Journal of Public Policy and Administration
2019; 3(1): 1-7
http://www.sciencepublishinggroup.com/j/jppa
doi: 10.11648/j.jppa.20190301.11
ISSN: 2640-2688 (Print); ISSN: 2640-2696 (Online)

SciencePG
Science Publishing Group

The Quandary of Cyber Governance in Ethiopia

Temesgen Aschenek Zeleke

Institute of Governance, Humanities and Social Sciences, Pan African University, Cameroon, Yaoundé

Email address:
taschenek@gmail.com

To cite this article:
Temesgen Aschenek Zeleke. The Quandary of Cyber Governance in Ethiopia. *Journal of Public Policy and Administration.* Vol. 3, No. 1, 2019, pp. 1-7. doi: 10.11648/j.jppa.20190301.11

Received: November 18, 2018; **Accepted**: January 2, 20198; **Published**: January 31, 2019

Abstract: The incorporation of Information Communication Technology to the human endeavor have brought cyber space as one of the major areas of cooperation and conflict for actors of international relations. Its decentralized nature challenges traditional conception of state as the sole actor to possess coercive power. As a response states design different ingenuities to incorporate cyber governance as one domain of policy making and research. Likewise a number of legal, policy and institutional initiatives have been designed to guide cyber governance in Ethiopia. However, the over all aspects of cyber governance have posed a peril to digital landscape. The short history of internet has been accompanied by deliberate interruptions and online manipulations by the government. Neither complementarity nor clearly set of line of authority characterizes the institutional and legal architecture of Ethiopian cyber environment. By employing descriptive approach and integrating primary and secondary data sources the article analyzed the overall dilemma of cyber governance and its implication in Ethiopia. Thus the article scrutinizes the institutional, legal and policy aspects of internet governance neither crafts conducive environment for non-governmental actors nor able to support to exploit digital opportunities. This brought socio-economic costs which is generally resulted in what is termed as “digital divide”.

Keywords: Cyberspace, Internet Governance, Digital Divide, Cyber Governance, Cyber Security

1. Introduction

In traditional concept of state sovereignty the main threats for states are come from other states in which conventional warfare had been the major source of a threat to state sovereignty [1]. Thus, the physical and territorial integrity has been the only manifestation of “Westphalian” concept of state sovereignty [2]. However with the advancement of information communication technology, threats for states are not only decentralized but also becomes apparent that means and ways of imposing threats also widely lingering [3]. The power of a state is highly depend not only military, territory and natural resources but information technology and institutional flexibility gained much importance in the relation between actors. The power of actors of international relations are inclined more on the information domain and gaining access to information as a central organizing principle of war [4]. In line with this, threats using the cyberspace become a major domain of attack and defense which entails cyber is becoming both a domain of conflict and cooperation for actors of global politics [5].

Such aspects brought the issue of cyber governance as a major policy and research arena for academics and governments [6]. In this regard internet policies, regulations and in general governance of the cyberspace become not only the domain of policy making but also one of the major priority sector for government budget [7]. Ethiopia has a short history of internet and is one of the lowest interconnected nation in Africa [8]. Absence of well-organized institutions in expanding the infrastructure, government’s restrictive approach and the monopoly of the sector by the government have encumbered to exploit digital benefits and opportunities [9].

This article intends to assess the ongoing dilemmas on internet governance in Ethiopia and its prospects. Qualitative research methodology is employed to conduct this research. Cyber governance involves the interaction of the policy environment, institutional framework, private and public actors. In line with this, the qualitative method is used to explain, interpret and analyze data and understanding of social phenomena in their contexts. Thus by employing descriptive and analytical approach the paper tires to assess the general frameworks of cyber governance and its implication for access to digital benefits in Ethiopia. Both primary and secondary sources are used to scrutinize the issue under inquiry. Secondary sources such as books, journals, articles, magazines, policy documents and internet sources are extensively used. Furthermore, news releases, reports and online resources are used. In addition online interviews was conducted to support the argument with primary data.

