HORN OF AFRICA BULLETIN

March-April 2017 Vol 29 Issue 2

Beyond Keyboard Warriors & Surveillance: Social Media Impact on Peace and Conflict in the Horn of Africa

Contents

The Horn of Africa Bulletin is a publication of the Life & Peace Institute

Editorial information
This publication is produced by the Life & Peace Institute (LPI) with support from the Bread for the World, Swedish International Development Cooperation Agency (Sida) and Church of Sweden International Department. The donors are not involved in the production and are not responsible for the contents of the publication.

Editorial principles
The Horn of Africa Bulletin is a regional policy periodical, monitoring and analysing key peace and security issues in the Horn with a view to inform and provide alternative analysis on on-going debates and generate policy dialogue around matters of conflict transformation and peacebuilding. The material published in HAB represents a variety of sources and does not necessarily express the views of the LPI.

Comment policy

All comments posted are moderated before publication.

Feedback and subscriptions

For subscription matters, feedback and suggestions contact LPI's regional programme on HAB@life-peace.org
For more LPI publications and resources, please visit: www.life-peace.org/resources/

ISSN 2002-1666

About Life & Peace Institute

Since its formation, LPI has carried out programmes for conflict transformation in a variety of countries, conducted research, and produced numerous publications on nonviolent conflict transformation and the role of religion in conflict and peacebuilding. The main focus of our work has been on Africa, with the Horn of Africa Programme being established and well-known in the 1990s, not least our work in Somalia. Other initiatives have been carried out in Congo-Brazzaville, Croatia, Sri Lanka and East Timor. We have strengthened the capacity of our civil society partners to address the conflicts in their own context, in some of the most difficult and war-torn countries.

Currently, we run conflict transformation programmes in the Horn of Africa and Great Lakes regions in partnership with local civil society organisations and universities in Somalia, Sudan, Ethiopia, Kenya and the DRC. There is also a common programme including publications, policy work and methodology design based in Sweden.

State fragility, authoritarianism and stalled or on-going democratisation processes, all of which in some ways define the African condition, makes Africa an interesting test case for the impact of the internet and social media on the dynamics of conflict, peace and political transformation. While social media platforms had arguably been assigned an outsized role in the outbreak and unfolding of the 'Arab Spring' which began in North Africa, the initial euphoria and enthusiasm regarding the emancipatory potential of social media has since cooled off appreciably. Developments in Libya and Egypt coupled with the masterful exploitation of social media platforms by 'extremist' groups for recruitment and propaganda purposes has underlined the inherently Janus-faced nature of social media platforms, a point underscored by several articles in this issue of the HAB.

The panoramic article by Desta reviews the Information and Communications Technology for Peace (ICT4P) literature on the Horn of Africa (the Horn) and showcases the varying levels towards which peacebuilders in the Horn have been able to exploit the internet and social media for conflict transformation and peace-building. His article shows that it is Kenya, the country with the highest internet penetration in the Horn, where several social media tools have been developed for conflict management and conflict transformation. On the other hand, the Ethiopian case is noteworthy for initiatives such as the WoredaNet, SchoolNet, etc. which have utilised the internet for socio-economic programs. The article by Omanga is an interesting piece which focuses on two cases where social media tools were deployed to enhance community policing and also to enable grassroots political deliberation. The empirically rich article by Omanga's explores the potential of social media to improve governance at the local level and as a tool to expand political participation and provides valuable lessons for the rest of the Horn. His article shows how the internet and social media have allowed actors and citizens to transcend the limits of traditional channels and processes of political participation.

In much of Africa where independent traditional media (radio, TV, and print media) are either absent or operate under tight constraints, the internet and social media can acquire an outsized importance and impact creating new channels of interaction and communication and enabling those who were previously 'quiescent' or 'detached' to participate in the public sphere. Across Africa and more so in the Horn social media platforms provide access to information and news outside the strictures of the authoritarian state and provide what little space there is for relatively autonomous debate and discussion. Interestingly, there is a growing tendency whereby the messaging and narratives articulated in state controlled traditional media are increasingly being challenged by counter-narratives and discourse generated in social media. Social media has also emerged as a key site for opposition ideological and organisational mobilisation against governments in power as underlined by recent events in Ethiopia, Uganda, Sudan, and Eritrea. In response, governments across Africa, in Egypt (2011), the Democratic Republic of Congo (January 2015), the Republic of Congo (2016) and closer to home in Ethiopia, Uganda, and Kenya have also utilised internet restrictions and in more extreme cases imposed full-fledged shutdowns of the internet in the context of electoral contests or large scale protests. A related development has been the growing expansion of legislation and policies in relation to the cyber realm including social media, that have the general goal of expanding state control over the internet and social media content, and penalising individuals and content providers producing content deemed 'offensive' or threatening to national security.

However, the dual nature and effect of social media alluded to earlier remains critical in terms of understanding, the correlation between social media activism and conflict, stability and peace, above all in the Horn of Africa. The articles by Michael and Carver focusing on Ethiopia

and South Sudan respectively, showcase the potential for social media activism to be exploited to generate 'fake news' and incite hatred and conflict. Michael's article underlines the tendency towards the emergence of the cyber-realm as a field of political contestation coupled with the attendant process of the securitisation of the cyber-sphere. Carver's article on the South Sudan at the same time shows how social media activism and its effects on peace and conflict in the Horn of Africa is inextricably linked to processes such as migration and the emergence of Diaspora communities coupled with the advent of satellite television and internet enabled money transfer schemes.

The article by Thomas focuses on internet shutdowns in the Horn which interestingly debunks the conventional wisdom that holds governments as solely responsible for internet shutdowns. His article discusses cases where internet service providers (ISPs) have been forced to cease their operations based on threats or actions by governments outside the Horn or 'extremist' movements.

The articles in this issue of the Horn of Africa Bulletin, in spite of their divergent thematic and geographical focus, emphasise certain themes: the inherent contradiction exemplified in the immense potential of the internet and social media for new and emancipatory politics coupled with their instrumentalisation to incite conflict and hate; the process of expanding state regulation and surveillance over the cyber realm which at the same time is being countered through recourse to tools and platforms designed to evade control. A recurring theme in several articles is the so far underutilisation of social media platforms and tools for peacebuilding, with the partial exception of Kenya.

Readers of this issue of the Horn of Africa Bulletin should also be aware that there are a few questions raised by the articles that have yet to be adequately answered. A key issue centres on the statistics on levels of internet penetration in the HoA at present. Several articles cite widely varying and contradictory figures for internet penetration in the Horn which suggests that there is a need for further research and more rigorous data.

The articles in this issue of the Horn of Africa Bulletin are not only topical in that they discuss a subject which will assume growing importance in the years to come with expanding internet access across the region, but also shed light on what is still a little studied area.

Demessie Fantaye, Editor

ICT4Peace in the Horn of Africa?

By Tedla Desta

The ICT4Peace Literature

The pioneer of peace studies Johan Galtung (1996) proposed two types of peace: negative peace meaning the absence of violence and positive peace where there is coexistence, restoration and sustainable absence of violence.[i] Direct violence is traceable violent action and indirect (structural) violence is violence rooted in the social, economic, or cultural conditions prevailing within or between societies. Nonviolent conflict resolution or peacebuilding studies have now diversified with branches on peace economics, peace journalism, peace and justice and so forth. With the rise of Information Communication Technologies (ICTs)[ii], the new field that integrates ICTs with international economic development has emerged and is known as ICT for Development or ICT4D. In early and mid 2000, capital D started to be succeeded by the big P, ICT for Peace (ICT4P) inclusive of new techno tools, the Internet and Social Networking Sites (SNSs) such as Facebook, Twitter, LinkedIn, YouTube, Instagram, blogs, and various other local online forum. Despite the growing hype about ICTs in general and for the purposes of peacebuilding in particular, some authors raise a moral question about the oxymoron application of ICT tools for conflict resolution when the very raw materials of our technological gadgets are sourced or are made through conflict and from conflict prone regions of the world.[iii] A recent study on the role of ICT in peacebuilding by Tellidis & Kappler (2016) came up with a conceptual framework of ICTs as tool for peacebuilding. The authors point to three distinct scenarios: "the hegemonic use of ICTs, their marginalisation or, alternatively, their use as a representative, participatory tool." They conclude from their study that ICTs have to be viewed in "a continuous tension between disempowerment, marginalisation and empowerment, and activated in different ways by the agents controlling and using them. This perhaps suggests that ICTs have, in the field of peacebuilding, a lesser determining role than commonly expected – they represent but a tool which needs to be activated and used by those capable of and willing to use it."[iv]

There are two main schools of thought regarding the role of technologies in peacebuilding. The techno-optimists, who see the positive, educational, and emancipatory potential of these tools these include academics, activists, the innovators of the technology themselves or groups with vested interests such as financers and the 'cyber-sceptics', who believe that they could be used for exploitation, surveillance, cybercrime, and extremism purposes.

