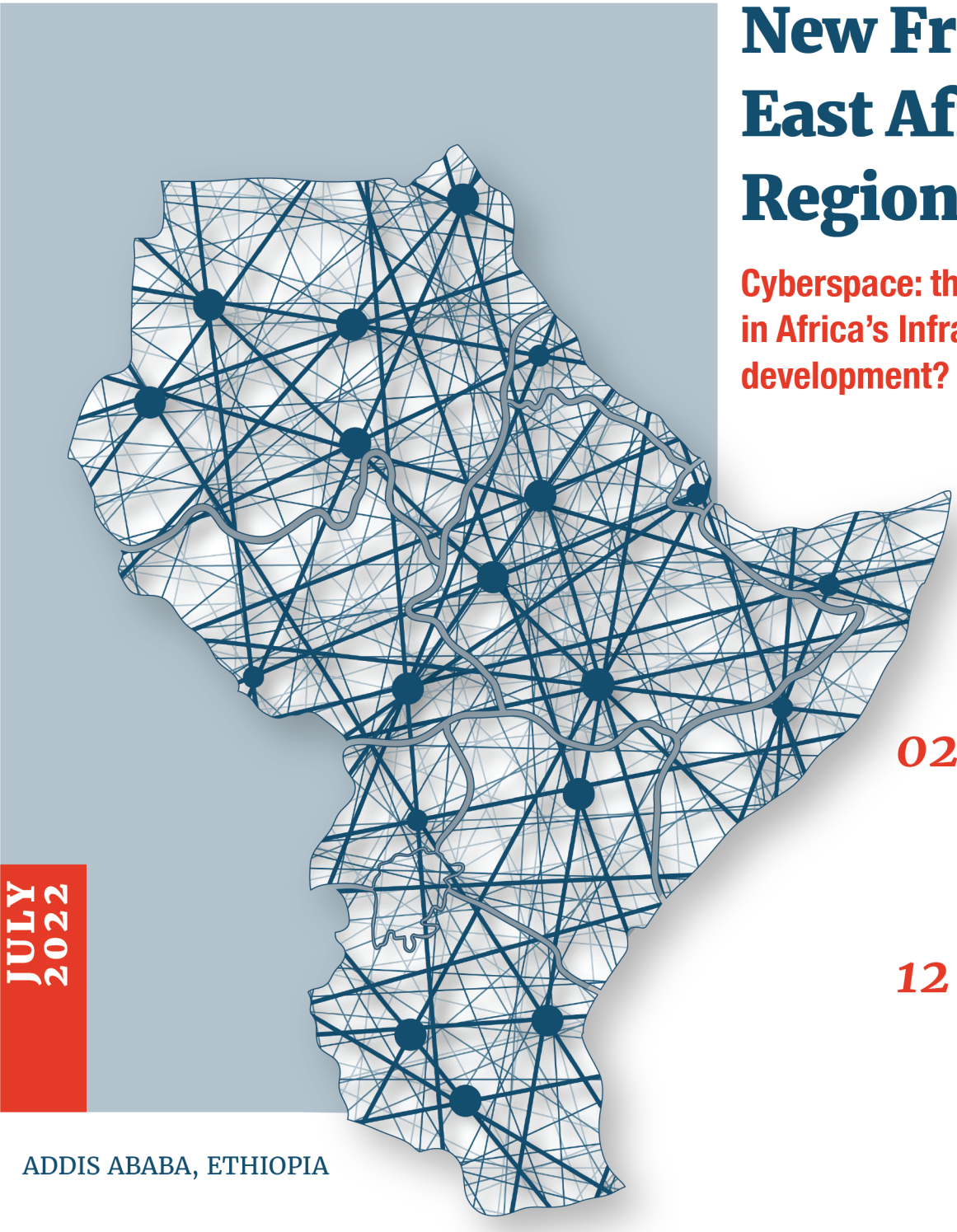
HORN REVIEW
IDEAS CONNECTIONS SYNERGY

Ninth Edition

New Fronts in East African Regional Security

Cyberspace: the new battleground in Africa's Infrastructure development?



JULY 2022

ADDIS ABABA, ETHIOPIA

About us:

Founded in 2021, Horn Review is a premier research and publication think-tank dedicated to exploring and amplifying African voices with a goal of interlinking subject matter experts, practitioners, and academics from Ethiopia, the Horn Region, and the African continent with the broader public. With a stated mission of Africa for Africans, Horn Review aims to amplify and mainstream uniquely African ideas and perspectives on sociopolitical, economic, and geostrategic issues relevant to the continent. Horn Review aims to connect African thinkers, practitioners, and policymakers with their respective communities to create greater synergy and a people-centered discourse on African matters.

@HornReview

www.hornreview.org

Horn Review

Table of Contents

Editor's Note :

Dear readers,

July saw intense attention to African engagement on the global stage with several high-profile visits to the continent. While China claims to remodel its development approach towards Africa to one that is more peace and good-governance centered, the United States has shortly followed suit. The United States also unveiled its intentions for a renewed African engagement with an emphasis on the continent's agency and active participation. Russian Foreign Minister, Sergei Lavrov, on his four-nation tour of Africa, stated that Russia plans to increase its partnership with African countries; he stated "no country should be forced to cut ties with old friends", particularly in what he views as a crumbling of the uni-polar international order.

With chilling global developments like the Russia-Ukraine conflict, political confrontation between Beijing and Taipei, renewed conflict in the Gaza Strip, and a looming food crisis due to a shock in the wheat and fertilizer supply chain, one must ask why global powers are eying Africa. The common theme seems to be a 'strategic' approach to engaging Africa. But what is "strategic engagement"? Broadly, and in the current context, strategic engagement between nations is a measured cooperation between states on matters of common interest. One must also ask, why now? And why not through international cooperative frameworks and agencies? Like the United Nations, for example. Does this 'diplomatic scramble for Africa' signal an eroding trust in international systems and institutions? If this is the case, should there be a framework for the subjective engagement of African countries in this multi-polar global order?

This 9th Edition of Horn Review discusses some of the immerging issues having to do with East African security. I would like to thank Brig. General Sebsibe Duba, Commandant, for speaking to Horn Review about the International Peace Support Training Institute (IPSTI) and availing their campus and facilities to our team. B/G Sebsibe describes the crucial work the Institute does for sustained peace in the HoA region, and salutes Ethiopia's decorated past with peace support operations in the Horn.

I would also like to thank Abdijabar Mohamed, a cybersecurity researcher and scholar, for running a cyber-attack scenario analysis and drawing attention to some of the tragic consequences of cyberattacks on the Grand Ethiopian Renaissance Dam. Abdijabar raises critical issues of early warning and preparedness and the need to ramp up efforts in securing critical infrastructure from cyberattacks and remote hacking.

I also thank Dr.Shimels Sisay Belete for his thorough examination of Ethiopia's legal framework for addressing terrorism. In Part II of his Article, Dr. Shimels shows the evolution, and contrast, between Ethiopia's various anti-terrorism proclamations through time.

