**KEY ISSUES** Special Issue 2019; 9-19

Venance Leonard Jeston Ntahondi*

# Authoritarianism and Internet Governance in Tanzania

**Abstract:** Although the development of the internet was not initially seen as a potential threat to the political stability of a country, following the collapse of authoritarian regimes in several African states such as Algeria and Sudan, in part, due to the use of the internet, the internet has been regarded as a potential weapon against the state. Internet governance has therefore taken on an increased significance, particularly in East Africa where many countries have witnessed the rapid growth of internet use. This paper undertakes a literature review to derive an understanding of how authoritarianism has been used by the government as a tool for internet governance in Tanzania. It starts by defining the meaning of the word authoritarian and then examines the practices used in the context of internet governance in Tanzania. It considers the different policies for protecting the use and misuse of the internet, the challenges faced by the government is doing so and the suggested strategies for protecting the internet from use and misuse in Tanzania. It concludes that authoritarianism has taken a lead on the use of internet in all government, non-government and individual activities, and that this is threatening citizens' rights of privacy and freedom of expression and is likely to undermine the positive impact of internet use in the country in terms of business, economic, educational and communication gains. In the longer term, this could dampen the uptake of these new ICT technologies. In seeking to address these issues, it recognizes that there is a need to review policies on internet use by the government and ICT institutions to put up guidelines that meet the interests of both the government and the local people. Once this is done, internet governance will not be seen as a threat by the people of Tanzania but as a positive strategy to promote the country and the rights of the people.

**Keywords:** Authoritarianism, internet governance, laws, Tanzania

## 1 Introduction

This paper undertakes a literature review to derive an understanding of how authoritarianism has been used by the government as a tool for internet governance in Tanzania. It starts by defining the meaning of the word authoritarian and then examines the practices used in the context of internet governance in Tanzania. Tanzania has been used as a case of reference because it is one of the African states where authori-

tarianism has not only intervened in terms of political freedoms but also the rights of nationals towards privacy and electronic transaction (Lubua & Maharaj, 2012). The paper looks at the different policies for protecting the use and misuse of the internet, the challenges faced by the government is doing so and the suggested strategies for protecting the internet from use and misuse in Tanzania.

# 2 Defining key terms

## 2.1 Authoritarianism

Glasius M, & Michaelson (2018) defined the term authoritarian in the digital sphere as the sabotage of accountability which violates the following; digital rights; rights to freedom of expression and disables voice. The term authoritarianism also includes arbitrary surveillance, secrecy and disinformation, and infringement on the autonomy and dignity of a person. These characteristics of the authoritarianism contribute to the violations of human rights and support authoritarianism politics.

## 2.2 Internet governance

Internet Governance (IG) is the development and application by Governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet (Shackelford & Kastelic, 2014). In reality, internet governance in Tanzania has been centralized by the government which has managed to control what should be communicated and what should not be communicated by claiming that it is "Defending National Security". In this way, any online communication which critiques the regime, or the president is deemed to be threatening national security (Comer, 2018). This work shall be characterized by the exploration of the divergence between supporting cybersecurity and maintaining international human rights concerning the use of the internet.

# 3 Internet Governance in Tanzania

The internet started to be used in Tanzania in the mid to late 2000s. The construction of internet infrastructures such as telephones lines, fiber optic cables, satellites, microwaves, wireless links, and electric grid resulted in increasing the number of inter-

net users to less half of the population in the country within one decade (Yonaz, 2012). This, in turn, has further promoted the need for the development of the electricity supply in both urban and some rural areas. The development of the internet has simplified communication in Tanzania. Wherever the internet has become accessible in Tanzania, it has positively affected economic development. However, although the internet has positively contributed to social-economic development, the literature used in this manuscript shows how internet use has been politicized by the government to maintain its interests (Olengurumwa, 2016).

The power exercised by the government of Tanzania over internet usage has amplified the fear of internet users of exercising their communication freedoms since any criticism of the government online could lead to unfortunate consequences. The government has given power to Tanzania Communication and Regulatory Authority (TCRA), the Tanzania Computer Emergency Response Team (TCERT) and the Police Cyber Security Unit (PCU) which are Information and Computer Technology (ICT) institutions of the government of Tanzania, to detect the flow of online messages and contents. The sender of any information considered by the government as misleading, defamatory, false or inaccurate could be subject to a ten years jail sentence (Kalemera *et al.*, 2018).

The PCU is mandated with wide-ranging powers to be able to search the homes of the suspected violators of the law whereby the law has affected the freedom of information and expression. This situation is against the International Covenant on Civil and Political Rights (ICCPR) as was ratified by Tanzania whereby article 17 reinforces article 12 of the Universal Declaration of Human Rights (UDHR) which states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor and reputation" (Olengurumwa, 2016).

