# Assessment of Cybercrime Governance in Ethiopia Since 2004

Misgana Yifiru Ayenew
Lecturer at Ambo University, Ethiopia

## Abstract

Communication technology is a recent phenomenon that links countries of the world together. Like other countries of the world Ethiopia also interconnected to global net work via internet technology and committed to expansion of the technology at home to substantiate its economic, social and political advancement goal. However, as a result of digitalization effort at home, the country becomes both source and target of cyber crime. Hence, in order to curb cyber crime, the government of the country engaged in to various activities and this work assess the initiatives under taken by Ethiopian government in the area of cybercrime governance. To do so, the research employs qualitative research methods and secondary source of data.To discharge its global responsibility and prevent itself from cyber crime, Ethiopian government works hard and undertakes various measures. Hence, the government begins its work of fighting cyber crime for the first time by initiating criminal code in 2004 that penalize limited cyber crime in the country. As such, the first initiatives followed by scattered legislations which cover limited area of cyber crime like Telecom fraud offense legislation, National payment system proclamation and recently computer crime proclamation. Similarly, the government also initiates policy measures like ICT policy and strategy, National information security policy and Criminal justice policy. To implement these policies and legislations the government also establishes various institutions.However, these all legislations and policy initiatives are inadequate in cyber crime governance in Ethiopia, due to failure of government to couple its unilateral effort and commitment of fighting cyber crime with transnational cooperation and capacity building. Hence, there is no meaning full and continues capacity building undertaken by Ethiopian government. As a result, there is gap of knowledge and human resource in the country related to cyberspace which in turn creates fertile ground for cyber crime. Ethiopian government also does not engaged into comprehensive and functional transnational cooperation and dormant to be party to any regional and international cyber crime convention. Thus, its domestic effort to fight cyber crime become less significant since cyber crime is borderless. Therefore, in order to successfully defense cyber crime, Ethiopian government should complement its domestic initiative by continues capacity building and transnational cooperation.On the other hand, legislated cyber crime in Ethiopia also infringes freedom of expression and privacy right of peoples. Thus, government should work hard to ensure compatibility within international human right law and cyber crime law as much as possible.

**DOI:** 10.7176/NMMC/96-01
**Publication date:**May 31st 2021

## Introduction

Present era is perceived as digital age because of technological revolution. This technological revolution tremendously spread all over the world and many countries of the world developed or developing, poor or rich, small or big experience this technological advancement especially internet technology. Thus, yet we have wide spread diffusion of the internet, mobile communication, digital media and a variety of communication technology which changes culture of communication in the world in general and in Africa in particular in which Our country is one among others (Halefom, 2015:1). Hence, this form of technological revolution affects all aspects of human life including international relation. It brings significant change on the way people and state communicate and exchange information by changing political, social and economic landscape of the world. The ongoing digital transformation also provide unique opportunity to the world to strengthen social cohesion, improve lives of people and develop strategic sectors like education, health, entrepreneurship, employment, peace and security as well as good governance[1].

However, this digital transformation of the world has also dark side like cyber attack which is common challenges to all countries. According to pool (2013), the rise of cyber war trace back to the history of cold war where USA exploited computer technology to overcome communication barrier at a time of nuclear attack from communist. From the time on wards, computer become weapon of war via arsenal digital warrior and many countries around the world like Georgia, Estonia, Iraq, Iran and other countries experienced cyber attack. Thus, countries of the world including USA, China, Russia and North Korea build and maintain their cyber warfare to protect themselves from cyber attack(ibid, 2013). Indeed, with the emergency of internet, reliance on computer and other digital technologies led to vulnerability to cyber attack and cyber attack became transnational challenges from which no country and individuals in the world are immune in which Ethiopia is not an

[1] . The first African forum on cyber crime hosted by African union commission at Addis Ababa, Ethiopia (16-18 October 2018)available at: https://www.coe.int>web>african

exception.