I would also like to thank Ato Getachew Nigatu for the timely discussion on the nature of loan agreements between the Chinese government and African officials. Ato Getachew raises the timely question: "who is to blame" for corruption-ridden loan practices?

Bethlehem Mehari

Ethiopia's Exposure to the Existing International Terrorism Law

Shimels Sisay Belete (Ph.D.)

Shimels Sisay

Dr. Shimels is a human rights lawyer by profession with a hybrid experience working both in academia as a lecturer and researcher, and through his practical engagement in the field of human rights advocacy. He holds a Doctoral Degree (Dr. iur.) in International Human Rights Law, Terrorism and Counterterrorism from the European University of Viadrina, in Frankfurt (Oder), Germany. He received his master's degree in Human Rights Law from Addis Ababa University and LLB Degree in law from Haramaya University.

Currently, Dr. Shimels serves as the Ethiopia Country Director for the International human rights NGO called Freedom House. He also works for European Center for Electoral Support (ECES) as Electoral Trainings Coordinator and the Legal Expert on Civic and Voter Education and Inclusion. He also holds a visiting professorship position and teaches the African Human Rights Regional System at the Faculty of Law, European University of Viadrina, Germany.

The 1957 Penal Code of Ethiopia

The Code's wide-ranging coverage of similar crimes committed against a foreign state or interstate organizations might also be cited as indicators of Ethiopia's earlier attempts and its political willingness to take part in the pressing demands of cooperation and transnational responses to crimes of international concern, despite that, an act of terrorism has never got an explicit mention within such category. A typical practical example that Ethiopia mentioned in its report was the successful investigation, prosecution, and trial of the offenders who participated in the assassination attempt of the former Egyptian President Hosni Mubarak.[24]

The third category of essential provisions of the old Penal Code – perhaps the most contiguous and highly affiliated offenses with that of the crime of terrorism, both in times of peace and war – are those proscribed in the second title of the Code, under Arts 280 and the following, as offenses against the law of nations. In exactly similar fashion or with direct reference to the international law instruments to which Ethiopia is a party, the Code had defined crimes of genocide; crimes against humanity; war

crimes against the civilian population; and war crimes against the wounded, sick, shipwrecked persons, prisoners, and interned persons and branded them as grave offenses against the international community. There are tendencies equating terrorism with that genocide when committed systematically against a particular targeted group of civilians, or as a war crime when perpetrated targeting civilians not actively taking part in hostilities during armed conflicts. Accordingly, only a few might have contested if one would have quoted these provisions of the Code in dealing with acts of terrorism in the absence of any discrete law explicitly addressing this conduct as a separate crime.

A typical practical example that Ethiopia mentioned in its report was the successful investigation, prosecution, and trial of the offenders who participated in the assassination attempt of the former Egyptian President Hosni Mubarak.

Apart from that, as provided under Art. 17, the Penal Code had also established national jurisdiction prosecuting crimes committed in a foreign state against international law or universal order – an international offense specified in Ethiopian legislation, or in the international treaty or convention to which Ethiopia has adhered and implemented in the domestic jurisdiction. With this integrationist approach, those specific conventions dealing with particular offenses, or acts related to terrorism, could have domestic application even if the proscribed conduct has been committed neither inside the territory of Ethiopia nor against the national interest of the state, hence giving effect to the already highlighted conventions beforehand.

Furthermore, stressing on the importance of some other sections of the penal code in the prevention of terrorism, Ethiopia had been invoking its capability of remedying any potential crimes of terrorism.[25] With a particular focus on the suppression of financing terrorism, for example, solicitation of funds for a commission of criminal acts, including that of terrorism, had been treated as intentionally associating oneself with the principal offense leading to criminal liability either as principal joint-offender or as an accomplice – pursuant to Arts 32 and 36 of the Code, respectively. At the same time, Arts 267, 438, 439, and 473 of the Code had been invoked as pertinent provisions in criminalizing failure of reporting the commission or preparation to commit serious crimes; harboring, comforting, or aiding of alleged offenders; and indirect aid or encouragement for the commission of such crimes, including a crime of terrorism. Besides, the recruitment of terrorist groups and the supply of weapons for the commission of the crime had also a special coverage under the Code as general offenses despite the absence of explicit reference to the crime of terrorism.

Apart from the general Penal Code of 1957, other proclamations enacted, either to amend a particular provision of the Code or to regulate a new criminal behavior had also been contemplated as pertinent normative frameworks, mainly in the prevention aspect of the State's obligation in relation to terrorism. Laws, such as the Amended Legal Notice No. 229/1960 and the Special Penal Code Proclamation No. 8/1974, alongside the Commercial Registration and Business Licensing Proclamation No. 67/1989 were enacted to regulate the manufacturing, repairing, import-export, selling, possession, and dispossession of weapons in Ethiopia, and thus criminalizing illegal trafficking in arms and explosives. The Provisional Military Administrative Council Revised Special Penal Code Proclamation No. 214/1981 had also apportioned a separate

provision in Art. 41 proscribing illegal trafficking in arms as one of the serious crimes punishable with the gravest penalty up to death.[26]

Besides, the recruitment of terrorist groups and the supply of weapons for the commission of the crime had also a special coverage under the Code as general offenses despite the absence of explicit reference to the crime of terrorism.

There had been also laws aimed at regulating the establishment, registration, and financial and operational supervision of associations – be it religious, charitable, cultural, or whatsoever – as potential normative watchdogging tools to monitor the legitimate functioning of the associations and minimize illegal purposes like that of channeling the financing of terrorism.[27]

The 2004 Revised Ethiopian Criminal Code

It has to be noted from the outset that almost all the values ascribed to the 1957 Penal Code and the other supplementary statutes mentioned hitherto in the context of the suppression and prosecution of terrorist crimes are also the defining characters of the Revised FDRE Criminal Code;[28] indeed with the more intriguing articulation of the provisions incorporating new advancements entrusted in modern criminal law as well as the radical changes in the political and socio-economic environment of the country. Accordingly, this section focuses only on those add-ons that the Code has brought into the domestic criminal justice system as the most significant progressions bearing upon or connected with the matter at hand.[29] Fathomably, one of the justifications necessitating the revision of the old Penal Code has been the need to proscribe the newly emerged crimes born out of the complexity of modern life, and hence terrorism being one as such.[30]

To begin with, the vain attempt made at the drafting stage of the Revised Criminal Code, the crime of terrorism was proposed as one of the newly included separate crimes of its own. In an exact replication of the definition provided under the OAU Convention on the Prevention and Combating of Terrorism, draft Art. 252 of the Criminal Code defined the crime as follows:

1. Whosoever commits a terrorist act which may endanger the life, physical integrity or freedom of, or causes serious injury or death to, any person, any number or group of persons, or causes or may cause damage to public or private property, natural resources, environment or cultural heritage and is calculated or intended to:

    a. Intimidate, put in fear, force, coerce or seduce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or

    b. Disrupt any public service, the delivery of any essential service to the public or

    c. to create a public emergency; or Create a general insurrection in a state; is punishable with rigorous imprisonment from ten to twenty-five years; or in grave cases, with rigorous imprisonment for life or death.