Tanzania has enacted various laws that govern the use of civic space. These laws include the 1993 Communication Act, 2010 Electronic Communication Act and the 2015 Cybercrime Act (Murray, 2018). The fact that these laws have been formulated in favor of government interests may threaten the level of future technological advancement. The fear is that the strict emphasis of authoritarianism placed on internet governance might sabotage all forms of activities done through the internet, which will lead to a limit on the country's economic development. These issues provide a backdrop for examining the state of authoritarianism and internet governance in Tanzania.

# 4 Objectives of the Research Article

Given the breadth of the issue of authoritarianism and internet governance, it has been decided to focus on three specific objectives;

1) To explore the different policies for protecting the use and misuse of the internet in Tanzania.
2) To examine the challenges faced by the citizens of Tanzania in using the internet due to the protecting use and misuse of the internet by the government of Tanzania.
3) To suggest possible strategies for protecting the internet from use and misuse in Tanzania.

# 5 Methodology

This paper adopted a library-based research approach using a document analysis approach. The document analysis approach allowed the author to go to libraries for reviewing documents related to authoritarianism and internet governance in Tanzania.

# 6 Findings: The Different Policies for Protecting Use of Internet in Tanzania

The Tanzania Cybercrimes Act of 2015 is one of the major policies formed for protecting the use and misuse of the internet in Tanzania. It was formulated to reduce the vulnerability of people, information, and devices such as computers and phones to attacks, attacks termed as cyber-crimes since they are conducted through the internet. Although the Cybercrimes Act, Act No 4 of 2015 is enacted to fight and address matters related to offenses against the internet and computer-related devices, the Act also came with violations against the right to privacy in Tanzania. As reviewers of this Act such as Kalemera *et al.* (2018) state, the Act gives strong penalties and restrictions on the use of the internet. For example, there are penalties for sending "unnecessary messages", for using pornography, child pornography and there are strong restrictions aimed at communication service providers. Currently, Erick Kabendera is an example of the journalist who is jailed without trial for writing on the conflict and division within the ruling party Chama Cha Mapinduzi, however, he is accused of money laundering, and cybercrimes which has no bail in Tanzania (Cengic I, 2019). This kind of internet governance has increased the penalties and restrictions on the use of

the internet. Furthermore, the Cybercrimes Act of 2015 makes provisions for criminalizing offenses related to computer systems and ICT and as such enables the investigation, collection, and use of electronic evidence (Marere, 2015). Although the policy seems to be designed to prevent cyber-attacks to individual and government data, in reality, it has blocked local people from the liberal use of electronic communication and commercial transactions. Moreover, although these policies were enacted in the name of protecting cybercrimes in the actual sense were done with the essence of protecting the governments' interests and power dominance (Kalemera *et al.*, 2018). The list below sets out some of the cases of when the Cybercrime Act 2015 has been used to put several nationals on trial:

1) Isaac Habakuk Emily was charged with referring to President John Pombe Magufuli as an imbecile via his Facebook account under Section 16 of the Cybercrime Act 2015. He was convicted and sentenced to a fine of 7 million Tanzania shillings (US$ 3,200) or imprisonment for a term of three years. He paid the fine and was released.
2) Naila Amin was also charged with the issue of abusive language against Martha Sebarua under Section 23 (1) and (3) of the Cybercrimes Act, 2015. He was convicted and sentenced to 3 years imprisonment or a fine of 5 million Tanzania shillings (US$ 2,200).
3) Bob Chacha Wangwe has been charged with publishing false information on his Facebook account - a statement to the effect that Zanzibar was a colony of Tanganyika, under Section 16 of the Cyber Crimes Act, 2015. This is still before the court of law.
4) Leonard Kyaruzi has also been accused, arrested and reprimanded following his post on a WhatsApp group criticizing how President Magufuli was running the country. He claimed the president either lacked good advisors or was mentally retarded. He was charged under Section 118(a) of the Electronic and Postal Communications Act, 2010.
5) Jericho Nyerere has also been accused of publishing false information which could provoke violence in the country during the electoral process under Section 16 of the Cybercrime Act. The case is ongoing before courts of law.
6) Benedicto Ngonyani, a student of Dar es Salaam Institute of Technology (DIT), has been accused of publishing information on Facebook that the Chief of Defense Forces was suffering from food poisoning under Section 16 of the Cybercrime Act. A constitutional petition challenging section 16 has been filed.