Now days Ethiopia is committed to ICT development to achieve economic development and poverty reduction goals. Number of mobile subscribers and social network users are steadily increasing from time to time despite low internet penetration in the country. Similarly, digitalization like electronic banking, electronic funds transfer, mobile banking, ATM service and e-governance to provide e-service increases in the country that also open opportunities for cyber crime. Hence, in order to overcome cyber crime the country engaged in different policy enactment and institutional set up. But still cyber security governance is at its embryonic stage and even existing cyber security laws are inadequate to govern cyber crime (Halefom, 2015:7). Thus, further engagement and collaboration is required to regulate cyber crime in full-fledged manner in Ethiopia context.

## Statement of the Problem

Today in the world cyber attack become serious challenge to all state of the world and cyber governance emerged as policy priority area of states across the world. Hence, this statement also applies for our country Ethiopia since the country does not live on island and immune from cyber crime. In Ethiopia, even though digitalization has short history, Utilization of social media via internet has shown incredible progress. Thus, individual peoples, business persons, students, government offices and officials, and various social group of the society use digital technology for different ends despite the existence of low internet penetration in the country.

Moreover, as digitalization increases, an opportunity for vulnerability to cybercrime is also increasing. According to Halefom (2015:8-9) Ethiopia is ranked seventy ninth cyber crime ridden country in the world and hosted top ten malicious URL. However, there is no consolidated report that shows the exact prevalence, impact and to extent the information societies of the country are vulnerable to cyber crime. For him, this problem emanates from lack of capability to detect cyber crime, neglecting cybercrime governance and ill prepared to deal with cyber crime. In line with this statement, Kinfe and Halefom (2015:109) in their article, assert that Ethiopia was delay in legislative measures in the area of internet law. Therefore, cyber crime governance measures in Ethiopia requires in depth assessment and examination to have full fledge understanding and draw lesson for the future.

As mentioned before, Ethiopia was late in cyber crime legislation that emanate from recent introduction and low penetration of internet technology. But the year 2004 was a land mark in history of cyber governance in Ethiopia, because of the enactment of the first legislation that addresses internet related crimes. As such in 2004 the country adopted Ethiopian criminal code that penalize short list of computer crime (ibid, 2015:110). From this time on wards, scattered legislations are adopted and institutions are established to deal with cyber crime governance. For instance, Telecom fraud offence legislation of 2012 and Ethiopian computer crime law of 2016 are the major legislation dealing with cyber crime even though they have their own deficiency. Similarly, Ethiopian information network security Agency (INSA) and National intelligence and security service (NISS) also institutions mainly dealing with cyber crime governance in Ethiopia (Kinfe, 2016). However, this institution, legal frame works and policy measures alone remain paper value. Thus, this paper engaged to assess cases behind inadequacy of legal frame work, policy measures and institution in fighting cyber crime in full fledged manner in Ethiopia.

In the world in general and in Ethiopia in particular, balancing cyber crime law with international human right law is the main challenge. Hence, cyber crime law should compatible with international freedom of expression guaranteed to people by domestic constitution and international treaties as well customary international law. But, in Ethiopia cyber crime legislations are infringing the right to expression and privacy of peoples which also requires investigation[1]. As a result, analyzing cyber crime law of Ethiopia in relation to freedom of expression and privacy right is one focus area of this paper. Furthermore, cyber crime governance in the country relies only on policy enactment and institutional set up. But this effort alone does not bear better result in fighting cyber crime and need to be complemented by capacity building, because full knowledge of the on line space in which cyber crime operating is crucial to prevent cyber crime successfully (Bjola,2018).Similarly, international cooperation to tackle problem of cybercrime is indispensable since cyber crime is cross border challenge and no single state or organ can defense cyber crime on its own effort effectively and efficiently ( pool ,2013). Thus, this research endeavors to explore performance of the country in the area of capacity building and international cooperation that are neglected or given little attention by Ethiopian government in the course of cyber crime governance.

