CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 15 — MAY 2015

Cyber Security and Cyber Resilience in East Africa

Iginio Gagliardone and Nanjira Sambuli

CYBER SECURITY AND CYBER RESILIENCE IN EAST AFRICA

Iginio Gagliardone and Nanjira Sambuli

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHORS

Iginio Gagliardone is research fellow in new media and human rights at the University of Oxford. He is a member of the Programme in Comparative Media Law and Policy, a research associate of the Oxford Internet Institute as well as an associate of the Centre of Governance and Human Rights at the University of Cambridge. His research focuses on the relationship between new media, political change and human rights, and on the emergence of distinctive models of the information society. His most recent research projects explore the nature and significance of hate speech online, with a particular emphasis on the trade-offs between freedom of expression and human dignity, and on how social networking platforms are responding (or failing to respond) to the challenges hate speech presents.

Nanjira Sambuli is a research manager at iHub, Nairobi, where she leads the Governance & Technology research pillar. Nanjira is trained as a mathematician with experience as a new media strategist for organizations such as the United Nations Environment Programme, United Nations Human Settlements Programme, Africans Act 4 Africa, and Global Power Shift, on their pan-African and international campaigns. She is also the editor of *Innovative Africa: The New Face of Africa*, a series of essays on the emerging African tech landscape. Nanjira is interested in understanding the unfolding impacts of information and communication technology adoption and how those impact governance, innovation, entrepreneurship and societal culture in her native Kenya, and also across the African continent.

EXECUTIVE SUMMARY

This paper analyzes continuities and discontinuities of collective efforts toward enhanced cyber security in Eastern Africa, with a particular focus on Kenya, Ethiopia and Somalia. Focusing on the challenges that have followed the contours of East Africa's distinctive digital cultures, it challenges the view that cyber security and cyber resilience are simply technical problems that can be solved by reducing the gap with more technically advanced nations. On the contrary, it shows how cyber security is an inherently political challenge and that, in the absence of adequate checks and balances, the increasing securitization of domestic and international politics may require costly trade-offs with individual and collective freedoms.

Three concepts are suggested — emulation, extraversion and enculturation — that can serve to better capture how Kenya, Ethiopia and Somalia have respectively answered emerging cyber threats. These concepts, rather than adding to the already abundant jargon in this area, are simply meant to encourage analysts to pay greater attention to how the technical, social and political interact in unique ways and produce distinctive outcomes in each national context. In Kenya, public and private actors have sought to live up to international standards, keeping up with the country's reputation as a regional information and communication technology (ICT) powerhouse, but it is unclear how such an ambitious agenda will find concrete applications. In Ethiopia, there is the risk that the need to guarantee better cyber security can further legitimize repressive measures in the new media sector. Finally, in Somalia, in the absence of a functioning state, hybrid solutions have been found that connect traditional practices and new technologies to offer some level of certainty to individuals using services that are vital for the region, such as local and international payments over mobile phones.

INTRODUCTION

Over the last few years, cyber security has gone from a concern that loomed large in the future for East Africa to an issue of pressing importance. In Kenya — one of Africa's largest economies and East Africa's central tech hub — it is estimated that cybercrimes cost the country more than 2 billion Kenyan shillings (US$22.56 million) in 2013 (Otieno 2014).

The increasing awareness of the need to address cyber-security threats in Africa, however, has also reproduced old clichés about gaps between the continent and more advanced areas of the globe. The few reports available on cyber security in Africa have been characterized by alarmist tones, asking, for example, whether Africa has become "a new safe harbor for cybercriminals" (Kharouni 2013). They have, however, offered very thin empirical evidence that Africa is any more dangerous than other continents and, in many cases, have been sponsored by cyber security firms with vested interests (Jackson 2015). From a different angle, the increasing presence of Chinese telecom companies in Africa has led to allegations that these companies may be hiding "backdoors" in their equipment to allow the Chinese government to spy on users, including African citizens, or to shield its own spying efforts elsewhere (Protalinski 2012). Recent leaks from the former US National Security Agency (NSA) contractor Edward Snowden, which revealed that the NSA itself tried to install backdoors in equipment produced by Huawei, China's largest IT company, have given such accusations an ironic twist. As Thomas Rid (2014) succinctly put it, "there is now more publicly available evidence that the [US] NSA exploited Huawei than there is public evidence that shows the PLA [People's Liberation Army] or other Chinese agencies did so."