2. Reviewing Literatures

2.1. The Concept of Cyberspace

Cyberspace is regarded as a virtual interaction that resulted with the collapse of temporal boundaries and time compression [7]. Debates surround on the definition and the understanding of cyber ecosystem. Many argued cyber like environment, climate and weapons of mass destruction (WMD) is a global common which affects the global communities [5]. Anonymity of cyber threats, limited traceability, and interconnected nature of the sector evidenced that to claim cyber as global commons [10]. In traditional understanding of power, control of a state lies on the control of the physical space and territoriality. National boundaries in which states are entitled to control are the three dimensions which are: territory, air, and sea [5]. However, the advancement of information communication technology brought a new dimension that connects all these elements of state i.e cyberspace which become a new claimed state territory [11]. Similarly, Sheldon, argued cyber must be seen as fifth geographical entities of a sovereign state next to land, sea, air, and space [5]. Some scholars tried to understand cyber by analyzing its function while others tried to understand by mentioning its unique characteristics. For example *Daniel* tried to grasp cyberspace as:

Cyberspace is a global domain within the information environment who's distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit informa1ion via interdependent and interconnected networks using information-communication technologies [11].

On the other hand Clark, tried to capture the concept of cyberspace from its intrinsic feature with in a four layer model [12]. He argued cyberspace is built from four layer components of the physical layer, logical layer, the information layer, and the people as a top layer. As a physical foundation cyberspace is built from real artifacts with real elements. The logical layer refers a series of platforms, on each of which new capacities are constructed which again serve as the next innovation. The information layer refers the storage, creation and transaction of Meta, static or dynamic data and the top layer refers active users of people who shape and manipulate the character and dynamism of the cyber ecosystem [12].

Broadly cyberspace is a digital network that is directly linked to all aspect of our daily life. Cyberspace is not only the internet but also encompasses critical infrastructure that supports modern society like water supply systems, electrical grids, and railway and ICT infrastructures [1]. In line with this, cyberspace like state territory is not immune from crimes. It is common to hear that cyber espionage, online theft, cybercrime, cyber terrorism and cyber fraud happening in many countries. It basically challenges traditional conception of power which was mainly state centric [4]. It challenges the historical understanding of boarders, national security, state sovereignty and state as the only actor to manage, possess and exercise military power. This brought the idea of cyberspace governance which encompasses, institutions, regulatory mechanisms and policy frameworks [1].

2.2. Cyber Governance

In the 21st century Cyberspace is becoming the main infrastructure that determines how modern societies associate and shape their aspect of relationships [13]. It is unlikely to see the impact of the revolutionized information communication technology affects the human life. It becomes the place where political and social agendas shaped, distributed and manipulated [5]. The decentralized nature of cyberspace that being operated by the private sector or small group of actors, makes cyber governance complex and contested in terms of defining and understanding it [14]. Similarly, defining cyber governance is difficult because of the dichotomy of vertuallity and reality. Cyber makes the division between national and international affairs untenable in which the forces of globalization and localization accelerated cross boarder movement of ideas and agendas that was hampered by space and time sometime in the past [4]. Then, what is cyber governance? Tunis Agenda for the Information Society cited by 'Internet Society' defined cyber governance as:

...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 [15]

Cyberspace is characterized as dematerialization (everything is paperless), de temporalization (instant communication), and reterritorialization (breaking the geographical boundaries and distances) [16]. Such unique features make cyberspace governance vague as it is difficult to frame who, how, and why cyber is being governed [1]. Some stick on the importance of cyberspace for national sovereignty and claims state should govern cyberspace. While others shared the idea that cyberspace should be governed by collective action by governments, organizations and the private sector.

In defining cyber governance focusing on Lexical definitions in which attempts made to report usage may mislead. Rather the concept can be best captured by applying extensional definitions in which attempting to grasp a list of all the approaches and models that the term applies. The following section tries to explore models and approaches of cyber governance.

2.3. Models of Cyber Governance

Despite the Internet is a recent development, how to govern the internet or cyber has a long history of confusion and contestation [16]. Cyber as one area of interaction for the actors of international relations, raises a number of questions on the modalities and approaches of governance. Is cyberspace a governable entity? If so how it should be governed? Who should be participated in cyber governance, how state sovereignty and cyber governance compromised? And a like questions have brought cyber governance in the public agenda. In historical analysis three broad perspectives or models on internet governance extensively shape the current idea of cyber governance which are distributed governance, multilateral governance, and multi-stakeholder governance [13].

