Global-Regulation of Cyberspace Security and the Ethiopian Context

Fikreselassie Getachew*

Abstract

Cyberspace has become an emerging target of invisible actors thereby calling for strict regulation of cyberspace a global agenda. Recently globe with embroiled with rising state-sponsored cyberattacks resulting in a diminishing trust and confidence among states. The vast and disruptive nature of cyberspace coupled with its anonymity creates a new and effective way for nations to pursue their national interest against their adversaries with great deniability and fewer consequences. Global effort toward regulating states' behavior within cyberspace is largely hampered by geopolitical tensions and disagreements between various countries. Despite continued global dialogues toward developing norms and new international laws capable of regulating state-sponsored cyberattacks, the world is still without a comprehensive and binding agreement that can restrain global peace and security threats. The article explores the ongoing global cybersecurity regulatory debates in line with its impact on Ethiopia's cybersecurity capability.

Keywords: Cyberspace, Cybersecurity, Cyberattack, Cybercrime, Cybernorms, State Actors, Critical Infrastructure

1. Introduction

With the ever-expanding technological advancement global cyber-threats have been increasing extensively in alarming rate. According to the World Economic Forum 2020 Global Risk Report, technology-related risks, specifically, cyberattack risk ranked 7th among the major catastrophes that could potentially endanger global peace and security in the coming 10 years.[1] Apart from the threat, cybercrime poses to the peace and security of the international community cyber-attacks have been causing adverse economic and social effects across the globe. Based on the Assessment of Cybersecurity Venture, the global damage arising out of cybercrime is expected to grow by 15 percent per year, thereby costing 10.5 trillion USD annually by 2025.[2]

*LL.B., LL.M.

[1] WORLD ECONOMIC FORUM, THE GLOBAL RISKS REPORT 2020 12, (15th ed. 2020).

[2] Steve Morgan, Cybercrime Magazine*, Cybercrime to Cost the World $10.5 Trillion Annually By 2025*, (Mar. 27, 2022, 09:30 AM), https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/).

Currently, a growing number of states are developing new policies and institutions for the political and military application of cyberspace.[3] We are witnessing phenomena whereby the number of ICT-related incidents involving nation-States is increasing both in number and sophistication.[4] Even though large-scale state-sponsored cyber-attacks are relatively a recent phenomenon, there are accounts of major state-sponsored cyberattacks that undermine trust between governments. Considering cyberattacks can originate in any part of the world, it is difficult for any single nation to adequately deal with cyberattacks, highlighting the need for an urgent and comprehensive international response. To this end, numerous states and international organizations embarked on making multifaced efforts to reduce the risks associated with the malicious use of ICT. Despite the efforts and ongoing dialogue, the world is yet to come up with a comprehensive agreement regarding the means and methods of regulating cyberspace. There are still unresolved questions at the global level regarding how the existing international law should be shaped and regulate responsible States' behavior within the cyber realm.[5]

Currently, only a handful of States (mostly European and the USA) have begun to express their position on the issue while the vast majority of nations including Ethiopia remain silent and inactive in the process.[6] Nations with strong cyberspace infrastructure and. Knowhow have started launching different initiatives that can potentially influence other nations toward setting new norms and rules in the field of cyberspace. Consequently, States weak and vulnerable infrastructure are facing an ultimatum in siding with stronger nations without properly scrutinizing the issue on their terms.

The extent of cybersecurity issue and continues threat that Ethiopia has been defending has increased in alarming rate. According to the 2020/2021 fiscal year national cybersecurity report, Ethiopia has encountered 2,800 reported cyberattack attempts targeting several institutions and key infrastructures.[7]The number of attacks recorded this year is more than double what has been

[3] Vladimir Radunović, *Cybersecurity and International Peace and Security*, https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Summary-International-Peace-and-Security.pdf. (Aug. 19, 2021, 11:15 PM).

[4] UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, THE UNITED NATIONS, CYBERSPACE AND INTERNATIONAL PEACE AND SECURITY: RESPONDING TO COMPLEXITY IN THE 21ST CENTURY 9 (2017).

[5] Duncan B. Hollis, *A Brief Primer on International Law and Cyberspace,* (Aug. 4, 2021, 10:08 PM), https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763. Same as above

[6] See *Id*.

[7] *Id.*

recorded in the previous 2019/2020 fiscal year (1080) showing the extent of the cyber incident growth in the country. According to Ethio-CERT,[2] the law enforcement operation that is being held in the northern part of the country, the second filling of the GERD, as well as the sixth national election were all responsible for the increasing number of cyber-attacks during the fiscal year.[8]

In the current northern Ethiopia conflict between the federal government and Tigray forces, cyberspace is being actively used by domestic and international actors to influence the outcome of the war. The apparent disinformation and misinformation campaign against the country through social media is hurting the social development and stability of the country as well as the psychology of its citizens. In line with the current information warfare, social media accounts of major Ethiopian institutions like Ethiopian Broadcasting Corporation and Ethiopian Airlines were recently hacked as part of this coordinated campaign. In this Hybrid type of warfare against Ethiopia, informational warfare tools are being deployed together with another wide array of powerful diplomatic, political, economic, and military tools by internal and external forces to weaken Ethiopia's national unity, security, and global influence.[9] Recently misinformation, fake news, and hate speech deployed within cyberspace coupled with willful and deliberate misinformation campaigns of western-backed mainstream media are becoming an existential threat to the country. Hence, the impact of information-based cyber warfare is becoming a well-anticipated and recognized threat to Ethiopia that needs to be addressed through a coordinated effort of multiple stakeholders.

Apart from the current disinformation campaign, another emerging challenge within cyberspace is those targeting the country's critical infrastructures. According to the head of Ethio-CERT,[2] one of the most prominent and persistent groups targeting Ethiopian cyberspace is hacker groups who call themselves the "Cyber Horus Group."[10] The group, supposedly affiliated with the Government of Egypt, was responsible for the attack on 37, 000 computers and government-associated websites between June 17-and 20, 2020.[11] These attacks ware coincided with the second filling of GRED

[8] Seblewoyne, *supra* note 68

[9] Interview with Hannibal Lemma, Division Head, Cyber Governance and Management Division, Information Network Security Agency (Jan 4, 2022).

[10] Seblewoyne, *supra* note 68.

[11] Addis Zeybe, '*Cyber Horus' hacking group mounts cyberattack on 37,000 computers in connection with Grand Ethiopian Renaissance Dam,* (Jan.9, 2020, 1:45PM), https://addiszeybe.com/featured/currentaffairs/technology/cyber-horus-hacking-group-mounts-cyberattack-on-37-000-computers-in-connection-with-grand-ethiopian-renaissance-dam.

and the escalating tension between Ethiopia and Egypt. The ultimate aim of the attack was to create confusion around the filling and operation of the dam and to put pressure on Ethiopia over its dispute with Egypt. During this attack, the hacking group attempted to attack several public service institutions, and private companies including some security agencies' websites, and try to disrupt the operation of certain critical infrastructures.[12]

Even though there is a lack of concrete evidence that links the hacker group with Egypt, the timing and the motives of the attacks coupled with pharaonic-themed nationalistic messages left by the hacker group raised suspicion as to who could be behind these attacks. The plausible deniability that is inherent to the anonymity of cyberspace crate makes it difficult to ascertain a cyber-attack by a particular threat actor. However, if proper cybersecurity measures are not taken, this sort of cyber-attack demonstrates the magnitude of the challenge that cyberspace poses in the future by providing fertile ground for different state and non-state actors. This goes to show how the cyber domain is being exploited by domestic as well as international adversaries to pursue their political and military agenda against Ethiopia.

Despite these national security threats Ethiopia's cybersecurity capability is still facing different challenges. Recent audits and evaluations conducted in 2020 among 61 institutions demonstrate that a lack of cybersecurity awareness; limited priority afforded to cybersecurity; absence of cybersecurity management and administration procedure; lack of cybersecurity technology; and lack of cybersecurity regulatory frameworks account for most of the cybersecurity vulnerability in Ethiopia.[13] Even if the cyber incidents that are being reported are increasing substantially, most of these incidents targeting Ethiopia were averted before causing significant harm to the country.[14] However, considering most critical infrastructures of the country and essential government services are recently starting to deploy and integrate ICT services, the impact of cybersecurity vulnerability would be a significant threat to national security.[15]

This article examines the ongoing global cybersecurity regulatory debate and its implication for Ethiopia's future cybersecurity capability by applying the traditional doctrinal research

[12] See *Id.*

[13] Cybersecurity Audit Report, Information Network security Agency /unpublished/2020.