This paper, while recognizing the threats posed by cyber security in East Africa and highlighting some fragilities and contradictions of the measures developed to date, focuses on the specific challenges that have followed the contours of East Africa's distinctive digital cultures. Mobile phone banking innovations have facilitated greater flows of currency and increased chances for skimming these transactions (Harris, Goodman and Traynor 2013; Herbling 2014). Remittance-based economies have presented opportunities for cyber attacks on the banking institutions that facilitate these transfers (Mukinda 2014; Quarshie 2012). Terrorist threats, in particular from the Islamist group al-Shabaab, have stressed the need to respond to militants employing digital media to further their cause (Kagwanja and Karanja 2014), but also to reflect on the possibility that the increasing securitization of domestic and international politics may require costly trade-offs with individual and collective freedoms, and offer excessive powers to executive bodies in the absence of adequate checks and balances (Makulilo 2012).

Through three case studies focusing on Kenya, Ethiopia and Somalia, national responses are connected to continental and global efforts to reinforce cyber security. These case studies offer the opportunity to understand how three neighbouring countries that have developed very different notions of their national information societies have elaborated distinctive responses to a similar challenge.

Kenya, given its ambition to emerge as East Africa's leading ICT innovator, has made the most effort to respond to cyber security threats. *Emulating* countries that have similarly emerged at the forefront of the information revolution, Kenya has made strides to adopt internationally recognized standards, seeking to offer a sense of readiness to withstand cyber attacks. By doing so, however, Kenya has also created high expectations about

its ability to adequately respond to growing risks, and will have to invest significant resources to live up to them.

Ethiopia, while similarly showing adherence to international standards, as displayed by its draft cyber security law, which incorporates many of the provisions in the Council of Europe Convention on Cybercrime, appears more exposed to the risk that the cyber security agenda could be exploited politically to further domestic goals. As the precedent of the Anti-Terrorism Proclamation analyzed below illustrates, the Ethiopian government has often relied on *extraversion* to achieve its goals, turning its unequal relations with the international environment in its own favour, and furthering its own agenda while giving the impression of responding to international calls.

Finally, the case of Somalia, or the Somali territories,[1] offers an example of how solutions may emerge through *enculturation*, relying on local knowledge to address global threats. As explained later, in the absence of a functioning state, customary law has been employed to ensure that people get compensated in cases of fraud perpetrated through mobile phones or has offered a response when sensitive data are released by mistake in the public domain.

These three mechanisms — emulation, extraversion and enculturation — are not mutually exclusive. On the contrary, while each of the countries surveyed displays one of them to a greater extent, these mechanisms can be found in all three countries to varying degrees. Approaching the analysis of cyber resilience through these lenses is meant to offer greater space to appreciate the nuances of how global and local agendas interact and to highlight the risks of international agendas that too flatly emphasize the need for countries in Africa to catch up with more resilient countries, without adequately considering the context in which legislations and technical measures develop.

The paper begins by clarifying the contours of cyber security and cyber resilience in Africa and then concentrates on the three case studies of Kenya, Ethiopia and Somalia, focusing on governments' role in shaping the cyber security agenda and drawing comparisons that can offer new lessons for, and beyond, East Africa.

CYBER SECURITY AND CYBER RESILIENCE IN EAST AFRICA

Debates on cybercrime and cyber security tend to concentrate around dramatic events such as the defacement of popular online spaces, sensitive information leaks or diffusion of particularly infectious malware. Less attention has been paid to broader issues of cyber resilience, that is, an organization or government's capability "to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain, and unexpected threats from activities in cyberspace" (ISACA 2014). Resilience refers to the idea that failures will inevitably occur, but promotes the adoption of holistic, cooperative measures that ensure a system does not wholly collapse. The objective is therefore maintaining as much normalcy as possible or returning to that level as quickly as possible following a cyber attack.