2.3.1. Distributed Governance

At the onset of internet as a global means of communication, little was understood on how to govern it. This model of governance was common during the early stages of internet usage. It favors decentralized self-reliance consensus [17]. However, this approach is challenged with the shift on the volume of the number of actors and the elevation of the heterogeneity of stakeholders. At the early stage of internet governance particularly from (1970s–1994), there was no central planning, no central institution to prepare general designs and it was more of developing cyber landscape on the basis of cooperative, consensus based decision that involves individual actors [16]. Thus at the early stage of internet development, governance was characterized as decentralized and distributive among private and public actors.

2.3.2. Multilateral Governance

Multilateral governance model of internet governance focuses on intergovernmental approaches which commands governments control the speed, depth and management of the cyber ecosystem [16]. The approach of multilateral governance puts cyber governance at the top realm of sovereignty of states that is being initiated and led by developed states and supported by emerging economies in the sense that the policies and powers to govern internet is in the hands of nation states [17]. This is exclusively a state centric approach to cyber governance.

2.3.3. Multistake-holderism

Who shall govern the cyberspace has been also challenged with the engrossment of many actors and powers on the cyberspace. The birth of multi-stakeholdersim is lies on the boost of the private sector, NGOs, MNCs and non-governmental actors' role to international affairs. Multistake-holderism empowers non-state actors in the process of policy implementation, development and thereby fosters inclusiveness and representation in cyber governance [14]. Supported by the United States, Britain, Australia, Canada and internet society this approach integrates state and non-state actors on the development, governance and management of cyber landscape [17].

2.4. Ethiopia and the Digital Landscape

The introduction of cyber or internet in Ethiopia is a recent phenomenon. It was in 1993 for the first time that Economic Commission for Africa in Addis Ababa used internet with the establishment of stored and forwarded email services. Full internet access was began by Ethiopian Telecommunications Corporation (ETC) in1997, though the number of users until 2001 is not more than 3,500 [18]. Currently only 15.3% of the population which is around 16 million people uses the internet. The penetration rate is 4.2 which is the lowest category in African internet status. In line with this, Ethiopia is categorized in the ten bottom least ICT development index in Africa with Congo, Eritrea and Niger [19].

Access and quality of telecom industry increased overwhelmingly at the end of the first Growth and Transformation Plan (GTP I)[20]. The number of customers of all kinds of telecom services increased from 7.7 million in 2009/10 to 39.8 million by 2014/15 [38]. During the same period, the number of mobile subscribers increased from 6.7 million in 2009/10 to 38.8 million by 2014/15. Likewise in the second Growth and Transformation Plan (GTP II) the telecom and digital infrastructure has given much priority. The target by 2020 is ambitious which aimed to reach mobile service subscription 103.7 million, and that of internet users will be 56 Million. In line with this, the mobile and internet penetration is expected to be 100% and 54% respectively [21]. However, the data on ICT infrastructure and telecom services provided by the government organs and the other independent organizations has slight variations.

3. Discussion and Results

3.1. The 'Cleft Stick' of Cyber Governance in Ethiopia

The formal or informal, rules norms, legal and policy architectures that guide any human activity are generally termed as governance. Such explanations can applied to any social activity that could be political, market, cultural or internet [22]. Internet governance has three main components. The first one is the technical component that allows different components of the internet interact. The second is coordination of key protocols and addresses that allow people to accurately contact in the internet and the last one is the public policy and regulatory environment. The first two components involves different governmental and nongovernmental actors while the third component is a domain of sovereign states but with prior consultation with stakeholders [23]. Some understand cyber governance in terms of Regime Theory which comprises a "sets of implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations." In line with this Mueller and Mathiason explained cyber governance in the perspective of regime theory by stating:

Agreements made by governments, civil society and *international organizations about how critical elements of the Internet should be managed so that the Internet functions effectively and in an orderly manner for the benefit of all [24].*

In contrary to the global moves for collective aspect of cyber governance, the governance landscape encompasses state monopoly in all aspects of technical and policy environment in Ethiopia. The government seems tensioned with twin demands of expanding the sector in the one hand and fear of liberalizing the sector.

3.1.1. The Institutional Architecture on Cyber Governance

The scope of governance and control is a blurred line in Ethiopian telecom industry. There are many government organs which are neither neutral nor independent of the ruling party to regulate and administer the cyber landscape. Furthermore, the Ethiopian internet governance and regulatory functions is not clearly demarcated. The administration of Ethiopian digital convergence is not yet clearly defined. It is clearly seen that the regulation of information technology, telecommunications and broadcasting media are neither have clearly specified line of authority nor have worked in convergence [25]. For example the Ethiopian Telecommunications Agency (ETA) which was reestablished in 2002 has been supposed to regulate the overall telecommunication industry. Furthermore, the Ethiopian Information Communication Development Agency (EICDA) was also established to regulate and activate information and communication technology services. Later Ministry of Communication and Information Technology (MCIT) was created for the overall regulation of communication technology in the country [25].

