Hate Speech Dissemination and Pseudo News Fabrication in Ethiopia

Fiseha Kiros Gebremamas[1], Dr. Zafar Alam[2]

[1]Debre Berhan University, Ethiopia

[2]Maulana Azad National Urdu University (MANUU), Hyderabad, India

Abstract: ***This research examines on the recent exhibition of rogue behavior in the Ethiopian spreading hatred speech and falsehood news. Informed by measures taken in other countries, it offers some thoughts on how best to overcome the rapidly growing ills of social media deception campaigns in Ethiopia. For the sake of convenience, this essay uses the terms 'problematic content', 'pseudo news' and 'deception' interchangeably unless the context dictates otherwise. Suggestions offered are likewise intended to apply to the phenomena of problematic internet content, deception and pseudo news campaigns. Governments of today exercise significant authority in the digital space. But challenges still remain especially in fully regulating what is called the dark web, where numerous criminal activities take place shielded; while cyber anarchist views soon surrendered to the reality of government - and substantial private - power, views of similar touch emerge occasionally in various forms.***

Keywords: Hate Speech, Pseudo News, Ethiopia, cyber command, Hacking, rogue behavior

1. The Fabrication and Dissemination of Pseudo News

We now live in a world of abundant computing, where access to information and communication technologies has increased profoundly in most corners of the globe. This access is mainly purveyed by social networking sites such as Facebook, Telegram, Twitter and video sharing platforms like YouTube, which have billions of users worldwide. Most individual Internet users increasingly rely very much on news and other forms of information shared through these platforms. Instead of watching television, listening to radio or even directly accessing sites of mainstream media organizations, many people now appear to prefer receiving their daily news through Facebook or webcasts - or amateurish videos uploaded by ordinary users on YouTube. These online platforms - in keeping with these developments - now have sophisticated software that determine what information should be allowed to circulate in their platforms, and tailored to the preferences of each profiled user. This increasingly - and worryingly -has transformed sites such as Facebook, twitter and Telegram from mere social networking platforms to the most powerful editor-in-chief of the globe as they curate vast amount of information disseminated both by the mainstream media and everyone else including those that disseminate hate speech and pseudo news. At times, fabricated lies that gain wider circulation on the web get picked up by the mainstream media, and once reported in the latter, it is more likely to be accepted as truthful information.

Concerns relating to problematic content are as old as the Internet but those regarding pseudo news and hate speech have particularly heightened in Ethiopia in the year 2018/9 and counting. Several coordinated misinformation and deception campaigns curated through social media sites have been felt in several parts of the world.

The 2016 US election has been controversial on several levels. The claims that the victory of the current President of US Donald Trump has been - to some degree - facilitated by Russia who allegedly coordinated a range of attacks to discredit the Democratic nominee Hilary Clinton were, however, significant according to the CNN news analysis. One of these alleged Russian-led attacks was that Russia had launched intensive campaigns of deception to change the course of the election. This was mainly carried out through dissemination of falsehoods about the candidates through social media platforms mainly Facebook. These deception campaigns were launched from websites which appeared legitimate to Facebook users. In highlighting the enormous impact of the campaign, former US President Barack Obama noted:

The ills of deception have also reached Ethiopia, where the impact was no less significant. The country was rocked by a series of protests since late 2015 that exhibited novel ways of airing grievance. In addition to generally peaceful street protests in some parts of the country, self-declared 'activists" - who mostly hail from the diaspora - have been actively engaged in 'activism'. Several government websites have been hacked, and defaced as part of the protests. The protests, however, took a destructive turn. National examination papers were leaked over social media, leading to postponement of the exams and blocking of access to social media sites.

A number of falsehoods have been running in social media platforms. The deception took a wild turn following the unfortunate stampede at a traditional ceremony. Diaspora based 'activists' widely propagated that the stampede - and the subsequent death - was caused by shootings by government troops from a helicopter. This fake news declared through social media, which - with a dis-informed, emotional and mostly unemployed youth - led to deaths and enormous destruction of private and public property. The attacks also had taken racial tone in some parts of the country. The alleged helicopter shooting was, however, shortly disproved by independent foreign journalists.15 Government subsequently declared a state of emergency for the duration of six months, and Internet access has been significantly restricted in some parts of the country.

