The threat of digital colonization in Africa

GA4 Special Political and Decolonization Committee

Empowering Future Generations:
Cultivating Global Literacy and Enlightenment

Forum: GA4 Special Political and Decolonization Committee
Issue: The threat of digital colonization in Africa
Student Officer: Kalliope Styliani Christopoulou
Position: Deputy President

Introduction

Digital colonialism is the use of digital technology for political, economic and social domination of another nation or territory.
Digital colonization could be achieved with the use of A.I. More specifically the threat of A.I lies in its potential to go beyond human control while the misuse of powerful A.I systems could lead to the endangerment of society.
A.I. is ripe to help resolve certain major problems in Africa, from farming to the health sector, but experts are warning of this new "colonization" especially if foreign companies continue to feed on African data involving local actors.
Summarizing the threats Africa is facing are multinationals leading to the possibility of dominating A.I solutions, talented individuals and lastly data control. Meanwhile the lack of local oversight and lastly later could oversight would pose the danger of Africa becoming a tasting ground for sometimes poorly, advanced technologies endangering its safety and autonomy.

Definition of key terms

Colonialism

The policy or practice of a country acquiring full or partial political, economic social control over another country.

A.I. (Artificial Intelligence)

In its broadest sense, it is intelligence exhibited by machines, particularly computer systems. It is a field of research in computer science that develops and studies methods and software that enable machines to perceive their environment and use learning and intelligence to take actions that maximizes their chances of achieving defined goals.

Multinational Corporations (MNC's)

They are corporate organizations that own and control the production of goods and services in at least one country other than its home country. Black's Law Dictionary suggests that a company or group should be considered a multinational corporation "if it derives 25% or more of its from out-of-home-country operations"

More Developed Countries (MDC's)

A developed country—also called an industrialized country—has a mature and sophisticated economy, usually measured by gross domestic product (GDP) and/or average income per resident. Developed countries have advanced technological infrastructure and have diverse industrial and service sectors.

Lesser Developed Countries (LDC's)

LDC's are defined as low-income countries that are suffering from long-term impediments to growth. They have low levels of human and economic development and are vulnerable to both socio-economic and environmental shocks.

General Overview

Digital Colonialism

Digital colonialism is the use of digital technology for political, economic and social domination of another nation or territory.

Digital colonialism is rooted in the domination of the "stuff" of the digital world that forms the means of computation —software, hardware and network connectivity.

It includes the platforms acting as gatekeepers, the data extracted by intermediary service providers and the industry standards, as well as private ownership of "intellectual property" and "digital intelligence." Digital colonialism has become highly integrated with conventional tools of capitalism and authoritarian governance, from labour exploitation, policy capture, and economic planning to intelligence services, ruling class hegemony, and propaganda.

Similar to the technical architecture of classic colonialism, digital colonialism is rooted in the design of the tech ecosystem for the purposes of profit and plunder. If the railways and maritime trade routes were the "open veins" of the Global South back then, today, digital infrastructure takes on the same role: Big Tech corporations use proprietary software, corporate clouds, and centralized Internet services to spy on users, process their data, and spit back manufactured services to subjects of their data fiefdoms.

Thus, tech corporations have expanded their products across the globe, extracting data and profit from users all around the world while concentrating power and resources in one country, the US (with China a growing competitor). Developing countries are overwhelmed by readily available services and technology and cannot develop their own industries and products that compete with Western corporations. They are also left unable to protect their people from exploitation.

The threat of A.I.