The concept of cyber resilience underlines the need for broad, concerted and comprehensive approaches to cyber security, but in reality, the implementation of measures to curb cyber attacks has been selective and driven by narrower agendas. Western powers with interest in East Africa have largely emphasized the need to combat extremism (Cassim 2011). The United States' efforts in East Africa, for example, have contributed to supporting greater preparedness for cyber attacks as a component of its larger anti-terrorist strategy, rather than as part of a coherent and concerted cyber security initiative for the region (Ploch 2010). China, for its part, through its increasing investment in telecommunication in Africa — more than US$3 billion went to Ethiopia alone to overhaul its telecommunication infrastructure — has largely favoured state-led initiatives, leading to fears that the state actors may be gaining too much power compared to other players involved in the shaping of national information societies (Gagliardone 2014).

It is in this light that the African Union Convention on Cyber Security and Personal Data Protection, which offers continental reference to improve cyber preparedness in Africa, has also raised concerns that in the charged political climate characterizing many countries on the continent, the heightened emphasis on security and state-led responses may impact free speech and privacy as governments that have been criticized for their abuses gain enhanced abilities to police the cyber world (Macharia 2014). The possibility that personal data could be processed without subjects giving free and informed consent when this is "in the public interest" (Art. 14.2.i), in particular, delineate scenarios where users may be stripped of their ability to be in control of their data and, on the contrary, be controlled in the name of agendas they had little voice in shaping (Access 2014). Concerns related to political tensions characterizing specific countries in Africa, as well as the fragility of institutions that should safeguard individual and collective freedoms, need to be taken into serious account. They should, however, avoid giving the impression that this is just an African problem, reproducing the cliché that unaccountable governments on the continent are simply implementing good provisions poorly. As the now abundant literature on the securitization

1 The term Somali territories is used to reflect the realities of governance within what is formally represented by the state of Somalia. In the north, the self-declared independent country of Somaliland has its own government, constitution and media legislation. Independent governance is similar in Puntland, the region south of Somaliland, although Puntland seeks a role in a greater Somalia. There are other smaller regions of the country that claim self-governance in the absence of a functioning central government.

of foreign and domestic policy (see, for example, Howell and Lind 2009), as well as on the abuses of individual rights perpetrated by the most advanced regimes (see Greenwald 2014) illustrate, the security agenda has created ample spaces for abuse by governments and private companies globally. The quest for more coordinated approaches to withstand cyber attacks should thus not be simply treated as a technical problem that requires technical solutions, but as a political one that requires transparent and open debates.

COUNTRY CASE STUDIES

Kenya: Putting Policies, Laws and Frameworks into Practice

Holding a dominant ICT position in East Africa, Kenya has made great strides in incorporating ICTs into various industry sectors. As of 2013, it was noted that ICTs contributed to 12.1 percent of the country's GDP (Mwenesi 2014a). International organizations appear to have bet on Kenya's ICT visions and ambitions. The World Bank Group alone invested around US$4.1 billion between 2003 and 2010 (Mwenesi 2014b). Such confidence presents massive opportunities, but can also be easily eroded if Kenya is not able to face emerging challenges in ways that match its ambition to be recognized as East Africa's ICT hub.

Kenya's first major international cybercrime case exposed some of the cyber vulnerabilities and gaps the country faces. In December 2014, 77 foreigners — one Thai national and 76 Chinese — were arrested in Nairobi; they were found in possession of equipment capable of a massive cyber attack, such as infiltrating Safaricom's[2] M-PESA (mobile money transfer) system, cash machines and bank accounts (Agence France-Presse 2014). Chinese officials claimed that this was another fraud den aimed outwardly at China, however, and not at Kenya (Otuki 2014). Even if this was the case, the cybercrime ring was only discovered by chance, when a fire broke out in a house some members were living in, and it had been operating completely hidden from authorities. According to the Kenyan police, the suspects were charged with operating an unlicensed telecommunication facility, and could face up to 15 years in jail or have to pay a 5 million Kenyan shilling fine (US$54,000), with more charges pending (Nzwili 2015). It is not clear yet under which specific law these suspects would be tried. The Chinese government assumes the criminal acts were targeted at them and has officially requested that its Kenyan counterpart extradite the suspects to face trial in China, where sound judicial procedures are in place, rather than potentially releasing the group in Kenya. The latter part of the Chinese government's reasoning was interpreted as indicating that Kenya may not have strong enough laws under which to prosecute the cybercrime suspects, eliciting reactions that Kenya must prove it has the "capacity, and will, to investigate and prosecute crimes of such magnitude and complexity" (*Daily Nation* 2015).