Incidents of pseudo news have also occurred in connection with other matters. A more recent such news was that Ethiopia allegedly severed diplomatic ties with South Sudan, and that the Ambassador was expelled. This was immediately dismissed as untrue by both countries. Another relates to the controversial travel ban introduced by the American head of state which some sources wrongly reported that it would affect Ethiopian travelers. This had stirred some dust but was soon disproved. False reports that allege dismissal or death of higher government official - or claims of internal political fallout within the government - or defection of high profile investors in opposition to the government or alleged sale of land to neighboring countries are rather too commonplace. Sometimes these campaigns of deception and pseudo news are run by platforms that are known to have links with or are avid supporters of the enemies of Ethiopian government, which maintains an open hostile policy towards Ethiopia.

The actual impact of these campaigns is not clearly known, and most of them have so far been carried out in a less coordinated manner to cause significant damage. But some of them undoubtedly have the potential to cause suspicions, uncertainty among the public and may also threaten internal security of the country.

2. Messy Actions Taken as Measures

The government has been engaged in several measures which appear to be ineffective, inefficient and legally questionable. Several reports often include Ethiopia among countries that actively filter the Internet by blocking access to several websites. Unofficial reports have also documented blocking of several dozens of websites. Aggressive use of cyber tools for Internet filtering and other major cyber operations have also been reported recently.

Ethiopia’s cyber command - Information Network Security Agency (INSA) - has also been implicated in the use of intrusive cyber tools such as Fin spy spyware and Remote Control System against individuals whom the government considers terrorists. These have resulted in lawsuits abroad against Ethiopia as well as a criminal complaint. The form of measures grew to Internet shutdowns and filtering of social media sites during the recent deadly protests in some parts of the country. The measure was taken following the leaking of national examination papers on social media sites.

These measures might be a short term solutions yet accompanies with several problems in different respects. First, the sporadic and piecemeal approach of the government reduces the effectiveness of these measures. Responses of the government are often reactive, uncoordinated and as such fall short of resulting in long-term solutions. Blocking social media sites and Internet shutdown merely offer short-term respite. There is no guarantee that similar or even more damaging incidents would not occur once Internet access is restored. The Government’s measures appear not to be guided by clear goals, and are taken randomly just to quell the dust for a while. This robs them of any value to sustainably address the ever rising and damaging rogue web culture in Ethiopia. Further, there are no known rules and procedures by which these measures are taken. Little is known about how blocked sites are selected, who does the selection, and whether it is possible to challenge such decision. The same applies with respect to use of DPI, Internet shutdowns and engagements in shoddy hacking and spying practices. This raises questions of legality both under domestic and international law, and as such impinges on several rights such as the right to privacy, freedom of expression and due process rights. Chances of overreach are also higher when measures are taken randomly and without clear accountability mechanisms.

Furthermore, the efficiency - both economic and diplomatic - of these measures is questionable. A recent report has indicated that Internet shutdowns have resulted in an estimated loss of eight million dollars to the fledgling Ethiopian economy.27 Recent leaks have also revealed that the Ethiopian government has spent about a million dollars for buying spyware and other cyber tools.28 And, having read the Hacking Team’s - one of the companies who sold these tools leaks, where Ethiopian authorities are ridiculed for poor use of the tools, one is bound to question the wisdom in making such expenditure.

In the diplomatic front, frequent association with censorship, labels of repression and authoritarianism haunts Ethiopian authorities in almost every engagement with foreign donors and dignitaries. This must have been a very uncomfortable topic for our officials. The diplomatic firefighting is not also without its economic costs. A recent report has revealed that Ethiopia spends millions of dollars for lobbying American lawmakers to, among others, block the passing of bills that paint the country’s image in the negative light such as frequent references to some people in jail as political prisoners or prisoners of conscience or labeling the government as authoritarian. One could expect similar costly lobbying campaigns on the other side of the Atlantic especially given some strong anti-government voices in the European Parliament.

Ethiopia’s unique position as a diplomatic capital of Africa also makes restriction of Internet access a cause for concern. More recently, Addis Ababa based diplomats have actually quizzed Ethiopian officials including the Premier on a number of occasions about the Internet shutdowns, and the effect on their operations. Doubtless, frequent and random practices of restricting access to the Internet are likely to lend new weight to those who are not happy about this diplomatic position. I proffer some suggestions below on how to mitigate these concerns while at the same time upholding rule of law in the Ethiopian cyberspace.