[14] Seblewoyne, *supra* note 68.

[15] Hannibal, *supra* note 73.

methodology. The article briefly explores the current cybersecurity measures and global cooperative efforts made by the Ethiopian government together with their challenges.

2. Cyberspace and State-Sponsored Cyberattacks

The fourth Industrial revolution has introduced fast processing and large-scale machine-to-machine communication stirring up major social, political, cultural, and economic changes.[16] These large-scale communication capabilities together with higher computing power prompted the creation of a more connected, complex, and strange new domain called Cyberspace. More recently, cyberspace is being considered the fifth operational human domain being added to the four well-established domains like land, sea, air, and space.[17] Even if there are several meanings attributed to the word cyberspace,[18] it is widely understood as an abstract world or alternative environment enabled by the internet and computer.[19]

One of the unique characteristics of Cyberspace is that it does not have a physical or geographical border as it exists and plays a major role in all of the other existing domains.[20]Unalike natural areas (air, sea, land, and space) cyberspace is not- territorial,[21] it is an omnipresent domain available to anyone in the globe where the internet is accessible. Because of this, cyberspace provides an opportunity for any individuals or groups with the necessary skill-set to execute cyberattacks in any dimension anonymously with limited or no risk of being caught. This character of cyberspace makes it difficult to attribute a certain malicious cyber incident or attack to a specific individual, organization, or state making the new domain a threat to national and international peace and security.

Cyberspace provides giant neighborhoods as well as the world's largest battlefield. It affects the operation of governments, the military, small businesses, corporations as well as the lives of almost every individual on the planet. As long as the internet exists and people continue to use computing

[16] CHRISTINA BOGUSZEWICZ and et. Al, THE FORTH INDUSTRIAL REVOLUTION AND CYBERSPACE'S MENTAL HEALTH STIGMA 2 (2020).

[17] Dan Efrony, *The Cyber Domain, Cyber Security and what about the international law?* (Aug. 20, 2021, 12:09 AM) https://csrcl.huji.ac.il/sites/default/files/csrcl/files/dan_efrony.pdf.

[18] Lance Strate, *Cyberspace: The Varieties of Cyberspace: problems in definition and delimitation,*63(3) W.J. Co 383 (2009).

[19] Riza Azmi and Kautsarina, *Revisiting Cyber Definition*, (Aug. 20, 2021, 2:27 PM) https://www.researchgate.net/publication/334989724_Revisiting_Cyber_Definition/link/5d5a18ca299bf151badeb164/download.

[20] Dan, *supra* note 8.

[21] Lino Santos, *Cyberspace regulation: Cesurists and Traditionalists*, 6(1) E.jo.Int. Re. 88 (2015).

devices in their personal and professional capacity there will be an underline concern originating from cyber threats and cyber-attacks. In the current technological landscape having entirely secure software from errors and bugs is impractical, making software flaws the underlying factor for most cybersecurity breaches. Cyber-attacks can occur whenever a threat actor identifies, analyzes, and exploit these software vulnerabilities for his/her benefit. Even though different descriptions can be attributed to cyberattacks, they are an attack initiated from a computer against a website, computer system, or computer that compromise the confidentiality, integrity, or availability of the computer or information stored on it.[22] Cyberspace facilitates an effective way of conducting many human conducts including crime. With sufficient know-how cybercrimes are easy to commit and hard to detect as compared to traditional crime,[23] thereby making cybercrimes a more dangerous and contemporary threat to global communities. Cybercrime has been adversely impacting the economy, social values, cohesion, and democratic assets.

The complex nature of cyberattacks attributed to their limitless realm of existence makes cyberspace an emerging global threat. This nature of cyberattacks coupled with its anonymity creates a new and effective opportunity for states to pursue their national interest agendas against their rivals with great deniability and fewer consequences. Even though technology influenced the outcome of conventional warfare since the first computer systems came into the picture, the utilization of cyber warfare as an alternative is a relatively new phenomenon. The introduction of weapons of mass destruction /WMD/ makes direct military confrontation between countries with WMD capability obsolete. As a result, developed States are actively working toward enhancing their technological capabilities to engage in cyber warfare to continue advancing their political, economic, and military interests without resorting to conventional warfare.

In light of these developments, global communities have been witnessing large-scale state-sponsored cyberattacks, that have the potential to cause significant and wide-ranging harm across several critical assists.[24] The most prominent and alarming state-sponsored cyber sabotage or

[22] Vince Farhat & ET AL, *Cyber Attacks: Prevention and Proactive Responses,* (Aug. 21, 2021, 3:36 AM) https://www.academia.edu/3785382/Cyber_attacks_preventative_proactive_responses.

[23] Vijaykumar S. Chowbe, *The Concept of Cyber-Crime: Nature & Scope,* (Aug. 21, 2021, 11:06 AM) http://ssrn.com/abstract=1766238.

[24] Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376 (2018).

disruption are cyberattacks targeting other states' critical infrastructure.[25] Critical infrastructures (CI) are the physical and non-physical resources and services that are fundamental to the minimum functioning of a society.[26] The infrastructures are crucial in ensuring public welfare, economic stability, law enforcement, and defense operations.[27] The extensive integration of ICT into CI increases CI's vulnerability and makes them a target of malicious attacks via cyberspace.[28] Hence, any attack campaign targeting CI can have a significant impact on the national security of any nation, contributing to diminishing trust and confidence among states.

Currently, some state-sponsored major cyberattacks on critical infrastructure which resulted in global tension and outcry. Estonia was the first country in the world to face a coordinated cyber-attack against its critical infrastructures. Following Estonian government decisions to reallocate soviet era war memorial, in May 2007 Estonian government networks were heavily harassed by Distributed Denial of Service /DDoS/ attack by foreign intruders (allegedly attackers associated with the Russian Government).[29] Over three weeks, Estonia's government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses were all crippled by unprecedented levels of internet traffic.[30]In an event widely regarded as the first major act of cyber warfare in the world, Estonia lost productivity, opportunity cost, remediation, and the acquisition of alternative web hosting at emergency rates estimated to be in the billions of Euros.[31]

The dialogue of cyber warfare resurfaces again in 2010 when researchers discovered Stuxnet, a resilient computer worm that damages the nuclear centrifuges in Iran.[32] Stuxnet forced the control systems of the Iranian nuclear centrifuges to spin out of control while preserving the appearance of proper function for the controllers.[33] The actor behind Stuxnet has not been identified officially.

[25] Vijaykumar, *supra* note 14.

[26] Viganò, Eleonora & ET AL, *Cybersecurity of Critical Infrastructure, in* THE ETHICS OF CYBERSECURITY 157, 158. (Markus Christen et al. eds., 2019).

[27] See *Id*.

[28] *Id*.

[29] Center For Strategic and International Studies, *Significant Cyber Incidents Since 2006,* (Aug. 24, 2021, 12:38 AM), https://csis-website-prod.s3.amazonaws.com/s3fs-public/210804_Significant_Cyber_Events.pdf? bzKYK94rq5 _ 3lrbYVK4fcL0rmkNq6lNI. See also Ministry of Defense Cyber Security Strategy Committee, Estonia Tallinn 2008 EE_NCSS_2008_en.pdf (last accessed July 23, 2022).

[30] Andreas Schmidt, *The Estonian Cyberattacks*, *in* THE FIERCE DOMAIN –CONFLICTS IN CYBERSPACE 1986-2012 52, 52 (Jason Healey ed.,2013).

[31] *Id.* at 53.

[32] JAY P. KESAN AND HAYES CAROL M. HAYES, CYBERSECURITY AND PRIVACY LAW IN A NUTSHELL 2 (2019).

[33] See *id.*

However, depending on the code size, complexity, and development efforts behind this lethal weapon, many sources strongly believe it to be a joint effort by the United States of America and Israel.[34] Stuxnet is considered to be the first well-known demonstration of the cyber attacker's ability to harm physical infrastructure.[35] Apart from attacks targeted toward critical infrastructures States meddling in the internal affairs of opponent States is becoming a new global security agenda. This form of intervention was witnessed when Russia allegedly set out to interfere with the 2016 US election. Throughout the election wide range of politically damaging information on the internet was released on social media platforms that can influence the outcome of the election. The US considers this meddling in the 2016 election as an attack on its national interest and its democratic values, making the country respond with hefty diplomatic and economic sanctions.