The techno-optimists maintain that lack of information leads to misunderstanding and violence, therefore, the availability of large data and information defuses rumours and misinformation that could lead to conflict. They also argue that the phases of the conflict are important. According to Hattotuwa (2004) ICT interventions can be more effective when used for peacebuilding after a ceasefire or peace agreement. This analysis is contrary to the perspective purported by Tellidis & Kappler, who find that widespread

information is causing conflicts. Pierskalla & Hollenbach (2013) also found that by statistically analysing spatially disaggregated data on cell phone coverage and the location of organised violent events in Africa "the availability of cell phone coverage significantly and substantially increases the probability of violent conflict."

The ICT4Peace study and literature is not yet charted but it is destined to be a field of greater interest due to both the fast development and use of ICT tools around the world and the increase of ICT related conflicts and insecurities. Specifically, when it comes to the literature and research for the Horn of Africa (the Horn), the very few articles available are based on projects in Kenya and these articles focus on the anecdotal application of technology for conflict prevention or a description of their application rather than evidences and impacts in sustainable peacebuilding programs or post-conflict reconciliation and mediation[v]. In a region, where almost all countries currently are affected by low and high intensity conflicts, where humanitarian crises are rampant, and the Internet, SNSs and mobile phones have become critical in conflict and security, reading the regional nexus is quite relevant and important.

Case Studies from the Region

Kenya, with a 68 percent Internet penetration, only preceded in the region by South Sudan at 71 percent, is broadly viewed as a country aspiring to build a knowledge or Internet economy[vi]. In the region of repressive states, Kenya has been attempting to be a place of liberalism and ICT innovation. In Ethiopia, with a 4.5 percent penetration the ICT and Internet sector is heavily government monopolised and controlled, which is very similar to the Rwandan model. Somalia with a 6.1 percent penetration is often led by the private sector and individuals owning and leading technological development.

Cases in the Horn show that the Internet has been used for national economic developments or what could also be called *control* by governments and to self organise and protest government repression by citizens.[vii] In Ethiopia, the government launched the largest wide area networks (WANs), the WoredaNet, which connects over 600 local administrative districts in the country with broadband Internet access for local administration efficiency and the SchoolNet to connect more than 550 high schools in the country to access video-based distance education.[viii] Similar projects such as AgriNet and RevenueNet have been launched but there are no cases of a *PeaceNet* or *ConflictNet* launched in the whole Horn region perhaps other than the Conflict Early Warning and Response Mechanism (CEWARN) project of the Intergovernmental Authority on Development (IGAD) region. CEWARN largely focuses on conflict early warning and analysis in the Horn IGAD member states using a software tool – *the Reporter* that collects weekly incident and situation reports. The Techno-sceptics often argue that SNSs are being used for surveillance or what the optimists might call early warning and intelligence missions, which the former deem invasive of the privacy and security of citizens. In the case of, at least, the Horn pastoralist and rural conflict prevention programs, the CEWARN has showed some value.

There are some individual cases showing the use of ICT for peacebuilding from Kenya.

Una Hakika, is run by Canadian non-governmental organisation (NGO) focusing on preventing genocide and atrocities, a violence prevention program that uses mobile phones to dispel rumours and misinformation in Kenya's Tana Delta region, and the *Sisi Ni Amani* project, which offers community training on peacebuilding.[ix] *Ushahidi* is crowd-sourcing software developed after the 2007 post election violence in Kenya to collect and map crises information, was extended and applied to map crises in Gaza, Afghanistan, Haiti, Chile and to monitor the 2016 election in the US.

In Ethiopia, Kenya as well as countries in the region the use of hashtags (#) for campaigns and protests has become popular. The #OromoProtests, #AmharaProtests, #OccupyHarambeeAve or #FeesMustFall were protest (sometimes referred to as conflict inciting) and campaign hashtags with a short-term goal and recognisable impact. There is a noticeable absence of either short-term or long-term peacebuilding orientated hashtags applied for peacebuilding and conflict resolution objectives. It is also not yet possible to witness if hashtag campaigns of peacebuilding could bring about sustainable peace or even end conflicts.

Since 2013, several African governments have disrupted or shut down Internet or electronic communication due to elections or anti-government protests. Since the Arab Spring wound down, Ethiopian Prime Minister Hailemariam Dessalegn became one of the first leaders to officially disparage social media at the United Nations in September 2016 blaming it for the local protests. The anti-government protests in Ethiopia in 2015 and largely of the 2016 were allegedly mobilised, coordinated, executed and communicated by local and Diaspora-based activists using social media tools. The declaration of a State of Emergency by the Ethiopian government in October 2016, the shutting down of social media helped to de-escalate the protests as well as the usefulness of the social media for opposition activists.

A study by a local South Sudanese peacebuilding organisation published in 2014 found that social media particularly Facebook users instrumentally 'facilitated' the 2013 conflict in the country.[x] In October 2016, the South Sudan government threatened that it could cut off access to social media and other online mainstream media "for circulating 'false information' about President Salva Kiir's health status."[xi] In 2016 social media activists in the Sudan organised a successful stay-at-home strike opposing the government but the Sudanese president Omar al-Bashir boasted that his government "will not be overthrown by keyboards" and dared the activists "to come out on to the streets."[xii] The events in Sudan suggest that the SNSs indeed can cause a headache to regimes but other factors are necessary for them to be fully effective. This overview of the Sudan, Somalia (except a mobile phone SMS assessment), South Sudan[xiii] (a developed #PeaceApp and peace messaging courses, whose impact has not yet been evaluated), Eritrea, Djibouti and Ethiopia did not come across unique cases where the Internet or SNSs tools, software or projects were applied for peacebuilding.

These eventualities indicate that the Internet and SNSs could be very effective tools for liberation and insurgency however; they could also be employed to impede the successes of popular causes as governments or Internet Service Providers (ISPs) can easily shut

them down. This means SNSs seldom lead to political changes or overthrow regimes unless they are supplemented by practical on-the-ground human actions.

So far the review of the secondary materials and empirical cases of ICT4Peace have not shown evidence and the impact of the Internet and SNSs used for structural, positive peace and peacebuilding projects in the HoA region other than few descriptive and anecdotal cases. The conclusion draws on the limited evidence of a nascent research field and inclines to the findings of Tellidis & Kappler that for peacebuilding, ICTs represent a tool "which needs to be activated and used by those capable of and willing to use it." It is also worth noting that SNSs are in a process of continuous innovations and redevelopment, therefore developing a permanent theory and analytical framework or reaching at a conclusion may not be an uncomplicated undertaking. Users, trends, and participation are high during crises, special events, and Breaking News announcements on SNSs, especially in the Horn, and these features gradually reduce or calm in times of "no news."

Future Scenario Analysis

- The digital divide narrows and more people would be online and the Horn's social media scene continues to be a chaotic space. Some countries recruit and deploy a 'social media army' to dilute and suffocate independent and protesting voices with pro-government and 'anti-insurgency or protest messages and malwares'. In line with this, the digital insecurity or vulnerability of citizens and activists will become a focus of intervention as well as huge investment and control by governments' cyber security agencies and Intel branches. Horn governments will follow the Chinese model of highly controlled Internet and SNSs governance and policy leading to the 'hegemonic use of ICTs and then their marginalisation'.
- There are hopes and opportunities for the development of digital peacebuilding, digital mediation and digital security in the region. This means the cyberspace will become a place of macro and micro conflicts between major non-state ICT actors, attackers and hackers versus state actors and multinationals or between 'Internet anarchists and controllers', between individuals and small groups on the cyberworld such as SNSs. These conflicts could be follow ups of the offline tensions and conflicts but could also be new digital conflicts and insecurities over problems that have entirely emanated on the digital world and could best be solved using innovative digital/cyber peacebuilding or mediation programs. Innovation, therefore, will be the catchword in the ICT for peace nexus in the region
- As much as these technologies could be threatening or forcing reforms of authoritarian regimes in the region (especially with the prospects of Free Basics or *Internet.org*), they may also likely save and prolong the lives of dictators. Regimes could use them to progress their political ends, intelligence or during disasters or coups – for example recently Turkey's president Tayyip Erdoğan used FaceTime to reach his supporters from outside Turkey calling them to successfully take to the streets and crush down the coup.
- The rise of fake news on SNSs is also likely to be a cause of concern with the increase of tribalist, ethnic, religious radicalism and extremism themed discourses and conflicts.