Kenya's strategy to strengthen the country's cyber resilience is caught between recognition of the still fragile status of the country in the digital realm and the ambition to make Kenya one of East Africa's leading players, emulating and seeking partnerships with actors that are better prepared to respond to emerging threats.

In 2012, with support from the International Telecommunications Unit as part of its Global Cybersecurity Agenda, the government created the Kenya National Computer Incident Response Team Coordination Centre (KE-CIRT/CC) to offer technical services in the management of cyber security.[3] More specifically, KE-CIRT/CC's role is to offer advice on national cyber-security matters and to coordinate responses to cyber incidents in collaboration with local, regional and international stakeholders. The centre falls under the Communication Authority of Kenya's docket, and offers what it dubs as "reactive and proactive services." The former service entails incident response, coordination and resolution, including the collection of national statistics about cyber incidents, while the latter entail technical advisory and capacity building, including technical research and development.[4] However, there is hardly any publicly available information, in the form of reports or news items on the centre's work or outputs, indicating if and how it has worked in conjunction with other government institutions addressing cyber-security matters. It has also been noted that due to capacity and requisite skills constraints, as well as engagement with other stakeholders, the centre's effects and impacts are hardly felt, and it could risk losing its relevance in the industry (Kigen et al. 2014, 41).

The contradictions between the tendency to emulate solutions adopted elsewhere and the need to concretely implement them into a national context have also been felt in more recent and apparently more coordinated efforts. Kenya's National Cybersecurity Strategy, developed in 2014, for example, aims to define the country's cyber-security vision, goals and objectives to secure the nation's cyberspace while continuing to promote the use of ICT to enable economic growth (Government of Kenya 2014, 5). In this strategy, the national government, through the ICT ministry, purports to enhance the nation's cyber-security posture by securing critical infrastructure, applications and services, with mention of (cyber) resilience through business impact analysis, continuity of operations and disaster recovery. These elements, however, are not

2 Safaricom is Kenya's leading mobile network operator.

3 See www.ke-cirt.go.ke/index.php/itu-to-support-kenya-cybersecurity-efforts/.

4 See www.ke-cirt.go.ke/index.php/services/national-cirt-services/.

articulated further, beyond being listed in a diagrammatic format (ibid., 7). The strategy document also talks of the government's awareness raising and training of the public and workforce on securing the national cyberspace by working in conjunction with academia to develop higher education curriculums on cyber security and specialized training programs. The third goal touches on developing required laws, regulations and policies to secure the nation's cyberspace as well as collaboration and information sharing; a comprehensive framework is envisioned to minimize duplication of effort as well as government-led approaches to designing and maintaining information-sharing capabilities to facilitate knowledge exchange and lessons learned among various stakeholders.

Given cases of fraud and of incitement to violence through ICTs that have occurred in Kenya, and given the aforementioned efforts from the government to tackle cyber security, the big question is how all the various institutions mandated with addressing the issue can work effectively and coordinate. The Kenyan case shows that theoretical attempts, while impressive, are not sufficient to address ever-growing cyber-security threats in the East African hub, and the region in general. There is a need to move from paper to practice, to strengthen existing institutions and processes, especially within the government, as well as recruit and build capacity well equipped to tackle emerging issues. That will form a critical stepping stone in moving from reacting to cyber threats or attacks, to setting in place strategies and measures to ensure cyber resilience in the country.