Currently, these international cyber incidents are not slowing down, as can be inferred from the recently deteriorating US-China relation in cyberspace.[36] Unfortunately, the difficulty of identifying cyber attackers and their motivations in cyberspace resulted in the Nations States classifying all serious cyberattacks as cyberwar.[37] This imminent cyber threat and agitations fuel a cyberwar arms race, resulting in more instability and less security around the world.[38] Hence, with increased cyberwarfare capabilities around the world, no single country is safe from cyber-attacks.

3. International Law and Cybersecurity

In recent years, the idea of global cyberspace governance as an operational domain has been gathering momentum from various state and industry actors. The complexity of cyberspace opens up a bunch of new and difficult legal issues like whether existing bodies of international law apply to cyberspace or not. In the current context, this open question surrounding the application of international law to cyberspace is entangled with disagreement among major geopolitical rivals. The geopolitical rivalry between the US and its allies on one hand and Russia and their allies emanate from their domestic policy toward regulating and utilizing cyberspace. The west advocate

[34] Siddharth P. Rao, *Stuxnet - A new Cyberwar weapon,* (Aug. 24, 2021, 2:18 AM), https://www.researchgate.net/ publication /267156195_Stuxnet_A_new_Cyberwar_weapon_Analysis_from_a_technical_point_of_view.

[35] See *id.*at 3.

[36] Ariel (Eli) Levite and Lyu Jinghua, *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?* (Mar. 27, 2021, 03:10 PM), https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213

[37] Bruce Schneier, *Cyberconflicts and National Security,* https://www.un.org/en/ chronicle/article/ cyberconflicts-and-national-security. (Accessed Aug. 24, 2021, 9:54 AM)

[38] *Id.*

cyberspace to be a domain that is an open, interoperable, secure medium that preserves the free flow of information globally.[39] The west is resistant to the enactment of a new international law that in any way control/censors the contents of cyberspace.

Contrary to the West's assertion, the group led by Russia and China promotes more controlled and regulated cyberspace whereby state sovereignty is well respected[40] and advocates for the creation of stricter rules of responsible state behavior in the cyberspace. To this end, Russia for the first time proposed a draft UN resolution in 1998 to establish a new and binding international law dealing with cybersecurity.[41] Russia and a handful of other states also submitted a proposal for a voluntary International Code of Conduct for Information Security in 2011 to re-affirm their long-standing position.[42] On the contrary, the western states categorically reject the idea of a new international legal framework regulating cyberspace and advocate for the development of norms as to how the existing international laws can be applied to cyberspace. Accordingly, international legal experts primarily from the Western Hemisphere developed the Tallinn Manual to serve as an international standard that can bring some degree of clarity to the complex legal issues surrounding the application of international law for cyberspace.[43] These Manuals address many international laws issue related to state cyber operations including general international law as well as specialized international law regimes like human rights, diplomatic laws, the law of the sea, air law, space law, and more.[44]

Nowadays, the issues of cyberspace regulation has become the agenda of the globe.[45] The regulation of information security /cyberspace security/ has been a hot discourse of the UN since 1998 after the Russian Federation had introduced a draft resolution on the subject in the First Committee of the UN General Assembly.[46] The request at the time was based on the assertion of the Russian government that new technologies could be used for purposes that are not compatible

[39] Elaine Korzak, Russia's Cyber Policy Efforts in the United Nation, 11 Tallinn Paper, 4, 20 (2021).

[40] See *id.*

[41] *Id* at 5.

[42] *Id* at 7.

[43] Eric Talbot, *The Tallinn Manual 2.0: Highlights and Insights,* 48 Geo. Jo. Int. Law 738, 736 (2017).

[44] See *id.*

[45] Ma Xinmin, *Key Issues and Future Development of International Cyberspace Law,* 2(1) Ch.Q.Int.St.S., 119, 120 (2016).

[46] United Nation, *Developments in the field of information and telecommunications in the context of international security*, (Aug. 25, 2021, 8:43 PM), https://www.un.org/disarmament/ict-security/.

with the objectives of international peace and security. This Russian initiative contributed to situating Nation-States cyber conduct as a global security issue for the first time. This Russian proposal on the issue of technology and its implications for global security face strong opposition mostly from western nations led by the US. However, it has gained enough support among other UN members to be included on the UN global security agenda.

Since the first Russian initiative, efforts of formulating international law for global cyberspace security have already been continuously proposed and contested by different international actors. Currently, global legislative development concerning cyberspace is largely influenced by different specialized institutions under the UN, regional actors, specialized international organizations, and governments and stakeholders from different states.[47]

3.1. UN Based Efforts Towards Global Cyberspace Security

Since the last two decades, the UN General Assembly (UN GA) has been pushing for a global dialogue to draw a line between responsible and irresponsible state behavior toward cyberspace. While noting the potential use of ICT for malicious purposes, Cybersecurity has become the agenda for the UN GA for the first time in 1998. Through Resolution 53/70 the UN GA decided to include development in the field of information and telecommunication in the context of international security.[48] After having several backs and forth forward and debates between the Western states and the Russian Federation, Russia's proposal for the establishment of a Group of Governmental Experts (GGE) to study the matter was endorsed.[49]

In 2003 through Resolution 58/32 The GA requested the Secretary-General (SG) to conduct a study on relevant international concepts aimed at strengthening the security of the global information telecommunication system with the assistance of a GGE to be established in 2004.[50] This Resolution triggered the establishment of the first GGE to examine the impact of technology on international peace and security.[51]Since then UN GA has adopted several Resolutions to convene five other GGEs and one Open-Ended Working Group (OEWG) to further develop norms that can

[47] Abid A. Adonis, *International Law on Cyber Security in the Age of Digital Sovereignty* (Aug. 27, 2021, 06:20 PM), https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/

[48] U.N. GA, 53th Sess., 79th plen. mtg. at 2, U.N. Doc. A/RES/53/70, (Dec. 4,1998).

[49] UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, *supra* note 4, at 15.

[50] U.N. GA, 58th Sess., 71th plen. mtg. at 2, U.N. Doc. A/RES/58/32, (Dec. 8,2003).

[51] Digwatch, *UN GGE and OEWG*, (Aug. 27, 2021, 2:58 AM), https://dig.watch/processes/un-gge.

help assure international cyber stability. These groups were created to discuss different key issues under the areas of information security identified by the General Assembly and the Secretary-General of the UN. These key issues include existing and emerging threats; norms, rules, and principles of responsible behavior of states; confidence-building measures; international cooperation and assistance in ICT security and capacity building, how international law applies to the use of ICTs, conclusions, and recommendations for future work.[52]

3.2. The Group of Governmental Experts

The first GGE was established in 2004 following the term of resolution 58/32 composed of experts from 15 states.[53]Taking into its mandate and the various reports submitted from the Member States, the Group had a comprehensive and in-depth exchange of views among its members on the field of cybersecurity.[54] However, the Group failed to reach consensus in the preparation of the final reports due to geopolitical tension between Russia and the USA. Considering the Group operates based on consensus the dissent of the US and its allies from the final report was enough to prevent the report from being issued. The second GGE was established in 2009 to continue studying the existing and potential threats in information security and possible cooperative measures to be taken. Unlike the first GGE, the second Group produced the first consensus report after a comprehensive exchange of views. The group identified threats, risks, and vulnerabilities associated with ICT and suggested confidence-building steps to be taken to mitigate the risk associated with cyberspace.[55] Even though the Group delivered a consensus report it failed to deliver on one of the tasks it set out to do concerning how international law applies to the use of ICT.

Building upon the 2010 report of the second GGE, the third GGE produced the second consensus report.[56] This was considered as one of the most successful Groups establishing the relevance of international law to cyberspace.[57] The report reflects the Group's finding that international law, in particular the United Nations Charter, is "essential in […] promoting an open, secure, peaceful, and

[52] Katherine W. Getao, *The Value of International Cooperation in Cyberspace; Lessons from the UNGGE Processes,* (Aug. 28, 2021, 5:51 PM), https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-03.pres_ungge_lessons_for_africa_katherine_g_.pdf.

[53] U.N. GA, 60th Sess., at 2, U.N. Doc. A/60/202 (Aug. 5,2005).

[54] See *id.*

[55] U.N. GA, 65th Sess., at 6, U.N. Doc. A/60/202 (July. 30,2010).

[56] U.N. GA, 68th Sess., U.N. Doc. A/68/98, at 6 (Jun. 13,2013).