4. Any promotion, sponsoring, contribution to, command, aid incitement, encouragement, attempt, threat, conspiracy, organizing, or procurement of any person, with intent to commit any of the acts referred to in Sub-Art. (1) of this Art. shall be punished in accordance with Sub-Art. (1) hereof.

Furthermore, some related crimes, inter alia, arson; damages to installations or protective works; explosions and causing dangers by the use of explosive, inflammable, or poisonous Substances; damages to services and installations of public interest; and grave endangering or sabotage of communications or transport could undoubtedly deter and incriminate conducts which terrorist perpetrators mostly employ as methods and means in the commission of the crime. Moreover, when the aforementioned crimes have caused loss of life, injury to the body, or impairment of health, the degree of the crime is treated as a grave offense with rigorous punishment up to life imprisonment or the death penalty.

Most importantly, prohibited acts proscribed under the discrete international terrorism-related conventions are explicitly criminalized on separate provisions of their own. Arts 507–511 of the Revised Criminal Code, for example, have integrated almost all acts proscribed under the 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft, the 1970 Convention for the Suppression of Unlawful Seizure of Aircraft, the 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, the 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, and the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation.

In doing so, Art. 507 criminalized unlawful seizure or control of an Aircraft or exercising control of a fixed platform on a continental shelf stating that:

> [w]hoever, by violence or threats thereof or by any other form of intimidation, by deceit or by any other unlawful means intentionally seizes or exercises control of a fixed platform on a continental shelf or an aircraft in flight or landing in an airport or a ship on navigation or harboring on a port, is punishable with rigorous imprisonment from fifteen to twenty-five years.[31]

Not only the seizure or excessing control of these protected objects but also an intentional and unlawful act of endangering these assets and any act of violence against a person on a fixed platform on a continental shelf or an aircraft in flight or landing in an airport or a ship on navigation or harboring on a port which is likely to endanger the safety of the platform, the aircraft, or the ship is also proscribed as one of the gravest crimes punishable with rigorous imprisonment or even up to death penalty if the act causes death or bodily injury or impairment of health.

one of the justifications necessitating the revision of the old Penal Code has been the need to proscribe the newly emerged crimes born out of the complexity of modern life, and hence terrorism being one as such

What can be asserted is, therefore, despite the absence of any distinct comprehensively articulated provision fastening the crime of terrorism with aptly defined legal, moral, and material elements of its own, the Revised

Criminal Code had further boosted the domestic legislative domain and the criminal justice machinery that the State needed to uphold its obligation in the prevention and combating of terrorism.

This said, however, such unwarrantable omission of the crime of terrorism from the newly Revised Criminal Code – a law enacted in 2004 by the time when terrorism has gained the choosiest attention as a serious threat to international peace and security, and given one of the justifications necessitating the revision of the old code being the need to incorporate crimes of such a threat – depicts the missed opportunity of the time. Perhaps, the drafters might have had better comparative insights and augmented portrait as to the distinctive features of terrorism and the abovecited crimes that are successfully inserted in the Code, but misleadingly assimilated or synonymized with an act of terrorism.

Tellingly, as it has been empirically witnessed in most terrorism charges instituted against alleged perpetrators since the adoption of a discrete antiterrorism law in 2009, there remains discernible purviews intermingling those genuine acts of terrorism with the aforementioned crimes, the commission of which by no means constitute an act of terrorism per se. [32]

Post-2009 Terrorism and Related National Legislation

The 'no-specific-terrorism' law standing came to an end in 2009 following the issuance of the Anti-Terrorism Proclamation No.652/2009 as one of the most controversial laws enacted in the recent legislative history of the State.[33] Soon after, the Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No.657/2009 proceeded,[34] which was later replaced by Proclamation No. 780/2013.[35] It is then in pursuance to these fledgling normative frameworks that the issue of terrorism and conducts allegedly constituting the crime are being regulated in the national criminal justice system.

Most notably, Art. 6 of the Anti-Terrorism Proclamation, which criminalizes any intentional or negligent publication of a statement that is likely to be understood by a section of a society either as direct or indirect encouragement to terrorism – showing no venial by imposing rigorous imprisonment up to 20 years

Indeed, the overall impact of these antiterrorism laws has not been limited only to the actual administration of the crimes. It goes rather beyond, to the extent of triggering the revision of the laws and policies which are deemed to have direct or implied 'cause–effect' corollaries in their enforcement. In this regard, the National Intelligence and Security Agency Re-Establishment Proclamation No.804/2013;[36] the Information Network Security Agency Re-Establishment Proclamation No.808/2013;[37] the Adver- tisement Proclamation No.759/2012;731 the Protection of Witnesses and Whistleblowers of Criminal Offences Proclamation No. 699/2010;732 the Computer Crimes Proclamation No.950/2016;733 and the Electoral Code of Conduct for Political Parties Proclamation No.662/2009734 are few among others, as laws inevitably moulded and reformulated to complement the nuanced contents and approaches tinted in the antiterrorism

proclamations.

The tilting repercussion of the 2009 Anti-Terrorism Proclamation is not only limited to the aforementioned laws enacted in the aftermath of its entry into force. Even laws that are proclaimed before have been retrospectively stricken and their content and normative values have appeared futile. The two most affected laws in this regard are the 2008 Freedom of the Mass Media and Access to Information Proclamation No. 590/2008 [38] and the 2009 Charities and Societies Proclamation No.621/2009.[39] Most notably, Art. 6 of the Anti-Terrorism Proclamation, which criminalizes any intentional or negligent publication of a statement that is likely to be understood by a section of a society either as direct or indirect encouragement to terrorism – showing no venial by imposing rigorous imprisonment up to 20 years – have accelerated the already thinning status of the right to freedom of expression and political dissent in the country. Ethiopia's marque image as a State with the highest number of journalists in exile next to Iran, and with the highest number of journalists in jail with speech related offences next to Eritrea, alongside the number of leading opposition figures held in prison would exhibit the untold implication of the proclamation on the ground. [40]

The same impact of the antiterrorism laws on the actual application of the Charities and Societies Proclamation can also be posited from the ever-increasing number of NGOs and Civil Society Organizations whose licenses are being annulled on allegations of violating their obligations imposed by the law, and their involvement in activities other than their objectives.[41] The more sensitive, unrestrained, and vaguely articulated provision under Art. 69 of the Proclamation authorizes the Ethiopian Charity and Society Agency to refuse a license if the proposed Charity or Society is 'likely to be used for unlawful purposes or purposes prejudicial to the public peace, welfare or good order in Ethiopia' [42] and thus, such a wider discretionary power has posed a loophole as a potential normative tool in stifling the work of human rights advocacy and human rights defenders under the guise of banning illegal organizations and their financial source from the outset in the larger context of preventing the financing of terrorism.[43] In this regard, the sceptics do not seem groundless if one takes into account the strict notion stipulated under Art. 12 of the Money Laundering and Financing of Terrorism Proclamation No.780/2013, as it subjected any religious or non-profit organization for oversight to ensure that the funds they collect are not used for financing of terrorism.[44]

The overall influence and thrums of the Ethiopian antiterrorism law have been also vividly noticeable in the recently drafted national criminal law policy.The Policy unequivocally, barred a crime of terrorism as one of the non-bailable offences proscribing that a person arrested with suspicion of having committed any terrorist crime shall not, in any circumstance, exercise his right to be released on bail.[45]

The other most contentious feature of the proclamation is traced under part five which addresses the mandate, justifications, and procedures in the course of proscribing an entity as a terrorist organization and the ramifications therefrom.