The issue of convergence is a major challenge in cyber governance in Ethiopia. There is neither coordination of activities among the institutions nor clearly defined frontiers in their sphere of activities. For example with regard to cyber related crimes the federal police commission has full power of enforcement. Similarly Information Network Security Agency (INSA) has significant power to defend and take measures against any targeted attacks to information communication technology infrastructure [26]. MCIT has also empowered full regulatory power over information security. In similar vein INSA is also tasked in cybercrime related offences. In line with this, most proclamations are drafted by INSA including Computer Crime Legislation and Telecom Fraud Proclamations. Ethio-telcom is also another organ of government responsible for internet and ICT governance. Thus we can infer that there is a confusion of authority and duplication of tasks as well as it is difficult to identify who is responsible for what. For example Genet a girl who was a victim of social media abuse with the fabrication of pornography with her name and pictures told the researcher that she unable to get responses from any of the organizations responsible in telecom sector [27]. She said

When I report the case to Ethio-telecom, the authorities said the responsible organ for this is Information Network Security Agency (INSA). While I called to INSA they asked me to go to Federal Police Commission. When I went there, nobody responded me.

Thus this shows that referring cyber related cases from one institution to another is either the result of lack of the organizations' coordination of tasks plus ambiguity on their core competencies or negligence of their public duties.

3.1.2. State Monopoly of the Sector

The major feature of Ethiopian cyber governance architecture is state monopoly on the development and provision of telecom services. One of the major point of debate in Ethiopian economic infrastructure is liberalizing major areas of economic activities like the telecom, the banking and the hotel sectors. With respect to the telecom sector although several studies shows the advantage of liberalizing to improve efficiency and quality of services still the government holds its monopoly [28]. The government repeatedly claims the monopoly will enable improving quality and security, affordability and capacity building and further more enables to finance huge government projects. For example in an interview with Ethiopian reporter on July 30/2016, Ethio telecom Chief Executive Officer, Andualem Admassie strongly disagree on liberalizing the sector by stating

"It is very early neither to liberalize the telecom sector in Ethiopia nor to provide second licenses, "For instance we have provided 20 billion birr financial support for the nation's railway projects and we have reached 28 billion birr annual revenue this fiscal year."

By mentioning the contribution of Ethio telecom in stimulating other infrastructural developments he explained the role of monopolizing the sector. However many are skeptical of this explanation and rational of the government. More than the economic advantages the government is tight on security issues. Currently sell or resell of telecom services on private basis are strictly forbidden and using telecom technology that bypass local network is declared illegal [28]. All these monopoly reflects the cyber governance ecosystem in Ethiopia is not based on participatory approach. Neither the private sector nor any civil society are allowed to involve in the sector. Many are also skeptical of the recent government announcement to liberalize the sector as it needs amendment on different proclamation and the overall "developmental state" narration.

3.1.3. The Legal Landscape

Another aspect of cyber governance in Ethiopia is in the perspective of policies and legal frameworks. Various policy and legal provisions have been in place in the guises of guiding the cyber landscape. However critics provided such legal and policy initiatives are intended to stifle freedom of access to information and ensures the monopoly of the government on the sector. For example the telecom fraud proclamation no 761/2012, article 9/1/b confirms

Whosoever:

a) Establishes any telecom infrastructure other than the telecom infrastructure established by the telecom service provider; or

b) *Bypasses the telecom infrastructure established by the telecom service provider and provides any domestic or international telecom service; are punishable with rigorous imprisonment from 10 to 20 years.*

Such provisions are vague that creates frustration among the public. Sub article (a) also shows that the firm stand and commitment of the government to sustain monopolizing the telecom sector. Furthermore, sub article (b) entails using communication through international calling applications like Yolla, WhatsApp, WeChat, Skype, Rebtel, Viber, Vonage, messenger and other international calling services are forbidden.