[57] Katherine, *supra* note 43.

accessible ICT environment."[58] Similar to the third Group, the fourth GGE produced the third consensus report reaffirming the 2013 third GGE stand that international law in particular the UN Charter, applies to states' use of ICT[59]. In addition to reaffirming this stand, the 4th Group further considered how international law applies to the use of ICTs by states. However, the most important milestone achieved by this Group was the adoption of 11 voluntary, non-binding norms for responsible states' behavior. [60]These norms guide nations to: [61]

- cooperate toward increasing the stability and security in the use of ICT and preventing harmful ICT practices;
- consider all relevant information in case of ICT incidents;
- not knowingly allow their territory to be used for internationally harmful ICT acts**;**
- consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICT;
- ensure the secure use of ICTs, to guarantee full respect for human rights, including the right to freedom of expression;
- not conduct or knowingly support ICT activity; that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure;
- take appropriate measures to protect their critical infrastructure from ICT threats;
- respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts;
- take reasonable steps to ensure the integrity of the supply chain, so end users can have confidence in the security of ICT products;
- encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities;
- not conduct or knowingly support activity to harm the information systems of another State's authorized Computer Emergency Response Team (CERT).

[58] U.N. GA., *supra* note 47.

[59] U.N. GA, 70th Sess., at 12, U.N. Doc. A/70/174 (July. 22,2015).

[60] See *id*. at 7and 8.

[61] UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, *supra* note 4, at 19.

The fifth Group was established by GA Resolution 70/243 with 25 experts to continue to study similar issues that have been specified in the GGEs.[62] However, during the discussion, of the Group significant differences in position and interest between states emerged regarding the means of applying the rules of international law to states' use of ICT.[63] Because of these differences, the Group failed to deliver a consensus report. The 6th GGE was established by GA Resolution 73/266. It successfully produced the 4th consensus report to the GA. The 2021 GGE, despite the occurrence of exceptionally high tensions between key players due to hostile cyber operations targeting GGE members, achieved consensus.[64] One of the major achievements of the Group was building up the eleven voluntary, non-binding norms developed by the fourth GGE report, and developing an additional layer of understanding of these norms.[65] The report underscored the value of these 11 norms and further developed their substantive contents by adding commentary on their meaning as well as the kind of institutional arrangements. [66]The other important milestone achieved by this Group was the acknowledgment that international humanitarian law (IHL) applies to cyber operations during an armed conflict.[67]

3.3. The Open-Ended Working Group

The UN GA through Resolution 73/27 established an Open-Ended Working Group (OEWG) in which all Member States are invited to participate. This group was created based on a Russian proposal to find a new way of re-engaging in the global information security negotiation that will avoid the group agreements created by the UN GGE.[68] Nonetheless, at the time, many delegations expressed their frustration with the creation of UN OEWG for discussion, which they considered as having a similar mandate to the UN GGE.[69] Unlike the GGE in which only a limited number of states participate, the OEWG was established to create more democratic, inclusive, and transparent

[62] U.N. GA., 70th Sess., 82nd plen. mtg. at 3, U.N. Doc. A/RES/70/237, (Dec. 23,2015).
[63] UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, *supra* note 4, at 19.
[64] Michael Schmitt, The Sixth United Nations GGE and International Law in Cyberspace, (Aug. 28, 2021, 6:15 PM), https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.
[65] U.N. GA, 76th Sess., at 8, U.N. Doc. A/76/135 (July. 22,2015).
[66] See *id.*
[67] See *id.* at 18.
[68] A surprising turn of events: UN creates two working groups on cyberspace, (Jan. 1, 2022, 3:15 PM), https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/
[69] See *id.*

groups that work on a consensus basis.[70]Accordingly, it opens the door for all states to participate express their views, and extend cooperation on cybersecurity.

The group was tasked to further develop the rules, norms, and principles of responsible behavior in the field of information and telecommunication in the context of international security. The Group was also allowed to hold consultative meetings with interested parties (business, non-governmental organizations, and academia). Following its mandate, the OEWG discussed the existing and potential threats in cyberspace and possible cooperative measures to address them and produce its report in March 2021.[71] The Group's Report is built on a framework already established in the previous GGE reports. Aside from further elaborating and commenting on these issues, the most important achievement of the OEWG was the engagement of a large number of UN members and other non-governmental actors who were ready to collaborate and contribute to the global cybersecurity agenda.

4. Ethiopian Cybersecurity Landscape

Since the last decade, Ethiopia has been working to place ICT within the wider context of its socio-economy development agenda and reap the potential benefit it has in terms of sustaining development. The Ethiopian government for the first time recognizes ICT as one of its strategic priorities with the adoption of the National ICT Policy in 2011.[72] This policy document demonstrates the government's commitment to developing ICT both as an enabler of socio-economic development as well as an industry on its own. The policy lays down the road map for transforming the country from a subsistence agricultural-based economy to a knowledge and information-based economy.

Since the approval of the first National ICT Policy, the government of Ethiopia has made several attempts to promote ICT as one of its strategic priorities in its national development plans. These government endeavor has been manifested in the adoption of the first and second Growth and Transformation Plan (GTP) and the 2016 updated national ICT policy. Currently, consistent with the 2019 Home Grown Economic Reform Agenda, the Government is implementing the 10-year

[70] U.N. GA., 73th Sess., 45th plen., at 5, U.N. Doc. A/RES/73/27, (December 5,2018).

[71] U.N. GA., at 2, Doc. A/AC.290/2021/CRP.2, (March 10 2021)

[72] FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA, THE NATIONAL INFORMATION AND TECHNOLOGY POLICY AND STRATEGY 1 (2011).

development plan and the Digital Ethiopia 2025 digital strategy to further embrace technology across all core development sectors to build a digital economy. To this end, the Ethiopian government recently has made several changes including its longstanding policy of opening up the telecommunications sector for the private sector to lay the foundation for future digital transformation. All advances and initiatives launched in the past couple of years toward mainstreaming digital technologies into the broad national development context resulted in the expansion of ICT infrastructure and access to technology across the country.

According to the Ethio Telecom 2021/2022 fiscal year first-half business performance report (as of 31st December 2021), its total subscribers reached 60.8 million.[73] Meanwhile, Ethio Telecom is currently running several projects on infrastructure and system capacity expansions to boost network coverage capacity and quality of services.[74] Similarly, the same report indicates exponential growth in mobile subscribers accounted for 96.5% of the overall subscription. In the same period fixed broadband access surged to 443,000 from 347,000 in just six month period, while a total of 23.8 million 'Data and Internet' users at the end of the reporting period.[75] This report indicates a fourfold increase in subscriptions from the 2010/2011 fiscal year.[76] Even though it is still underdeveloped as compared to other developing countries, the expansion of ICT infrastructure and the ever-growing access to technology in Ethiopia has profound implications for development as well as a new form of cyber threats.

4.1. National Cybersecurity Challenges

Ever since the country has centered ICT into its wider socio-economic development context the country has increasingly become dependent on the vast and global cyberspace domain. Accordingly, as reliant of computer technology, Ethiopia has been facing the security challenges that strung along with being part of cyberspace. Simply put, due to the ever-increasing dependency and accessibility of technology we are witnessing an increasing number of cyber-attacks that are becoming a challenge to the socio-economic development and stability of the country. Cyberspace

[73] Ethio telecom 2014 EFY (2021/22) First Half Business Performance Summary Report, (Apr. 16, 2022, 04:21 AM) https://www.ethiotelecom.et/የኢትዮ-ቴሌኮም-የ2014-በጀት-ዓመት-የመጀመሪያ/

[74] See *id.*

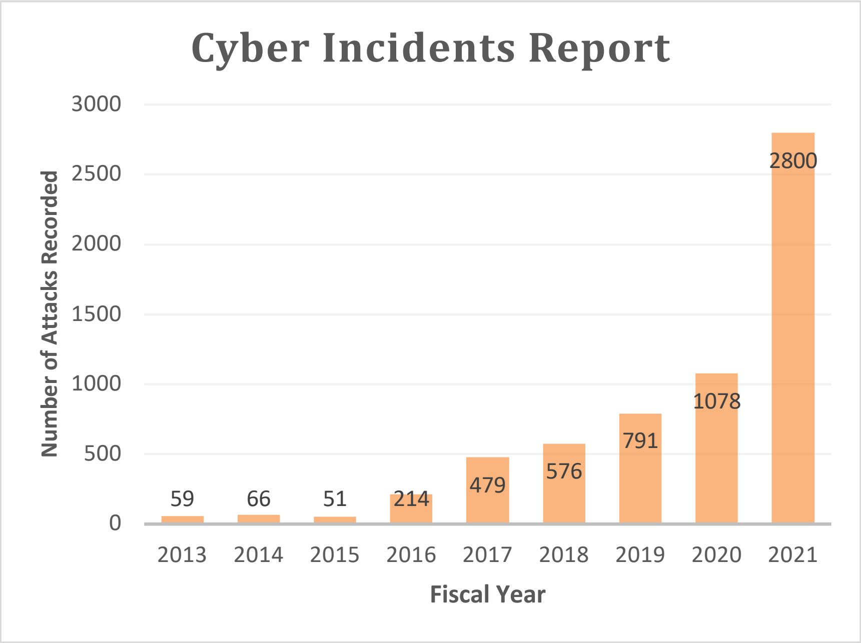
[75] See *id*

[76] Comms Update*, Ethio Telecom reveals financial results, subscriber data for most recent financial year*, (Nov. 25, 2021, 10:44) https://www.commsupdate.com/articles/2011/09/15/ethio-telecom-reveals-financial-results-subscriber-data-for-most-recent-financial-year/.

has been actively exploited recently by different extremists, terrorists, criminal groups as well as nation-states to advance their interests against the country, making it a new source of national security threat.