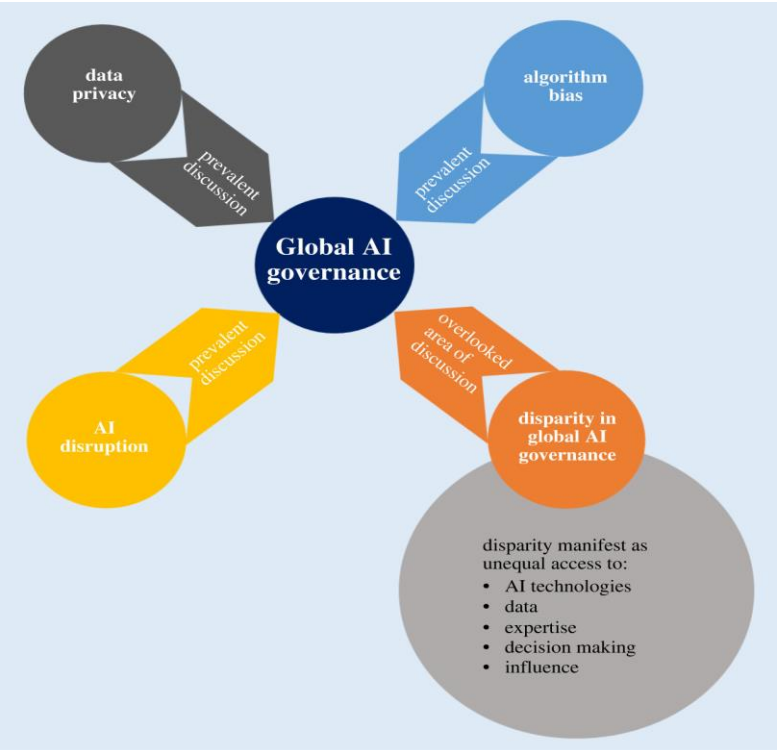
The tech industry is racing to add to the pileup of generative AI models. The goal is to steadily demonstrate better performance and, in doing so, close the gap between what humans can do and what can be accomplished with AI.

There is another gulf, however, that ought to be given equal, if not higher, priority when thinking about these new tools and systems: the AI trust gap. This gap is closed when a person is willing to entrust a machine to do a job that otherwise would have been entrusted to qualified humans. It is essential to invest in analysing this second, under-appreciated gap — and in what can be done about it — if AI is to be adopted widely.

The AI trust gap can be understood as the sum of the persistent risks (both real and perceived) associated with AI; depending on the application, some risks are more critical. These cover both predictive machine learning and generative AI. According to the Federal Trade Commission, consumers are voicing concerns about AI, while businesses are worried about several short- or long-term issues. The following examples are 11 AI risks that are among the most cited across both groups:

- Disinformation
- Safety and security
- Ethical concerns
- Bias
- Instability
- Hallucinations in LLMs*
- Unknown unknowns
- Job loss and social inequalities
- Environmental impact
- Industry concentration
- State overreach

*Hallucinations in LLMs refer to the generation of content that is irrelevant, made-up, or inconsistent with the input data. This problem leads to incorrect information, challenging the trust placed in these models.



Digital Infrastructure

Nearly 300 million Africans live more than 50 km from a fibre or cable broadband connection, hence the lack of widespread availability of high-speed (broadband) internet remains a significant hurdle for Africa to fully harness the full potential of digital transformation. Mobile devices remain the primary way by which people access internet today, and dedicated internet connections to homes and offices (such
as with fibre-to-the-premise) are mostly absent, except in some capital cities.