The legal and institutional frameworks in governing internet shows Ethiopia is following the multilateral style of cyber governance which is strict state control with no room for other stakeholders. This is manifested in the "Computer Crime Proclamation No.958/2016". Article 41/1 stated that

The Federal Attorney General shall cooperate or enter in to an agreement with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, and extradition….

Such articles included in the legislation shows that the tendency of the government to interact with government authorities in cyber related crimes. As it is clearly seen the government is willing and has a tendency to interact only with state agents in cyber related matters.

3.1.4. Surveillance and Censorship

Cyber governance as a global domain of interaction which involves collective action by the private sector, the public and civil societies. In Ethiopian case not only monopolization of the sector matters but also the approach of governing cyberspace is exclusively based on combative approach. Ethiopian model of internet governance is closed where all powers on the internet exclusively rests on the hands of the government with no room for engaging and entertaining alternative means of managing the internet [9]. Furthermore, accessibility of information in Ethiopia is very limited. The trend even become more intense since these times as the restrictive nature of the government expanded with full powers as a response to political demand and popular demonstrations in the last three years [29].

Looking back since 2012 the status of internet freedom in Ethiopia is at risk. Series of annual reports of 'Freedom House' and 'Access Now' shows that Ethiopian cyber landscape is deteriorating from time to time [29]. The situations have become worse than the previous year's particularly since 2015 due to the use of internet for social mobilization [30]. Restrictions on connectivity; blocking and filtering; online manipulation; restrictive legal environment; prosecutions and detentions for online activities features Ethiopian internet governance [29]. Such activities are termed as "second-generation" or "next-generation controls" of the cyber ecosystem [31].

Evidences also show that internet shutdown is accompanied by violation of human rights and freedom of information. According to Deji Olukotun, Senior official from 'Access Now' told Associated press once that

"In Ethiopia there's been consistent blocking of social media and internet,"adding that people have died "during the kind of blackout where it's difficult to report on what's happening."

Furthermore, Ethiopian internet ecosystem is one of the most repressed in Africa based on three main variables obstacle to Access, limits on content, and violations of user's right [29].

3.2. Socio-economic Repercussions

It seems that internet shutdown is becoming a norm for most countries in the global south. Taking political and national security concerns as a pretext, government initiated internet disruptions are becoming "a new normal" [15]. Likewise, the status of internet in Sub-Saharan Africa, twelve countries imposed state sponsored internet restrictions which can be categorized as total national blackouts, regional interruptions, and selective social media restrictions [29]. In this instance, Ethiopia is one of the aforementioned examples in internet shutdown and disruptions. A number of instances have been recorded between 2015 and 2018 that the government interrupts in total blackout or in partial [8]. Internet governance basically is how to deal the proper functioning of the internet. However, in Ethiopian case it seems the government formula to govern the cyberspace is simply "shutdown" which a complete array of the principle of governance. The government justifications is always a shallow explanation of maintain peace and reducing negative impact of social media in fabricating rumors and falsehood [32].

Such sluggish internet and digital crackdowns are not without socio-economic and political costs. The first impact is measured in terms of economic cost. Poor internet access has a great impact to local business and international transactions. Even though Ethiopian economy is less dependent on digital market, some financial sectors are becoming inter connected. Evidences shows that poor internet accompanied by blackout linked with the general mobile network and it affects local business communications and transactions. Although it is difficult to vividly calculate the economic cost of internet interruptions, some attempts are made so far. In this regard CIPESA, Developed a model and calculate sub-Saharan African countries economic lose due to internet shut down [8]. Accordingly Ethiopia takes the lead where 36 days internet shut down costs the country 125,990,676 USD in 2017.

Secondly, with the advancement of Information communication technology, the sphere and influence of it on human rights is also not minimal. Human rights activists, human rights organizations and think tanks have given much attentions on it. UN special reporter in freedom of expression applauded the strong link between the violation of human rights and internet access. Usually states which have been accused of internet interruption are also condemned internet censorship. In line with this, Human Rights Council adopted in 2016 resolution, clearly stated the link between internet shutdown and human rights by stating:

"Condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law"

The idea behind the supporter of human rights is that people who enjoyed rights offline must be respected online. In this regard evidences shows that Ethiopian government violets human rights not only with shutdown of the internet but also application of sophisticated software to spy and censor online community [31].