3. How to Decrease the Problem

Ethiopia is just beginning to see the menace of 'pseudo news' and deception campaigns. With increasing Internet access, rise of extremist foreign based media (traditional and new), shrinking independent local media and apparent distaste to state-run media, the threat is yet to increase and prove destructive. This state of affair requires the government to take a range of measures. The government must break away from its habitual piecemeal approaches such as temporary shutdown of the Internet, and follow a considered and sustainable policy path to meet the challenge head on. It has taken encouraging steps in rolling out useful policy documents such as the information security policy. These policy documents, however, must be revitalized based on new developments and put forward clear policy direction.

The ruling party has aptly acknowledged the threats of pseudo news and deception, and has vowed to create a social media army to counter the challenge by providing accurate information to the public. Of the stated roles of the Institute include training an ethical, educated and patriotic cyber army that responds to the country's cyber war. The envisioned cyber combatant roles of future trainees sound absurd but we shall wait and see how the said regulation reads once published in the law gazette in due course. That the government pursues the case of a social media army openly, and with a clear legal framework is promising. This creates a sense of certainty, and hopefully accountability. However, it must be taken at national level, and pursued more vigorously. Such efforts would allow the government to look into long-term measures in dealing with not just pseudo news but also all other forms of hybrid threats presented by the Internet.

Countries like China - known for their fierce online censorship - have been suspected of secretly hiring about two million individuals to weigh in on social media debates on behalf of the government. But these government employees do not appear to engage in constructive debates but in infusing onto social media sites information that praises the government, and its achievements, thereby overwhelming users engaged in other useful debates. Ethiopia's planned social media army must distance itself from such unhelpful engagements as this would further distort the flow of information, burden legitimate speech, and ultimately reinforce pseudo news. The aim should rather be to counter falsehood by presenting the public with truthful information based on reliable and verifiable facts, than to dictate the truth.

Further, the government must adopt clear rules by which measures such as blocking of websites, Internet shutdowns or even offensive or defensive cyber operations are taken for legitimate purposes. The procedures by which websites are assessed for filtering, the body responsible for such assessment and an oversight mechanism by which requests for blocking or other measures could independently b e assessed must be clearly spelt out by law. In the absence of transparent rules, these measures risk impinging upon human rights enshrined under international and domestic laws, such as the right to freedom of expression, the right to privacy and due process rights. Transparent and accountable procedures also avoid unnecessary but damaging diplomatic blows and image tarnishing reports of human rights groups.

Furthermore, the threats of pseudo news and deception could barely be addressed unless the government put in place a dedicated and well-equipped institution that monitors, assesses and determines websites or social media accounts that pose real threats to the country. Useful lesson could be drawn from the recent experience of other countries. As early as 2002, South Africa has established a body called Cyber Inspector with broader powers under the Electronic Communications and Transactions Act of 2002. Cyber Inspectors are empowered to monitor and inspect any web site or activity on an information system in the public domain and report any unlawful activity to the appropriate authority and to conduct searches and seizures to prevent or tackle illegal activities on the Internet with court warrants.43

With the proper regulatory and procedural safeguards as well as an oversight mechanism, a dedicated body could be installed within Ethiopia's INSA to deal with matters of pseudo news and deception campaigns. This would make sense as the Agency is responsible for coordinating the country's cyber response against all forms of threats posed in the cyber realm. Of statutory powers of INSA, its authority to take measures to counter all forms of cyber threats, collect, analyze and disseminate information on trans-boundary cyber threats to national security as well as power to conduct cyber operations makes it the right institution to deal with menacing hybrid threats in cyberspace.

Another crucial practical measure is to engage in raising awareness of the public about the ills of problematic content on the Internet. Most of the rogue web culture flourishing in the Ethiopian cyberspace is a result of lack of awareness about the legal and ethical consequences of some social media activities. This is understandable given that the Internet is a recent phenomenon in Ethiopia but it must carefully be addressed by teaching ethical use of social media. The best way to deliver this is through already existing subjects like civic and ethical education. Didactic measures about Internet etiquettes starting from primary schools would significantly reduce rogue web culture among the gullible youth. Responsible use of social media or other web platforms - which could very well be attained through awareness raising measures - is crucial in eroding the rein of pseudo news and deception.