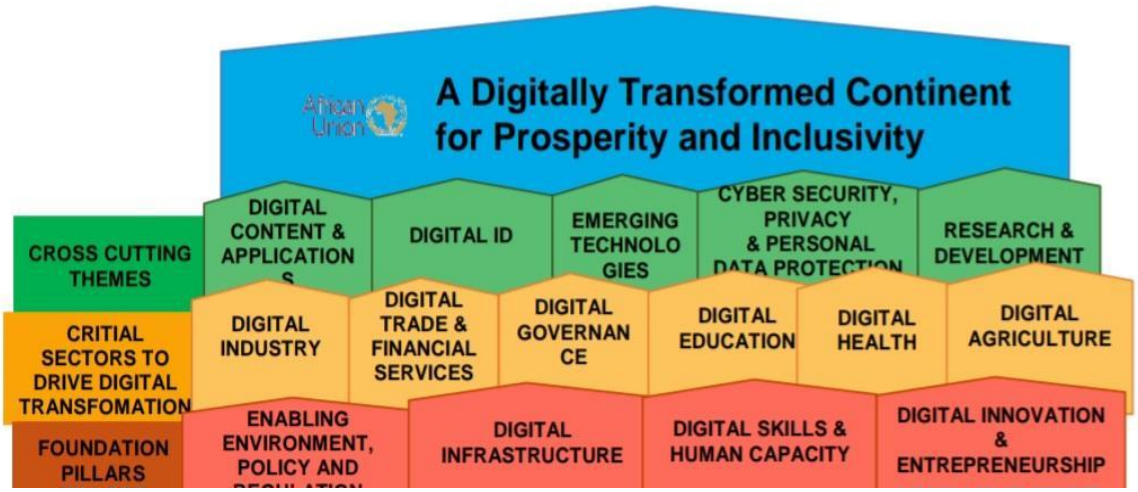
Dependence on mobile rather than fixed-line broadband means that unmetered pricing, or unlimited data use, is not very common in Africa. The mobile phone revolution has however opened the door to private sector investment in telecoms and now new business models and services have extended sustainable communication services significantly further. The value chain of digital infrastructure networks has been unbundled, and new private sector players are developing network infrastructure like independent broadband operators and tower companies. Previously, to enter a market, an operator needed to invest in international (first mile), national (middle mile), and end-user (last mile) infrastructure. Now there is competition in each of these segments in most Member States of the African Union, with specialist service and infrastructure providers either competing or providing services to vertically integrated network operators.

A.I. and the threat of digital colonization in Africa

More and more, young people in Africa launching startups are interested in this, and they have a real thirst for knowledge in the field of AI. This growing interest can be accelerated with international help.

However, there is a wall in some areas, and AI can in fact be used to solve certain problems, including in agriculture. In the health sector, AI could in fact solve a lot of problems, especially the problem of a lack of personnel.

The other element that is also very important is the development of cultural identity. Africa has been seen as a continent with a cultural identity that has not been able to impose itself across the world. With the development of AI, we could use this channel so that African cultural identities are better known and better valued.



The biggest threat is colonization. Africa may end up with large multinationals in AI that will impose their solutions throughout the continent, leaving no room for creating local solutions. Most of the data currently generated in Africa is owned by multinationals whose infrastructure is developed outside the continent, where most African AI experts also operate. It's a loss of African talent.

The other important element to consider is in the context of the fourth industrial revolution. The power of AI combined with advances in biotechnology or technology could be used, and Africa could be the place where all these new solutions are being tested.

If it's not supervised, Africa could end up with tests that would take place on humans with chips or even integrated biotechnology elements. These are technologies that haven't really been mastered well. In regulatory terms, there are certain aspects that have not been considered. The very framework for the application of ideas and existing regulations is not effective.

In concrete terms, and when you don't control these things, it could happen without anyone knowing. We could have Africa being used as a Guinea pig to test new solutions, and this could be a great, great threat for the continent.

Digital Skills and Human Capacity

There is an African digital skills gap and there is also the locally trained human potential that African countries are struggling to keep and use at national level. Ensuring the widespread availability of Digital Skills which allows individuals and businesses to harness the opportunities and guard against the risks of the digital economy is fundamental.

With the advancement of the digital economy and the encroachment of labour-saving technologies, African countries will need people with skills that complement these technologies to allow new pathways to emerge. Considering this, any capacity development effort to digitize the African society must be people-centred, locally owned, deliberate and a systematically designed process to empower individuals, organizations and the society, to unleash, strengthen, create, adapt, and maintain capacity over time. Such a holistic digital capacity development approach allows the continual building of both the requisite digital skills and competencies and enabling environments.