Generally, it has to be noted, therefore, when it comes to thoughts regarding the Ethiopian legislative and policy frameworks on issues of terrorism, the bigger theme has to be posturized beyond the two antiterrorism proclamations currently in force given the direct or indirect stamp that these laws have cemented, at least, as inspirational standard precursors in the drafting and/or application of the other highly connected laws and policies hitherto discussed.

This said in regard to the opposite broader picture while harnessing the national statutory amasses pertaining to terrorism in general, the Anti-Terrorism Proclamation No.652/2009 remains, however, the solitary domestic law that set out and attempted to respond to the two most pivotal, but controversial, issues in terrorism discourse. That is, matters concerning the definition and scope of the crime of terrorism and issues relating to the power, reasons, and procedures of proscribing entities as terrorist organizations. Needless to say, be it in dealing with the rest of the related crimes prohibited in this proclamation – such as membership, incitement, encouragement, financial or material support, training, or participation – or other prohibitions and restrictions postulated in allied statutes referred above, the foundational basis for each of the crimes radiates from the definitional stance on the very concept of the crime of terrorism itself and the prescription measures. Furthermore, the special and extended investigative powers and tactics entrusted to the old or newly restructured enforcement organs as well as the slackened evidential standards are also justified based on the definitional characteristics of the crime of terrorism and the perceived distinctive features of entities purportedly branded as masterminds of the act.[46]

Glancing the Content and Structure of the Anti-Terrorism Proclamation No. 652/2009

The Anti-Terrorism Proclamation is a composite of only thirty-eight provisions, with a considerable number of them vested on matters substantially insignificant as such, like the title and miscellaneous parts.[47] Given the very first of its type, and considering the national statutory and jurisprudential dearth on the subject, it is not snobbery to reasonably expect a full-bodied and more comprehensive with detailed regulatory frameworks. Perhaps, such a thicker approach might have minimized the undesired outcomes of those contentiously and vaguely articulated sections of the proclamation, and it might also have genuinely responded to many of other issues left unsettled and muffled lacking an apposite legislative answer.

These thirty-eight provisions of the Proclamation are subsumed into seven sequential constellations. Whilst Art. 2 of the general part provides a definition of terms used in the text, the second section has stipulated a comprehensive definition and elements of a 'terrorist act' under Art. 3, followed by a bunch of other crimes related to terrorism. These crimes include planning, preparation, conspiracy, incitement, and attempt of terrorist act; rendering support to, and encouragement of terrorism; participation in terrorist organization; possessing or using property for terrorist act; possessing and dealing with the proceeds of terrorist act; false threat of a terrorist act; failure to disclose terrorist acts; and inducing or threatening witness and destroying or hiding evidence relevant to the case. Alongside the crimes, the corresponding

penalties upon conviction are robustly cemented ranging from the least intrusive three years of rigorous imprisonment to that of the gravest punishments of life imprisonment or sentence to death.[48]

The third part – embracing the other ten provisions of the proclamation – on the other hand, embodies the conspicuous rules on investigation powers and measures in the prevention of terrorism. Of more intriguing in this section are the rules governing the conditions and procedures in the exercising of powers vested to the police and the National Intelligence personnel for the gathering of information, operationalizing sudden searches, and covert searches, effecting arrests, and the taking of samples. Whereas, evidentiary and procedural rules on cases relating to terrorism are governed by Arts 23 and 24 of the proclamation. Accordingly, some critical quarries on the source of th evidence and its admissibility, the weight, and credibility of the evidence, the burden of proof and statute of limitations for prosecution are inexplicably entrenched.[49]

The other most contentious feature of the proclamation is traced under part five which addresses the mandate, justifications, and procedures in the course of proscribing an entity as a terrorist organization and the ramifications therefrom.

The other most contentious feature of the proclamation is traced under part five which addresses the mandate, justifications, and procedures in the course of proscribing an entity as a terrorist organization and the ramifications therefrom.[50] Accordingly, apart from the aforementioned individual criminal liabilities as a result of participation in different forms, inter alia, as leader, trainer, recruiter, or supporter of the organization in question, measures against the legal status quo and the various interests of organization on its own personality, particularly the ceasing of its legal personality, the freezing and seizure of, as well as forfeiture of its property are also incorporated as consequences of the decision of proscription.

Last but not least, part six of the proclamation tends to accredit the directly responsible institutional setups entrusted to follow-up cases of terrorism with a special mention to the ministry of Justice, Federal Police and the National Intelligence and Security Service, the latter being in charge of the leadership role. Besides, unlike other crimes, the jurisdiction to adjudicate terrorism cases is solely restricted as a federal matter, as such an exclusive power is vested in the Federal High Courts and the Supreme Court.

The New Anti-Terrorism Proclamation No. 1176/2020: Substantial discoursal change or a piecemeal move entwined with the older purview?

As one of the bolder moves driven by the post-2018 legislative and political reform initiatives, Ethiopia revised the previous draconian anti-terrorism law and adopted Proclamation No. 1176/2020 as a new regulatory framework aimed at preventing and controlling the crime by enabling the security forces to take strong

precautionary and preparatory acts centered at the nature of the crime while ensuring the rule of law and fundamental rights of individuals as for provided under the FDRE Constitution and international human rights instruments ratified by Ethiopia.

While the new proclamation is commended for its progressiveness in terms of addressing some of the normative, interpretational, and enforcement gaps under the previous law, this latest legislation has also encountered substantial critics as it still reflects specific problematic nuances.

While the new proclamation is commended for its progressiveness in terms of addressing some of the normative, interpretational, and enforcement gaps under the previous law, this latest legislation has also encountered substantial critics as it still reflects specific problematic nuances of the old version that may have a negative impact in legitimizing potential abuse by the government as some of the provisions and the practical interpretation and application of which may create loopholes to erode fundamental rights and freedoms of citizens. In this context, some of the proscribed acts as crimes of terrorism – such as the vaguely articulated crime of "intimidation to commit a terrorist act as stipulated under article 5 of the Proclamation" – lack clarity to the extent of defining the legal, the moral, and material elements of the crime. Other components of the new proclamation, such as the mandate and the procedure under which a certain entity could be proscribed as a terrorist organization; the degree and gravity of the punishments which still maintain the death penalty; and standards and degree of evidential proof while establishing criminal guilt also call for an in-depth and critical review and auditing vis-à-vis their compatibility with that of the international law relating to terrorism and international human rights law standards.