Tedla Desta (PhD) is a Research Assistant at the Edward Kennedy Institute for Conflict Intervention in Maynooth University, Ireland. His teaching and research areas are interdisciplinary but with a focus on ICT4D, peacebuilding, mass media, and development in its broader understanding. Tedla is also a SARChI on Innovation and Development *Research Associate*, Tshwane University of Technology, Pretoria, South Africa. He can be reached at dteklet@tcd.ie.

Sources

[i] *Galtung, J. (1996) Peace by peaceful means: Peace and conflict, development and civilization.* London: Sage Publications.

[ii] Hamelink's defines ICTs as "all those technologies that enable the handling of information and facilitate different forms of communication among human actors, between human beings and electronic systems, and among electronic systems" (Hamelink, 1997: 3). For more see Hamelink CJ (1997) "New information and communication technologies, social development and cultural change" *UNRISD Discussion Paper No. 86.* Geneva: United Nations Research Institute for Social Development

[iii] Tellidis, I & Kappler, S. (2016) "Information and Communication Technologies in Peacebuilding: Implications, Opportunities and Challenges", *Cooperation and Conflict* 51, 1, 75-93.

[iv] ibid.

[v] For more see Gagliardone, I., Kalemera, A., Kogen, L., Nalwoga, L., Stremlau, N., & Wairagala, W. (2015) "In Search of Local Knowledge on ICTs in Africa. ICTs, Statebuilding and Peacebuilding in Africa", *Stability Journal*, retrieved from http://repository.upenn.edu/africaictresearch/

[vi] Outside its capital, Nairobi, Kenya is building the Kenyan equivalents of Silicon Valley, the Malili Technopolis and the $14bn *techno city*, Konzo Tech City. In 2016, Kenya allocated KES 6.1 billion for ongoing ICT Projects. Kenya and South Africa lead the continent in mobile commerce. Kenya's ICT policy aims to boost ICT's GDP contribution to 8 percent and create 180,000 jobs to emerge as the ICT hub of Africa.

[vii] Major e-government, fiber optic and ICT development projects in Kenya and some countries of East Africa in general helped make life easier, better and efficient. Yet, the Internet as well as SNS have been exploited by governments and non-state actors to control, spy and harass dissidents and political targets respectively – prime examples are several Ethiopian digital dissidents at home and in the Diaspora who have been unfairly accused of treason and terror.

[viii] For more see Lemma, L. Mesfin, B. & Salehu, A. (2011) "Sustainability of E-Government project Success: Cases from Ethiopia", *AMCIS 2011 Proceedings – All*

Submissions. Paper 411. http://aisel.aisnet.org/amcis2011_submissions/411"

[ix] Shields, C.M. (2014) "ICTs in conflict early warning – possibilities and challenges", *Insight on Conflict*, retrieved from https://www.insightonconflict.org/blog/2014/07/icts-conflict-early-warning-possibilities-challenges/

[x] For more see Insight on Conflict https://www.insightonconflict.org/blog/2014/10/role-social-media-south-sudan-crisis/

[xi] For more see Sudan Tribune http://dev.sudantribune.com/All/Article/Index/10-13-2016-S.-Sudan-threatens-internet-shutdown-over-Kiir-s-health-rumour/60520

[xii] For more see The Guardian https://www.theguardian.com/global-development/2017/jan/11/sudan-social-media-drive-for-civil-dissent-boosts-hopes-of-change

[xiii] A South Sudanese youth founded Junab Games to produce peacebuilding video games in 2017. One of the games known as Salaam (peace) is a game in which the gamer must destroy symbols of war to [to promote peace). This is still a very tender project to evaluate. For more see http://www.aljazeera.com/indepth/features/2017/02/building-peace-video-games-south-sudan-170209114717744.html

Mollifying the Web in Ethiopia: Matching Practice to Policy

By Kinfe Micheal Yilma

Ethiopia is one of the least connected countries in the world. Although Internet was introduced in Ethiopia as early as 1997, the level of Internet use density remains low.[i] With recent huge investments – reportedly accounting around 10% of the country's Gross Domestic Product – in the country's Information and Communication Technologies (ICT) infrastructures, the level of Internet use is gradually growing. Provision of public and private sector services increasingly rely on Internet protocol based technologies. Ethiopia also has one of the largest social media user bases in Africa. It is now evident that the use of and reliance on Internet – and allied technologies – is set to grow in the coming years.

This growing reliance on Internet-enabled technologies, however, exposes the country to various forms of risks such as threats of cyber-attacks against the country's critical infrastructures that are crucial for provision of vital public and private services. Ethiopia is not new to the world of cyber-attacks from overseas. Hundreds of hacking and defacement of government websites occurred in the past decade but these had limited economic or political ramifications at the time.[ii] This appears to be changing over time, however. More recently, the country has been gripped by reports of an attack against a major private bank from which a huge sum of money was stolen.[iii]

Recent turn of events have also signalled threats to peace and security that the country is bound to face as it moves to fully join the information society. The anti-government protests in some parts of the country – mediated largely through social media platforms – had shaken the nation's stability to its core. The street protests were initially accompanied by random hacking and defacement of government websites thereby opening up a new form of airing dissent – *hacktivism*.[iv] This later grew into what now come to be referred to as 'hybrid' cyber-attacks, in the form of 'disinformation' campaigns and circulation of 'fake news' in social media platforms.

An example of such misleading or false information circulating on social media was the bogus accusation that the cause for a deadly stampede in October 2016 in Bishoftu was the unprovoked police shooting from a helicopter on people attending a festival, had perilous consequences.[v] This led to 'five days of rage' by misinformed youth against public and private properties ultimately prompting a state of emergency. The declaration of the emergency – which still is in place – for the first time in a quarter of a century, speaks to the emerging significant impact of ICTs and social media will have on the stability of the nation.

What made these social media mediated violent protests significant is the key role that the social media are poised to play in shaping the domestic peace and security dynamics in Ethiopia. With increasing access to the Internet, social media will soon be an important variable in gauging Ethiopia's internal stability. With the apparent

militarisation of cyberspace – and of course visible signs of cyber conflict, threats to the country's critical Internet infrastructure from adversaries appear to be insidious. Moreover, the fact that most of the 'hybrid' attacks emerge from overseas by actors actively working with the hostile government regime in Eritrea makes the situation more precarious.

Internet Policy Making in Ethiopia

Recent developments should not, however, be a reason to adopt a pessimistic vision of the Internet or social media. Over regulation – or an overly securitised vision of the fledgling Ethiopian new media landscape – might stand in the way of properly exploiting the benefits that these technologies offer. What is needed, instead, are well thought out policy principles and well equipped institutions to enforce them. Of course, the Ethiopian government has generally been progressive in rolling out relevant policy and legal instruments to effectively address the Internet and threats that its (mis)use could pose. Ethiopia issued its first national ICT Policy in 2002, which has since been updated in 2009 and 2016.