## Method of Data Collection

Given explorative nature of the article, the study employed a qualitative research method. In order to achieve the study objective, secondary data has been used. Thus, the paper has given emphasis on the analysis of the relevant

[1] "Ethiopia: Computer crime proclamation," Article 19,( 2016), available at: https://www.article 19.Org/data/files/medialibrary/38450/Ethiopia-Computer-Crime-Proclamation-Legal-Analysis-July-(1).pdf

available literature on the subject. In relation to literature, the researcher has specifically relied on examining academic articles, journals, MA thesis, conference papers, conventions related to the topic and major legislation on cyber crimes, which have relevance to the study.

## Assessment of Cybercrime Governance in Ethiopia

### Conceptual clarification

Cyber warfare is recent phenomena since it is related with internet technology which has short history. Because of this, comprehensive definition of the term is not developed yet and different nations and scholars have different definitions for similar terms. Similarly, because of the newness of concept of cyber warfare even within one state, different government agencies differ in their definition of certain terms (pool, 2013:308). For instance, United State department of defense define cyber as "global domain within the information environment consisting of the interdependent network information technology infrastructures including internet, telecommunication net work and computer system." But congressional research service report defines the term as "total inter-connectedness of human being through computer and telecommunication without regard to physical geography." Additionally, the national military strategy for cyberspace operation defined it as "domain characterized by use of computer and other electronic device to store, modify, and exchange data via networked system and associated physical infrastructure"(ibid, 2013:308).

Therefore scholars and different organizations are not dire to develop single definition of cyber crime and this resulted in multiplicity of definitions and terminologies for the same term. As such absence of conceptual clarity of term within international community hinders development of legal frame work and treaties to defense cyber crime within global states. Thus, most of the time states and international organization while developing legislation for cyber crime, refrain from defining the term and simply classified cyber crimes as our country Ethiopia does while legislating computer crime proclamation of 2016 ( Kinfe, 2016). Thus, challenge of cyber crime governance begins here from absence of unanimous and comprehensive definition for the term.

### Historical Evolution of cyber crime

It is obvious that cyber crime is an outcome of digitalization that emerges with internet technology. Hence, ever since the Internet technology became available to the general international public in the early 1990s, its ever-increasing role in the conduct of politics, economics, and society has been evident in both the international and national arena. The emergence of social media sites such as Facebook, Twitter, You Tube, blogs and other networks have begun to shake the status quo traditionally dominated by the traditional media institutions shifting the balance of information and communication power to multidirectional and horizontal flow of information and communication.

From the time on wards, internet technology serves as double face, one as positive role to make life easy by disseminating information irrespective of communication barriers and physical distance and at opposite side transformed to safe haven for criminals(Halefom, 2015:2). Indeed, cyber crime started in simple way while people sent virus and worms to one another's computer to annoy each other. But later on, cyber space used as political warfare within countries and used for political purpose for first time during cold war period between USA and communist. Thus, computer has been used as weapon of war via arsenal digital warrior for cyber crime. Arsenal digital warrior disrupt the normal function of computer using denial service program and malicious programming like virus, worms, Trojan horse and digital manipulation that helps to stole and transmit information (pool, 2013:301-302). So, cyber crime becomes serious economic and national security challenge across the world in which Ethiopia is not an exception.

Coming to Ethiopia, the advent of Internet in general and social media in particular is a recent phenomenon which is also true for cyber crime. According to Amayu (2015) Internet began to exploit in Ethiopia around 2001 at UN economic commission for Africa. But the technology was opened for wide use in the year of 2005 when Ethio-telecommunication Corporation started to deliver the service and 2007 marked the year when internet technology was provided via phone. Thereby, following incredible increase of digitalization in the country individuals, government office and private companies which rely on computer via internet are target of the crime since no one can immune from cybercrime even though there is no consolidated report that show extent and severity of crime in the country. This lack of data emerges from low experience of cybercrime investigation and absence of reporting habit to the concerned organ.