Even though the number of cyber-attacks is still relatively low as compared to other developing countries,[77]reports coming out of the Information Network Security Agency /INSA/ indicate these numbers are exponentially increasing in recent years. Ever since INSA start reporting Ethiopia's annual cyber security incident in 2013, evidence suggests an increasing number of cyber-attacks are targeted toward Ethiopia.[78] Accordingly, the 59 /fifty-nine/ cyber-attacks registered in 2013 have increased more than 47-fold to 2800 (one thousand seventy-eight) cyber incidents in 2021.

Figure 1. **INSA Cyber Incidents Report (between 2013 and 2021)**



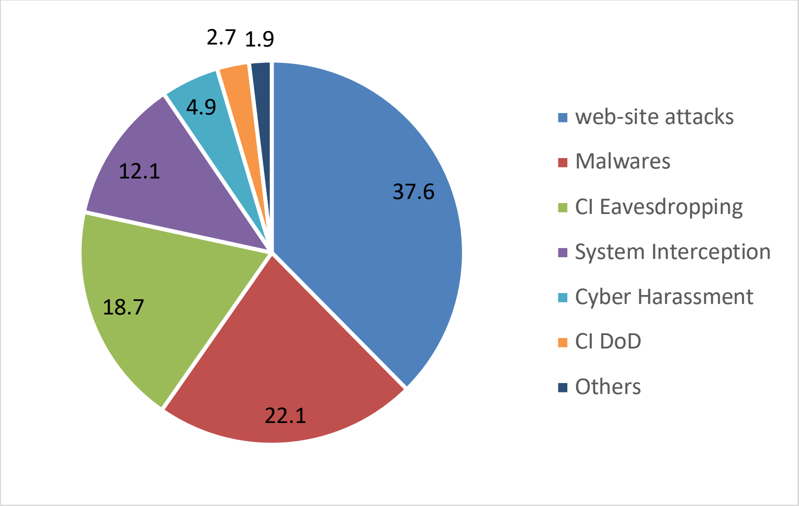
During these periods different types of cyber-attacks were targeted toward Ethiopia. For instance, the distribution of cyber-attacks that were attempted in the year 2020, including harmful malware,

[77] Interview with Seblewoyne Assefa, Head of Ethiopian Computer Emergency Readiness and Response Team, Information Network Security Agency, (Jan 5, 2021),

[78] ኢንሳይት, ኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ, ልዩ ዕትም ህዳር 2013, ገፅ 35.

website attacks, Interception, critical infrastructure eavesdropping, critical infrastructure denial of service, and cyber fraud were the most prominent ones.[79]

Figure. 2: **2020 Fiscal Year Cyber Incident Distribution Report**



4.2. Cybersecurity Measures in Ethiopia

In the past two decades, Ethiopia has been exploiting the opportunity and facing the security challenges that are parallel to the ever-growing ICT infrastructure.[80] Accordingly, cyber threats and attacks are increasingly becoming an additional challenge for the socio-economic development of the country. The report of the Ethiopian Cyber Emergency Readiness and Respond Team indicates the frequency and type of cyber-attack targeting Ethiopia have increased in recent times.[81] Accordingly, this emerging cybersecurity threat across the country is attracting the attention of the government. To prevent the challenges posed by cyber threats toward the socio-economic development aspiration of the nation as well as national security, in the past decade, the Ethiopian government has taken different policy, legal and institutional measures.

4.2.1. Policy Measures

For long Ethiopia did not have a functional cyber security policy at the national that can protect its people, economy, critical infrastructure, and essential public services against cyberattacks and

[79] Information Network Security Agency, *Fiscal year report 2020/2021*, /unpublished/, 2021.

[80] Information Network Security Agency, The National Cyber Security Policy and Strategy 1 (2021)/ Draft /unpublished/.

[81] Seblewoyne, *supra* note 68.

associated risks. Even if there were different prior efforts from various actors to incorporate the issue of cybersecurity into the national agenda, it is only in 2011, that Ethiopia had its first coherent and comprehensive cybersecurity policy with the adoption of the National Information Security Policy /NISP/. The primary mission of the Information Security Policy was to create and sustain a secure, safe, and resilient information environment [cyberspace] to enable the country to use information and information infrastructure for the implementation of peace, democratization, and development programs. [82] To satisfy this mission and ensure the confidentiality, integrity, availability, and authenticity of the national information assets, the policy outlined the promotion and strengthening of international cooperation as one of its six strategic pillars. [83]

The National policy emphasizes the need to develop national cybersecurity capabilities to prevent information security threats, information warfare, and cyber terrorism through the promotion and strengthening of regional and international cooperation and coordination. The policy also reiterates the need for global collaboration on technical and legal matters to curb national, regional, and international cybercrimes, organized crimes, cyberterrorism, and other information security threats.[84] Accordingly, the policy affirms the Ethiopian government's commitment to work with nations and international organizations to ensure the integrity of the global information network through raising awareness, increasing information sharing, promoting security standards, investigating and prosecuting information security threats, and facilitating foreign investment in the sector.[85]

To resolve the jurisdictional issues emanating from the borderless nature of cybersecurity and to promote global efforts and best practices, the National Information Security Policy outlines different implementing strategies. Ensuring the harmonization of all national information security policies, laws, and regulations to international laws, standards and best practices is one of the strategies adopted by the policy to complement the national cybersecurity effort. The other strategy endorsed through the policy toward promoting international cooperation is the adoption and ratification of regional and international cooperative agreements on information security issues

[82] See *id.* at 4
[83] See *id.* at 5
[84] See *id.* at 14
[85] See *id*. at 14

based on their merits.[86] The policy also further advocates for the country to actively participate in all relevant international cybersecurity bodies, panels, forums, conferences, and multi-national agencies to promote cybersecurity.

Currently, the National Information Security Policy is being modified by INSA to make it compatible with existing international treads and to address the current complex challenges facing cyberspace.[87] Prior research conducted to assess the existing information security policy indicates the policy was not successful in achieving its intended objectives and goals due to a lack of substantive content, scientific perspective, inconsistency with other national policies, and detachment of its strategic pillars and implementation tools.[88]

4.2.2. Legal Measures

In Ethiopia, the regulation of cybersecurity through legislation is a relatively recent phenomenon that came in to picture in parallel with the advancement of ICT. For a long period, there was a lack of appropriate and enforceable substantive and procedural laws that can help Ethiopia adequately deal with cybercrimes and cybersecurity challenges. The delay in the proliferation of the internet witnessed in the country has played its role in delaying legislative measures within cyberspace.[89] The first attempt to regulate cybercrime was made in 2004 with the enactment of the Criminal Code of Ethiopia. In its preamble, the criminal code asserts the failure of the 1957 Penal Code in terms of properly addressing crimes born of advances in technology, and the complexities of modern life as one of the reasons for the revision of the penal code.[90] To this end, the existing Criminal code for the first time incorporates new types of crimes including Computer crimes.

Under Section II of Crimes Against Rights in Property title, the Criminal Code regulates a handful of computer crimes. Within its provisions, the Criminal Code provides substantive provisions outlawing illegal access to a computer, computer system, and computer network; causing damage

[86] See *id.* at 14

[87] የኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ, የሳይበር ደህንነት ፖሊሲ እና ስትራቴጂ ማብራሪያ ሰነድ, ገፅ 7 2013, (21, 2021, 9:30 AM) https://www.insa.gov.et/documents/20124/0/National+Cyber+security+Policy%26+StrategyFDRE.docx/03b2d42e-5cb3-f29e-f8f8-fe4ad3d94586?t=1639143692057&download=true

[88] See *id.* at 7-11.