The compilation of the above cases indicates the level at which authoritarianism has acted in the interest of the state in terms of internet governance. It is not surprising that as a result, Tanzanians are fearful about making political comments online, thus

protecting the interests of the ruling government (Marere, 2015). The right to privacy is central to the protection of human dignity, forms the basis of any democratic society, and supports other rights, such as freedom of expression, information, and association (Lyon, 2014). In the same line of argument, Comer, (2018) asserts that it is essential therefore for states to have policy, administrative and legal frameworks that robustly protect the individual from the invasion of their privacy and abuse of their data. However, in Tanzania, the weak or missing legal protections for personal data, the abuse of existing laws by state agencies in service of often partisan interests, and poor digital security practices by citizens are significantly undermining citizens' privacy and personal data (Darczewska, 2014). Furthermore, Marere (2015) complains that the enactment of the cyber laws in Tanzania suppresses human rights such as the right to privacy and freedom of expression and has given arbitrary and excessive powers to the police. Without having these privacy protections and security practices in place to counterbalance the Cybercrimes Act, the legislation can easily be used for political purposes.

It is surprising that despite the increasing policies and laws on internet use, cybercrime activities are still increasing, thus making a mockery of the efforts made by the government to enforce strict laws and penalties on misuse of internet. For example, Mwananchi (2012) reports that the use of the internet in Tanzania especially in urban areas is increasing and comes at the price of increased criminal activity online with Tanzania reportedly losing approximately 892.18 billion Tanzania shillings through online crimes in 2012.

In addition to the problems surrounding the Cybercrimes Act 2015, Lubua & Maharaj (2017) found out that in Tanzania, despite efforts demonstrated by the government through the formulation of legislation in favor of ICT use, there remain other laws which inhibit and contradict progressive legislation. Some of these laws date as far back as the 1970s and negatively impact meaningful citizen participation, the free flow of information, access to information and freedom of expression. For example, Article 18(b) of the Constitution of Tanzania gives every citizen the "right to seek, receive and, or disseminate information, regardless of national boundaries." However, Section 5 (1) of the National Security Act (1970) gives government officials the power to withhold information from citizens stating: "Any person who communicates any classified matter to any person other than a person to whom he is authorized to communicate it, shall be guilty of an offense." The Newspapers Act (1976) is another legislation that affects information sharing. Section 25 (1) of the Act grants the minister in charge the power to prohibit the publication of a newspaper, if s/he thinks that it is in the public interest or the interest of peace and good order. The clause gives the government the power to assume two positions at the same time -that of a complainant and judge (Ministry of Information, Sports & Culture, 2014). The dominance of

these laws and policies has suppressed the cybercrime act, 2015 which has no power over the previous laws stated in this paragraph thus credits the continuation of authoritarianism in Tanzania due to the increasing fear among users of the internet.

# 7 The challenges faced by the government of Tanzania in protecting the use of internet

The rapid and relentless pace of technological change in Tanzania minimizes the opportunities for protecting internet use and misuse in the country. Glasius & Michaelsen (2018) found out that just over a decade ago, the most popular Internet applications and products were not even in existence. Other dynamic features include rapid growth and rising social and economic dependencies that introduce new stakeholders and new institutions into Internet governance arenas. Innovations and new actors create new governance challenges in critical areas including cybersecurity, privacy and freedom of expression. Evan (2014) calls for more creative internet governance approaches that can keep up with fast-paced technological innovation.

Language and content limitations also affect the success of efforts done towards implementing policies and laws of internet governance in developing countries. This is because Tanzanians use Swahili as the first language in communicating which affects the interpretation of the laws which are written in the English language. It requires experts to translate the bills into their common understanding and applicability. About this, Darczewska (2014) argues that the lack of local and community-related content, as well as content in local languages, continues to be a major barrier in the use of ICT for economic empowerment. ICT can only be useful and meaningful, particularly to rural and poor citizens, if they provide relevant information and the tools needed to address citizens' needs and demands. Multimedia tools are essential, as they can be developed to provide information both in spoken and written languages. The challenge is to develop content that is relevant and useful to communities in their language. ICT advocates must work hard to ensure that such content is developed, and funds are allocated for these activities (Burrows & Stephan, 2015).

Education and skills also affect the success of law and policies implemented towards internet governance in developing countries. Comer (2018) states that the implementation of ICT policies face tremendous challenges in circumstances where a large percentage of the community are women with low levels of educational attainment who speak many local and national languages, Again, recent experiences show that it is possible to address these issues (such as the CD ROM projects in Tanzania), and ICT advocates and policy-makers should focus on developing programs that

address the development needs and demands of these communities in ways that they can benefit from it. Particularly, it is important to involve community women in the process of deciding what kind of projects will be most useful. ICT requires that users have some skills, and no one should assume that by providing the facilities, everyone in the community will immediately embrace the technology (Darczewska, 2014).

