cable to land there. The cable is a private project by a subsidiary of China-based Hengtong Group and it is operated by HMN Tech (formerly Huawei Marine).[38]

5G networks are another example of diversification. Safaricom has been working with both Nokia and Huawei on its 5G network testing.[39] By December 2021, the company had reportedly rolled out over 200 testing sites in towns like Nairobi, Kisumu, Kisii, Kakamega, and one rural area – Ol Tukai at Amboseli.[40] In another diversification effort, Telkom Kenya has partnered with NEC XON and Ericsson to modernise its sites. The deal also involves growing an additional 2,000 sites for 4G coverage by 2023.[41]

The country's role in global digital developments is recognised in ICANN's 2022 decision to have root server clusters deployed in Kenya.[42] By answering queries for domain names in Africa, Kenya's root server cluster will contribute to reducing latency and improving user experience.

Digital standards. Kenya intends to promote the development and use of open internet standards, and to encourage adherence to globally accepted standards in innovation and the design of devices or software (*National Broadband Strategy*).

---

37 The document was launched for public consultation in late 2021. At the date of publication of this study, it is unclear whether the strategy has been formally approved. Communications Authority of Kenya. (2021). *Public Consultation on the Roadmap and Strategy for 5th Generation Mobile Communications in Kenya.* https://www.ca.go.ke/wp-content/uploads/2021/10/Public-Consultation-Paper-on-5G-Roadmap.pdf

38 PEACE Cable. (2022). *PEACE Cable and Telkom land new submarine cable in Kenya*. http://www.peacecable.net/News/Detail/16640

39 Sharma, R. (2021, March 29). *Safaricom launches 5G in Kenya with Huawei and Nokia*. The Fast Mode. https://www.thefastmode.com/technology-solutions/19389-safaricom-launches-5g-in-kenya-with-huawei-and-nokia

40 Kamau, G. (2021, December 23). *State of 5G in Kenya: What to expect in 2022.* Techweez. https://techweez.com/2021/12/23/state-of-5g-kenya/

41 Telkom. (2021, November 2). Telkom partners with Ericsson and NEC XON to expand its mobile data network. *Telkom News*. https://www.telkom.co.ke/telkom-partners-ericsson-and-nec-xon-expand-its-mobile-data-network

42 Internet Corporation for Assigned Names and Numbers [ICANN]. (2022, February 28). *ICANN-managed root server clusters to strengthen Africa's internet infrastructure*. Press release. https://www.icann.org/resources/press-material/release-2022-02-28-en

Nigeria

Digital profile

Population 2022, estimate	Internet penetration Dec. 2021	Internet users Dec. 2021	Internet growth (2000–2021)	Facebook subscribers Apr. 2022	Number of data centres 2022
211,400,708	73.0%	154,301,195	101,484%	31,860,000	10

Signatory of

- CoE Convention on Cybercrime (Budapest Convention)

Classement (out of 132 countries)

Source: Global Innovation Index 2022

Global Innovation Ranking	ICT access	ICT use	E-participation	Citable documents H-index	Country-code TLDs/th pop. 15-69	High-tech manufacturing %
114	116	110	105	61	99	n/a

Key policies and strategies

- *Digital Economy Policy and Strategy*
- *National Cybersecurity Policy and Strategy*
- *National Broadband Plan*
- *National policy on 5G networks*
- *Guidelines for Nigerian Content Development in ICTs*
- *Cybercrime Act*

Digital economy. Nigeria not only wants to actively participate in the global digital economy, but also to leverage digital technologies in order to become 'a leading player', as noted in its *National Digital Economy Policy and Strategy*.[43] For example, the country aims to become a global outsourcing destination for digital jobs. The plan also highlights a goal of facilitating partnerships with multinational tech companies 'to create platforms for indigenous vendors to serve global markets'.