The nation's ICT policy mandates the need to put in place the requisite legal and institutional framework to exploit the benefits of ICTs while also countering their possible threat to national peace and security. A fairly elaborate Cybersecurity Policy has also been adopted by the Council of Ministers in 2011.This policy updates the country's Foreign Affairs and National Security Policy (2002) in the context of the digital space, and underlies that information security forms an integral part of national security, public peace and security.[vi]

These policy instruments are translated into a number of legal instruments, and several others are in the offing. More recent pieces of legislation include the Telecom Fraud Offense Proclamation (Proclamation No. 761/2012) and the Computer Crime Proclamation (Proclamation No. 958/2016). The telecom fraud offense legislation – contrary to the narrow scope that its nomenclature might suggest – covers a broad range of matters including offenses that concern domestic peace and security. Indeed, the law explicitly stipulates that telecom fraud, over and above the economic losses it results in, may threaten the national security of the country.[vii] The cybercrime law likewise penalises a number of crimes that threaten peace and security in general and cybersecurity in particular.[viii]

Institutions with statutory powers to implement and enforce these policies instruments have also been installed. A principal such government agency is the Information Network Security Agency which is tasked, *inter alia*, to protect the country's critical infrastructures from possible attacks.[ix] The National Intelligence and Security Service's general power to collect intelligence on matters of national security including those of cybersecurity makes it another important body in the area.[x] The Federal Police is tasked to investigate crimes relating to information network and computer systems, alongside its general role of maintaining peace and security.[xi] Other bodies such as the former Ministry of Justice – now the Federal Attorney General and the

Ministry of Communication and Information Technology also assume some roles in dealing with threats to national peace security posed in the cyber front. At a judicial level, the Federal First Instance court has a subject matter jurisdiction to adjudge cases relating to ICTs in general while cases under the recent cybercrime legislation fall under the jurisdiction of the Federal High Court.[xii]

Matching Practice to Policy

Ethiopia's progress in the policy field does not, however, match well with the practice. Despite relatively modern and comprehensive policies and laws already in place, little appears to have been achieved in terms of translating these policy principles into actions. The government often resorts to piecemeal and reactive measures in dealing with emerging cyber threats. This, in turn, has substantially robbed them of efficacy, efficiency, and sustainability in aptly overcoming the ever growing cyber threats. The legality of some of these measures – both under domestic and international law – is mooted. A few examples illustrate the rift between policy and practice.

One is that the Ethiopian government increasingly relies on temporary closure of social media sites – and sometimes nationwide Internet shutdowns, blocking, and filtering of certain websites – to quell dissent channelled via the web. These measures have repeatedly been taken during the recent protest in some parts of the country. Besides the legality issues that such measures bring up as well as their significant effect on the economy, it is doubtful whether these measures have resulted in sustainable peace in the country. Similar rounds of social media mediated violence could occur at some point. With increasing use of circumvention tools, blocking of websites is already proving futile. And that Internet shutdowns have broader legal, economic, and diplomatic ramifications makes their utility lower. In the course of implementing these measures, there were also instances of major technical errors affecting the whole Internet system, a fact admitted even by a government spokesperson.

The recent unrest has also prompted the government to consider creating what it calls a 'social media army' to counter circulation of misleading information and falsehood in social media. To this effect, the Council of Minister's has adopted a Regulation that establishes an Institute that would train members of this 'army'.[xiii] From all that we know so far, it appears that the government is resorting to similar measures taken in other countries such as Iran and China of infusing social media platforms with users loyal to the government. By running ideologically polemic information on the web, such methods do more harm than good by burdening free flow of information and expression. Instead of overcoming falsehoods that upset the domestic peace matrix, chances are that 'social media soldiers' might distort the truth and reinforce the real threats of 'fake news'.

Another measure taken by the government is to deploy Internet surveillance tools against persons believed to pose threats to national security. This path does not seem to be taking the government a long way in ensuring domestic peace and security as recent developments suggested that these cyber tools have not been used judiciously. The

government is also known to be taking a heavy-handed approach against the fledgling community of local bloggers. Prosecution of these bloggers for vague crimes including a controversial charge for using encryption tools has been unprecedented. [xiv]The government's goal of maintaining peace and security could have been very well reinforced by tolerating civil discussion in online platforms. Heavy-handed approaches by the government against peaceful dissenters is likely to push them to the extreme and take the path of violence and even disinformation campaigns, which then threatens peace and security.

Maintaining domestic peace and security – including cybersecurity – requires a coordinated, sustainable and goal-oriented approach towards the Internet and its potential for good or bad. In translating the goals set out in the above policy documents, the government must enhance the institutional capacity of all bodies tasked with regulating the Ethiopian web. The technical nature of the Internet requires qualified experts in investigation, prosecution and even in adjudication processes. The global nature of the web also dictates a reliable international cooperation mechanism including with regional bodies. As a prominent member of the African Union (AU), Ethiopia should even take the lead in ratifying the AU Convention on Cybersecurity and Personal Data Protection (2014), and engage towards realizing a robust regional cybersecurity regime.

While the recent move by the government to take the matter more seriously is a positive development, it is vital that the measures that will follow are well thought-out and pragmatic to ensure legality, sustainability, feasibility and efficiency. Pragmatic measures of pacifying the Ethiopian web will ultimately yield not only economically but also diplomatically. Ethiopia's leading role in regional peace and security efforts also makes it imperative, not only to maintain its domestic stability, but also to lead by example.

Kinfe Micheal Yilma is a Doctoral & Teaching Fellow at The University of Melbourne Law School, and a Lecturer-in-Law at Addis Ababa University Law School. His research interests and publications are in the fields of Internet law and policy, human rights and law reform. He can be contacted at kinfe.desta@unimelb.edu.au or followed on twitter @Ethiokinfe.

Sources

[i] A 2016 government figure caps the use density as at 12.5%. See "Ethio-telecom Soars with 10.9 Billion Birr Half-year Profit", *Addis Fortune*, 29 March 2016, available at http://bit.ly/2oR5S2R (Last accessed on 15 April 2017).

[ii] See Kinfe Micheal Yilma, "Developments in Cybercrime Law and Practice", *Computer Law and Security Review*, Vol. 30, No. 6 (2014):726-729.

[iii] See Dawit Endashaw, "North Korea-linked Hackers Target Ethiopian Banks", *The*

Reporter, 8 April 2017, available at http://bit.ly/2nOhF2B (Last accessed on 15 April 2017).

[iv] See Kinfe Micheal Yilma, "Hacktivism: A New Front for Dissent, Regulation", *Addis Fortune*, 14 February, 2016, available at http://bit.ly/2nV9HDx (Last accessed on 15 April 2017).

[v] For more on the "fake news" phenomenon in Ethiopia, see Kinfe Micheal Yilma, ""Fake News" and Its Discontents in Ethiopia", *Mekelle University Law Journal*, Vol. 5, No. 1 (2017) [Forthcoming], available at http://bit.ly/2oHEvHN (Last accessed on 15 April 2017).

[vi] See *National Information Security Policy of Ethiopia*, 2011, Para 1.1 (3).

[vii] See *Telecom Fraud Offence Proclamation*, Proclamation No. 761/2012, Preamble.

[viii] See *Computer Crime Proclamation*, Proclamation No. 958/2016, Art 14.

[ix] See *Information Network Security Agency Re-establishment Proclamation*, Proclamation No. 808/2013 *cum* Council of Ministers Regulation No. 320/2014.

[x] See *National Intelligence and Security Service Re-establishment Proclamation*, Proclamation No. 804/2013.

[xi] See *Ethiopian Federal Police Commission Establishment Proclamation*, Proclamation (as amended), Proclamation No. 720/2011, Art 6.

[xii] See *Federal Courts Proclamation*, Proclamation No. 25/1996 (as amended), Art 4(7) *cum* Art 15(1); see also *Computer Crime Proclamation*, supra n 8, Art 40.

[xiii] See "The Council of Ministers Adopts A Regulation Establishing Youth Development and Cyber Talent Institute", *Fana BC*, [Amharic: Author's Translation], 18 March 2017, available at http://bit.ly/2nV9HDx (Last accessed on 15 April 2017).

[xiv] See "Soliana Shimelis G.Mariam and 9 Others", *Ethio Trial Tracker*, 20 February 2017, available at http://bit.ly/2pWfLdw (Last accessed on 15 April 2017).

KENYA

Social Media, Community Policing and the 'Digitisation' of public participation in Kenya

By Duncan Omanga

Since the turn of the century, the mobile phone and the growth of the internet is changing how Africans interface with power. Scholars on Africa have shown how local participation in governance issues has been energised through these developments.[i] The Arab spring, which began in Tunisia in 2010 has stimulated increasing interest in how social media mobilises people and convenes publics in Africa.[ii] With visible shift in social media, especially in the explicit 'convoking logics' such as 'liking' 'friending' and 'following', the convergence of social media and mobile telephony is central to new debates on how digital publics are constituted in Africa. In the book, "Mobile Phones: The new Talking Drums of everyday Africa" the term 'revolution' is deployed to characterise the massive changes in Africa occasioned by the use and rapid spread of mobile telephones in the continent.[iii] These transformations are not merely limited to communication, but can also be observed in multiple domains such as the political, where they mediate between social individuals and groups, creating new forms of social mediation, where various kinds of agency emerge.