REFRENCES:

24 The first Ethiopian Report to the 1373/2001 Committee, supra note 33, p. 6.

25 See generally: Supplementary Report of the Federal Democratic Republic of Ethiopia Pursuant to Paragraph 6 of Security Council Resolution 1373 (2001), United Nations Security Council, S/2002/1234, 8 November 2002. 701 Ibid., p. 5.

26 Art. 41, Revised Special Penal Code of Proclamation No.214/1981, Federal Negarit Gazeta, No.2, Provisional Military Administration Council, 5 November 1981.

27 The Supplementary Report, supra note 56. In this regard, Regulation No.321/1966 and Proclamation No.84/1994 had paramount importance.

28 The Criminal Code of Federal Democratic Republic of Ethiopia, Proclamation No 414/2004 [hereinafter, the Revised Criminal Code], entered into force on 9 May 2005. See generally Arts 238–280.

29 See more on the overall justifications necessitating the new criminal code: Kassa, W. D., Examining Some of the Raisons D'être for the Ethiopian Anti-Terrorism Law, Mizan Law Review, 7:1 (2013), pp. 49–66. 30 See the Preamble of the Revised Criminal Code. Supra note 64.

31 Art. 507 (1), Revised Criminal Code.

32 See more: Gordon, L. (ed.), Ethiopia's Anti-Terrorism Law: A Tool to Stifle Dissent, The Oakland Institute and Environmental Defender Law Center, Report, 2015. See also: Sekyere, P. and Asare, B., An Examination of Ethiopia's Anti-Terrorism Proclamation on Fundamental Human Rights, European Scientific Journal, 12:1 (2016), pp. 351–371.

33 Anti-Terrorism Proclamation No. 652/2009, supra note 5.

34 The Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No.657/2009, supra note 6.

35 The Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No.780/2013, Federal Negarit Gazeta, 19th year, No 25. Addis Ababa, 4 February 2013.

36 House of Peoples' Representatives; The National Intelligence and Security Service Re- establishment Proclamation No. 804/2013, Federal Negarit Gazeta, 19th Year, No. 55, Addis Ababa, 23 July 2013. For more details on the overall implication of this proclamation, see infra, Chapter 9, Section 9.7.

37 House of Peoples' Representatives; The Information Network Security Agency Re-establishment Proclamation No. 808/2013, Federal Negarit Gazeta, 20th Year, No. 6, Addis Ababa, 2 January 2014.

38 House of Peoples' Representatives, Freedom of the Mass Media and Access to information Proclamation No.590/2008, Federal Negarit Gazeta, 14th year, No. 64. Addis Ababa, 14 December 2008.

39 House of Peoples' Representatives, Charities and Societies Proclamation No .621/2009, Federal Negarit Gazeta, 15th year, No 25. Addis Ababa, 13 February 2009.

40 Tadeg, M. A., Freedom of Expression and the Media Landscape in Ethiopia: Contemporary Challenges, University of Baltimore Journal of Media Law and Ethics, 5:1-2 (2016), pp. 69–99; Ali, M. S., Jurisprudential Challenges to Freedom of Expression in Ethiopia: Critical Reflections on Selected Legislations of the Country, the Internet Journal Language, Culture and Society, 42 (2016), pp. 1–12.

41 During the year 2008 Ethiopian calendar alone (July 2015–June 216), 108 organizations were banned while other 167 were given warnings of different levels. Ethiopian News Agency, 27 June 2016.

42 Art. 69 (2) Charities and Societies Proclamation, supra note 92 [emphasis added].

43 Centre for International Human Rights North Western University School of Law, Sounding the Horn: Ethiopia's Civil Society Law Threatens Human Rights Defenders, November 2009.

44 Art. 12, The Money Laundering and Financing of Terrorism Proclamation, supra note 82.

45 Federal Democratic Republic of Ethiopia, Ministry of Justice, Criminal Justice Policy (unpublished), 4 March 2011.

46 Conte, A., Human Rights in the Prevention and Punishment of Human Rights: Common Wealth Approaches: The United Kingdom, Canada, Australia and New Zealand, Springer, Heidelberg, 2010, pp. 424–425.

47 See Arts 1, 37, and 38, the Anti-Terrorism Proclamation, supra note 80.

48 See the penalties imposed up on conviction on crimes under Arts 3, 4, 5 (2), and Art. 7 (2) of the Anti-Terrorism Proclamation.

49 On evidence-related concerns arising from the Proclamation, see, generally, Chapter 8, Section 8.5.

50 Art. 25–27 of the Anti-Terrorism Proclamation.

The Grand Ethiopian Renaissance Dam (GERD) as an African Cyberwarfare Front: A Simplified Cyber Attack Scenario & Some Plausible Cyber Attack Consequences

Abdijabar Yussuf Mohamed

Abdijabar Yussuf Mohamed

Abdijabar Yussuf Mohamed is an incoming graduate student and Kennedy Fellow at Harvard University in Cambridge, Massachusetts, where he will be pursuing a Master of Public Policy (MPP) at the John F. Kennedy School of Government. His research interests span from computational public policy, Artificial Intelligence (AI), cybersecurity & cyberwarfare, Sino-Africa relations, to armed conflicts in the Horn of Africa.

Wartime thriller enthusiasts are familiar with Alfred Hitchock's Saboteur (1942). In this enthralling American spy film, famous for its climactic sequence atop New York City's Statue of Liberty, the protagonist, Barry Kane (as portrayed by Robert Cummings), a California-based aircraft factory worker, is falsely accused of committing an act of sabotage that led to the demise of a co-worker. Determined to exonerate himself, Kane flees from police custody and, accompanied by Patricia Martin (acted by Priscilla Lane), sets on a perilous cross-country chase to catch the actual criminal. During the course of the manhunt, the protagonists thwart a sabotage plan by American fifth columnists who were conspiring to blow up the Hoover Dam (formerly known as the Boulder Dam) that harnessed the waters of the mighty Colorado River to provide electricity to Los Angeles-based American defense plants. The Hoover Dam, still one of America's largest hydroelectric facilities and an engineering marvel, is a concrete arch-gravity dam situated across the Black Canyon of the Colorado River and straddles the U.S states of Nevada and Arizona. Today, the threat of hydroelectric dams and reservoirs being blown up is neither limited geographically to America nor is it a preserve of riveting American thriller films.