Cybersecurity. The *National Cybersecurity Policy and Strategy* and the *National Digital Economy Policy and Strategy* highlight the importance of international cooperation on cybersecurity-related issues. Moreover, an entire section of the *Cybercrime Act* is dedicated to international cooperation on jurisdictional issues and law enforcement.[44] Dealing with cybercrime in a cross border context has been a challenge for Nigerian law enforcement agencies since the early 1990s, when the notorious 'Nigerian prince' scam took off, triggered by the economic hardship experienced by the

[43] Federal Ministry of Communications and Digital Economy, Nigeria. (2020). *National Digital Economy Policy and Strategy.* https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file

[44] National Assembly, Nigeria. (2015). *Cybercrimes (prohibition, prevention, etc) Act*. https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

country (caused by failing oil prices, rise in unemployment, etc.). With the emergence of new types of cybercrimes – such as ransomware and other sophisticated social engineering schemes[45] – Nigerian authorities are stepping up international cooperation in cybercrime.

An international juridical aspect was introduced by the March 2022 decision of the ECOWAS Court of Justice, which requested Nigeria to amend its Cybercrime Act to ensure compliance with the country's obligations under the continental and international human rights instruments. The court considered that certain 'vaguely worded and ambiguous' provisions could lead to violations of rights to freedom of expression, information and other rights of human rights defenders, activists, bloggers, journalists, broadcasters, and social media users.[46]

Data governance. The *Guidelines for Nigerian Content Development in ICTs* forbid telecommunication companies from transferring any government, subscriber, and consumer data outside the country.[47]

Digital identity. Nigeria focuses on building a digital identity infrastructure and supplying biometric identity to all citizens, through a project funded by the EIB. Recently, the National Identity Management Commission has been called upon by Nigeria's new data privacy authority to set high standards for data protection and privacy to strengthen the country's digital ID ecosystem.[48]

Diaspora and digital diplomacy intersect in the activities of the Nigerians in the Diaspora Commission (NIDCOM), which was established in 2019 and became particularly active during the pandemic. The Commission took full advantage of online tools – website, social media, and online conferencing – to inform and engage Nigerian diaspora worldwide.[49] In one example of a simple, yet impactful service, NIDCOM provided Nigerians abroad with regular updates on evacuation flights and processes. Nigeria's practical and good practice of digital and diaspora diplomacy could be an inspiration for other African countries in their activities to engage diaspora in their digital foreign policy activities.

Digital infrastructure. The *National Broadband Plan* calls for the creation of new landing points for international submarine cables.[50] The *National Policy on 5G Networks* notes that the government will contribute to global processes on 5G standards while enabling and encouraging the active participation of relevant stakeholders in ITU meetings and events, as well as in the development of national positions for such events.[51]

---

45 Lin, S. (2022, April 10). *The long shadow of the 'Nigerian Prince' scam*. Wired. https://www.wired.com/story/nigeria-cyber-security-crime-antiblackness/

46 ECOWAS Court of Justice. (2022). *Court orders Nigeria to align its cybercrime law with its international obligations*. http://www.courtecowas.org/2022/03/27/court-orders-nigeria-to-align-its-cybercrime-law-with-its-international-obligations/

47 National Information Technology Development Agency, Nigeria. (2019). *Guidelines for Nigerian Content Development in Information and Communication Technology.* https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf

48 Macdonald, A. (2022, April 19). *New Nigerian data protection body calls for stronger privacy standards to drive digital ID.* Biometric Update. https://www.biometricupdate.com/202204/new-nigerian-data-protection-body-calls-for-stronger-privacy-standards-to-drive-digital-id

49 Adesina, O. (2020, September 18). *The Nigerians in Diaspora Commission (NIDCOM): An example of digital diplomacy in practice*. African portal. https://www.africaportal.org/features/nigerians-diaspora-commission-nidcom-example-digital-diplomacy-practice/

50 National Broadband Committee, Nigeria. (2020). *Nigerian National Broadband Plan 2020–2025*. https://www.ncc.gov.ng/documents/880-nigerian-national-broadband-plan-2020-2025/file

51 Federal Executive Council, Nigeria. (2021). *National Policy on Fifth Generation (5G) Networks for Nigeria's Digital Economy.* https://www.ncc.gov.ng/accessible/documents/1019-national-policy-on-5g-networks-for-nigeria-s-digital-economy/file