### What Constitute Cyber crime?

Criminals of cyber crime employed arsenal digital warrior to commit cyber crime against targeted entities whether individual, states or organizations. According to pool (2015), arsenal digital warrior exploited denial service program and malicious programming as weapon to disrupt normal function of computer. For him, there are different varieties of malicious programming used for cyber crime commission. Hence, virus is one among others that corrupt data and consume memories. Similarly, worm also used information transfer system to spread from computer to computer and thus more aggressive and pervasive weapon. Moreover, Trojan horse use deceit to gain users trust and digital manipulation help attackers to alter an image or video to change meaning of the image or video. More importantly IP spoofing malicious programming allow hackers to create web page that appears identical to trusted web page on line which deceive users to enter into fraudulent web page . From this, we can understand that cyber crime committed through various mechanisms and progress and broaden with technological advancement.

In Ethiopia, those cybercrimes are committed even though there is variation of degree and extent. For instance, the first cybercrime legislation in Ethiopia penalizes hacking, dissemination of malware and denial service attack (Knife, 2016:448). Similarly, Halefom (2015:8) asserted that computer viruses, malware malicious attack, website defacement, illegal access and spam are more common form of cybercrime that occur frequently and cybercrime incidents like damage to computer data, denial of service attack and system interference occur infrequently in the country. Moreover, computer crime proclamation No.958/2016 extended and introduces new cyber crime in the country and outlaws them.

According to the proclamation, cyber crime is classified in to four categories. The first categories related with crime against computer system and computer data. Under this category, crime like illegal access and interceptions, interference with computer system, causing damage to computer data and criminal acts related to use of computer device and data are legislated as cybercrime and penalized. Similarly, under the second category, computer related forgery, fraud and identity theft are punishable. Furthermore, cyber crimes like child pornography, spamming, on line defamation, intimidation and crime against public security are outlawed under the third categories. Finally, the fourth categories deal with miscellaneous crimes namely breach of duty and hindrance of cybercrime investigation, liability of judicial person and internet provider. Hence, this implies as cybercrime evolved and progress with technological transformation, adoption of more dynamic and adequate cyber crime is indispensable to prevent, control, investigate and prosecute cyber crime suspects.

## Cybercrime Governance Initiatives in Ethiopia

Ensuring cyber security is prerequisite for economic development, human right protection, maintenance of world peace and free flow of transnational information. It is also one aspects of world peace and common interest and responsibility of all states. Moreover, cyber security is priority of states across the world for economic prosperity and national security interest (Kettemann, 2017).Thus, countries of the world build and maintains their cyber warfare to protect themselves. Even though there is no single treaty that governs cyber crime at international level, it can be derived from customary international law and principles of international law. Accordingly states should exercise their jurisdiction over their territory and ICT appropriately and refrain from damage of internet function in another state. Similarly they should guided by principle of ban on aggression and good neighborliness related to internet. Moreover, state are responsible to prevent cyber attack originated from their own territory, establish legal system to ensure and foster cyber security and cooperate together in prosecuting attackers and conducting investigation of cyber attack (ibid, 2017).

On the other hand, countries also unilaterally formulate policies at domestic level to defense cyber crime. Additionally, they engaged in institutional set up, capacity building and to less extent engaged to cross border cooperation via international organizations like African union and European Union initiatives to fight cyber crime. Here, this section assess legal frame work and policy measures, institutional set up, capacity building activities and transnational initiatives undertaken by Ethiopian government to regulate cyber crime.