Lastly, now a days, internet is one of the main mediums to narrow down knowledge gaps. The decentralized nature of the medium helps online communities to garner a wealth of ideas through entertainment and other means. However continuous interruption and lethargic access of the internet in many countries including Ethiopia causes disproportionate diffusion of information which amplifies the national "digital divide". For example Mengistu, a student from Addis Ababa University told the researcher that he unable to apply scholarships plus attend online short course training due to the sluggish and poor connectivity [33]. He stated that

I am trying to apply scholarships abroad online, but unable to submit my applications because of the poor connections. I also registered for online short training. However it is difficult to get access to internet which able to visit online videos.

In addition, a student in Oromia region once told to VOA that he has similar problems that he unable to contact his supervisor via emails and social media channels due to the interruptions of internet in many parts of the country [34]. Similarly, in September 2017, Henok an Ethiopian PhD student told to 'Access Now' that he even unable to browse lectures by stating,

"Not having internet in the 21st century is hard, it's catastrophic! You can't go and browse lectures on YouTube... Every media, all of them are restricted" [30].

The cyber governance architecture is thus, organized neither in the way to exploit digital opportunities nor to allow foreign and private actors to involve which leads us to conclude Ethiopian cyber governance is in quandary.

4. Conclusion

It is clear that the forces of information globalization makes everyone to live alone impossible. In line with this pace, it is unlikely to see the life of man unaffected by the digitalization of social, economic and political spheres of human endeavor. Thus, cyber governance is and will be one of the main arena of policy making and research in the ages yet to come. It is because not only it affects the national sovereignty of the state but also it tremendously affects the socio-economic and political life of individuals. However the major challenges in many developing nations are not only lag behind in providing access to internet to their citizens but also their deterring approach for internet diffusion is continuing to be a major source of "digital divide".

In similar vein in the Ethiopian digital landscape excessive control and restriction of access to information is the major feature of internet governance. Institutional structures lack transparency and coordination of tasks for responsive service delivery. The legal and policy environment is also shaped on the way to limit full utilization of digital opportunities other than creating conducive environment. Thus, as one of list connected nation in Africa, the government must focus on expanding the infrastructure to assure accessibility and revising the policies and legal instruments to ensure digital freedom so as to get the maximum blessings that the digital world has brought to us.

References

[1] Liaropoilos N. Andrew (2017). Cyberspace governance and state sovereignty, in democracy and an open economy world order. Page 25-37.

[2] Lewis A. (2010). Sovereignty and the Role of Government in Cyberspace. The Brown Journal of World Affairs volume xvi, issue ii, page 55-65.

[3] Perritt, Henry H. Jr. (1998) "The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance," Indiana Journal of Global Legal Studies: Vol. 5: Issue. 2, Article 4. Available at: http://www.repository.law.indiana.edu/ijgls/vol5/iss2/4.

[4] Wenger A. (2001). The internet and the challenging face of International relations and security. Journal of Information and Security. Vol, 7 P 5-11.

[5] Sheldon, J. (2014). Geopolitics and cyber power: Why geography still matters, in American foreign policy interests. *The Journal of the National Committee on American Foreign Policy, 36* (5), 286-293.

[6] Adams J. and Albakajai M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. Management Studies, 2016, Vol. 4, No. 6, 256-265.

[7] Laguerre, M. (2004). Virtual time, in information. Communication & Society, 7 (2), 223-247.

[8] Collaboration on International ICT Policy for East and Southern Africa ((CIPESA), 2017). Calculating the economic cost of internet shut down in sub Saharan Africa.

[9] Gagliardone, I and Golooba-Mutebi, F (2016). The Evolution of the Internet in Ethiopia and Rwanda: Towards a "Developmental" Model? Stability: International Journal of Security & Development, 5 (1): 8, pp. 1–24, DOI:

[10] Xiao Yingying, & Yuan Zhengqing. (2016). A primary exploration on cyber security governance in Africa, West Asia and Africa, No. 3: 121–137.

[11] *Daniel T. Kuehl (2009).* From Cyberspace to Cyber power: Defining the Problem, US Naval Institute. Available at http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf.

[12] Clark D. (2010). *Characterizing, cyberspace: past, present and, future*. MIT, Csail.

[13] Jensen T. (2015). Cyber Sovereignty: The Way Ahead. Texas International Law Journal, volume 50 issue 2, page 274-302.

[14] The Hague Institute for Global Justice (2015). Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance. Policy Brief 17, November 2015.

[15] Internet Society (2017). Policy Brief: Internet Shutdowns https://www.internetsociety.org/policybriefs/internet-shutdowns accessed on April 10,/2018.