South Africa

Digital profile

Population 2022, estimate	Internet penetration Dec. 2021	Internet users Dec. 2021	Internet growth (2000–2021)	Facebook subscribers Apr. 2022	Number of data centres 2022
60,041,994	57.5%	34,545,165	1,339%	24,600,000	27

Signatory of

- CoE Convention on Cybercrime (Budapest Convention)

Ranking (out of 132 countries)

Source: Global Innovation Index 2022

Global Innovation Ranking	ICT access	ICT use	E-participation	Citable documents H-index	Country-code TLDs/th pop. 15-69	High-tech manufacturing %
61	74	83	57	31	41	62

Key policies and strategies

- *ICT and Digital Economy Masterplan*
- *Integrated ICT Policy White Paper*
- *South Africa Connect*
- *National Cybersecurity Policy Framework*
- *National Digital and Future Skills Strategy*
- *National Policy on Data and Cloud (draft)*
- *Protection of Personal Information Act*

South Africa is among the most industrialised African countries, with a highly vibrant technological and digital scene.

Digital economy. Supporting domestic businesses to increase their competitiveness on regional and global markets – in particular in emerging tech domains – is among the goals included in South Africa's *ICT and Digital Economy Masterplan*.[52] Another goal is to 'facilitate investment and partnerships with global buyers of digitally traded services'.

Digital governance. South Africa is one of the leading proponents of multilateral internet governance anchored in the UN system, as outlined in the country's *ICT Policy White Paper*.[53] The

[52] Although various online governmental sources indicate that the plan has been approved, we were unable to locate the final version of the document. Therefore, throughout this document we refer to an intermediate draft: Knowledge Executive and Genesis. (2020). *ICT and Digital Economy Masterplan for South Africa. Draft for discussion*. https://www.ellipsis.co.za/wp-content/uploads/2020/08/ICT-and-Digital-Economy-Masterplan-for-South-Africa_Draft-for-discussion_-August_-2020.pdf

[53] Department of Telecommunication and Postal Services, Republic of South Africa. (2016). *National Integrated ICT Policy*

overarching goal is 'ensuring that the internet is governed in the public interest, taking into account the diverse needs of all countries across the world and in line with the principles of the open internet'. Other principles and objectives the paper highlights (when it comes to the position the country should take in international processes) include open internet, central role of governments, equal participation of all governments worldwide, inclusive participation of non-governmental actors 'in their respective roles'.

Digital infrastructure. *South Africa Connect,* the country's broadband policy, indicates that stable, reliable, and widely available broadband infrastructures create 'a context for the development of globally competitive niche ICT-related manufacturing industries'.[54] The deployment of 5G has been a more controversial issue. In the context of the pressure placed on internet resources during the pandemic, the telecom regulator – the Independent Communications Authority of South Africa (ICASA) – issued temporary radio frequency spectrum licences, allowing telecom providers MTN, Telkm, and Vodafone to start emergency 5G deployment in main cities.[55] These licences were set to expire in November 2021,[56] but the operators brought ICASA to court over the decision.[57] Eventually, in March 2022, the regulator announced that spectrum licences were granted to multiple operators, including Vodacom, MTN, Rain, Telkom, and others.[58]

Digital standardisation. A 5G Forum was established by ICASA in 2017 to, among other tasks, assist the authority in preparing contributions to ITU and other relevant standards bodies on 5G-related matters. South Africa is actively participating in standardisation work at ITU; the country's standardisation body is also a member of IEC and ISO.

Cybersecurity. The *National Cybersecurity Policy Framework* for South Africa is intended to provide a holistic approach to cybersecurity and sets out the promotion and strengthening of local and international cooperation on cybersecurity as one of the country's priorities.[59]

Data governance. The *Protection of Personal Information Act* regulates the transfer of personal information about a data subject to a third party in a foreign country under several conditions. In April 2021, discussions on a *National Policy on Data and Cloud* were initiated; an objective outlined in the policy was for the government to introduce strict data localisation requirements for economic development.[60]

South Africa hosts 26 data centres, the highest number in Africa. US-based company Oracle opened the first African data centre in Johannesburg in January 2022; the centre serves some of the major public institutions such as Airports South Africa, the Government Pensions Administrative Agency, and the National Treasury of South Africa.