[89] Kinfe Micheal Yilma and Halefom Hailu Abraha, *The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media*, 9(1) MIZAN LAW REVIEW 108-153 (2015).

[90] The Criminal Code of the Federal Democratic Republic of Ethiopia 2004, Proclamation No.414/2004.

to computer data, and disrupting the use of a computer.[91] To this end, the Criminal Code provides different punishments for the perpetrators of these crimes ranging from simple fines up to rigorous imprisonment not exceeding five years.[92] Apart from these specific crimes the Code also criminalizes actors involved in the facilitation of the aforementioned crimes by way of importing, producing, selling, offering, distributing, buying, receiving, and possessing instruments, secret codes, and passwords with simple imprisonment and/or fines.[93]

The Ethiopian Government issued the first comprehensive cybercrime proclamation in 2016, to address, the challenge that exists in terms of regulating offenses committed within cyberspace. Research conducted before the enactment of this proclamation demonstrates the gaps that exist within Ethiopian laws in regulating the new and sophisticated types of cybercrimes as well as computer-enabled old crimes.[94] The major gap concerning the Criminal code was the absence of procedural and evidentiary provisions that are necessary to investigate and prosecute computer crimes. The Code also failed to incorporate emerging computer crimes that are affecting major corporations and citizens that came along with higher technology dependency in the country. The Computer Crime Proclamation No.958/2016 similarly cites the inadequacy of existing laws in preventing, controlling, investigating, and prosecuting suspected cybercriminals as one of the reasons for the government to enact the law.[95]To this end, the proclamation was enacted to address these challenges and combat cyber-related offenses that are a threat to the countries growing information infrastructures and digitalization initiatives.

This Computer Crime law contains substantive, procedural, and other preventive provisions that are necessary to mitigate harm targeting individuals, organizations, and public infrastructures. The substantive provisions of the Proclamation include laws that prohibit a specific type of cybercrime in three categories. The first category of cybercrimes incorporated those crimes targeting the confidentiality, availability, and integrity of computer systems and computer data. These mainly include illegal access, Illegal interception, Interference with a computer system, causing damage to computer data, and other related offenses.[96] In this regard, taking into account the rapid

[91] See *id.* at Art.706, 707, and 708.

[92] See *id.*

[93] See *id.* at Art.709.

[94] ኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ, የኮምፒውተር ወንጀል አዋጅ ማብራሪያ, 2005 ዓ.ም, ገፅ 3.

[95] Computer Crime Proclamation No.958/2016, Negarit Gazeta No. 83, 7th, July, 2016, page 9104.

[96] See *id.* at Art. 3, 4, 5, 6 and 7.

technological advancements and complexity of cyberspace, the proclamation seems to recognize the challenge of illustrating all known types of cybercrimes. Accordingly, the proclamation prefers to use technology-neutral terminology to make the law applicable to future cases. For the aforementioned crimes targeting computer and computer data, the Proclamation set different levels of criminal culpability ranging from one-year simple imprisonment up to 25 years rigorous imprisonment depending on the degree of the illicit act.[97] The criminal liability of such acts will be aggravated if such crimes are committed against legal persons, critical infrastructures, and top secrets designated for military or international relations purposes or if they are committed during a state of emergency.[98]

The second category of computer crimes stipulated under the proclamation is computer-related forgery, fraud, and theft.[99] These are crimes that exist throughout human history that are enabled and empowered by technology. The last category of crimes under the proclamation are crimes related to illegal content data like obscene or indecent crimes against minors, crimes against liberty and reputation of a person, crimes against public security, and dissemination of an advertisement.[100] The procedure part of the proclamation incorporates several provisions necessary to investigate and prosecute cybercrimes. Owing to the non-territorial and complex nature of cybercrime the proclamation also provides an international cooperation clause, stating the need to cooperate and enter into agreements with other countries' competent authorities concerning the exchange of information, joint investigation, extraditions, and other assistance. [101]

5. *Institutional Measures*

The fight against emerging cybersecurity threats requires an effective institutional structure at the national level that can enforce national cybersecurity policies, strategies, and legislation enacted by the government. Accordingly, institutional measures include all national governance and coordination mechanism set up by the government to reliably deal with cyber threats and incidents. Despite the government initiative to embrace ICT into the country's socio-economic agenda, for long Ethiopia did not set up a national cybersecurity agency that is solely responsible for the

[97] See *id.* at Art. 7(5) and 8.

[98] See *id.* at Art. 3, 4, 5, 6 and 7.

[99] See *id.* at Art. 9, 10, and 11.

[100] See *id.* at Art. 11, 12, 13, 14 and 15.

[101] See *id.* at Art. 42.

protection of the country's growing ICT infrastructures and services. Due to this, most institutions disregard the issue of cyber security while some ICT infrastructures, internet service providers, and institutions are forced to develop their cybersecurity standards and management systems to deal with their cybersecurity challenges.[102]

Even though the former Ethiopian Information Communication Technology Authority was given the power to deter and offset national security threats emanating from ICT utilization,[103] the first attempt to establish a national cybersecurity organ was made with the establishment of the Information Network Security Agency /INSA/. Before the formation of INSA in 2006 Information Network Security Center was established under the FDRE Ministry of Defense with 37 military members.[104] In the same year, this center was upgraded to INSA with the enactment of Regulation No.130/130. INSA was established to ensure the security of the country's use of information and information communication network technologies so that they can help enforce peace, democratization, and development programs.[105]

Since then, the Agency has to be re-established twice through regulation No 250/2011 and proclamation 808/2013 to cope with the growing need of the nation and contemporary cybersecurity challenges. In addition to ensuring the security of information and information infrastructures, in the existing Re-establishment Proclamation, the Agency among other things is empowered to defend and take countermeasures against any cyberattacks targeted against the national interest and citizens' psychology.[106] Similarly, the Agency is also mandated to establish necessary international collaboration while discharging its mission.[107] This mandate was further reaffirmed with the enactment of Information Regulation No.320/2014 which provides a general guide as to the Agency International cooperation engagement by stating all interaction with foreign government

[102] Hannibal, *supra* note 73.

[103] Art.6(2) of Ethiopian Information and Communication Technology Development Authority Establishment Proclamation No. 360/2003, Federal Negarit Gazette No.82, 2nd, July 2003, page 2327.

[104] ኢንሳይት, *supra* note 69, at 20.

[105] Art. 6 of Information Network Security Agency Establishment Council of Ministers Regulation No.130/2006, Federal Negarit Gazeta, No 5, 24th, 2006, Page 3498.

[106] Art. 6(4) of Information Network Security Agency Re-establishment Proclamation No 808/2013, Federal Negarit Gazette No.6, 2nd, Jan 2012, page 7132.

[107] See *id.* Art 6(18).

institutions, security institutions, and associations to be in a manner that ensures the protection of national interest and respect the sovereignty of the country.[108]

The other institutional setup established to adequately and effectively respond to cybersecurity incidents is the National Computer Incident Response Center (CIRC). CIRC which was later renamed as Ethiopian Cyber Emergency Readiness and Response Team (Ethio-CER^{2}T), is established within the structure of INSA,[109] to serve as a single point of contact for reporting and responding to cybersecurity incidents in Ethiopia. Accordingly, Ethio-CER^{2}T assists organizations and the general public in preventing and handling cyber-security incidents collaborate with law enforcement agencies and local authorities, and coordinates national cybersecurity response.[110] Ethio-CER^{2}T Monitor the country's cyberspace 24/7 to quickly identify and respond to potential cyber incidents. Once a cyber incident is identified or reported Ethio-CER^{2}T first tries to contain the damage of the attack. Afterward, the Team proceeds to collect necessary artifacts and tries to analyze the cause and the objective of the attack. In doing so, Ethio-CER^{2}T works closely with other regional and global partners like AfricaCERT and Firs.org.[111]

6. International Cooperation Toward Secure Cyberspace in Ethiopia

The non-territorial and increasingly sophisticated landscape of cyberspace and its global security threats demand cooperation and collaboration between states, international organizations, and other global actors. Cyber threats and cybercriminals cannot be bound to geographical locations and, states cannot shut down their boundaries to incoming cyberattacks.[112] Hence, there is no country in the world including Ethiopia that is capable of assuring and protecting cyberspace and its critical infrastructure from cyberattacks without having a wide range of international partners. International best practices reveal to large extent cybersecurity depends on the political will of different actors

[108] Art. 17(2) of Information Network Security Agency Re-establishment Proclamation Execution Council of Ministers Regulation No.320/2014, Federal Negarit Gazette No.78, 22nd, Oct 2014, page 7695.