[16] Kurbalija K.(2016). *Introduction to internet governance* (7th ed.). Malta, diplo foundation.

[17] West M. Sarah, (N. d). *Globalizing Internet Governance: Negotiating Cyberspace Agreements in the Post Snowden Era.* University of Southern California, Annenberg School for Communication and Journalism.

[18] ITU (2002). Internet from the Horn of Africa: Ethiopia case study. Geneva, Switzerland.

[19] https://www.internetworldstats.com/stats1.htm, is a website that provides statistics on internet users world wide.

[20] Ministry of Finance and Economic Development (2014). Growth and Transformation Plan Annual Progress Report for F. Y. 2012/13. Addis Ababa, Ethiopia

[21] National Planning Commission, (2016). Ethiopian Growth and Transformation Plan II (GTP II) (2015/16-2019/20). Addis Ababa, Ethiopia.

[22] Ernest j. Wilson,(2005). *What is Internet Governance and Where Does it Come From?*. Cambridge University Press.

[23] International Chamber of Commerce (2004). Issue Paper on Internet Governance. Paris, France.

[24] Mueller, J. Mathiason, H. (2007). The Internet and global governance: principles and norms for a new regime, Global Governance, Review of Multilateralism and International Organizations, n. 13.

[25] Kinfe Micheal and Halefom Hailu, (2015). The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media. Mizan Law Review, Vol. 9, No.1, p 108-153.

[26] Ethiopian Federal Democratic Republic, Federal Negarit Gazeta (2016). Computer Crime Proclamation No. 958/2016, Addis Ababa, 22nd Year No. 58th July, 2016.

[27] Online Interview with Genet Yigrem (the name changed for security reasons), date of interview 25/04/2018. Interviewer, the researcher

[28] Minyahel Desta (2012). Liberalization of telecommunication in Ethiopia challenges and prospects: citizens' view and opinion Research paper submitted to trade policy training center in Africa (trapca) for the 2012 annual conference. AddisAbaba, Ethiopia.

[29] Freedom House,(2018). Freedom on the Net 2018 - Ethiopia, available at: https://www.refworld.org/docid/5be16b1a4.html.

[30] Access Now (2017) Shutdown Stories Project. https://www.accessnow.org/shutdown-stories-project/Accessed on May 01/2018

[31] Marczak B., Alexander G. and etal (2017). CHAMPING AT THE CYBERBIT Ethiopian Dissidents Targeted with New Commercial Spyware. https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/ Accessed on May 15/2018.

[32] The Brookings Institution, (2016). Internet shutdowns cost countries $2.4 billion last year Washington, DC.

[33] Online Interview with Mengistu Bayih (the name changed for security reasons), date of Interview 30/04/2018. Interviewer the researcher.

[34] Voice of America (2017). As Violence Flares in Ethiopia, Internet Goes Dark https://www.voanews.com/a/as-violence-flares-in-ethiopia-internet-goes-dark/4164223.html Accessed on May 15/2018.

[35] Calandro. E, Galpaya H., Jaume-Palasí L., Lara C., Spielkamp M. (2016). *Guidebook Internet Governance, Media freedom in a connected world*. Germany, Bonn.

[36] Ethiopian Federal Democratic Republic, Federal Negarit Gazeta (2012). Telecom Fraud Offence Proclamation No. 761/2012, 18th Year No. 61 Addis Ababa 4th September, 2012.

[37] Ethiopian Reporter (2016). Ethio-Telecom plans continental expansion. Retrieved from https://www.thereporterethiopia.com/content/ethio-telecom-plans-continental-expansion.

[38] Freedom House (2017). Freedom on the net 2017. Freedom house report 2017.

[39] Lucchi N.(2014). Internet Content Governance and Human Rights. Vanderbilt Journal of Entertainment & Technology Law. Vol. 16, No.4 Page 809-856.

[40] Oguno P. (2016). Cyber Security, Sovereignty and democratic governance in Africa, challenges. Global Journal of Politics and Law Research Vol.4, No.2, p.43-54.

[41] Solum B. Lawrence (2008). Models of Internet governance. University of Illinois, Public Law Research Paper No. 07.

[42] Weber R. (2015). *Principles for governing the Internet a comparative analysis (6th ed.).* United Nations Educational, Scientific and Cultural Organization, France.