White Paper. https://www.dcdt.gov.za/documents/legislations/white-papers/file/109-the-national-integrated-ict-policy-white-paper-3rd-october-2016.html

54 Department of Communications, South Africa. (2013). *South Africa Connect: Creating Opportunities, Ensuring Inclusion. South Africa's Broadband Policy.* https://www.ellipsis.co.za/wp-content/uploads/2013/10/NBP-2013.pdf

55 Reuters Staff. (2020, April 17). *South Africa's mobile operators granted emergency lockdown spectrum to meet demand*. Reuters. https://www.reuters.com/article/health-coronavirus-safrica-spectrum-idINKBN21Z17G

56 Independent Communications Authority of South Africa [ICASA]. (2021). *Three months grace period to allow licensees to wind down their use of temporary radio frequency spectrum.* https://www.icasa.org.za/news/2021/three-months-grace-period-to-allow-licensees-to-wind-down-their-use-of-temporary-radio-frequency-spectrum

57 Independent Communications Authority of South Africa [ICASA]. (2021). *ICASA intends to oppose litigation by Telkom SA on the temporary spectrum*. https://www.icasa.org.za/news/2021/icasa-intends-to-oppose-litigation-by-telkom-sa-on-the-temporary-spectrum

58 Independent Communications Authority of South Africa [ICASA]. (2022). *ICASA concluded successful spectrum auction and collects more than R14.4 billion proceeds*. https://www.icasa.org.za/news/2022/icasa-concludes-successful-spectrum-auction-and-collects-more-than-r14-4-billion-proceeds

59 South Africa Government. (2015). *National Cybersecurity Policy Framework for South Africa*. https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

60 Ministry of Communications and Digital Technologies, South Africa. (2021). *Invitation to submit written submission on the proposed National Data and Cloud Policy.* https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

Digital identity. South Africa is among the countries with national IDs with electronic components such as microchips or machine-readable barcodes.

Digital skills. In addition to outlining measures to be taken at the national level to advance digital skills, the *National Digital and Future Skills Strategy* also has an international component. It notes that international collaboration with other higher education institutions, research entities, the private sector, and international bodies, such as ITU and the ILO, is essential for digital R&D and critical to build research capacity.[61]

[61] Department of Communications and Digital Technologies, South Africa. (2020). *National Digital and Future Skills Strategy*. https://www.gov.za/sites/default/files/gcis_document/202009/43730gen513.pdf

Côte d'Ivoire

Digital profile

Population 2022, estimate	**Internet penetration** Dec. 2021	**Internet users** Dec. 2021	**Internet growth** (2000–2021)	**Facebook subscribers** Apr. 2022	**Number of data centres** 2022
27,473,629	44.6%	12,253,653	30,534%	6,554,100	0

Not a signatory of

- AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)

Invited to accede to

- CoE Convention on Cybercrime (Budapest Convention)

Ranking (out of 132 countries)

Source: Global Innovation Index 2022

Global Innovation Ranking	ICT access	ICT use	E-participation	Citable documents H-index	Country-code TLDs/th pop. 15-69	High-tech manufacturing %
109	105	101	113	96	107	n/a

Key policies and strategies

- *National Digital Development Strategy*
- *National Cybersecurity Strategy 2021–2025*5

Digital infrastructure. The country is working on expanding its infrastructure. In 2020, Orange launched its Djoliba submarine cable system covering Cote d'Ivoire and seven other countries across West Africa. The 2Africa submarine cable, which should be connected to Cote d'Ivoire in late 2023, is expected to strengthen connectivity in the country.[62]

Digital economy. The *National Digital Development Strategy* (2021–2025) proposes to accelerate digital transformation at the national level, in order for Africa to be one of Africa's top innovator leaders by 2025.[63]

[62] Barton, J. (2022, April 11). *Cable landing to boost fixed and broadband in Cote d'Ivoire.* Developing Telecoms. https://developingtelecoms.com/telecom-business/market-reports-with-buddecom/13340-cable-landing-to-boost-fixed-and-broadband-in-cote-d-ivoire.html