Education is

a universally accepted basic human right that plays a decisive role in determining the society' capability to survive and thrive in the digitized global world. A skill-focused education system produces the required number, type and quality of workforces to develop and adopt digital systems, while the application of digital technologies further enables and continuously reshape the education curriculum, delivery and administration processes at all levels – from pre-primary to tertiary and lifelong learning.

Accordingly, this requires education systems to be flexible, inclusive, proactive and tuned into producing a new breed of workforce that readily and continually learns and unlearns on a wide array of complex skills and competency required in the ever-changing digital world. The report by the Pathways for Prosperity Commission on digital readiness stresses that harnessing the digital age requires two types of skills to develop at national and continental level. The first set of skills is Digital Skills. Each society will need to have a sufficiently large group with advanced digital knowledge and engineering skills. These skills are also required at the government level to be able to make decisions, support and take advantage of emerging opportunities. For the broader workforce, digital literacy is

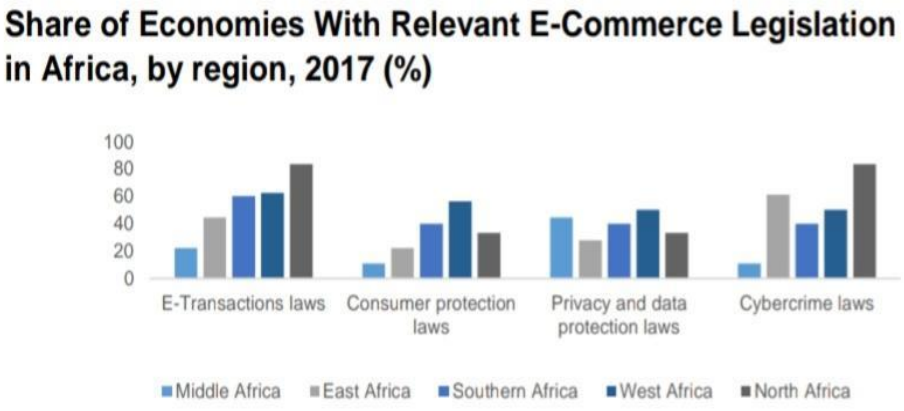
essentially required. For this, expanding access to the internet is essential for basic digital skills. The second set of skills that need to be cultivated are Digital Complementary Skills. Those skills that cannot easily be automated or codified will be increasingly in high demand in the digital economy. Skills such as empathy, personal communication, business consulting, communication and language skills as well as creativity and adaptability. Socio-emotional interpersonal skills as well as hard cognitive skills that
are difficult to computerize and would need to be developed and nurtured further. These are the skills of the future that any of the countries in Africa need not underestimate and seek to capitalize on in terms of crafting clear and strategic policy in making themselves digital ready.

Enabling environment, Policy and Regulations

Governments have a responsibility to create an enabling environment with policies and regulations that promote digital transformation. Political commitment at the highest level, ensuring stability and predictability of the policy environment, promoting sustainable environment for the private sector to invest, adopting regulatory best practice and stimulating demand for digital solutions are all part of the enabling environment. A conducive enabling environment across foundation pillars and critical sectors for digital transformation is fundamental.

Policy makers and regulators need to keep pace with advances in technology, address the new regulatory frontiers and create the foundation upon which digital transformation can achieve its full potential. Being prepared for digital transformation and emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), Machine to Machine communications (M2M) and 5G is fundamental.

Public policy, Legal and regulatory frameworks need to be up-to-date, flexible, incentive-based and market-driven to support digital transformation across sectors and across the continent regions. The Figure below shows the status of regions in Africa with regards to having in place relevant e-Commerce
Legislation



Source: OECD. 2018

Major Parties Involved

China

Through major tech companies like Huawei, and initiatives under the Belt and Road initiative, China has heavily invested in African digital infrastructures such as 5G network, and submarine internet cables While these investments have improved connectivity, they have also increased concerns that China could exert control over digital access and data on the continent, potentially compromising African nation's independence in their digital policy and security independence.

