African Perspective

Cyber Governance and Diplomacy

Moctar Yedaly

Information and Communications Technologies (ICTs)

• The former U.S. president Ronald Reagan told a London audience in 1989, ***"More than armies, more than diplomacy, more than the best intentions of democratic nations, the communications revolution will be the greatest force for the advancement of human freedom the world has ever seen."***

•**Remember**:

•Power is the currency of international relations. It is the difference between weak states and strong ones, between those who set the terms of the geopolitical order and those who must accommodate the will of others.

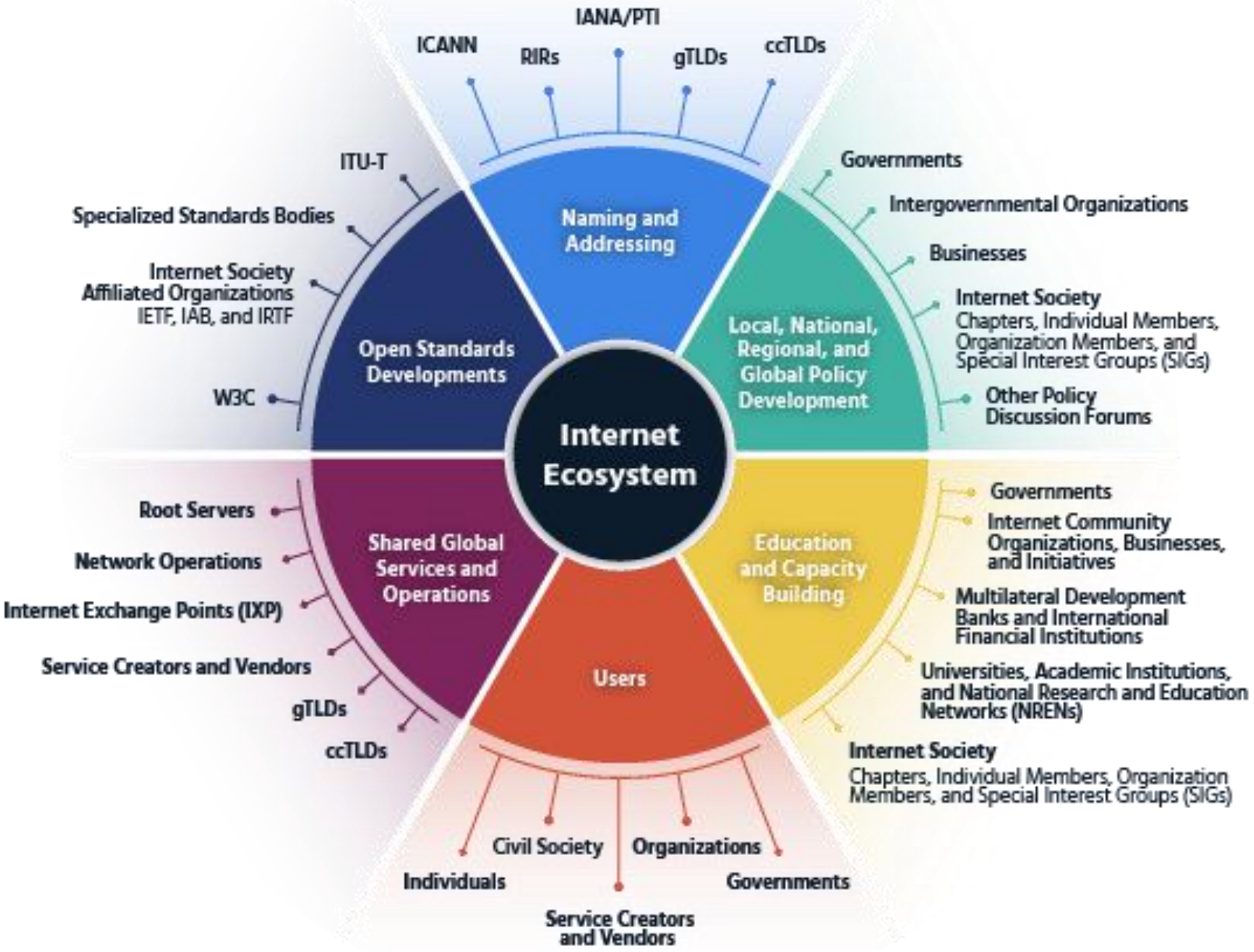
•Taking this into consideration, the race for ICTs began.

- **China** has become not only the biggest of big brothers but also the world's largest provider of communications technology.
- **Russia** on of the biggest hackers in the world.
- **United State** - Snowden revelations has said it all
- **Africa** - is simply the biggest consumer. And again, the terrain for racing, testing.

Africa is a net consumer of Digital products and barely produces any

- African people with their leaders and everyone who counts plunged into an extensive consumption of digital Technologies and social media with NO proper security and safety diligence.
  - No Digital governance.
  - NO much care of Digital Sovereignty
- Africa is a (Human/ Natural) resource-rich continent but often identified as the world's DIGITALLY poorest continent;
- Some are saying that there are several reasons for Africa's poor economy that:

- 1. historically, even though Africa had a number of empires trading with many parts of the world, many people lived in rural societies;
- 2. colonization ***and later Cold War*** created political, economic and social instability.