[63] Ministry of Digital Economy, Telecommunications and Innovation, Republic of Côte d'Ivoire. (2022). *Stratégie Nationale de Développement du Numérique en Côte d'Ivoire (National Digital Development Strategy of Côte d'Ivoire).* https://telecom.gouv.ci/wp-content/uploads/2022/02/Strategie-Nationale-Developpement-du-Numerique-2021-2025.pdf

Cybersecurity. Cote d'Ivoire's *National Cybersecurity Strategy 2021–2025* envisions a leadership role for the country in cybersecurity, within Africa. In addition, the goal to strengthen international cooperation in cybersecurity matters is outlined by the *National Digital Development Strategy*. This also includes specific action lines that relate to active participation in the FIRST network or in the ITU Cyberdrill initiative.

Data governance. The *National Digital Development Strategy* identifies the importance of strengthening national legislation regarding data protection since it is inextricably linked to the safety of cyberspace.

Namibia

Digital profile

Population 2022, estimate	**Internet penetration** Dec. 2021	**Internet users** Dec. 2021	**Internet growth** (2000–2021)	**Facebook subscribers** Apr. 2022	**Number of data centres** 2022
2,587,344	52.1%	1,347,418	4,391%	792,000	0

Signatory of

- AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)

Ranking (out of 132 countries)

Source: Global Innovation Index 2022

Global Innovation Ranking	ICT access	ICT use	E-participation	Citable documents H-index	Country-code TLDs/th pop. 15-69	High-tech manufacturing %
96	106	103	103	104	91	99

Key policies and strategies

- *Overarching ICT Policy*
- *Broadband Policy*
- *National Cybersecurity Strategy and Awareness Raising Plan 2022–2027*

Namibia's *Overarching ICT Policy* aims to ensure that the country is anchored in the 'global information society' and to increase the competitiveness of ICT businesses on international markets.[64]

Infrastructure. Namibia's national broadband policy requires telecom service providers to ensure that the broadband systems they develop comply with international standards.

Data governance. The *Overarching ICT Policy* notes that, to ensure a proper regulation for the 'interface between technology and rights to privacy', the collection and protection of data will comply with international standards.

Gender equality. In 2022, Namibia was ranked 8th in the Global Gender Gap Index by making significant progress from the 12th position in the 2020 report.[65]

[64] Ministry of ICT, Namibia. (2009). *Overarching Information Communications Technology (ICT) Policy.* http://www.nied.edu.na/assets/documents/05Policies/NationalCurriculumGuide/ICT_in_GRN_Policy.pdf

[65] World Economic Forum [WEF]. (2022). *Global Gender Gap Report 2022*. https://www3.weforum.org/docs/WEF_GGGR_2022.pdf

Digital skills. According to the *National Broadband Policy*, access to ICTs and developing ICT related skills in the younger population are national imperatives in enabling Namibia's participation in a competitive global economy.

Cybersecurity. The *National Cybersecurity Strategy and Awareness Raising Plan 2022–2027* includes elements related to advancing international cooperation on cybersecurity-related issues.[66]

[66] Namibia Media Trust. (2021). *Review of Namibia's National Cybersecurity Strategy & Awareness Raising Plan 2022–2027*. https://www.nmt.africa/uploads/614346b1d2ebb/NMTsubmision-ReviewofnationalcybersecuritystratA(22-27).pdf. Some sources note that the strategy was approved by the government in March 2022, while others indicate that, as of October 2022, the strategy was yet to be finalised.

Rwanda

Digital profile

Population 2022, estimate	**Internet penetration** Dec. 2021	**Internet users** Dec. 2021	**Internet growth** (2000–2021)	**Facebook subscribers** Apr. 2022	**Number of data centres** 2022
13,276,513	45.1%	5,981,638	119,532%	806,200	0

Signatory of

- AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)

Ranking (out of 132 countries)

Source: Global Innovation Index 2022

Global Innovation Ranking	ICT access	ICT use	E-participation	Citable documentsH-index	Country-code TLDs/th pop. 15-69	High-tech manufacturing %
105	111	115	82	111	111	93

Key policies and strategies

- *ICT Hub Strategy*
- *Broadband Policy*
- *ICT Sector Strategic Plan*
- *Smart Rwanda Master Plan*
- *National Cybersecurity Strategic Plan*
- *Child Online Protection Policy*
- *National Data Revolution Policy*
- *National Talent Policy*

Rwanda is a fast-growing digital economy, having achieved high visibility due to its digital achievements.