The European Union

Through partnerships like the AU-EU and the Digital D4D (Digital for Development) Hub the EU seeks to support Africa's digital development by investing in areas such as connectivity, digital skills, and regulatory harmonization. This cooperation aims to foster growth and governance in the African digital economy. However, critiques arise regarding the EU's potential to impose European-centric regulations and data policies that may not fully align with Africa's needs or ambitions.

The United States

The United States role in Africa's digital development has sparked concerns about digital colonialism, as tech giants like Google, Microsoft and Facebook (Meta) continue to expand their presence across the continent. These companies offer services that connect millions of Africans to digital resources but often come with conditions that grant these corporations significant control over local digital infrastructure, and data. One key area of influence involves digital infrastructure projects. Such initiatives, while beneficial for expanding internet access, also allow companies to capture large volumes of data without adequate local control, leaving African nations with limited autonomy over their digital economies. This dynamic has been compared to the extraction-based nature of historical colonialism, where valuable in this case, data- are extracted and primarily benefit foreign entities, rather than contributing to local economies.

Kenya

Kenya is at the centre of the conversation around digital colonization in Africa due to its rapid digital transformation and key role in the tech ecosystem on the continent. Its approach has included a mix of partnerships with foreign technology firms and infrastructure investment, though these developments raise concerns about the extent of external control over Kenya's digital landscape.
Kenya has increasingly attracted foreign tech multinationals, leveraging Kenya as a base for their African operations. These companies provide essential infrastructure, often in regions where local technology is scarce. However, with foreign companies controlling much of the internet infrastructure and digital services such arrangements can limit the autonomy of local entities and governments of digital spaces and data sovereignty. Kenya’s 2019 Data Protection Act attempted to address these concerns by creating stronger data privacy requirements.

Nigeria

Nigeria plays a prominent role in the phenomenon of digital colonization in Africa, acting as both a centre of technological growth and focal point of international influence.

The significant aspect of Nigeria's role in digital colonization is through its heavy reliance on Western social Media platforms, which have vast influence over local information flows. With limited data protection laws, Nigerian user data becomes a resource for tech firms, who harvest it for advertising and influence operations without full accountability.

This raises concerns about local user's privacy and makes the population vulnerable to misinformation campaigns that can exploit social and political divisions. For example, manipulative political campaigns and misinformation, as seen in Nigeria and Kenya leverage local user data to influence voter behaviour and, in some cases, stir conflict. This data is controlled primarily by foreign firms rather than local governments.

South Africa

The dominance of foreign companies in South Africa's digital ecosystem can be seen in the extensive presence of major tech firms, particularly in data-driven fields like fintech. This sector collects vast amounts of personal data from South African consumers, often for use in predictive modelling to determine creditworthiness. However, these practices raise concerns about digital extractivism, where local users' data is exploited for profit without substantial benefits returning to the communities themselves. South Africa has also introduced data localization laws, requiring that data on their citizens be stored domestically rather than in foreign data centres.

Human Rights Agency (HRA)

The Human Rights Agency (HRA) and other human rights organizations have raised substantial concerns regarding digital colonization in Africa. Their focus is on safeguarding individual rights, protecting data sovereignty, and ensuring equitable digital development across the continent. Human rights organizations, led by the HRA are advocating for a balanced digital future in Africa - one that promotes innovation and growth but safeguards against a new form of dependency on foreign tech interests, which could undermine local agency and digital rights.

The African Union

The African Union (AU) plays a central role in shaping Africa's response to digital colonization, focusing on policies that promote digital sovereignty and a self-sufficient digital economy across the continent. The AU faces challenges, particularly the need for infrastructure and regulatory alignment across its member states, many of which have differing levels of digital readiness. Moreover, the AU's approach to internet governance emphasizes inclusivity, but this can create difficulties in balancing open international collaboration with the need to protect digital sovereignty in a rapidly evolving global digital landscape.