Ethiopia's Cyber Resilience: Turning International Priorities into National Agendas

Ethiopia has emerged as a paradox in East Africa with regard to ICTs and cyber security. Despite lagging behind in access, with only two percent of its population connected to the Internet in 2014 (ITU 2015), the Ethiopian government has developed increasingly advanced legal and technical means to ensure greater control over the information transiting over communication networks and to defend the country from cyber attacks. These measures have been publicly justified by the need to align with international standards and respond to mounting cyber threats, but have also significantly boosted the ability of centralized power to persecute individuals and organizations, often without adequate oversight and checks and balances.

The Information Network Security Agency (INSA), first created in 2006 and then "re-established" in 2011, has been at the forefront of attempts to improve Ethiopia's cyber resilience. Shaped in the guise of the US NSA, the INSA has taken on the responsibility of "protecting" the national information space, taking counter measures against information attacks, which the law frames as any attack against the national interest, constitutional order and nation's psychology by using cyber and electromagnetic technologies and systems. It is answerable to the prime minister's office and every other governmental body has the duty to cooperate with the INSA. Its wide powers have caused concern, however. It empowers the director of the agency to designate the profiles, financial documents, equipment, methods and work outputs of certain personnel, as "top secret" and render them inaccessible to individuals, including the auditor general, if it is believed that national security would be at stake if otherwise disclosed. The law also allows the agency's investigators to conduct "virtual" forensic enquiries without judicial warrant on computers or infrastructures that are purported to be attacked or to be the source of attacks, eroding the constitutional right to privacy of users by leaving interpretation of their rights at the mercy of intelligence officers (Yilma 2014).

One of INSA's first acts has been the drafting of what later became the Telecom Fraud Offences Proclamation, passed by the Council of Ministers in 2012, which reaffirmed the state monopoly over telecommunications, imposed severe sanctions for any operator trying to compete with or bypass Ethio-telecom, and with Article 6 it extended the provisions of the Anti-Terrorism Proclamation to the online sphere. The proclamation can be considered the first "Internet law" in Ethiopia and contained measures aimed at combatting cyber attacks, including "unlawful interference," "unlawful interception" and "illegal access to a telecom network." In 2014, INSA proceeded to draft Ethiopia's first dedicated cyber security law, which incorporates many of the provisions included in the Council of Europe Convention on Cybercrime as well as the African Union Convention on Confidence and Security in Cyberspace. This could be seen as a welcome move, but should be considered also in the context of how similar laws have been previously used to stifle dissent. French political scientist Jean Francois Bayart (2000) has suggested analyzing the interaction of numerous governments in Africa with the international system through the lens of extraversion, to understand how they have turned their weaknesses in their favour. The Anti-Terrorism Proclamation in Ethiopia, passed in 2009 — five years before the cyber-security law began to be drafted — is a clear example of this mechanism. Framed as an effort to comply with the UN Security Council requests that "terrorist acts are established as serious criminal offences in domestic laws" (UN Security Council 2001), it also created the legal preconditions to actually prosecute critical voices within Ethiopia (or Ethiopians in the diaspora). Out of the 33 individuals convicted under the Anti-Terrorism Proclamation between 2009 and 2014, 13 have been journalists, leading organizations such as Human Rights Watch to denounce the law and its application as "deeply flawed" (Human Rights Watch 2013). The proposed cyber-security law may risk following a similar path.

In an ironic twist, the Ethiopian government has been accused of being behind cyber attacks targeting some of its political opponents. According to the Citizen Lab, software developed in the United Kingdom and in Italy has been employed to breach the computers of political opponents living abroad and spy on their communications (Citizen Lab 2013; 2015). This led an Ethiopian citizen residing in the United States to sue the Ethiopian government for infecting his computer. The Electronic Frontier Foundation is representing the plaintiff in this case.