## Legal frame work and Policy measures

As it is mentioned before, Ethiopia was late in initiating legal frame work and policy measures as response to cybercrime. However, this does not mean complete absence of laws and policies dealing with cybercrime in the country. As such, there are various legal frame work and policy initiatives that directly or indirectly address cybercrime. According to Kinfe and Halefom (2015: 128) the country adopted criminal code in 2004 for the first time to penalize acts of cybercrime like computer hacking, spread of malware and denial of service attack. However, they asserted that, the code is in adequate to govern cybercrime because of its limited scope, fail to accommodate the growing evolution and diversification of cybercrime, does not provide procedural and evidentiary provision that helps to investigate and prosecute cybercrime and neglected cross border nature of cybercrime and need for international cooperation for investigation and prosecution of the crime.

Following the legislation of the code, there are also fragmented and scattered laws that deal with cybercrime. Telecom fraud offense proclamation No. 761/2012 is one among others. Hence, this legislation technically resembles to cybercrime law since it outlaw unlawful interference, unlawful interception and illegal access to telecom network and telecom system. Indeed, telecom service includes internet service and data communication service (ibid, 2015:129). Similarly, National payment system proclamation No. 718/2011 and Registration of vital event and national identity card proclamation No.760/2012 also address cyber issue in one or another way. But those legislations deal with certain cybercrime issues in Ethiopia and none of the legislation comprehensively combats cybercrime (Halefom, 2015:17). Thus, comprehensive cyber security laws are required in the country to address cybercrime adequately and because of this the country come with the first and second draft cyber law which culminated to computer crime proclamation in 2016.

More or less computer crime proclamation No. 958/2016 accommodates the deficiencies of previous cyber law by introducing various reforms. But this does not mean that the new proclamation is absolute and complete. According to Kinfe (2016:450-451) the new law is distinct from the previous legislations in ways that it broaden the scope of cybercrime by introducing and criminalizing new cybercrimes, has detailed provision of procedural and evidentiary rules that are vital for investigation and prosecution of cybercrime, contain definitional provision that define set of technical concepts unlike 2004 criminal code, shifts enforcement role from INSA and federal police to Federal General Attorney and punish crimes that are committed intentionally and only few cybercrimes are punished when committed negligently.

Our country Ethiopia also introduced various policy measures to combat cyber crime. Hence, Ethiopian government adopted general ICT policy and strategy in 2009 with cyber security implication that focus on safeguarding and securing national electronic communication, protection of data and network integrity, prevention, detection and respond to cyber crime (Iyasu, 2018:53). Similarly, National information security policy is also adopted in 2011 with the objective of ensuring confidentiality, integrity, availability and authenticity of national information asset. Moreover, in 2011 the country introduced Criminal justice policy that calls for progressive capacity building program for all organs responsible to detect, investigate and prosecute cyber crime and promoting international cooperation (Halefom, 2015:10-12).

### Institutional Set up

Establishment of robust and specialized institution to effectively implement legal and policy frame work enacted by the country to regulate cyber crime is very important. As such, various institutions are set up to deal with cyber crime in Ethiopia. Ministry of communication and information technology (MCIT) is principal organ in charge of ICT, cyber security in general and cyber crime in particular. It has a power and duties to initiate policies and laws in ICT area to ensure provision of quality, reliable and safe ICT service (Kinfe and Halifom, 2015). Additionally, Ethiopian information Network Security Agency (INSA) established in 2006 and re established in 2011by council of ministers to deal with cyber security. Hence, the institution is empowered to formulate national policy, laws and standards to ensure security information and computer based key infrastructures. It assume significant power in taking all necessary counter measures to defend cyber attacks on information and computer based infrastructures and provides assistance and support in respect to preventing and investigating cyber crime to federal police and other organ empowered by the law. Similarly, National Intelligence and security service (NISS) also involved in investigation of cyber crime especially in collecting intelligence on cyber criminals. Federal police commission also another important institution dealing with investigation and prosecution of cyber crime (Iyasu, 2018:49-52).