In Africa today, the use and impact of the social media are huge, to say the least. This situation has been bolstered by the increase in mobile telephony which has made access to the internet convenient and easy. According to a British Broadcasting Corporation's (BBC) report, the number of subscribers on the continent has grown almost 20 percent each year for the past five years, and it is expected that there are more than 735 million subscribers today in Africa. Meanwhile, huge submarine cable infrastructure has seen an increased growth of internet access in the entire continent.

According to the latest statistics from the Communications Commissions of Kenya, mobile phone subscriptions stand at slightly over 38.9 million out of a population of about 43 million people (87 percent). Additionally, a similar number of Kenyans have access or subscriptions to the internet (87.9 percent) and slightly more than half this number access the internet through their phones.[iv] It is the mostly younger subscribers in this category that have facilitated the meteoric rise of the social media in Kenya and the rest of Africa. The combination of social media and smartphones have 'liberated' and emancipated mediated communication from the centre (state and institutions) and given more agency to ordinary individuals insofar as political debate and action is concerned. In a context of political devolution, social media has become an important aspect of how citizens in Kenya mobilise, and how they, through both discourse and social action, imagine and reconstruct their relation to the state. Today, besides connecting friends and groups, social media has become an integral aspect of Kenya's social and political dynamics and has been effectively used in driving positive change like community policing, galvanising and channelling public discontent, grassroots political mobilisation.

In this article, I wish to highlight how social media has been deployed in the county of

Nakuru, in central Kenya first, by state actors to support community policing and second by ordinary citizens for the non-formal political deliberation at the grassroots. In both cases, I argue, social media provides specific affordances previously not available, which affects agency, grassroots empowerment and reproduces a more accountable local governance.

Social Media, Chiefs and Community Policing in Nakuru

The 2008 post-election violence in Kenya marked a watershed moment for forty-year-old Francis Kariuki. The school where he served as a head teacher was badly affected by the violence and he felt working directly with the locals would be a much better challenge. When a chief's job fell vacant in Lanet Umoja location, Nakuru County, he quickly turned in an application. But he was least prepared for the sudden shift from dealing with honest, innocent children to the rigours that comes with being in charge of the entire location of more than 30,000 residents. His job now includes chairing the local security committee with village elders, assistant chiefs, and opinion leaders. With two administration police seconded to him to ensure he executes his mandate he is loved and loathed in equal measure depending on who you talk to. He reports to the District Officer (DO) every other week although hardly a day passes before he makes or receives a call from the DO. More important, he must hold a *baraza* (open public meetings) at least twice, in a month. The more *barazas* he convenes the better for his resume. His adoption of Twitter as in interactive platform with members of his location was accidental. According to Chief Kariuki, the initial idea of getting onto Twitter was merely to send notifications of upcoming *baraza* meetings without the inconvenience and expense of pinning up public notices.

Chief Kariuki began constituting his initial Twitter 'followers' with the handful of *baraza* attendees who would occasionally peak at 150 people. At the *baraza*, he would show residents how to 'follow' him on Twitter. He assured them that the new initiative would allow access to the chief at all times with no costs on their part. While a few managed to subscribe to the micro-blogging site, the lack of internet enabled smart phones and the difficulty of navigating the social media for first time users was a challenge. But since almost everyone had access to a mobile phone however simple it was, he negotiated with a mobile network provider, who linked his Twitter account to a unique four-digit number which allowed his tweets to bounce off this number and instantly appear as a short message (SMS) to anyone linked to the four-digit number. Subscription to the four-digit number proved easy and practical. Villagers would only be required to send the message 'follow @Chief Francis' to this number and from then on would receive the Chiefs' tweets in the form of an SMS. Later, all his three assistants, Florence, Mundia and Maina joined Twitter (@AsChief Florence, @AsChiefMundia@ AsChiefMaina), and using the same code, all these platforms formed a network that changed local administration.[v] At present, Chief Kariuki has over 56,000 followers on his twitter handle. The assistant Chiefs have a combined following of over 3000 followers.

The use of Twitter and mobile phones for community policing in Lanet Umoja is a huge success. Usually, once a crime or an emergency occurs, the victim or a neighbour informs one of the chiefs through a text message, the Chief in turn, retweets to other chiefs and it is instantly shared. Twitter produces a space, or a ´digital baraza´ where speed, simplicity and immediacy converge to make potent tool for community policing. The platforms show a pattern of crimes and related emergencies that are reported and addressed instantly through group action. In the texts below for instance (in Kiswahili), the chief posts that a house belonging to one mama Gathoni is being burgled, he calls out the public to help, singling out those living in the area known as '*murunyu*', then the burglars, having most probably received the texts on their phones too, hurriedly leave the scene (Figure 1). Members rise from their sleep to help a neighbour in the full knowledge and assurance that a significant number of people will respond.

Figure 1 See translation [vi]

WhatsApp, Tweet-ups and Public Participation in Nakuru Local Governance

At well over sixty-years-old, Elijah Kinyanjui hardly fits the stereotype of the typical African blogger. A native of Nakuru town, Kinyanjui is a veteran journalist who has worked for all the notable media houses in Kenya as a print journalist and has, depending on who you ask, established himself as one of Nakuru County's most prominent bloggers. In early 2013, he set up the news blog 'Nakuru County Online', whose focus was primarily news relevant to the county of Nakuru. His experiment with local county news was in the spirit of Kenya's new constitution of 2010 that primarily sought to devolve the formal and informal structures and discourses of governance. According to Kinyanjui[vii], the newspaper failed due to technical issues. He transferred the blog to a Facebook page and renamed it the *Nakuru Analysts*, a name that suggested the deliberative objective of the page, and also its socio-political scope. Although the Facebook version of *Nakuru Analysts* still runs, it is not as politically sharp as its WhatsApp affiliate. According to information on the group profile, *Nakuru Analysts* was constituted as a WhatsApp group on 23 January 2015, with Elijah Kinyanjui, and Jane Kinuthia (Jenny) as administrators of the group. Following its successes in convening and bringing into being a digital public, where members engaged in what they felt were deliberative acts on the affairs of the county government, *Nakuru Analysts* was registered as a community based organisation (CBO) in December 2015 and interim

officials were elected to run the social arm of the organisation. A man named Hamisi Mutura was appointed Chairman, Jane Kinuthia became the group's treasurer, and Patrick Kinyua was its secretary.[viii] Elijah Kinyanjui remained the chief executive officer (CEO) of *Nakuru Analysts* in a non-electable capacity. According to interviews with the original founding administrators of the group[ix], the new CBO was to act as a bridge between discourse and action, or what is sometimes known broadly as 'Tweet-ups', where digitally convened publics meet face-to-face with the intention of actualising specific action (In Nakuru this includes such things as urban protests, fund raisers, and meetings summoned to encourage and 'anoint' specific political aspirants).

The *Nakuru Analysts* was envisioned as a digitally-convened space where ordinary citizens had an equal chance of posing relevant questions and getting the answers from the county officials concerned. Using his networks, Kinyanjui collected the contacts of the Governor,´County officials, County Cabinet Secretaries and elected members of the County Assembly, and linked them together with those of several opinion leaders, future political aspirants, business people, and professionals to form the *Nakuru Analysts.* Whilst the group comprised of a specific social category, the vast majority of current WhasApp members are ordinary engaged citizens of Nakuru County.

In the *Nakuru Analysts* WhatsApp group, debate is informed by both argument and comparisons with other counties that are perceived to be doing generally well, as a basis for evaluating the performance of the Nakuru county government. For instance, on 30 August 2016, a participant posted a picture of a famous refurbished public market in Mombasa County. The picture elicited praise for Mombasa Governor Hassan Joho, but also prompted debates on unfulfilled campaign promises in Nakuru County:

> ***Mike:*** *Comparing Kongowea Market and Nasher (local Nakuru county market) is like comparing day and night.*
>
> ***Elijah Kinyanjui:*** *Wow…it really puts Nakuru County government to shame for lack of a similar project.*
>
> ***Miguel:*** *Kongowea market used to be dusty place for campaigns and drug peddling, amazing transformation.*
>
> 31 August 2016 (Nakuru Analysts, 20:32-2038)

Often, the convergence of online news and social media, and the convenience of mobile phone nourish local debates and stimulate further comparisons between counties. These comparisons aid in the energising of local debates, and for calling to account of the county government.