In the 21st century, as such critical infrastructures as massive hydroelectric power plants (dams and reservoirs) are connected to the internet, there is a palpable threat posed by cyber terrorists who are hellbent on wreaking havoc on targeted critical infrastructures. Hackers, largely sponsored by rival nation-states, wage borderless battles on enemy nation-state's critical infrastructures such as hydroelectric power plants, water supply systems, the power grid, hospitals, etc.... In this regard, cyber attacks on critical infrastructures continue to emerge as a force to reckon with and form a significant component of the arsenal in geopolitical conflicts. A case in point is the GERD (shown in Figure 1 below), Ethiopia's $4.5 billion

flagship project and Africa's largest hydroelectric power plant. The GERD, the epicenter of the geopolitics of water pitting the Horn of African nation against the downstream riparian states of Egypt and Sudan, will arguably become one of the defining fronts of cyberwarfare in Africa.

In June 2020, Ethiopia's Information Network Security Agency (INSA) reported that it thwarted cyber attacks carried out by Cyber_ Horus Group, a state-sponsored Egyptian hacker group. Aimed at mounting pressure on Arat Kilo over the construction and filling of the GERD, the group hacked numerous Ethiopian government websites under an image depicting a skeleton pharaoh and defaced the websites with the following threatening message:

"If the river's level drops, let all the Pharaoh's soldiers hurry and return only after the liberation of the Nile, restricting its flow. To prepare the Ethiopian people for the wrath of the Pharaohs."

"If the river's level drops, let all the Pharaoh's soldiers hurry and return only after the liberation of the Nile, restricting its flow. To prepare the Ethiopian people for the wrath of the Pharaohs."

Again, in May 2022, INSA reported that the agency had foiled a cyber attack attempt targeting the GERD and other Ethiopian critical infrastructures. According to Shumete Gizaw, Director General of INSA, in a bid to frustrate the works of the GERD and major financial institutions, the state-sponsored malicious hackers affiliated with a foreign nation that envies "the peace and development endeavors of Ethiopia" targeted approximately 37,000 interlinked computers used by the Horn of African nation's financial institutions. He further alleged that this is part of a cyber war campaign against Ethiopia, code-named the "Black Pyramid War".

Figure 1: Satellite of Image of the GERD (source: Maxar Technologies)

Organizational Structure

That Egyptian-affiliated hackers pose an unprecedented threat to Ethiopia's national critical infrastructures, specifically, the GERD is given. However, little is known regarding the nature of cyber warfare that Ethiopia will be embroiled in with Egypt (and potentially Sudan as well) over the GERD. Despite its limited purview, this short work - the first part of a series of informative pieces available in future Horn Review publications- aims to enlighten the Ethiopian authorities and the public on this matter. In this part, I start with a simplified but possible cyber attack scenario on the GERD. Then, this is followed by an analysis of some possible effects of a cyber attack on a computerized GERD. Part II of the following publication will delve deeper into Ethiopia's preparedness on the digital battlefield vis-à-vis Egypt and Sudan, the rationale for establishing

a dedicated Ethiopian Cyber Command, the place of an African Union (AU) Cyber Command that would conduct "virtual peacekeeping" over the GERD and other critical Ethiopian institutions in the likely event of destructive cyber-attacks that follow when GERD negotiations falter, and policy recommendations to facilitate towards shaping a cyber resilient Ethiopia.

A Simplified Cyber Attack Scenario on the GERD

For the sake of the hypothesis and as it is in many parts of the world, let us assume that the operations of the dam are remotely controlled by a contractor (let us call it Gidibachin, an imaginary contractor based in the Bole, Addis Ababa) that employs about 100 specialists who remotely work on different parts of the GERD. A malicious attacker, based in Cairo, Egypt, sends a barrage of meticulously crafted phishing emails that contain malicious payloads to all of Gidibachin's 100 employees. As soon as the emails are received, one of Gidibachin's employees falls for the ruse and instantly downloads the malware. As a consequence, the Egyptian hacker gains access to the employee's user credentials and other critical data. Utilizing the stolen user credentials, the hacker gains remote access into GERD's networks through a Virtual Private Network (VPN) in order to hide his digital footprints. Immediately afterward, the hacker maintains access to the GERD's systems using an undetectable backdoor. The criminal familiarizes himself with the GERD's intricate details and subsequently gains control of the dam's automated components.

Plausible Impacts of Cyber Attacks on the GERD's computers

By its very nature, critical infrastructure such as a hydroelectric power plant is a complex system. To ensure smooth operations, dam operators and technicians must continuously monitor the different parts of the system. Thus, operating such a complex system as the GERD implies that there is a need for administrators and other relevant authorities to frequently interact with the systems. This calls for the adoption of Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems to enable the dam administrators and authorities to regulate the processes both locally and remotely. If hackers gain access to the ICS/SCADA systems (the dam's command and control systems), then they can wreak unprecedented cyber-physical havoc in several ways. To mention some but few key risks, hackers can cause the following: (1) flooding the waters ; (2) poisoning the waters of the GERD; (3) engendering power blackouts to the national and regional power grids connected to the GERD; and (4) leveraging the GERD's systems as a launchpad for conducting transnational cybercrime activities in Ethiopia and beyond.

Although we have not yet witnessed such devastating effects on GERD, the possibility of such consequences is not far-fetched. A historical precedent for such potential consequences exists.

Flooding the Waters of the GERD

The village of Bameza, Benishangul-Gumuz Region (BGR), where the GERD is located, and the BGR in general, has been historically prone to flash floods. Adverse

weather phenomena like the El Nino and heavy rainfalls during the rainy season frequently induce deadly floods and landslides that are detrimental to human lives and crop production. Alongside the natural disasters that the BGR is vulnerable to, the region is now vulnerable to the man-made impacts of a devastating cyber attack on the GERD. If Egypt-based hackers gain access to the GERD's system, they could empty the reservoirs by simultaneously opening the floodgates and other outlets of the dam. As a result, the rapid flow obliterates the adjacent turbines and power stations and leads to destructive floods that, in addition to destroying crops, could claim many lives and force residents to evacuate from the area. Although we have not yet witnessed such devastating effects on GERD, the possibility of such consequences is not far-fetched. A historical precedent for such potential consequences exists.

In 2016, the U.S Justice Department unsealed an indictment against Hamid Firoozi, an Iranian who, along with other six Iranians acting on behalf of the Islamic Revolutionary Guard Corps (IRGC), the ideological custodian of Iran's 1979 revolution, was allegedly involved in a 2013 intrusion into the SCADA systems of the modest Bowman Avenue Dam near Rye Brook, New York. The dam's SCADA systems that were installed a few years before the Iran-backed security breach incident was connected to the internet through a cellular modem. The access level that Firoozi and his accomplices had would have allowed them to obtain critical information on the dam's water level and temperature information. Furthermore, this access would have allowed them to remotely operate the dam's floodgates. It is only that during the period of intrusion into the dam's systems, the electronic gate was taken offline for maintenance purposes. Even though Rye Brook, located outside New York City, is a low-population area, a 2007 flood caused more than $80 million worth of damages to the nearby City of Rye. If the Iranian hackers had access to the dam's command and control systems during a storm, they would have been in a position to open the dam's floodgates and cause more damage to the local community living near the Bowman Avenue Dam. Extrapolate this logical point of departure to the devastating effects that could emanate from Egyptian hackers obtaining access to the floodgates of the massive GERD. Thousands of lives in the Bameza villege, BGR, would be claimed, crops destroyed, and an Internally Displaced People (IDP) crisis could follow.