### Capacity Building Activities

Ethiopia is doing more in policy initiative, legislation of cybercrime law and setting institutions to fight against cyber crime at domestic level. However, this all are useless unless it is complemented with capacity building and international cooperation. In Ethiopia, population of the country in general and government sectors and institutions that directly and indirectly connected to internet technology and target of cyber crime have no full knowledge of the on line space, because of the newness of the technology and less government engagement in area of capacity building. Similarly, higher educational institutions of the country are less emphasized on offering courses that introduce students to the new realities presented by internet and cyber crime. Because of this, there is little cyber crime investigation and prosecution experience in Ethiopia (Kinfe, 2016:455-456). In line with this statement, Halefom (2015:14-15) assert that law enforcement mechanism also not equipped with necessary resource and expertise for investigation and prosecution of cybercrime and thus rely on conventional investigation methods for fighting ordinary crime in order to identify, arrest and prosecute cyber criminals. Hence, these all problems led to reluctance in reporting cyber crime, lack of evidence and enforcement failure to enforce the existing cyber crime related provision.

Therefore, successful cyber crime defense requires actual launch of continues capacity building program. Cyber law enforcement agents like police force who engaged in cyber crime investigation and judges must be properly acquainted with nature and scope the crime. Government also must allocate sufficient resource to raise public awareness and fill the gap of qualified work force. Similarly, the government also should work with intellectuals, academicians and private stake holders on creating awareness to institutions and public at large (Kinfe, 2016: 457). As such, recently government of the country to some extent working hard for capacity building even though much work is expected in the future. Ethiopian information Network Security Agency (INSA) also building reliable cyber security capacity and systems for various institutions to enable them develop self-assessing capacity and active cyber defense mechanisms (Iyasu, 2018:50). Moreover, Addis Ababa and

Mekelle University are now offering PHD program on the subject.

**Transnational Initiatives**

The scope of cyber attack is global and there is no border in the space**.** Because of this, unilateral effort of countries to tackle cyber crime is meaningless without global coordination within global societies. In the world, there is no single treaty that governs cyber crime and binding up on world states. However, this does not mean complete absence of treaties since there are certain treaties that cover certain aspects of international cyber war. For instance, Tele communication convention, Outer space treaty and convention on international civil Aviation related to cyber warfare are few of them. But, those respective treaties are failed to cover the entire areas of cyber warfare (Pool, 2013). On the other hand, there are also cyber crime related conventions at regional level. Hence, council of Europe's Budapest convention on cyber crime and African Union convention on cyber security and personal data protection (AUCCSPDP) are the most relevant regional and international instrument in matters related to cyber crime[1]. But countries around the world are reluctant to be members of either of the convention and hindered from ratification of the convention.

Examining Ethiopian situation, there is no meaningful and comprehensive international cooperation activities related to cyber crime defense. Here, council of Europe convention on cyber crime is open for all countries around the world to be membership and it provide technical and other assistance for member countries to effectively investigate and prosecute cyber attack. But, unlike African countries like South Africa, Seychelles and Senegal, Ethiopia is failed to membership of the convention. Similarly, Ethiopia also not part to African union convention on cyber security and personal data protection. Hence, Ethiopia is dormant when it comes to any international cooperation on cyber crime. It has not participated in any regional, sub-regional and international cooperation in fight against cyber crime (Iyasu, 2018:63-64).But there are little collaboration with countries like USA, and UK as well with United Nation Economic commission for Africa (UNECA), European Union and Interpol in the areas of capacity building (ibid, 2018:51). Thus, Ethiopia is failed to substantiate domestic initiatives with international cooperation in fighting cyber crime and this made the unilateral engagement of the country in regulating cyber crime less significant since the challenge is transnational and beyond its sovereignty. This clearly implies traditional sovereignty conception of the state is severely challenged by cyber space in technological age and on the way of shrinking.