> **Gitau**: **Can Nakuru Learn from Kiambu County? * The Kiambu government's Youth Affairs department has launched a mobile loan service called Mobiloan. Applicants will access it using mobile phone money*

transfer services. Governor William Kabogo on Wednesday said the county, through its Biashara Fund, has partnered with the Kenya Commercial Bank to make the service possible…Kabogo said the service will allow the youth, women and persons living with disability easy access to money to grow their businesses…..

Nono: *This is what we need in this county, but with an allocation of Kes. 65 million for youth and all this go to the construction of polytechnics it will remain a mirage unless KM is interdicted* (sic)

01 January 2016 (Nakuru Analysts, 1:57 -2:02 pm)

Nakuru Analysts remains a powerful space for the formation of a prototype digital public that is able to engage in the critical debates that matter to the locals. Often, not only does it call the county government to account directly through its dialogue with members of the county government, but the platform uses the digital space to explain and debate how county governments work.

Conclusion

While the constitutionally recognised spaces of participation and meaning making for ordinary citizens with regard to County governance and accountability are public participation forums, the popularity and vibrancy of WhatsApp groups like *Nakuru Analyst,* shows how digital publics are complementing, and often outdoing, other traditional, formal spaces of deliberation. At the same time, the affordances of digital media and the attribute of convergence allows Kenyan chiefs to repurpose and refashion the classic *baraza* and mobilise it for social action. In the case of Lanet Umoja in Nakuru, Twitter routinely summoned a public that acted corporately (to a degree) to the substance of the texts that constituted it. This active 'social action' went beyond a mere perfunctory attention, but imposed an urgent responsibility and obligation on citizens.

Thus, the use of Twitter by local chiefs in Nakuru and the powerful role played by WhatsApp groups in Nakuru town show how the affordances of social media combines with the convenience of internet enabled smart phones to empower ordinary citizens. This is attained through the capacity of social media to convene groups for specific action, and at the same time, the possibility of social media in facilitating a continuous conversation among a dispersed audience. This quality of social media, according to Clay Shirky, qualifies to be labelled a revolution.

Dr. Duncan Omanga is a lecturer at Moi University, Kenya and the head of the department of Publishing and Media Studies. He holds a Doctorate in Media Studies from the University of Bayreuth, Germany. Dr. Omanga was an African Peace Network (APN) Grantee in 2014. His research interests are on social media, democracy and digital publics in Kenya. He can be reached at ankodani@yahoo.com.

Sources

[i] Gagliardone, Iginio et al. “Stability: International Journal of Security and Development.” *In Search of Local Knowledge on ICTs in Africa* 4, 2015; Mudhai, Fred, Wisdom Tettey and Fackson Banda, ed. *African Media and the Digital Public Sphere*. NY: Palgrave Macmillan, 2009; Lopes, Abreu, and Sharath Srinivasan. “‘Africa’s Voices: Using mobile phones and radio to foster mediated public discussion and to gather public opinions in Africa’.” *CGHR Working Paper* University of Cambridge Centre of Governance and Human Rights, 9 2014.F

[ii] Meraz, Sharon, and Zizi Papacharissi. ” Networked Gatekeeping and Networked Framing on #Egypt.” *The International Journal of Press/Politics,* 18, 2013: 138-166; Tully, M, and B Ekdale. “Sites of Playful Engagement: Twitter Hashtags as Spaces of Leisure and Development in Kenya.” *Information Technologies & International Development* 10, 2014: 67-82.

[iii] de Bruijn, Mirjam and Francis Nyamnjoh. *Mobile Phones: The New Talking Drums of Everyday Africa*. Oxford: African Books Collective, 2009.

[iv] Sector Statistics Report 2016/7, Communications Authority of Kenya, 2017

[v] Lanet Umoja Location is headed by a Chief who is supported by three assistant Chiefs. These three oversee 3 specific sub-locations (Umoja, 2 sub location; Muronyo Sub-Location and Kiamunyekei Sub Location).

[vi] There is a scream near the PCEA church in Baraka…There are thieves at Gathoni’s mum. Her house is near the corner towards Murunyu. Kindly come out and help…People of Murunyu please help, police are n the way. Let us all wake up….The thieves have run away.

[vii] Interview with Kinyanjui, 5 August 2016.

[viii] Phone Interview with Elijah Kinyanjui, Feb 2017

[ix] Interview with Kio Kinuthia and Elijah Kinyanjui, 2 Nov. 2016, Nakuru

Webs of peace and conflict: diasporic engagement in South Sudan

By Freddie Carver

Given the low levels of internet penetration in South Sudan[i] and poor telecommunications infrastructure, it might be thought that the internet is of little relevance to the conflict there. However, it has become a key enabler of a system of interaction and communication amongst a South Sudanese population that has become ever more globalised after more than 50 years of conflict and forced displacement. This includes a significant and currently growing population of both refugees and more settled communities in the region, particularly in Kenya, Uganda, Ethiopia, and Sudan (what might be called the 'near diaspora') as well as communities further afield, predominantly in the United States, Canada, Australia, and the United Kingdom, many of whom were resettled in the 1990s and 2000s (the 'far diaspora'). Statistics on all of these populations are poor, but collectively the total number of people is in the millions (with the population of South Sudan estimated in 2015 to have been 12.34 million[ii]). The extended nature of South Sudanese kinship systems mean that it is therefore likely that the vast majority of South Sudanese citizens have networks reaching into these locations. Current telecommunications technology enables these networks to operate in new and important ways.

Studies on diasporic engagement with conflict have been a feature of the conflict literature of the last 20 years, including in relation to Ethiopia and Somalia, but with a very limited focus on South Sudan. Since Collier and Hoeffler's landmark finding in 2004, that "a large diaspora considerably increases the risk of repeat conflict"[iii], much of this research has emphasised the negative role played by diaspora communities. Typical stereotypes, both of which are prevalent in the South Sudan context, include:

- at one end of the spectrum, the "keyboard warrior", inciting violence and hatred from safety thousands of miles away, perhaps even contributing financially to armed groups;
- and, on the other, those without much understanding of the realities on the ground but with an inflated sense of the role they can play thanks to qualifications and experiences they have gained in their new homes, and who return to the country with a patronising attitude and easy escape routes.

As with most stereotypes, there is a grain of truth in these characterisations, but they obscure both the complexity and the importance of diasporic engagement, and how it has evolved with technological advances.

The starting point, therefore, needs to be a more objective understanding of how this system actually operates and the opportunities and challenges it may present. While the psychological and geographical distance between individuals in, say, Australia, who may be struggling with unemployment and discrimination, and South Sudanese communities facing immediate threats of hunger and violence are indeed significant, regular communication starts to narrow this divide. Tools such as WhatsApp, Viber, and Skype

enable this communication to happen in a much more regular way, and even where internet connections do not exist at the South Sudanese end, can be used to connect directly to phones. This starts to undermine the reliance on traditional gatekeepers with access to satellite phones: satphones (often military commanders) or international organisations' VSat networks, and enables information to be shared more widely and rapidly. It means that the conversation taking place online, whether on social media (particularly Facebook) or via blogging websites such as www.PaanLuwelWel.com, is able reach those in rural areas. Disturbingly – and as has been documented elsewhere[iv] – this raises the prospect of 'fake news' and rumour being used to mobilise violence in specific locations, but it also presents significant opportunities. In a country where so much of the population is often inaccessible due to insecurity and logistical challenges, it provides a potential entry point for providing these communities with access to more reliable information, as well as giving them a more meaningful a voice about the future of the country.

This complex information network places an important responsibility on all those involved in providing information and analysis on South Sudan online to reflect seriously about the potential impact of what they produce – at all possible levels. One example provides an illustration of the challenge: Australian-based SBS (Special Broadcasting Service) Radio's Dinka Service. SBS radio is an Australian institution focussed on providing access to diverse media to Australia's many linguistic communities in the interests of community confidence and integration, and after the growth of the South Sudanese community there in the 2000s decided to add a Dinka programme to its roster. Being online has enabled this programme to become one of the most prominent and regular sources of news and information in Dinka worldwide. It is accessed by the community across the world (including in South Sudan where it can be distributed offline e.g. via MicroSD cards compatible with basic smart phones) and attracts high-profile interviews with leaders from the Dinka community. This is a very different proposition from that originally intended, largely outside the control of those who launched the initiative in Australia.