The cost of access and lack of affordable solutions further affects the implementation of policies and laws for internet governance. About that argument, Comer (2018) asserts that even when infrastructure is available, affordable access is a concern in most developing countries like Tanzania. The recent trends in policy to move from universal service (one telephone per household) to universal access policies (access to communications and ICT through community access points) reflect concerns related to the cost of infrastructure as well as consumers' ability to pay for service, particularly in rural and poor areas. Universal access policies aim at developing solutions that provide community access at affordable prices. New technologies have made these solutions more promising and Tanzania is investing in such policies. Expansion of public telephones and ICT access points (in post offices) are examples of these solutions (Deibert, 2015).

Furthermore, unfair laws, which favors the government interest but never it considers freedom of expression has threatened users of the internet (Marere, 2015). Cybercrime policy formulation and enactment of laws are highly politicized.

# 8 Possible Strategies for Protecting and governing Internet freedom space in Tanzania

First, reviewing the laws to fit in the proximity/understanding of the local people to promote the applicability of laws on internet governance. In fulfillment of this, the commission is intending to review the laws affected by the development and use of the internet. Marere (2015) asserts that the rationale behind is to protect the consumers and facilitate business transactions. Before this Cybercrimes Act of 2015, the commission recommended also on the enactment of the new laws to cover the crucial area that has a high impact on the economic development in Tanzania. Also, the policymakers have to involve citizens and civil society organizations to get balance and fairness before laws are passed.

Also, increasing the provision of security has been a strategy adopted by governments as a way of reducing the growing insecurity of internet misuse. Bennett & Livingston, (2018) assert that states have an increasing desire to extend their sovereignty into cyberspace and are seeking the technological means to do so. As Diebert

and Rohozinski (2010) put it, “securing cyberspace has entailed a ‘return of the state' but not in ways that suggest a return to the traditional Westphalian paradigm of state sovereignty.” Moreover, while accounts of cyberwars have been exaggerated, cyber espionage is rampant and more than 30 governments are reputed to have developed offensive capabilities and doctrines for the use of cyberweapons (Garamone, 2014).

Also, strengthening national policy institutions and processes has been useful in the implementation of policies governing the use and misuse of the internet in developing countries (Bennett& Livingston, 2018). Although establishing a global network is important, it is also essential to strengthen capacity at home. National and regional institutions in developing countries are frequently weak on several levels. At the national level, political leadership is often lacking, national ICT strategies are often absent, and coordination between government departments and agencies is often inadequate. At the regional level, coordination between governments and user groups sharing common interests is often lacking. Further weaknesses at this level include poor preparation for international meetings and ineffective use of human and financial resources (Bueger & Gadinger, 2015).

Finally, fair laws which does not only favor the government interest rather provides freedom of expression to the internet users are the key to the good governance of the internet (Marere, 2015). Cybercrime policy formulation and enactment of laws should not be politicized.

# 9 Summary

The elements of authoritarianism in Tanzania are evident. The means with which free space is increasingly being restricted over in Tanzania has taken the cyberspace approach. This is where state censorship of dissenting views and opinions critical of the state are tracked and dealt with. The debate on internet governance can no longer be marginalized if political tolerance and liberal communication approaches are to be embraced. Political legitimacy must not be based upon appeals of emotions and political suppression of anti-regime activities. Tanzania must open up and harmonize internet governance with other important actors like civil society, academia, and private sectors to achieve the best from this widespread technology. Non-governmental organizations and civil society representatives have to be included in ICT policy formulation to bring up the inclusive environment of ICT implementation and internet governance. The use of the police force unit in the undertakings of the internet and its governance has violated international human rights and restricted internet rights and freedoms in Tanzania. (Marere, 2015). The Government of Tanzania must ensure that

the same rights enjoyed offline must be also be enjoyed online and where these rights are protected in the offline world, the same must be applied in the online space.

# 10 Recommendations and conclusion

The Government of Tanzania needs to explore ways and propose concrete measures to address the governance of the internet. These measures should include awareness-raising campaigns as well as policies that prevent internet restrictions among internet users. The Ministry of ICT in Tanzania needs to provide formal and non-formal education, critical knowledge, skills and attitudes in the digital world. This includes providing guidelines for digital citizenship education in schools, the promotion of a network of schools and the creation of digital badges for democratic skills based on the framework of competencies for democratic digitalization. Also, the Ministry of ICT in Tanzania is required to strengthen dialogue amongst monitoring institutions and on the exchange of best practices for the creation, access, and management of digital culture that allow management of ICT use in Tanzania.