International aspects are stressed in Rwanda's *ICT Hub Strategy*, which calls for partnership with global organisations/institutions to develop the tech-based solutions needed to address socio-economic challenges in areas such as education, health, and agriculture.[67]

Cybersecurity. The *National Cybersecurity Strategic Plan* and the *ICT Sector Strategic Plan* outline the objective of promoting regional and international cooperation, research, and development in the field of cybersecurity. It further talks about the importance of ensuring that ICT-related legal and regulatory frameworks comply with international cybersecurity standards and best

[67] Ministry of Information Technology and Communications, Republic of Rwanda. (n.d.). *ICT Hub Strategy 2024.* https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/ICT_HUB_STRATEGY.pdf

practices.[68] The National Cyber Security Authority is in charge, among other issues, of regional and international cooperation, and research and development in cybersecurity.

Establishing partnerships with international organisations for capacity building in cybersecurity is envisioned in the *ICT Hub Strategy.* Notable is the country's goal of becoming a regional hub for security, through building a sustainable cybersecurity industry as outlined in the *ICT Sector Strategic Plan* and ensuring a secure and resilient cyberspace as outlined in the *Smart Rwanda Master Plan*.

Child online protection. The *Child Online Protection Policy* calls for the establishment of formal cooperation frameworks with regional and global COP communities. It also envisages the ratification of COP-related treaties and protocols and the strengthening and amending relevant criminal laws in line with international standards and best practices.[69]

Data governance. The concept of data sovereignty has been at the core of the government's *National Data Revolution Policy,* which requires that national data be hosted locally: 'Rwanda shall retain exclusive sovereign rights on her national data with control and power over its own data.' However, the policy mentions the importance of collaborating with regional and international stakeholders in building a data industry, and notes that the government will work on attracting investors in the data industry.[70]

Data protection regulations adopt the extraterritorial approach of the EU's GDPR.[71] This means that entities outside of the country that handle citizens' data are subject to the law.

Rwanda intends to develop a national AI policy focused on the ethical use of AI in support of social and economic development.[72]

Gender equality. Rwanda is positioned 6th on the 2022 *Global Gender Gap Index.*[73]

Digital skills. The *National Talent Policy* aims to transform Rwanda 'from a consumer/importer to a producer/exporter of ICTs to the region and global scene' by setting up an IT elite corps. Other policy objectives include digital literacy for all by enhancing digital literacy across all levels of society; a digitally savvy workforce, by workforce upskilling; and coordination of digital literacy initiatives by formulating standards and providing relevant coordination mechanisms.[74]

Digital governance. Smart Africa is an alliance of African heads of state and government dedicated to accelerating sustainable socio-economic development in the knowledge economy. Initiated by Rwandan President Paul Kagame, the alliance began with seven heads of states from Rwanda, Kenya, Uganda, South Sudan, Mali, Gabon, and Burkina Faso. Smart Africa has been working towards a single digital market for the continent. To this end, it has facilitated digital economy policies that each of the alliance members have adopted and is implementing at different stages.

---

68 Ministry of Information Technology and Communications, Republic of Rwanda. (2017). *ICT Sector Strategic Plan*. https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/ICT_SECTOR_PLAN_18-24_.pdf

69 Ministry of ICT and Innovation, Republic of Rwanda. (2019). *Rwanda Child Online Protection Policy*. https://rura.rw/fileadmin/Documents/ICT/Laws/Rwanda_Child_Online_Protection_Policy.pdf

70 Ministry of Youth and ICT, Republic of Rwanda. (2017). *National Data Revolution Policy*. https://statistics.gov.rw/file/5410/download?token=r0nXaTAv

71 Rich, C.J. (2022, January 11). Africa and the Near East: The Region's Privacy Landscape Facing Rapid and Dramatic Changes. *Morrison and Foerster.* https://www.mofo.com/resources/insights/220131-africa-and-the-near-east.html