The network also creates new opportunities for financial transfers and remittances, which act as an important glue to the relationship between those inside and outside the country. Again, there is inadequate data available on the extent of remittance flows[v], but anecdotally they are clearly significant and will have only grown in importance as the value of the South Sudanese Pound has fallen. Direct transfers from abroad into remote areas of South Sudan are challenging due to the lack of access to banking facilities. Therefore, it appears that the 'near diaspora', many of whom are in countries such as Kenya and Uganda with access to mobile banking networks and who are able to more easily move back and forth into the country and access the informal networks that operate there, play an important bridging role. There is also consistent anecdotal evidence of financial support to armed groups operating along similar channels[vi]. The systems that enable these financial flows need to be understood far better if the war economy of the country is to be fully grasped.

It is also critical to recognise the fluidity that exists within this network, and which the

term ‘diaspora’, suggesting a fixed group operating from outside the country, does not adequately capture. There are a large group of people able to operate in multiple locations at once, providing direct physical connections between different geographical locations. Most obvious are the elites who, as 2016’s Sentry report[vii] documented, tend to have their families spread over multiple locations for purposes of maximizing education and investment opportunities, and who move back and forth regularly. This enables, for example, Members of Parliament who are traveling while parliament is on recess to hold community consultations in Calgary or Phoenix.

Beyond that, there are individuals that work for companies or aid organisations with an international presence who move between multiple locations, prominent activists or opinion leaders who no longer feel safe in the country (Riek Machar is arguably currently the most high profile diaspora member worldwide), and individuals that have sought to return to South Sudan to bring their new skills and experiences to bear, both for personal profit and public service (and, in recent years, for the purposes of participating in armed violence). While regular travel from distant locations is beyond those without significant resources, the movements in and out of the country are extensive, particularly around the time of independence, and ensures that these webs of connections are more meaningful than is suggested by the stereotypes outlined above.

While the fact that conflicts are closely connected with dynamics and actors beyond their national borders is hardly new, the combination of accelerated global migration and modern communication technologies does mean that the communities affected by the conflict are more widely dispersed and interact more directly with events on the ground. The question for those seeking to have an impact on conflict dynamics is what risks and opportunities this presents.

There are undoubtedly challenges to seeking to engage with these networks. South Sudanese diaspora communities are often polarised and fragmented, with ethnic identity a primary organising principle and the on-going violence taking place in the country continues to damage trust and relationships on all sides. This fragmentation is one of the driving factors behind the high level of online hate speech, something that has become increasingly high profile in the last year thanks to the work of organisations such as Peace Tech Labs[viii] and #defyhatenow[ix], and has recently been highlighted by the UN Special Representative for the Prevention of Genocide[x]. Their work has illustrated the feasibility of using online monitoring as an early warning system for violence within South Sudan, as well as raising awareness amongst South Sudanese about bottom-up methodologies to combat hate speech online. Thinking is also emerging about ways in which those governments that host diaspora communities might be able to use domestic legislation to prosecute those responsible. These issues should also form part of the growing global debate around the responsibilities of the biggest social media companies in ensuring their sites are not used for criminal purposes.

Nonetheless, it is essential that this issue is not solely framed along negative lines, and the potential for these diaspora networks to enable positive change is fully explored and, where appropriate, supported. There are many individuals and groups within diaspora

communities that recognise the opportunity they have to speak more freely than those inside the country, and who are seeking to break down tribal divides and promote alternative visions of South Sudan – they can be found blogging or setting up community development organisations or lobbying governments for action. Efforts are underway at the moment to develop a global diaspora network to increase the coherence and effectiveness of these efforts, and while the unity aspired to will undoubtedly be challenging to obtain, this represents important social capital that can be of benefit to South Sudan. If those involved can make the most of the web of interactions and relationships described above, helping give a voice to those who too often do not feature in discussions about South Sudan's future, then such efforts could become a powerful tool to drive positive change in the country.

There may also be a limited time window for harnessing this energy, at least from the 'far diaspora', although this issue needs further study. Much of the migration out of the region took place in the 1990s and 2000s, and is unlikely to be repeated at scale given the current domestic attitude to immigration in many of the host countries. The door has therefore largely shut behind this community, and while many individuals still retain a strong connection back to the "homeland" this may start to weaken as time passes, particularly as the baton is handed to a generation that have never known South Sudan themselves.

There is therefore an onus on international policymakers seeking to improve the situation in the country to think harder about this system, particularly given the lack of leverage and influence that the international system currently appears to have in the country. The first step is to understand it better and to start to fill in the gaps in our collective evidence base. But if this can be done, then for the United States government, for example, the opportunities that should arise to engage directly with these communities, as well as to work with the American technology companies that are so deeply enmeshed with them, might provide valuable new threads of a more comprehensive strategy on South Sudan.

Freddie Carver is an independent Conflict & Peacebuilding Adviser, with a focus on South Sudan, currently working as a consultant. Freddie can be reached at Freddie.carver@gmail.com or through his LinkedIn profile at https://www.linkedin.com/in/freddie-carver-4aa3423a/

Sources

[i] Internet World Stats (www.internetworldstats.com) provides an estimate of 16.6% penetration as of March 2017, well below the African average of 27.7%, although even this figure should be treated with caution given uncertainty over population figures in South Sudan.

[ii] UN World Population Prospects (2015)

[iii] Collier, Paul and Anke Hoeffler (2004), 'Greed and Grievance in Civil War', Oxford Economic Papers, p. 575

[iv] See in particular recent articles on Public Radio International (https://www.pri.org/stories/2017-04-25/online-fake-news-an--hate-speech-are-fueling-tribal-genocide-south-sudan) and Buzzfeed (https://www.buzzfeed.com/jasonpatinkin/how-to-get-people-to-m-rder-each-other-through-fake-news-and?utm_term=.hqb5AlMQX#.qtBmBN0DJ), both accessed on accessed on 26/4/17

[v] The World Bank, the main source of such data, does not publish figures for South Sudan. A 2013 report (Mamer and Maher, 2013, "Remittances to South Sudan – an unrecognized source of aid" accessed on 26/4/17 at the website Right Now – Human Rights in Australia) gave a figure of USD 24.6m as the annual contribution from Australia.

[vi] Authors' interviews, 2017

[vii] War Crimes Shouldn't Pay, the Sentry (2016)

[viii] www.peacetechlab.org

[ix] www.defyhatenow.net

[x] For example, see https://www.theguardian.com/global-development/2016/dec/14/south-sudan-swift-action-genocide-un-human-rights-chief

Internet shutdowns as major constraints for digital political activism in the Horn of Africa

By Mengnjo Tardzenyuy Thomas

At the dawn of the 21st century, the Internet is increasingly being used by citizens around the globe as leverage for political expression and to hold governments accountable for their actions. But in authoritarian regimes especially on the African Continent, the use of Internet for citizens' activism is often interrupted by these regimes, whenever they perceive that its use by any political actor might jeopardise their political offices. Summarily, digital political activism in this write up refers to a situation where digital tools such as internet, mobile phones, and social media are used to bring political change. It is aimed at serving five main functions which amongst other things include: shaping public opinion, planning an action, sharing a call to action, taking action digitally, and the transfer of resources. Through online political activism, large communities can be connected around the globe[i]. On the other end, the Horn of Africa (the Horn) in this context refers to the Eastern Region of Africa which is comprised of the following countries: Djibouti, Eritrea, Ethiopia, Somalia, Kenya, Sudan, South Sudan, and Uganda[ii]. Some of these countries according to Njiraini Muchira (2016) are among the top violators of freedom of expression online[iii].

Online suppression in these countries have over the years been manifested through internet shutdowns, principally masterminded by governments, powerful states such as the United States (US) and terrorist groups such as *Al Shabaab*. Nonetheless, shutting down the internet no matter its justification, contravenes Article 20 of the Twentieth-Session of the United Nation (UN) Human Rights Council's Agenda 3 on: "The promotion, protection and enjoyment of human rights on the internet"[iv]. As such, in disregard of this resolution, a number of factors have over the years been held accountable for internet shutdowns experienced in the Horn. Internet shutdowns in these countries have not only manifested themselves in diverse ways but have equally stifled citizens' basic human rights to freedom of expression online.