[109] Information Network Security Agency Re-establishment Proclamation No 808/2013, *supra* note 106, at Art. 6(4).

[110] Seblewoyne, *supra* note 68.

[111] See *id.*

[112] ITU, ITU GLOBAL CYBERSECURITY AGENDA: FRAMEWORK FOR INTERNATIONAL COOPERATION IN CYBERSECURITY 10 (2007).

to come together and collaborate on the issue of information and intelligence sharing and mutual assistance.[113]

Accordingly, the Ethiopian government views international cooperation as a means of securing the country's information assets through the adoption of NISP and different cybersecurity legislations. Since the enactment of this policy INSA as a government agency mainly responsible for the implementation of the policy was largely engaged in harmonizing cybersecurity legislation and standards with international best practices. [114] During the drafting of the Computer Crime Proclamation No.958/2016, different efforts were made to harmonize the draft legislation with international experience and model laws aiming to create a conducive global cooperation environment for cybercriminals' exchange through the application of the double criminality principle. [115] In doing so, the drafting of the proclamation consults with various international experiences such as the European Council Cybercrime Convention, ITU model cybercrime law, UN Economic and Social Commission for Western Asia /ESCWA/ model cybercrime law, G8 cybercrime prevention principles, and UN Computer crime-related decisions as well as different African, European and American cybercrime legislations.[116]

In addition to the Computer Crime Proclamation, the 2009 Critical Mass Cybersecurity Requirement Standard /NCMCS/ enacted by INSA to secure and certify the critical information and information system of federal and regional government organizations and key private organizations of the country is also largely based on internationally accepted best practices. This national standard is well harmonized with other globally endorsed practices as well as International Organization for Standardization /ISO/ approved standards.[117] Similarly, the drafting process of the new draft National Cybersecurity Policy and Strategy indicates several attempts that have been made to harmonize the draft policy with relevant international cybersecurity best practices[118] Accordingly,

[113] UN Chronicle, Towards Cyberpeace: Managing Cyberwar Through International Cooperation, (Jan.10, 2021, 10:33 AM) https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.

[114] Hannibal, *supra* note 73.

[115] Interview with Seble Girma, Head of Legal Affaires Directorate, Information Network Security Agency (Jan 5, 2022).

[116] ኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ, *supra* note 94, at 5.

[117] INFORMATION NETWORK SECURITY AGENCY, CRITICAL MASS CYBER SECURITY REQUIREMENT STANDARD VERSION 1.0 10 (2011).

[118] Hannibal, *supra* note 73.

one can appreciate the government's commitment to keeping the promises made within the NISP in terms of harmonizing the countries policies, legislation, and standards.

On the other hand, contrary to the harmonization efforts, the government's commitment toward engaging in global cybersecurity platforms and bodies is very much limited. Apart from some endeavors made to be a member of global cybersecurity bodies such as First.org and AfricaCERT (CERT-to-CERT arrangements), Ethiopia's engagement in international cybersecurity bodies and organizations is almost nonexistent. In the current context when it comes to cybersecurity issues, Ethiopia is a passive participant in almost all international, regional and sub-regional levels as well as other less formal settings. This being the case, it is difficult to find an effort made by the government concerning signing bilateral and multilateral agreements within the context of cybersecurity. Due to this, Ethiopia is not a signatory to both the African Union Convention on Cyber Security and Personal Data Protection /Malabo Convention/and the Council of Europe Convention on Cybercrime which is open to any non-member states around the world.

Recognizing the potential benefits of being a signatory to these agreements in terms of attracting investment and strengthening Ethiopia's cybersecurity capabilities, INSA is starting efforts toward conducting a national survey to study the impact of joining the Malabo Convention.[119] However, the process is in its early stage and faces challenges in terms of bringing together different stakeholders to pursue this endeavor. Especially, considering the Convention accommodation of issues other than cybersecurity such as data security and electronic transactions and trade, other government stakeholders the likes of the Ministry of Trade and Regional Integration and the Ministry of Innovation and Technology are expected to take part in the process of adopting this regional convention.[120] However, contrary to the ongoing effort to study the impact of signing, there is no available evidence to suggest there is a plan to consider being a member of the European Council Cybercrime Convention. Similarly, there is an absence of data that can attest to the fact that Ethiopia has entered into any bilateral agreement with any other state on the issue of cybersecurity. Consequently, one can argue not being part of these two available multilateral agreements and bilateral agreements would harm the country's cybersecurity capabilities in terms

[119] See *id.*
[120] See *id.*

of accessing cybersecurity technology; cross-border criminal exchange and investigation; information and intelligence sharing; capacity building; and mutual assistance.

7. The Global Cybersecurity Regulation Efforts and its Relevance to Ethiopia

Ever since Russia's made the first proposal to the General assembly in 1998, the issue of global regulation of cyberspace in the context of international security has been at the forefront of the UN agenda. Accordingly, several platforms have been formed under the umbrella of the UN for member states to discuss the topic of international law applicable to cyberspace and advancing norms governing responsible states' behavior toward cyberspace. Notably, the debate that took place among states within the framework of the GGE and the newly formed OEWG is actively shaping the global understanding of the contemporary issue of cyberspace governance. Even though these global debates are largely entangled by geopolitical differences, they have resulted in some positive progress toward advancing the global cybersecurity environment through the recognition of international law applicable in cyberspace and the adoption of 11 norms that dictate responsible state behavior in Cyberspace.

However, to date, these global debates are largely influenced by developed nations of the world while most developing nations of the world including African states remain silent or passive on the issue. As the world moves toward cyber diplomacy to ensure their national interests in these sorts of international platforms, African countries [including Ethiopia] have been largely absent from the evolving UN-based cyber norms development over the last two decades.[121] Due to the region's cybersecurity maturity level and other competing policy priorities, cybersecurity was given less priority in many African countries.[122] Since 2004, only Kenya, Egypt, South Africa, Mali, Ghana, Mauritius, Senegal, Botswana, and Morocco have held membership in the UN GGE, while Egypt, Kenya, and South Africa each took part in three of the 6 GGE groups formed by the GA. Hence, most of the outcomes of GGE platforms, including the 2015 11 voluntary UN norms are not grounded in the current realities of the resource-constrained continent with different levels of ICT development.[123]

[121] Directions, Partnering with Africa on Cyber Diplomacy, (Jan.11, 2021, 10:33 AM), https://directionsblog.eu/partnering-with-africa-on-cyber-diplomacy/.

[122] See *id.*

[123] See *id.*

Accordingly, like most African nations, Ethiopia has never been elected to serve as a member of the Six GGE established by the UN to advance responsible states' behavior in cyberspace between 2004 and 2019. Subsequently, when the global debate was opened to all the Member States of the UN through the introduction of the Open-Ended Working Group in 2019, the Ethiopian government failed to seize the opportunity to provide an opinion or a statement regarding the country's position concerning the ongoing global cybersecurity debate. Hence, contrary to the policy commitment made toward actively engaging in this form of the international platform in advancing the country's cybersecurity capabilities, Ethiopia is mostly absent in this UN-based norm-setting process. Interview conducted among relevant members of the government coupled with a lack of any viable evidence to that effect suggests Ethiopia has no established positions in terms of what has been discussed and debated on these international platforms.

The only available evidence suggesting Ethiopia's involvement in these global debates is the statement made at the first substantive session of the OEWG held between 12-16 December 2021. A statement made on behalf of Ethiopia concurs with the Non-Aligned Movement and does not take any side concerning the global cybersecurity regulation agenda.[124] Even if Ethiopia did not hold any concrete position toward this UN-led platform, however, the country emphasizes the advantages of rule-based order.[125] Accordingly, Ethiopia's permanent representative to the UN Ambassador Taye Atske-Selassie states *".... treaties with the strongest guarantee of reciprocity stand a better chance of compliance and uninterrupted application."*[126] In the same statement, Ambassador Taye Atske-Selassie provides an impetus for the development of an equitable international order that promotes an open, secure, stable, accessible, and peaceful ICT environment.[127] Accordingly, from a reading of this statement, one can observe Ethiopia prefers to stay neutral without establishing any position on the matter.