All the above measures are essentially local which the Ethiopian government could achieve on its own accord. But that is not enough to address the matter fully. The global nature of the Internet and Internet firms such as Facebook and YouTube makes national measures half full. This is more so because most of the problematic content targeted at Ethiopian users emerge from overseas particularly from some groups of the Ethiopian diaspora. International cooperation mechanisms, both with Internet firms and states where some of the perpetrators reside must be sought. This would permit targeted measures against perpetrators rather than indiscriminate measures such as blocking sites or shutting down the Internet.

Recent developments, especially the dialogue with American State Department officials on how to counter hate speech on the Internet is encouraging. The government must further seek collaboration with other countries as well as Internet firms that have strong user base in Ethiopia. Useful lessons could be drawn from the European Commission, which has recently joined forces with big tech firms, such as Facebook, to jointly deal with extremist and hate speech in online platforms through a co-regulatory mechanism. The

Premier’s unprecedented frustration expressed at a global stage should serve as a genuine motivation for an effective, efficient and legally defensible response to the „pseudo news‟ phenomenon. In present day Ethiopia, where destructive, activism‟ is as fashionable as ever, robust policy, legal and institutional mechanisms must be put in place to tame the rising rogue web culture.

4. Conclusions

This is more so given that hybrid threats such as deception campaigns are increasingly posing threats to national security worldwide. That some members of the diaspora actively engaged in these campaigns are apparently working with foreign state actors makes the matter more of a national security concern. This makes INSA a more pertinent body in this particular scenario.

Measures taken to tackle threats to internal security must, however, not open the door for an overreach. Powers of institutions charged with such powers must be upended with an oversight mechanism in the form of judicial or, at least ministerial oversight. INSA already has the power to launch cyber operations by its own motion -and based on a request from the federal and state governments- but without judicial oversight. This must be reformed to require some form of independent oversight so that measures do not overrun fundamental rights and freedoms. With a proper oversight and accountability mechanism - and of course proper capacity building - introduced into the present regime, INSA could be a useful body to coordinate the country’s efforts towards tackling emerging cyber threats.

Beyond this, the government must also take some practical measures that reinforce the above measures. One important practical measure is to support the local independent media to engage in professional journalism. This would significantly aid in countering deception campaigns as the rise of pseudo news and deception is attributable partly to the lackluster approach of the mainstream media to the truth. With reliable information from trusted media organizations, social media users are less likely to be allured by pseudo news. Pseudo news could significantly be countered with authentic news. The government support to the media could take both hands on and hands off forms.

On top of building the capacity of the media, the government should comply with requests of the media for information. The government’s apparent heavy- handed approach towards the media must be reversed, and the relationship must be built on a new ground. Measures that tend to pull the media towards extreme views must be eased to allow a balanced, impartial and professional journalism that purveys for the public good. Instead of seeing the media as the opposition, the government must develop trust and thick skin to harbor criticism. This, of course, does not absolve the media from responsibilities to distance themselves from practices that undercut their reliability, impartiality and loyalty to public interest. More so in the case of the state-run media, which are misguided, approach has actually lent weight for the spread of distorted information on the web. The state-run media may not have been engaged in deception - or may not have run pseudo news as such - but it has clearly been under-informing the public. This has allowed for it to be overrun by „pseudo news‟. In the campaign to reclaim the truth in public discourse, government must reorient its self- inflicting use of the public media. Reclaiming the truth must start with allowing the public to reclaim its media that serves the interest of all. A truly public media that professionally, impartially and independently serves the interests of all voices will have the potential to considerably overcome the falsehood mill easily and effectively.

References

[1] Daniel Berhane, *Ethiopia: Hacking Team Irked by INSA‘s _Reckless and Clumsy Usage‘*, (Horn Affairs, 9 July 2015).

[2] Kinfe Micheal Yilma, *Developments in Cybercrime Law and practice in Ethiopia*, Computer Law and Security Review.

[3] Kinfe Micheal Yilma, *Mollifying the Web in Ethiopia, Matching Practice to Policy*, Horn Africa Bulletin.

[4] Kinfe Micheal. (2015). Fake news and its discontent.

[5] Minale Gedamu. (2010). The Quest for peace.

[6] Paul Schemm, “Ethiopia Shuts Down Social Media to Keep from „Distracting‟ Students”, The Washington Post, (13 July 2016),

[7] Ronald Deibert *et al*, Access Denied: The Practice and Policy of Global Internet Filtering, MIT Press, (2008).