The justification and manifestation of internet shutdowns in the Horn of Africa

From the eight countries in the Horn identified above, internet disruptions have occurred in Ethiopia, Somalia, Sudan and Uganda. In justification for Internet shutdown, Kifle Eskedar has intimated that most governments wholly or partly disrupt the operation of internet services due to national security, public safety, economic reasons, and to maintain control [v]. In addition to these justifications, Philip, N. Howard, Sheetal, D. Agarwal, and Muzammi, M. Hussain have further contended that governments disrupt digital networks in order to protect political leaders and states institutions, prevent election crises, eliminate propaganda, and to mitigate dissidents [vi]. Relative to the foregoing, it should be underscored here that, internet shutdowns in the Horn can be explained from two main angles, that is, from the perspective of governments and from the standpoint of other political actors such as the United States government and extremist organisations such as the *Al Shabaab*.

Many governments in the Horn consider the internet especially during electoral periods as a threat to their continuous grip on state power and hence, are often willing to use whatever means at their disposal to prevent the dissemination of any information which might likely shape public opinion against their political power. In the wake of the 2016 Ugandan Presidential Election, the Ugandan government blocked the Internet on February 8th. This shutdown was intended to stifle the spread of online messages linked to the forceful arrest of the main opposition contestant, Dr. Kizza Besigye and alleged human rights abuses orchestrated by the police on members of the opposition few days to the election. Furthermore, the Internet shutdown was also aimed at paralysing Besigye's online platform popularly known as "Power 10" (P10), which was constructed to monitor polling operations and to report any cases of electoral malpractices nationwide[vii].

Secondly, internet shutdowns in the Horn have also been aimed at repressing citizens' organised mass protests against the government in situ. Examples abound. In October 2016 the Ethiopian government blocked the Internet as a pre-emptive measure to halt the viral spread of online messages, which were mobilising citizens to participate in protests against the government of Ethiopia. According to the Ethiopian Prime Minister, Hailemariam Desalegn, the internet in this scenario was used as a tool to "spread messages of hate and bigotry without any inhibition"[viii].

Aside from the foregoing governments related motives, internet shutdowns in the Horn also have exogenous roots. For instance, in November 2001, the United States coerced Somalia's telecommunication firm, Somalia Internet Company and a money transfer company, *Al Barakaat,* to close down their Internet services. The U.S. suspected these companies of terrorist links as plainly elaborated by the British Broadcasting Corporation's (BBC) Network African Program in the following words: "The two firms…both appear on a US list of organisations accused of funnelling money to the al-Qaeda network and featured in a UN Security Council resolution"[ix].

In another focus, threats from extremist groups have also led to Internet shutdown in the Horn. In February 2014, the largest telecommunication company in Somalia, *Hormuud*, was forced by the *Al Shabaab*, to shut down the provision of its internet services. From the standpoint of *Al Shabaab*, officials of this company were western spies and Christian crusaders[x]. In this light, Abdi Aynte, a Somali Analyst at the Heritage Institute of Policy Studies contended that *Al Shabaab's* intimidatory move for Internet shutdown was as a consequence of the realism that, they were: "…afraid that this technology will be used to track some of their top fighters as the operations of drones permeate in the areas that al Shabaab controls in South and Central Somalia"[xi]. In order to justify their Internet shutdown, one of the officials of this telecommunication company in his position statement affirmed that they had no other option than to close down their internet operations as follows*:* "I don't think we had another alternative … we are just business people and cannot confront an armed group's orders"[xii].

From the foresaid, it is apparent that Internet shutdowns are the main obstacles to digital political activism in the Horn. Most political actors seldom reflect on the

consequences of shutting down the Internet[xiii]. To this end, Internet shutdowns in the Horn have obstructed citizens from freely expressing their opinions online. This contravenes Article 20 of the UN Human Rights Resolution. For instance, in June 2016, the UN while underscoring that the right of expression through the internet should be respected by all countries observed as follows: "Deeply concerned by all human rights violations and abuses committed against persons for exercising their human rights and fundamental freedoms on the Internet, and by the impunity for these violations and abuses…Deeply concerned also by measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law"[xiv].

Besides denying citizens the right to freely express themselves online, the economic repercussions of Internet shutdowns have also been expensive in the Horn. According to a study carried out by the Brookings Institute and Global Network Initiative (GNI), Ethiopia lost about US $500,000 per day in Gross Domestic Product (GDP) when the government shutdown the internet in 2016[xv], while the Ugandan economy also lost close to about US $26 million during its internet shutdown in 2016[xvi]. Apart from Internet shutdowns, other underlining factors hindering digital political activism in the Horn include: illiteracy in Internet usage, inadequate developed telecommunication infrastructures, and low online political culture.

Policy recommendations

In order to curtail the disruption of the Internet and to avert its consequences in the Horn, the following policy recommendations are necessary:

1. There is need for governments in the Horn to develop the spirit of online tolerance which is one of the basic tenets of democracy. Online tolerance would mean willingness to accept online criticisms from opponents by translating them into good policy options.
2. There is also need for sensitisation programs to be organised in order to enhance the capacities of both governmental officials and the citizens on the responsible use of the internet. These programs are crucial so as to better educate governmental officials on the repercussions of internet shutdowns on the one hand, and to sensitise internet users to avoid online hate speech and to use the internet responsibly.

Mengnjo Tardzenyuy Thomas is a Ph.D Candidate in Political Science at the University of Dschang, Cameroon. He is also a tutorial master in the Faculty of Law and Political Science in the mentioned University. He can be reached at mengnjotthomas@gmail.com.

Sources

[i] Rees, Anna (2015). *Digital and online activism*.https://en.reset.org/knowledge/digital-

and-online-activism accessed on 05/04/2017

[ii] Encyclopaedia Britannica (2017).*Horn of Africa Region, Eastern Africa*.https://www.britannica.com/place/Horm-of-Africa accessed on 05/04/2017.

[iii] Muchira, Njiraini (2016). *African govts adopt Internet shutdowns to quell crises in 2016* accessed from http://www.theeastafrican.co.ke/2456-2456-ekxxsk/index.html on 05/04/2017

[iv] United Nations General Assembly Human Rights Council Twentieth Session, 29th June 2012.

[v] Kifle, Eskedar (2016). *Internet stoppage costs nation USD 9 million*. www.Internet-stoppage-costs-nation-20USD-20million-Capital-Ethiopia-Newspaper accessed on 05/04/2017.

[vi] Philip, N. Howard, Dheetal, D. Agarwal, and Muzammi, M. Hussain (2011).*The Dictators' Digital Delemma: When do States disconnect their digital networks*? In Issues in Technology Innovation, Number 13, October 2011.

[vii] Ojok, Donnas (2016). *Social Media Lockdown and Elections in Uganda*. http://blogs.lse.ac.uk/africaatlse/2016/03/02/social-media-lockdown-and-elections-in-uganda/ accessed on the 05/04/2017

[viii] Zondi, Nolwandle (2017). *Hands On Social Media: Five times African governments shut down the internet*. http://www.africanews.com/2016/12/04/ethiopia-partially-restores-mobile-internet-after-2-month-shutdown// accessed on the 05/04/2017.

[ix] BBC News (2001).*US shuts down Somalia internet*. www.BBCNews-AFRICA-shuts-down-Somalia-internet. Accessed on the 05/04/2017.

[x] Karimi, Faith (2014). Somalia *warns telecom companies not to comply with Al-Shabaab Internet ban*. http://edition.cnn.com/africa accessed on the 05/04/2017.

[xi] Writer, Staff (2014).*Terrorists shut down internet access in Somalia*. http://innovation-village.com/news/ accessed on the 05/04/2017.

[xii] Osman, Ahmed (2014). Somalia *Powerless to Stop Al-Shabaab Mobile Internet Shutdown*. http://www.ipsnews.net accessed on the 05/04/2017.

[xiii] Kifle Eskedar., Op. Cit

[xiv] UN Human Rights Council Thirty-second session, Agenda 3, 27th, June 2016.

[xv] Matinde,Vincent (2017). *What is the impact of Africa's (many) internet shutdowns?*. http://www.idgconnect.com/ accessed on the 05/04/2017.

[xvi] Mohapi, Tefo (2016). *The internet shutdown in Ethiopia costs $500,000 a day in lost GDP*. Cipesa.org/2016/10/the-internet-shutdown-in-ethiopia-costs-the--ountry-approximately-500000-a-day-in-lost-gdp/ accessed on the 05/04/2017.