Despite the statement made during the first OEWG substantive session, Ethiopia's involvement in this ongoing global dialog is passive and low on the government's priority agenda. However, some efforts have been recently made by INSA to incorporate cyber diplomacy into the wider national

[124] Statement On Behalf of The Federal Democratic Republic of Ethiopia: At the First Substantive Session Of the Open-Ended Working Group on Security of And in The Use of Information and Communications Technologies 2021–2025: Delivered by Ambassador Taye Atske-Selassie, 12 – 16 December 2021, New York

[125] See *Id.*

[126] See *Id.*

[127] See *Id.*

security and foreign policy agenda through the newly drafted national cybersecurity policy.[128] Currently, INSA is also on the onset of conducting national research to identify the possible responsible stakeholders and demarcate the role they are going to play in terms of handling cyber diplomacy and taking part in the ongoing global cybersecurity agenda.[129] Even though, the approach followed to address such a sensitive and highly geo politicized issue through research is commanding, the current efforts are long overdue.

Not having a national position concerning the ongoing debate on establishing international regulation and code of conduct or norms of state behavior in cyberspace will have an impact on Ethiopia's capability to defend against cyber security threats, vulnerabilities, and attacks. Without reliable global partners and allies, the country's ability to acquire technical and financial assistance, technological transfer, information sharing, capacity building programs, and experience sharing will be affected. Besides, the lack of a rational and well-established position on the global cybersecurity debate may force Ethiopia to support other developed nations' global norm-setting initiatives without analyzing the merit of its term.

The absence of Ethiopia in this global debate and the lack of a clear position will affect the country's interest, in terms of adopting and implementing norms developed over the year to regulate cyberspace. Considering Ethiopia's limited financial resources, institutional capacity, and technological advancement, most of the current UN-based voluntary norms to govern responsible states' behavior in cyberspace are not in line with the country's cyber maturity level. For instance, norms like states' responsibility for cyberattack committed in their territory toward another state's critical infrastructure,[130] would put Ethiopia in a disadvantageous position considering the country's ability to screen, detect and guard its networks are limited. Since most of the norms adopted by the GGE in 2015 were largely influenced by developed countries, they tend to disregard the digital divide and capacity difference that exists between developed countries and developing countries like Ethiopia. Hence, the lack of necessary cybersecurity capacity will hinder Ethiopia's ability in upholding or implementing these UN-based norms.

[128] Information Network Security Agency, *supra* note 80, at 21.

[129] Hannibal, *supra* note 73.

[130] U.N. GA, *supra* note 50, at 8.

Despite having a clear policy direction and legal ground to pursue Ethiopian cybersecurity interests through international cooperation and diplomacy, Ethiopia's involvement in the global cybersecurity agenda is largely hampered by various challenges. Among these challenges, the lack of awareness among relevant stakeholders as to the ongoing global debates on cybersecurity and their implication is very much observed. There is only limited knowledge within INSA cybersecurity professionals regarding the stakes and tones between the two blocks regarding the global cybersecurity regulation issues. Similarly, the lack of capable diplomats that are well acquainted with the current cybersecurity landscape and its real impact, was also observed as another challenge that adversely affected Ethiopia's bargaining power in global cybersecurity platforms. Apart from this obvious awareness and capacity gaps, weakness witnessed in terms of collaboration and alignment among different stakeholders is also a challenge to the country's international cooperative efforts. Considering cybersecurity is a cross-sectoral issue, there is an absence of structured discussion and coordination among all relevant public and private stakeholders at the national level to shape and coordinate the country's position and response to this ongoing debate[131].

The other challenge affecting Ethiopia's international cooperative endeavors lies in the fact that the issue of global cyberspace governance is intertwined with a geopolitical struggle between the major cyber powers. The competition between the US and its allies on one side and Russia, China, and their allies on the other concerning the global cybersecurity norm-setting process creates a difficult environment for developing countries. With cyberspace fast becoming a new frontline for opposing norms and influence, different countries are launching different initiatives to seek as many countries as possible in their corner. In light of these recent developments, supporting a cyber norm-setting initiative in these developed countries becomes an integral part of bilateral cybersecurity agreements. [132] Hence, entering into an international cybersecurity agreement with one of these opposing states will most likely affect Ethiopia's foreign relations with opposing states. Accordingly, considering Ethiopia's long-standing foreign policy principle which is based on neutrality and impartiality, entering open-ended /non-exclusive/ agreements and reaching consensuses with developing countries is becoming a real challenge.

[131] Hannibal, *supra* note 73.

[132] See *id.*

8. Conclusion

As the world continues to migrate toward digital technology in managing their day-to-day activity, attacks and threats emanating from the digitally connected world have presented a new and complex set of challenges to society. Currently, challenges resulting from a complex set of cybercrimes and behaviors are adversely impacting human rights, economy, social cohesion, and critical infrastructure. In the context of responding to this emerging global security threat in recent years, cybersecurity negotiations have come to the forefront of the international agenda. Accordingly, the international community has started to engage in dialogues to regulate the malicious behavior of state and non-state actors in cyberspace. However, despite all the ongoing dialogues and debates among various actors and stakeholders, as of yet, there is no consensus as to how the existing international law would be applicable to govern the global cybersecurity environment.

The current global effort toward developing a cybersecurity norm is largely hindered by geopolitical tensions. However, despite geopolitical differences, the GGEs established under the UN composed of both of these contrasting sides have reached some important milestones in terms of advancing responsible states' behavior toward the use of ICT. Among these milestones, the recognition of the application of existing international law (UN Charter) in cyberspace in the 2013 third GGE; and the introduction of eleven voluntary norms governing responsible state behavior in cyberspace are the most fundamental.

In light of this ongoing global cyber security governance debate, the paper uncovers only a small number of states around the world that openly declare their position concerning the debate regarding responsible states' behavior within cyberspace. As of yet, these debates are largely dominated by developed nations with high cyber maturity levels while the vast majority of developing nations including Ethiopia remain silent on the agenda. Except for the neutral statement made in the first session of OEWG, Ethiopian involvement in the current dialogue is somewhat passive. Despite the implication and the stakes of these ongoing global debates in terms of determining the country's future cybersecurity and warfare competence, Ethiopia’s involvement is very much non-existent. Considering most of the norms that have been developed under the UN GGE framework are very much aligned with the interest of developed countries with advanced cyber maturity, countries with limited cyber security capability like Ethiopia would be challenged to cope with international obligations that are put in place through this newly developed cybersecurity norms. Accordingly, not being part of this ongoing global agenda will likely have an impact on Ethiopia's prospects in terms of attaining international technical assistance, capacity building, technology transfer, funding, and cross-border collaboration on other cybersecurity issues. Consequently, taking into account the government's recent vigorous effort toward integrating the country's critical infrastructures with ICT, disregarding these global agendas would have a detrimental impact on the country's national security in the near future.

Empirical data coming out of the government show cyberattacks targeting Ethiopian critical infrastructure are on the rise. The current growing threat landscape will have an even higher impact on the socio-economic development of the country as the country becomes more and more dependent on ICT. However, in the last decade, Ethiopia has been taking some encouraging steps toward managing these contemporary cybersecurity challenges. Even though there is still more to be done in terms of their implementation, Ethiopia is actively trying to catch up with the world through the enactment of national cybersecurity policy, legislation, and the establishment of responsible agencies.

However, contrary to the aforementioned cybersecurity measures, Ethiopia's global cooperative and cyber diplomacy engagements are very much lagging even in comparison with some other developing African nations like Kenya, Egypt, and South Africa. In addition to being absent from the current ongoing global cybersecurity norm-setting debates, Ethiopia is neither a signatory to the African Union Convention on Cyber Security and Personal Data Protection nor the Convention on Cybercrime Council of Europe which is open to all countries around the world. Similarly, it is difficult to find any bilateral cybersecurity agreement signed by Ethiopia with other countries. Although Ethiopia has a clear cybersecurity policy direction and legal frameworks supporting the country's engagement in global cooperative frameworks and agendas, the study shows that the current implementation of this policy direction and legal framework is very much limited. Hence, there is an obvious lack of strategic direction to position the country in a manner that can address the issue.

Consequently, considering international cooperation is one of the most important cybersecurity measures that can be taken to mitigate cybersecurity threats, the country's reluctance on this front would have a lasting impact on the country's effort in securing critical infrastructures and addressing cyber threats. Hence, to create resilient cyberspace that is capable of supporting the socio-economic development ambition of the country, it is recommended for the government to begin assessing the potential impact of the ongoing global cybersecurity agenda and provide a strategic direction that can promote the version of global cybersecurity norms and agreements that can closely align with the country’s national interest.