**Law of cyber crime, freedom of expression and the right to privacy**

Now days' balancing of cyber crime law with human right law is the most challenge and headache to state of the world in the course of cyber crime governance (ketteman, 2017). Hence, cyber crime is a violation of human right, but cyber crime law serves as double fold. This means that, cyber crime law in one hand enacted to protect human right which is violated by cyber crime and at the same time the law itself violates human right like freedom of expression and the right to privacy guaranteed to peoples by international human right law and municipal law. Thus, ensuring compatibility of human right law with that of cyber crime law is the home work of countries of the world including Ethiopia.

Freedom of expression is protected under article 19 of United Nation Declaration of Human right (UDHR), article 19 of international covenant on civil and political right (ICCPR) and article 9 of African charter on human and peoples right (ACHPR). Hence, article 19 of ICCPR protects all forms of expression and all forms of their dissemination including electronic and internet based mode of expression. As such ICCPR and ACHPR are binding international treaties ratified by Ethiopia and UDHR is binding on Ethiopia as rules of customary international law. Similarly, the right to privacy also guaranteed by article 17 of ICCPR to which Ethiopia is state party. Moreover, freedom of expression and privacy right also guaranteed and protected by Ethiopian constitution. Thus, even though international laws on cybercrime recognize the importance of balancing human security with fundamental human right, freedom expression and privacy rights are violated by cyber crime law in countries like Ethiopia[2].

Most of the time, Ethiopia is blamed for violating internet freedom which is against freedom of expression. Hence, there is no law in Ethiopia that governs means through which illegal and harmful content could be blocked and filtered. As such where government believes certain content is problematic order state owned Ethio-telecom that block internet access which is triggering problem in Ethiopia at previous, present and may be in the future unless Ethio-telecom is privatized. Thus, Ethiopia is the first country in sub-Saharan African country to filter internet and this filter targeted to journalist, bloggers and opposition party officials who are against government (Amayu, 2015).

In addition to blocking internet access, freedom of expression also violated by cyber crime law in Ethiopia. For instance, under article 13 and 14 of computer crime proclamation of 2016 many forms of legitimate

[1]. See the first African forum on cyber crime of African union, Supra note1

[2] .See Ethiopia: computer crime proclamation- legal analysis, supra note2, pp.7

journalism will be criminalized. Hence, through interpretation of article 13 of the proclamation, media out let's reporting on government corruption or ethnic conflict would commit offence against public security and subjected to punishment. Article 14 also punishes publication of any content that incites chaos, violence or conflict since such reporting incites fear among public directly affected by the event, even though the reporting is still legitimate. This clearly implies under the proclamation, there is a situation in which legitimate journalist are subjected to punishment[1]**.**

Similarly, the newly legislated cyber crime law also infringes privacy right of peoples. According to Kinfe (2016:452-454) the second draft cyber crime law authorize INSA to undertake sudden digital forensic investigation without judicial warrant against suspect computer as source of cyber attack for preventive purpose. However, the final version of the law mandates prior judicial warrant before such measures are taken by INSA. Even though this is the case, INSA still yields the power to conduct warrantless virtual not physical investigation under its re establishment proclamation of 2013. Adding more, he noted that, computer crime proclamation of 2016 allows the use of single judicial warrant issued for specific computer system to be used in conducting investigation in another computer system. Hence, such vague and general warrant erode individual right of people whose computer system would be accessed even without their awareness. Finally, the law also negates crucial principles of procedural justice such as due process of law. As such ,the court allows investigation of personal computer at a time of request and this in turn discloses personal computer data that implicates data privacy right of peoples (ibid,2016).

## Conclusion

Today global states across the world are interconnected irrespective of physical distance and communication barriers via internet technology. Hence, internet technology helps to save time and finance spent for transport in traditional time. However, this digitalization technology births cyber crime which is also common challenges to all countries irrespective of boundaries. This implies that countries of the world reap both benefit of communication technology and its burdens like cyber crime in which our country Ethiopia is not an exceptional.