72 Smart Africa. (2021). *Blueprint: Artificial Intelligence for Africa*. https://smart.africa/board/login/uploads/70029-eng_ai-for-africa-blueprint.pdf

73 World Economic Forum [WEF]. (2022). *Global Gender Gap Report 2022*. https://www3.weforum.org/docs/WEF_GGGR_2022.pdf

74 Ministry of Youth and ICT, Republic of Rwanda. (2016). *National Digital Talent Policy*. https://rwandatrade.rw/media/2016%20MINICT%20Digital%20Talent%20Policy.pdf

Senegal

Digital profile

Population 2022, estimate	**Internet penetration** Dec. 2021	**Internet users** Dec. 2021	**Internet growth** (2000–2021)	**Facebook subscribers** Apr. 2022	**Number of data centres** 2022
17,196,301	56.7%	9,749,527	24,273%	3,802,000	0

Signatory of

- CoE Convention on Cybercrime (Budapest Convention)
- AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)

Ranking (out of 132 countries)

Source: Global Innovation Index 2022

Global Innovation Ranking	ICT access	ICT use	E-participation	Citable documents H-index	Country-code TLDs/th pop. 15-69	High-tech manufacturing %
99	109	106	110	92	110	59

Key policies and strategies

- *Strategie Senegal Numerique 2016–2025 (Digital Senegal Strategy 2016–2025)*
- *National Broadband Plan*
- *National Strategy for the Development of E-commerce*
- *National Cybersecurity Strategy*

Digital economy. The *Digital Senegal Strategy 2016–2025* outlines the goal of developing a digital economy that is competitive at both on regional and global levels.[75] This strategy describes the future steps to promote e-commerce as well as digital financial services. In 2019, the government adopted a *National Strategy for the Development of E-commerce.*

Infrastructure. The *National Broadband Plan* lists the World Bank, the French Development Agency, and the Asian Development Bank as potential funding sources to support broadband deployment projects.[76]

Cybersecurity. Sub-regional, regional, and international cooperation on cybersecurity issues is envisioned in the *Senegalese National Cybersecurity Strategy*[77] and the *Digital Senegal Strategy.*

[75] Ministry of Post and Telecommunications, Republic of Senegal. (2016). *Stratégie Sénégal Numérique (Digital Senegal Strategy).* http://www.numerique.gouv.sn/sites/default/files/Numerique%202025_0.pdf

[76] Ministry of Communication, Telecommunications, Post and Digital Economy, Republic of Senegal. (2018). *Plan National Haut Débit du Sénégal (National Broadband Plan of Senegal).* http://www.numerique.gouv.sn/sites/default/files/Senegal_Plan_National_Haut_Debit_30062018.pdf

[77] Ministry of Communications, Telecommunications, Post and the Digital Economy, Republic of Senegal. (2017). *Sene-*

Digital governance. The *Digital Senegal Strategy* identifies as a priority updating legal frameworks on digital issues, including data protection.

Digital skills. The *Digital Senegal Strategy* considers 'human capital' as one of three prerequisites for a digital Senegal, along with legal and institutional frameworks and digital trust.

galese National Cybersecurity Strategy. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SNC2022-Senegal-NCS-Jan-2018_eng.pdf