Timeline of Events

22nd of January 2001	Establishment of the first African data privacy law in Cape Verde.
2007-2010	Growth of the internet and social media in

	Africa.
20th of August 2013	Establishment of “free basics" by Facebook to provide free access to a limited suite of websites in Africa.
27th of June 2014	Adoption of the AUs Conventions on Cyber security and personal data protection.
2016-2018	Rapid growth of Chinese tech influence.
January 2018	China-African Union espionage allegations.
1st of May 2018	Cambridge Analytica scandal, referring to a UK based political consultancy, implicated in manipulating elections in Kenya.
2018-2019	First specific calls for decolonizing AI in Africa.
9th of February 2020	Adoption of the Digital Transformation Strategy by the AU.
2021	Intensification of concerns over data sovereignty and AI.
13th of October 2021	Sixty percent of all African countries – thirty-three of the 55– have enacted data privacy laws as of late-2021.
28th of July 2022	The AU drafts the African Union Data Policy Framework.
22nd of May 2024	Announcement of a comprehensive package of digital Investments in Kenya by Microsoft.corp and G42.

Previous attempts to solve the issue

Kenya’s Data Protection Act

Kenya’s Data Protection Act was enacted and came into effect right away on November 25, 2019, making the country one of the first ones in Africa to have a comprehensive data privacy law. The Act requires Data Controllers and Processors to process data lawfully; minimizes collection of data; restricts further processing of data; requires data controllers and processors to ensure data quality; that they establish and maintain security safeguards to protect personal data.

The AU’s Digital Transformation Strategy

Based on African Union Executive Council Decisions related to ICT1, ECA Resolution (812–XXXI) on the African Information Society Initiative and the Smart Africa Board meeting held on the margins of the 32nd African Union Assembly of Heads of State and Government that highlighted the need for the ICT sector to lead the process, the AU Commission undertook to develop a comprehensive Digital Transformation Strategy for Africa in collaboration with the UN Economic Commission for Africa, Smart Africa, AUDA-NEPAD, Regional Economic Communities, African Development Bank, Africa Telecommunications Union, Africa Capacity Building Foundation, International Telecommunication Union and the World Bank. The main objectives of the Digital Transformation Strategy are to harness digital technologies and innovation to transform African societies and economies to promote Africa's integration, generate inclusive economic growth, stimulate job creation, break digital divides, and eradicate poverty.

South-South Cooperation

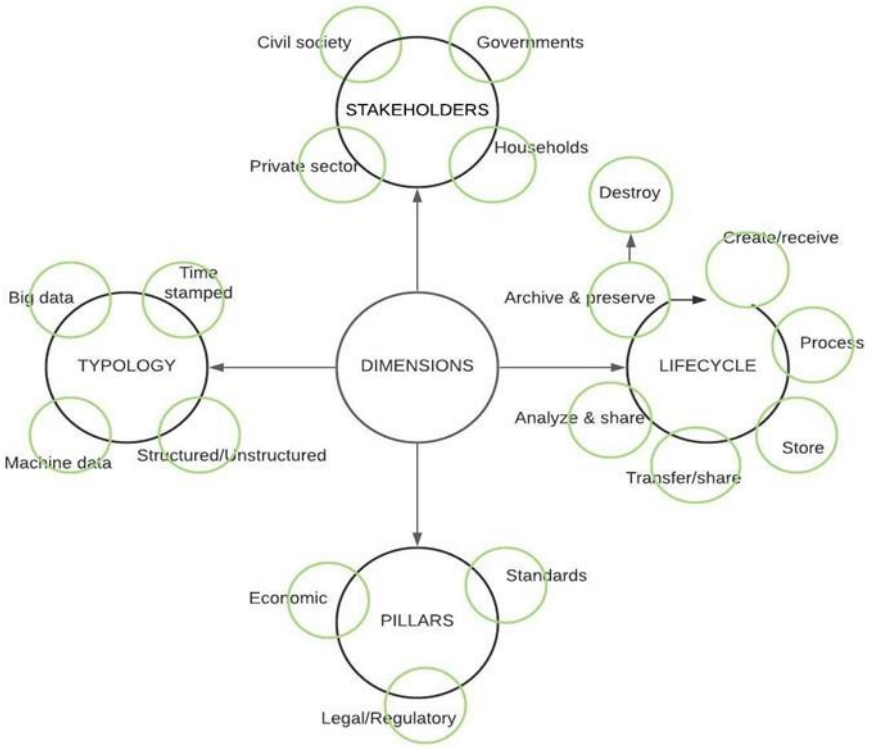
South-South cooperation refers to development cooperation between developing countries in the Global South. When South-South Cooperation is implemented with the support of a Northern partner, it is referred to as Triangular Cooperation. South-South and Triangular Cooperation (SSTC) is a tool used by governments, international organizations, academics, social partners, civil society and the private sector to collaborate and share knowledge, skills, know-how, and good practices in decent work and lifelong learning approaches as well as successful initiatives in specific areas such as agricultural development, human rights, urbanization, digital policy, health, climate change, social protection and employment generation. The extensive collaboration between countries in the South- South Cooperation has led to knowledge sharing, resources and technical expertise aiming to develop greater digital infrastructure and resist dependency on Western tech multinationals.