Poisoning the Waters of the GERD

Malicious cyber actors with access to the GERD's internal systems can cause wanton destruction by increasing the Chlorine levels. By increasing the amount of water treatment chemicals such as Chlorine beyond what is fit for human consumption, cyber attackers on the GERD can kill people who drink the dam's waters. In the recent past, hackers attempted to poison water treatment facilities.

In 2000, the police in Queensland, Australia, arrested a man for deploying a computer and a radio transmitter to take control of the Maroochy Shire Council's Sewerage System and subsequently released sewage into parks, rivers, and even the grounds of a Hyatt Regency Hotel. Similarly, In 2021, malicious hackers gained unauthorized access to a water treatment

Although we have not yet witnessed such devastating effects on GERD, the possibility of such consequences is not far-fetched. A historical precedent for such potential consequences exists.

plant located in the small American town of Oldsmar, Florida. Upon gaining access into the plant's networks, the hackers momentarily adjusted the levels of lye (Sodium hydroxide) in the drinking water before being mitigated by the state's cyber incident responders. In small amounts, lye is a chemical used for treating the acidity of water and removing metals from the water before being supplied to the residents. In larger amounts, it is a toxic chemical that can lead to the death of people who consume the resultant poisoned waters. A similar attack by Egyptian hackers into the GERD's water filtering system would have dire consequences for Ethiopia.

If hackers sponsored by foreign governments successfully infiltrate the GERD's networks, then they could escalate their access privilege to eventually disrupt power distribution and even cause a nationwide and region-wide power blackout.

Catastrophic Power Outages

Many Ethiopians, especially those living in rural areas of the emerging states such as the BGR, Gambella Region, and Somali Region, lack access to electricity. To enhance its citizens' access to energy, the Ethiopian government is eyeing to provide electricity to Ethiopia by harnessing the Blue Nile Waters in the GERD reservoirs. Additionally, it aims to be a regional powerhouse that sells electricity to neighboring countries in the Horn of Africa, and beyond. If hackers sponsored by foreign governments successfully infiltrate the GERD's networks, then they could escalate their access privilege to eventually disrupt power distribution and even cause a nationwide and region-wide power blackout. Such apocalyptic scenarios are tantamount to the loss of millions of dollars for Ethiopia and its future electricity customers in neighboring countries such as Kenya, Somalia, and Djibouti.

Leveraging the GERD's computers as a Transnational Cybercrime Station

Besides the aforementioned risks, hackers with diverse affiliations and hats (nation-state-sponsored hackers, hacktivists, local cybercrime syndicates, etc.) could attempt to gain access to the GERD's networks. If they successfully manage to do so, they may initially deliberately refrain from causing damage to Ethiopia's critical infrastructures. Instead, they could leverage the robust computerized systems that undergird the massive as a station for hosting robot networks (botnets) that will be used for mounting Distributed Denial of Service (DDoS) attacks, malware attacks, phishing attacks, and ransomware attacks, among others, to local and international businesses and governments. In such a scenario, the GERD could be reduced to a cybercrime Mecca that attracts sophisticated transnational cybercrime syndicates and serves as a testing ground for the so-called script kiddies (novice hackers).

Part II of this article will be published in subsequent editions.

Cartoon by Alex Teferra

Exploring the International Peace Support Training Institute (IPSTI) with Brig. General Sebsibe

Brig. Gen. Sebsibe Duba
Commandant of IPSTI

Brig. General Sebsibe Duba is the commandant of the Ethiopian International Peace Support Training Institute. A highly-decorated 29-year veteran of the Ethiopian National Defense Forces, Brig. General Sebsibe most recently served as Chief Training Officer at AMISOM Force Headquarters. He has a Bachelor of Arts in Leadership and Military Sciences from the Ethiopian Defense Command Studies and Staff College and served as Head of the Security and Strategy studies department at the Ethiopian Defense Command. General Sebsibe obtained his Master of Arts in Managing Peace and Security in Africa from Addis Ababa University and holds a post-graduate Advanced Diploma in Defense and Strategic Studies from the National Defense University (NDU) of China.

Ethiopia has a long and illustrious history of international peacekeeping support. As a founding member of both the United Nations (UN) and the African Union (AU), the nation's participation in UN-authorized operations dates back to 1951; since then, Ethiopia has deployed over 150,000 personnel for peace operations, both under Chapters 6 and 7 of the UN Charter. Its deployments range from infantry units, tactical and utility, helicopter units, motorized battalions, and mechanized battalions, to hospital and well drilling units.

Established under the Peace Keeping Center (PKC) in 2010, the IPSTI is dedicated to training security sector leaders both from Ethiopia and other African countries. The IPSTI provides over 25 courses on various thematic and functional areas tailored for both national and international participants, i.e. military, police, and civilian students. The institute's coursework is structured around conflict prevention, post-conflict recovery, and other cross-cutting disciplines. IPSTI is lauded for its individualized attention to participants and discussion-based learning. The Institute's campus includes training and office facilities, a canteen, accommodations, and a theatre facility. According to the Commandant of the Institute, IPSTI aims to become a premier center of excellence in peace support training, education, and research in Africa.

Ethiopia has deployed over 150,000 personnel for peace operations, both under Chapters 6 and 7 of the UN Charter.


Student Residence on campus, Addis Ababa.

Commandant Brig. Gen. Sebsibe adds that the Institute aims to become a frontier in peacekeeping pre-deployment training, particularly on UN mandates and compliance, human rights, and gender equality support in Africa. Secondly, the IPSTI offers specialized foreign language training, as well as testing, in preparation for international deployments. The IPSTI offers a robust English and French language training program and is in the process of crafting additional language training and soft-skills programs. Third, IPSTI has a highly specialized Peace and Conflict Management graduate program which comprises accomplished military leaders, as well as enrollees, from around the African continent. Participants are often sponsored by their respective governments to complete the coursework. Lastly, the institute conducts various research on peace support operations and conflicts to promote regional peace.

According to the commandant of the school, regional peace, particularly in a crucial geo-strategic location like the Horn, is a collaborative effort that requires the attention and participation of various stakeholders. Hence, the IPSTI has a range of core and institutional partners ranging from nations like Germany, Japan, and the UK to the United Nations Development Program (UNDP) and the African Union (AU). Through the support of various national and international partners, the IPSTI is able to enhance the capacity of its regional standby forces and further expand its training modules into academic programs.

IPSTI training Facility, Near Kebena, Addis Ababa.