Annex II
Abbreviations and acronyms

3GPP	3rd Generation Partnership Project
A4AI	Alliance for Affordable Internet
ACHPR	African Commission on Human and Peoples' Rights
ADFI	African Digital Financial Inclusion Facility
AfCFTA	Africa Continental Free Trade Area
AFI	Alliance for Financial Inclusion
AfIGF	African Internet Governance Forum
AfNOG	African Network Operators Group
AFRALO	African Regional At-Large Organization
AFRIPOL	African Union Mechanism for Police Cooperation
AI	artificial intelligence
AIGS	AI Global Surveillance index
AFRINIC	African Network Information Centre
APC	Association for Progressive Communications
ARSO	African Organisation for Standardisation
ASO	Address Supporting Organization
ATAF	African Tax Administration Forum
ATU	African Telecommunications Union
AU	African Union
AUC	African Union Commission
AUDA-NEPAD	AU Development Agency
BEAC	Bank of Central African States [Banque des États de l'Afrique Centrale]
BEPS	Base Erosion and Profit Sharing
BMZ	German Federal Ministry for Economic Cooperation and Development
BRI	Belt and Road Initiative
CBDC	central bank digital currency
CBM	confidence-building measures
ccNSO	Country Code Names Supporting Organization
ccTLD	country code top-level domain
CCW	Convention on certain conventional weapons
CEMAC	Central African Economic and Monetary Community
CEN-SAD	Community of Sahel–Saharan States
CERT	computer emergency response team
CIPESA	Collaboration on International ICT Policy in East and Southern Africa
CIRT	computer incident response team
COMESA	Common Market for Eastern and Southern Africa
COP	child online protection
CSG	Commercial Stakeholder Group
DFS	digital financial service
DPA	data protection agency

DSR	Digital Silk Road
DST	digital service tax
DTS	Digital Transformation Strategy for Africa
EAC	East African Community
ECCAS	Economic Community of Central African States
ECOWAS	Economic Community of West African States
EIB	European Investment Bank
ENBIC	ECOWAS National Biometric Identity Card
ETSI	European Telecommunications Standards Institute
FOCAC	Forum on China-Africa Cooperation
G-77	The Group of 77 at the UN
GAC	Governmental Advisory Committee
GD	General Debate (at the UN General Assembly)
GDPR	General Data Protection Regulation
GEO	geosynchronous equatorial orbit
GFCE	Global Forum on Cyber Expertise
GIZ	German Agency for International Cooperation [Deutsche Gesellschaft für Internationale Zusammenarbeit]
GNSO	Generic Names Supporting Organization
GRULAC	Latin America and the Caribbean Group
GSMA	GSM Association
HRC	Human Rights Council
ICANN	Internet Corporation for Assigned Names and Numbers
ICASA	Independent Communications Authority of South Africa
IDA	International Development Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEEE SA	IEEE Standards Association
IETF	Internet Engineering Task Force
IFC	International Finance Corporation
IGAD	Intergovernmental Authority on Development
IGF	Internet Governance Forum
IGO	intergovernmental organisation
IP	internet protocol
IPv6	internet protocol version 6
ISO	International Organization for Standardization
ISP	internet service provider
ITC	International Trade Centre
ITU	International Telecommunication Union
ITU-D	ITU Development Sector

ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
IXP	internet exchange point
JSI	Joint Statement Initiative on e-commerce
JTC1	Joint Technical Committee 1
LAWS	lethal autonomous weapons systems
LDC	least developed country
LEO	low-Earth orbit
NADPA	Network of African Data Protection Authorities
NCS	national cybersecurity strategy
NIDCOM	Nigerians in Diaspora Commission
NITDA	National Information Technology Development Agency
NSCG	Non-Commercial Stakeholder Group
OCC	offensive cyber capabilities
OECD	Organisation for Economic Co-operation and Development
OEWG	Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security / Open-Ended Working Group on security of and in the use of information and communications technologies
PAPSS	Pan-African Payments and Settlement System
PGII	Partnership for Global Infrastructure and Investment
PP-22	ITU Plenipotentiary Conference 2022
R&D	research and development
REC	regional economic community
SADC	Southern African Development Community
SDG	sustainable development goal
SDO	standards developing organisation
SG	study group
TC	technical committee
UMA	Arab Maghreb Union
UN	United Nations
UNCTAD	UN Conference on Trade and Development
UN ECA	UN Economic Commission for Africa
UNESCO	UN Educational, Scientific and Cultural Organization
UNGA	UN General Assembly
UN DESA	UN Department of Economic and Social Affairs
UN GGE	UN Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security
UNODC	UN Office on Drugs and Crime
VAT	value added tax
W3C	World Wide Web Consortium

wCBDC	wholesale central bank digital currency
WEF	World Economic Forum
WEOG	Western Europe and Others Group
WGDY	Women, Gender, Development and Youth Directorate
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WTO	World Trade Organization
WURI	West Africa Unique Identification for Regional Integration and Inclusion