Somalia and Somaliland: Resilience from the Ground Up

The Somali territories have become synonymous with stereotypes of chaos and lawlessness. This common perception, however, obscures examples of trust, security and regulation that have emerged in several areas, including trade and telecommunications. Despite decades of conflict, an externally oriented, open and relatively unrestricted economy has flourished (Little 2003). Enterprising companies, not shattered institutions, have provided ways for Somalis to send and receive money. These companies are primarily owned and initiated from the Somali diaspora, and have responded to the needs of Somalis and found opportunities in a remittance-based economy. Radio stations and telecommunications companies have also been able to function, and sometimes thrive. Hormuud Telecom is the largest of these companies and has been turning a profit since 2002. Hormuud also runs a mobile money transfer system, and plans to launch 3G network capacity soon, despite recent orders from al-Shabaab to close in some regions (Nyambura-Mwaura 2013). Another telecommunications firm, Telesom, has led the way in Somaliland, and also has a mobile money transfer system, Zaad. This model has been praised by Bill Gates, and was modelled after Kenya's M-PESA system, and has flourished in a region where 26 percent of the population pay bills over mobile, the highest rate in the world (Stremlau and Osman 2015; Penicaud and McGrath 2014).

The particular growth of mobile banking has been connected to the lack of regulation and formal institutions that have slowed its growth elsewhere. As Stremlau (2012) and Carrier and Lochery (2013) have noted in their studies of trade and mobile banking in Somaliland and Eastleigh,[5] trust networks and traditional *xeer*[6] law contribute to the functioning of these informal systems. Trust is essential. In an environment of real physical insecurity, services such as EVCPlus, Hormuud's money transfer system, make much more sense than cash. EVCPlus has a US$300 limit, which does not reduce the risk of skimming or fraud, but is still safer and more convenient than using cash (Mohamed 2013). Furthermore, mobile money has emerged to fill a major gap in the banking sector whereby consumers can hold their money in "e-wallets." While some technical solutions have been advanced to reduce or avoid the likelihood of fraud, it is in the solving of disputes related to the increasing reliance of transfer on ICTs that the most interesting phenomena have emerged.

In the absence of formal regulatory and banking systems, complex relations among courts, clan-based governance and companies have been able to regulate and resolve conflicts (fraud, mistaken transfers or disputes over the amount of the transfer) over mobile money. This "hybrid judicial process" (Stremlau and Osman 2015) that has emerged to resolve disputes is an example of what we refer to as enculturation, a process by which local knowledge and resources are adopted to address issues that have found different solutions elsewhere. Companies in Somalia are increasingly regarded as the first authority to effectively resolve the conflict. In an area of instability and fierce competition among telecommunications and mobile money providers, their reputation for fairness and effectiveness is critical for their success. Government courts are generally regarded as corrupt and easily manipulated by the wealthier party, but are nevertheless part of a more formal complaints procedure if the conflict involves two individuals or families. *Sharia* courts are regarded as more trustworthy and, in some disputes, they may have a role if one party advocates for their intervention. But, in many cases, the most effective way of resolving a conflict between two people is the intervention of elders. This approach draws on traditional mechanisms for resolving property disputes, including those that would also be applied to more traditional businesses such as the livestock trade. It has also been refined and tested through the dynamic remittance industry, upon which the mobile banking and other ICT projects have been built (ibid.).

This combination of different mechanisms of conflict resolution, however, has been more difficult to implement in the areas controlled by al-Shabaab, which has highly restricted the use of ICTs and banned Internet use, declaring it to be un-Islamic. The group, however, uses social media to advance its agenda, presenting potential threats to its neighbours. Al-Shabaab has posed a different set of challenges and issues. Certainly its use of new technologies and the potential threat of cyber attack have been taken seriously in anti-terror efforts.

5 Eastleigh is a suburb of Nairobi that is populated mainly by Somali immigrants. The Somali diaspora has led a thriving economy and communications sector, but has also garnered attention from both the Kenyan police and al-Shabaab.

6 *Xeer* is analogous to a customary law regime but more extensive, in that it serves as an overall social contract governing relations between clans as well as defining the role of the individual within the community (Stremlau 2012, 160).

CONCLUSION

The analysis of how Kenya, Ethiopia and Somalia have offered distinctive responses to increasing cyber threats offers an important comparative angle to understand the continuities and discontinuities of collective efforts toward enhanced cyber security at the global, regional and national levels. International and national legislations, from the Council of Europe Convention on Cybercrime, to the African Union Convention on Cyber Security and Personal Data Protection, to the national laws seeking to implement the norms included in those conventions, may offer the impression of a growing consensus on how to strengthen cyber resilience. The analysis of the three countries indicates significant variance in approaches and responses to cyber security and cyber resilience.