Possible Solutions

Considering the ever-evolving nature of the data-driven digital economy, all countries, whether in the Global North or Global South, must continuously reassess their policy choices regarding cross-border data flows. This approach aims to strike a balance between fostering domestic economic growth, safeguarding critical public policy interests and promoting an integrated global digital ecosystem.

The rapid expansion of digitalisation has undeniably reshaped our global landscape, introducing unprecedented opportunities and deep-seated disparities. The dominance of the Global North in the digital realm, driven by data monetisation practices, has amplified existing regional inequalities, raising urgent concerns about ethics and equity. Addressing these challenges necessitates a concerted effort to align data governance policies, empower the Global South, and foster international cooperation. Furthermore, continuous policy adaptation and developing a global framework for cross-border data flows are imperative to balance economic growth, public policy interests and global digital integration. Bridging the digital divide, promoting inclusivity and

upholding ethical standards are paramount in ensuring a more equitable and interconnected digital future that benefits all humanity.



The most effective way to combat digital colonialism is through capacity building. Member States should focus on programs that transfer skills and knowledge to local populations. This includes training in digital literacy, software development, and IT infrastructure management. By empowering local talent, Member States can reduce the reliance on foreign expertise and technologies, helping communities build sustainable and self-sufficient digital ecosystems.

Open-source technology can play a significant role in reducing the dominance of proprietary systems controlled by multinational companies. Nations can support the development and use of open-source platforms, which are customizable and can be adapted to local contexts without the need for costly licenses. This promotes digital sovereignty and ensures that local organizations have full control over the technology they use.

Nations should prioritize investment in local digital infrastructure and support local tech ecosystems. This includes funding locally run data centres and cloud services, promoting local content creation, and advocating for open access to the internet. Encouraging local innovation helps build the capacity of developing nations to control their digital futures. By doing so, they can reduce dependency on foreign tech giants.

Useful Documents

- Kenya's 2019 Data Protection Act
- The African Union's Digital Transformation Strategy
- EU-AU Digital Economy Task Force
- Africa-Europe Digital for Development (D4D) Hub
- UNCTAD's 2021 Technology and Innovation report
- The African Digital Single Market (DSM)- (under the AU Digital Transformation Strategy (DTS) for Africa 2020-2030)
- Protection of Personal Information Act 4 of 2013 (Popia)
- African Union convention on cyber security and personal data protection
- The African Union's Data Policy Framework.