In Ethiopia, internet technology has an age of almost 20 years which is also true for cyber crime since it is associated with internet. The country is committed to expansion of ICT to support its economic development. Hence, this expansion of ICT provide an ample opportunity for wide spread and expansion of cyber crime in the country. Therefore our country Ethiopia along with other countries of the world becomes target of cyber crime which emanates from outside and within the country even though there is no exact report that reflects the scope of the problem. As a result, the country engaged into different cyber crime defense mechanism like enactment of legal frame work, policy measures, institutional set up and capacity building activities.

Because of short history of internet technology, introduction of legal frame work also late in Ethiopia and 2004 was starting point for regulation of cyber crime with enactment of criminal code to criminalize limited cyber crime. From this time on wards, various policy initiatives and legal frame works are adopted. Here, the most important cyber crime law today in Ethiopia is computer crime proclamation of 2016. Similarly robust institutions like MCIT, INSA, NISS and federal police commissions are established to execute the enacted legal frame work and policies related to cyber crime.

However, in Ethiopia this policy initiatives, legal framework enactment and institutional set up alone are inadequate and deficient to defend cyber crime, because these all initiatives are not supported by meaningful transnational cooperation and capacity building. In the country, there is no tangible and functional capacity building activities provided to societies of the country to raise their awareness. Government institutions like University also less engaged in filling human resource gap related to subject of cyber space. As a result, there is failure to enforce the existing cyber crime related provision. So, successful cyber crime defense is unrealizable unless complemented with continues capacity building to close existing knowledge gap that emanate from newness of cyber crime in the country. Similarly, transnational cooperation also indispensable for regulation of cyber crime since cyber crime is cross border and no country is immune from the problem. But our country Ethiopia is reluctant and left behind in supporting its domestic unilateral effort by operational transnational cooperation to curb cyber crime. Therefore, achieving international cooperation and being a part of existing regional and international cyber crime convention is urgent home work of the country to regulate ever increasing cyber crime.

Finally in Ethiopia, enacted legal frame work related to cyber crime play double folds. Hence, in one way the law protects human right which is violated by cyber crime, but on the other hand it violates human right provided to people by international human right and domestic constitution like freedom of expression and privacy right. Therefore, ensuring compatibility between human right and cyber crime law as much as possible is the only existing alternative for democratic countries like Ethiopia in which freedom of expression is respected and protected.

[1] . ibid, pp.17

## Reference

Amayu Etana (2015). "Social media and journalist: journalist and media outlets use of social media network in Ethiopia". AA: AAU, MA thesis

Bjola, C. (2018). Diplomacy in Digital Age: oxford, Article

Halefom Hailu (2015). The state of cyber crime Governance in Ethiopia,Article

Iyasu Teketel (2018). "Cybercrime in Ethiopia: Lesson to be learned from international and Regional experiences". AA: AAU, MA thesis

Kettaman, C.Mathias (2017). Ensuring cyber security through international law:Publication of Asociacion Espanola de profesores de Derecho International y Relaciones Internationales .

Kinfe Micheal (2016). Some Remarks on Ethiopia's new cyber crime legislation, mizan law review, vol.10/2.

Kinfe Michael and Halefom Hailu(2015). The Internet and Regulatory Response in Ethiopia: Telecom, cyber crimes, privacy, E- commerce, and the new media, mizan law review, vol.9/1.

Pool, Ph.(2013). War of cyber world: The law of cyber warfare:Publication of American Bar Association.

Ethiopia: Computer crime proclamation, Article 19, (2016), available at:

https://www.article19.Org/data/files/medialibrary/38450/Ethiopia-Computer-Crime-Proclamation-Legal-Analysis-July-(1).pdf

Ethiopian Computer Crime Proclamation No.958/2016.

The first African forum on cyber crime hosted by African union commission at Addis Ababa, Ethiopia (16-18 October 2018), available at: https://www.coe.int>web>african