Finally, the Ministry of ICT in Tanzania should promote the setting up of a network of national institutions to guide Internet users who seek redress and remedies when their human rights have been restricted or violated based on the Council of Guide to human rights of Internet users.The government of Tanzania is argued to manage the use and misuse of the internet by considering the international human rights laws on the use of the internet and the constitution of Tanzania (Article 18b) among other laws that promotes the use and enjoyment of internet by the people as their basic right.

# References

Bueger, Christian/Gadinger, Frank (2015): The play of international practice. In: *International Studies Quarterly*, 59 (3), 449-460.

Burrows, Matthew/Stephan, Maria (eds.) (2015): *Is authoritarianism staging a comeback?* Washington, DC: Atlantic Council.

Cheeseman, Nic (2018): *The State of Democracy in Africa*. Oxford: Cambridge University Press.

Comer, Douglas (2018): The Internet book: everything you need to know about computer networking and how the Internet works. Chapman and Hall/CRC.

Darczewska, Jolanta (2014): *The anatomy of Russian information warfare. The Crimean operation, a case study*. Warsaw, Poland: Ośrodek Studiów Wschodnich im. Marka Karpia. Centre for Eastern Studies.

Deibert, Ron (2015): Cyberspace under siege. In: *Journal of Democracy*, 26 (3), 64-78.

Carroll, Evan (2014): "What Will the Next Billion Internet Users Look Like?". *The Digital Beyond*, September 11. Retrieved September 11, 2019 (www.thedigitalbeyond.com/2013/09/what-will-thenext-billion-internet-users-look-like).

Cengic Imelda (2019): "Tanzania Journalist Charged with Economic Crimes". Organized crime and corruption reporting project (OCCRP), August 6. Retrieved September 11, 2019. (https://www.occrp.org/en/27-ccwatch/cc-watch-briefs/10414-tanzanian-journalist-charged-with-economic-crimes).

Franzese, Patrick (2009): Sovereignty in Cyberspace: Can it exist? In: *Air Force Law Review*, 64, 523-541.

Glasius, Marlies/Michaelsen, Marcus (2018): Illiberal and Authoritarian Practices in the Digital Age. In: *International Journal of Communication*, 12 (2018), 3795-3813.

Hofmann, Jeanette (2016): Multi-stakeholderism in Internet governance: putting a fiction into practice. In: *Journal of Cyber* Policy, 1 (1), 29-49.

Kalemera, Ashnah et al. (2018): *State of Internet freedom in Africa 2018 - Privacy and data protection in the Digital Era: Challenges and trends in Africa*. Kampala, Uganda: Collaboration on International ICT Policy for East and Southern Africa (CIPESA).

Lubua, Edison/Maharaj, Manoj (2012): *ICT Policy and e-Transparency in Tanzania*. IST-Africa 2012 Conference Proceedings. IIMC International Information Management Corporation, 2012.

Lyon, David (2014): Surveillance, Snowden, and Big Data: Capacities, consequences, critique. In: *Big Data and Society*, 1 (2), 1-13.

Marere, Michael (2015): The Cybercrimes Act of 2015: A weed in the Garden of Freedom of Expression in Tanzania. Unpublished dissertation, Mzumbe University.

Murray, James (2018): "Cloud Network Architecture and ICT-Modern Architecture". *IT Knowledge Exchange*, December 18. Retrieved September 11, 2019 (https://itknowledgeexchange.techtarget.com/modern-network-architecture/cloud-network-architecture-and-ict/).

Olengurumwa, Onesmo (2016): *Situation of Internet freedom in Africa. Consider Internet Freedom as a Human Right in Tanzania*. Banjul, Islamic Republic of the Gambia: 59th Session of the African Commission on Human and People's Rights - Consider Internet Freedom as a Human Right in Tanzania.

Shackelfold, Scott/Kastelic Andras (2014): Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity. In*: New York University Journal of Legislation and Public Policy*, 15 (4), 1-66.

Waiswa, Robert/Okello-Obura, Constant (2014): To what extent have ICTs contributed to e-Governance in Uganda? In: *Library Philosophy and Practice (e-journal)*, 1125, 1-19.

Welzel Alexander A. (2011); Measuring Effective democracy; The Human empowerment Approach, pp.99-100.

Alexander, Amy/Welzel, Christian (2011): Measuring Effective Democracy: The Human Empowerment Approach. In: *Comparative Politics*, 43 (3), 271-289.