Internet Ecosystem
Naming and Addressing
IANA/PTI
ICANN
RIRs
gTLDs
ccTLDs
Local, National, Regional, and Global Policy Development
Governments
Intergovernmental Organizations
Businesses
Internet Society
Chapters, Individual Members, Organization Members, and Special Interest Groups (SIGs)
Other Policy Discussion Forums
Education and Capacity Building
Governments
Internet Community Organizations, Businesses, and Initiatives
Multilateral Development Banks and International Financial Institutions
Universities, Academic Institutions, and National Research and Education Networks (NRENs)
Internet Society
Chapters, Individual Members, Organization Members, and Special Interest Groups (SIGs)
Users
Individuals
Civil Society
Organizations
Governments
Service Creators and Vendors
Shared Global Services and Operations
Root Servers
Network Operations
Internet Exchange Points (IXP)
Service Creators and Vendors
gTLDs
ccTLDs
Open Standards Developments
ITU-T
Specialized Standards Bodies
Internet Society Affiliated Organizations
IETF, IAB, and IRTF
W3C

A pervasive lack of awareness among African individuals and organizations

- African entities vulnerable to various cyber threats affecting the livelihoods of African people, the stability of their economies, and the sovereignty of their nations.
- **Geopolitics and this new global digital context world in the context of Africa**
  - Africa has recently focused on an ambition to achieve digital transformation through the pursuit of various flagship initiatives which are aimed at achieving its '**Agenda 2063' objectives**.
  - Africa adopted several documents which factor cybersecurity:
    - ✓ In 2008 AU Reference Framework for the Harmonization Telecom/ICT policy and regulation in Africa adopted by the CITMC-2 in Cairo in 2008 and endorsed by the Executive Council
    - ✓ In 2014 (entered in force in 2024) A Convention on Cybersecurity and Personal Data protection
    - ✓ in 2020 a **Digital Transformation Strategy 2020-2030**
    - ✓ 2023 A digital Compact

1. Cyber governance in Africa

- Around the world Cyber governance has come to the forefront of diplomatic and political agendas of important bilateral and multilateral
- There are concerns about:
  - the preparedness of African states for regulation of the cyberspace through appropriate policies to meet international standards.
  - The disparities in digital capacities and political structures are also an appearing challenge for the implementation of principles of responsible state behavior in cyberspace by African states.
  - Concerns regarding African leaders stance and approach toward digital sovereignty: ***Digital cooperation could imply digital dependence in the face of differing digital capacities.***

2. Centering cybersecurity in digital transformation

- Responsibility for African governments: Creation of an enabling environment with policies and regulations that promote digital transformation across foundation pillars which includes cyber security
- The Strategy AU Digital transformation strategy adopted by the head of States states in 2020: "***collaborative ICT regulatory measures and tools are the new frontier for regulators and policy makers as they work towards maximizing the opportunities afforded by digital transformation across industries***".
- **Malabo Convention**: 2014, the Head of States adopted the AU Convention on Cyber Security and Personal Data Protection to provide fundamental principles and guidelines to ensure cyber security, effective protection of personal data and creation of a safe digital environment.

3. A Crossroads of Politics, sovereignty and cooperation

- **African countries continue to exhibit weak cyber maturity levels**:
- **A challenge for Africa in addressing cyber governance:** The AU member states have diverging interests, and the ineffectiveness of governance mechanisms and lack of capacity in policies, strategies and infrastructure
- **The creation of legal frameworks and diplomatic relations have political foundations:** dialogues about digital sovereignty which resonates with the historical context of Africa in terms of colonization.

4. Challenges with laws and policies

- **Compared to regions such as Europe, Africa lacks a united and cooperative cyber governance agenda**
- **Some governments still regard cyber governance as a non-priority**:
- **Lack of capacity, expertise and skills moves into the cyber-legislation process**
- **Research shows that:**
  - Only seventeen (17) out of the fifty-four (54) African countries have a national cybersecurity strategy
  - Only three (3) of those countries possess the minimum essential criteria for an adequate cybersecurity strategy.
  - only twenty-nine (29) out of fifty-four (54) African countries have promulgated a cybersecurity legislation
- **Cyber-legislation literacy is a challenge for African law makers.**
- **Gaps for parliamentarians and policymakers.**
- **Minimal understanding of cyber governance realities :** Contradictions in legal texts is common. And transplanting of Western cyber governance legislation which often ignore cultural realities and domestic capabilities is common in African jurisdictions.

5. Ideologies on digital sovereignty

- **The borderless nature of the internet presents challenges:** there is a constant resurgence of the digital sovereignty narrative in the Africa region.
- **Regular occurrence for African governments to restrict internet access for citizens**: misunderstanding of the cyber governance agenda.
- **The UN Norms of Responsible State Behavior in Cyberspace** calls for states to respect the Human Rights and to promote and protect the enjoyment of human rights on the internet.
- The United Nations Secretary have also formally affirmed that ***"blanket Internet shutdowns and generic blocking and filtering of services are considered by United Nations human rights mechanisms to be in violation of international human rights law***."
- **Controlling the internet is always regarded as a cybersecurity-national security measure** and a reinstatement of digital sovereignty by such African states.

Thank you