Bibliography

"Digital colonialism is threatening the Global South." Al Jazeera 13 March 2019
https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south

"Electronic Colonialism" Wikipedia 26 September 2024 (Last edited)
https://en.wikipedia.org/wiki/Electronic_colonialism

"AI Colonialism" MIT Technology Review 2024
https://www.technologyreview.com/supertopic/ai-colonialism-supertopic/

"AI and Machine learning" Harvard Business Review 3 May 2024
https://hbr.org/2024/05/ais-trust-problem

"INTERVIEW: AI expert warns of 'digital colonization' in Africa" UN News 3 January 2024
https://www.un.org/africarenewal/magazine/january-2024/interview-ai-expert-warns-digital-colonization-africa

"Artificial Intelligence" Wikipedia 9th November 2024 (Last edited)
https://en.wikipedia.org/wiki/Artificial_intelligence

"Digital Colonialism: The evolution of the US empire" tni Longreads
https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire

"Multinational corporation" Wikipedia 28 November 2024 (Last edited)
https://en.m.wikipedia.org/wiki/Multinational_corporation

"Developed Country" bdc
https://www.bdc.ca/en/articles-tools/entrepreneur-toolkit/templates-business-guides/glossary/developed-country

" Less Developed Countries" ITU
https://www.itu.int/itu-d/sites/ldcs/focus-areas/least-developed-countries/

"What are LLM Hallucinations ?" Iguazio
https://www.iguazio.com/glossary/llm-hallucination/

"Digital Colonialism on the African continent" IBW21 19 October 2018
https://ibw21.org/editors-choice/digital-colonialism-on-the-african-continent/

"Undersea cables in Africa: The new frontiers of digital colonialism: first Monday 10 March 2024
https://firstmonday.org/ojs/index.php/fm/article/download/13637/11600

"4 Ways to Stop Digital Colonialism in International Development" ICTworks 17 September 2024
https://www.ictworks.org/stop-digital-colonialism-international-development/

"Cybercrimes Act in South Africa | Overview and Read" michalsons
https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#

"South-South and triangular cooperation" International Labor Organization
https://www.ilo.org/partnering-development/south-south-and-triangular-cooperation

"Technology and Innovation Report 2021" UNCTAD
https://unctad.org/page/technology-and-innovation-report-2021

"Building a connected Africa: The path to a single digital market and a prosperous future" Mar 22, 2023 World Economic Forum
https://www.weforum.org/stories/2023/03/building-a-connected-africa-the-path-to-a-single-digital-market-and-a-prosperous-future/

"Deploying the largest subsea fiber-optic cable system ever" 2Africa
https://www.2africacable.net/updates

"South Africa's Protection of Personal Information Act (POPIA) Explained" Termly 12 November 2024
https://termly.io/resources/articles/south-africas-protection-of-personal-information-act/

"Internet.org" Wikipedia 9 October 2024 (Last updated)
https://en.m.wikipedia.org/w/index.php?title=Internet.org&action=history

"Cambridge Analytica" Wikipedia 17 November 2024 (Last updated)
https://en.m.wikipedia.org/w/index.php?title=Cambridge_Analytica&action=history

"International and regional commitments in African data privacy laws: A comparative analysis" ScienceDirect 22 December 2021
https://www.sciencedirect.com/science/article/abs/pii/S0267364921001114

"Law in Cape Verde" DLA PIPER
https://www.dlapiperdataprotection.com/index.html?t=law&c=CV

"African Union Convention on Cyber Security and Personal Data Protection" African Union 11 May 2020
https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

"Addressing digital colonialism: A path to equitable data governance" UNESCO Inclusive Policy Lab 8 August 2024
https://en.unesco.org/inclusivepolicylab/analytics/addressing-digital-colonialism-path-equitable-data-governance

"Decolonizing AI" Boston Review 20 May 2021
https://www.bostonreview.net/forum_response/decolonizing-ai/

"Microsoft and G42 announce $1 billion comprehensive digital ecosystem initiative for Kenya" Microsoft 22 May 2024
https://news.microsoft.com/2024/05/22/microsoft-and-g42-announce-1-billion-comprehensive-digital-ecosystem-initiative-for-kenya/