China's "Peaceful Development" agenda in the Horn of Africa

Getachew Nigatu
Horn Review

Getachew obtained his first degree from Addis Ababa University's Political Science and International Relations department PSIR. He holds an M.A. in International Relations from Addis Ababa University and an M.A. from the University of Leeds, UK, in Political Communication. Getachew served as Director General at the Ethiopian Ministry of Foreign Affairs and worked as Secretariat for the Foreign Policy Review Team. Upon Joining the private sector, Getachew worked as a senior political editor at The Reporter Newspaper in Ethiopia.

China's Foreign Ministry appointed a Special Envoy to the Horn of Africa, Xue Bing attended the first ever 'China-Horn of Africa Good Governance, Peace and Development Summit held in Addis Ababa, Ethiopia, from June 20 to June 22, 2022. Senior officials and representatives of Ethiopia, Djibouti, Somalia, Kenya, Uganda, Sudan, and South Sudan were in attendance at this event that is to mark a shift in China's partnership model, particularly with Eastern Africa. Zhao Zhiyuan, China's Ambassador to Ethiopia, who was also in attendance, insisted on the presence of the Chinese Special Envoy at the summit upon invitation; adding that China doesn't have any other agenda than assisting development and peace prospects in the Horn of Africa.

The conference, led by H.E. Xue Bing, was also intended to encourage dialogue between the Government of Ethiopia (GoE) and the Tigrayan People's Liberation Front (TPLF) but looked into discussing the crisis and conflict plaguing the broader region. This raises several critical questions worth considering.

First, what is the actual interest of the Chinese government in the Horn of Africa, particularly, how may this summit serve in bolstering regional peace? It is a fact that Horn States owe the Chinese government billions of dollars in debt, hence conflict conditions and instability in the region will not only result in the loss of critical partners in the region but also a massive economic loss incurred by the Chinese government.

> **The Chinese Government's Belt and Road Initiative (BRI) lays out a clear framework for diplomatic engagement, economic cooperation, resource self-sufficiency, and more to expand China's cooperation with African partners.**

The Chinese Government's Belt and Road Initiative (BRI) lays out a clear framework for diplomatic engagement, economic cooperation, resource self-sufficiency, and more to expand China's cooperation with African partners. Despite multiple security threats posed by various entities, one must ask: "if not for the geostrategic and economic incentives the Horn region offers, would China's government have prioritized such a high-level engagement with the region's governments?" The answer is likely NO. Given the Chinese government's prior engagements with the African States, it is a recent phenomenon for China to pioneer good governance and peace initiatives in other countries. As is the case with most Horn Governments, China seldom comments on political developments and prefers not to involve in protection, de-escalation, or peacebuilding initiatives. However, The contrary is true when it comes to its deeply entrenched involvement in African economies. What accounts for the sudden shift towards peace and development, as well as good governance? Could it be a protective mechanism for its investment holdings in these countries?

Africa's stability matters to China. China is not only involved in trade and investment and infrastructure development but Chinese companies are also heavily involved in mineral exploration and widespread mining in Africa. The continent's rich natural resources, and ample market for services and goods, are increasingly attractive to China; hence instability in Africa means it cannot exploit the mineral and economic prospects in Africa.

Infrasture development in Ethiopia and other African countries often fails to repay their loans, further entrenching the into dependency.

Africa's raising debt to the Chinese government exceeds 140 billion USD and at least 18 African countries have been renegotiating the terms of their past agreements. However, the terms of these loans are not disclosed to the public- remaining a secret between the signatory African heads of state and China. These loans, through the so-called "Peaceful Development initiative" often take infrastructures from poor African countries as protection or guarantee. It only becomes public knowledge when countries in debt default on their payment and settlements become difficult.

Chinese loans are often considered predatory. When asked, most African governments and China would claim that their partnership is a "win-win." However, heavy Chinese investments, particularly in infrastructure development are said to be highly impropriety; the African officials signing these loan agreements often advance their individual

However, the terms of these loans are not disclosed to the public- remain a secret between the signatory African heads of state and China.

interests under the cover of secrecy. The Chinese government itself provides certain shields for corrupt African officials. This is by providing officials from African governments with the power of signing infrastructure loan agreements a grand corruption platform that makes them commit to these unethical loans. The Heritage Foundation in its piece 'Chinese Corruption in Africa Undermines Beijing's Rhetoric about friendship in Africa' claims' that Beijing either encourages or ignores corruption and that China's government-linked and government-owned companies habitually use corruption that hurts ordinary Africans.

Infrasture development in Ethiopia and other African countries often fails to repay their loans, further entrenching the into dependency. For example, six years after launching the first Sub-Saharan Africa light rail system, the Addis Ababa transit system went from bad to worse. According to *The Reporter* news Paper, during its first four years, the transit system earned a gross revenue of 11 million USD; it, however, needs 154 million USD to operate. The General Auditor's report shows that the rail system falls far short of its original feasibility study. 'The feasibility study has been inadequate, and it was conducted without collecting enough information.' Who is responsible for these kinds of irresponsible loans? Officials in African governments or China?

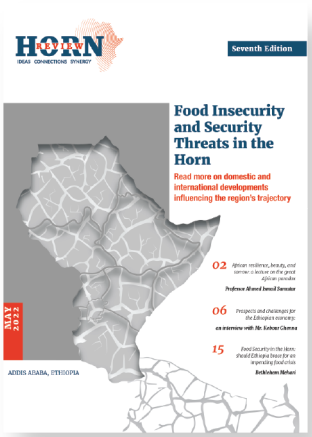
Part II of this piece will be published in subsequent editions.

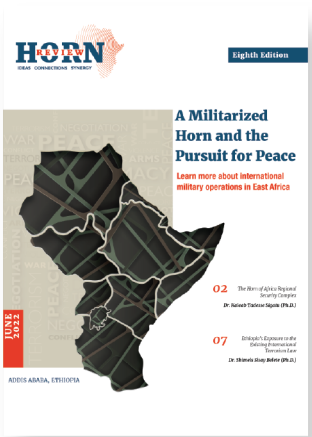
On the occasion of the first year since its founding, Horn Review will be hosting an award dinner in early November, 2022, for distinguished professionals in the following categories:

Social Entrepreneur Award
Cultural Diplomacy to the Horn Award
Diaspora Initiative of the Year Award
Friends of Ethiopia Award
Lifetime Diplomat Award
Climate Justice Pioneer Award

Distinction in each category is awarded to individuals and/or organizations with laudable contributions in research, advocacy, or service for the advancement of their community or country.

To send your nominations, or to learn more about the award categories, please email awards@hornreview.org





@HornReview

Horn Review

@Horn Review

@horn_review

info@hornreview.org

Behind Sapphire Addis Hotel,
Bole Atlas, Addis Ababa

Read our previous issues on our website : *www.hornreview.org*

Price: ETB 100.00

Published by Demera Media and Communications PLC

Addis Ababa, Ethiopia