This state of affairs is open to competing interpretations. From a more positive angle, this diversity can be perceived as the result of a successful interaction between international norms, which establish broad frameworks and set shared standards, and national legislations and practices, which adapt and localize these norms to ensure their local relevance. From a more critical point of view, some of the laws that are being discussed or the practical responses that are being publicly articulated can be seen instead as a tactic to please donors and international organizations, while implementation takes a different route.

As this short paper seeks to explain, a third interpretation is possible, which calls for a more participatory agenda in deciding norms and procedures to reinforce cyber resilience at the national and regional level. Rather than reproducing the cliché that good provisions are poorly implemented in Africa, either because of a lack of means or because political actors on the continent may use them to pursue particular agendas, this interpretation more broadly cautions toward the ample discretionary power entrusted to governments and private companies by the (global or national) securitization agenda, and suggests avoiding treating cyber security as simply a technical problem requiring technical solutions. The three concepts of emulation, extraversion and enculturation adopted here are meant to establish clearer links between the technical, social and political. The debate about cyber resilience in Africa is in the early stages and these categories should be interpreted simply as an encouragement to break down the prevalent narrative that Africa needs to catch up with other countries, and highlight some of its contradictions. There are multiple paths that can lead to reinforcing a country's ability to withstand or respond to an attack and some of them may need spaces for discussion among a broader variety of stakeholders than the small niche that has driven the agenda to date.

WORKS CITED

Access. 2014. "African Union Adopts Framework on Cyber Security and Data Protection." www.accessnow.org/blog/2014/08/22/african-union-adopts-framework-on-cyber-security-and-data-protection.

Agence France-Presse. 2014. "Kenya Arrests 77 Chinese Nationals in Cybercrime Raids." *The Guardian*, December 5. www.theguardian.com/world/2014/dec/05/kenya-chinese-nationals-cybercrime-nairobi.

Bayart, J.-F. 2000. "Africa in the World: A History of Extraversion." *African Affairs* 99 (395): 217–67.

Carrier, N. and Lochery, E. 2013. "Missing States? Somali Trade Networks and the Eastleigh Transformation." *Journal of Eastern African Studies* 7 (2).

Cassim, F. 2011. "Addressing the Growing Spectre of Cybercrime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players." *Comparative and International Law and Justice South Africa* 44: 123–38.

Citizen Lab. 2013. "You Only Click Twice: FinFisher's Global Proliferation." https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

———. 2015. "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware." https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

Daily Nation. 2015. "Try Crime Suspects Here." *Daily Nation*, January 15. www.nation.co.ke/oped/Editorial/China-Kenya-Hacking-Trial/-/440804/2590722/-/fcv6r1z/-/index.html.

Gagliardone, I. 2014. "Media Development with Chinese Characteristics." *Global Media Journal* 4 (2): 1–16.

Government of Kenya. 2014. Cybersecurity Strategy. Ministry of Information Communications and Technology.

Greenwald, G. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books/Henry Holt.

Harris, A., S. Goodman and P. Traynor. 2013. "Privacy and Security Concerns Associated with Mobile Money Applications in Africa." *Washington Journal of Law, Technology and Arts* 8 (3): 245–64.

Herbling, D. 2014. "Kenyans Move Sh 1.1trn on Mobile Phones in 6 Months." *Business Daily*, August 10. www.businessdailyafrica.com/Kenyans-move-Sh1-1trn-on-mobile-phones-in-6-months/-/539552/2414794/-/y22x2tz/-/index.html.

Howell, J. and J. Lind. 2009. *Counter-Terrorism, Aid and Civil Society: Before and After the War on Terror*. Basingstoke, UK: Palgrave Macmillan.

Human Rights Watch. 2013. "Ethiopia: Terrorism Law Decimates Media." www.hrw.org/news/2013/05/03/ethiopia-terrorism-law-decimates-media.

ISACA. 2014. "European Cybersecurity Implementation: Resilience." www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Resilience_res_Eng_0814.pdf?regnum=256607.

ITU. 2015. ICT Statistics. www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Jackson, T. 2015. "Can Africa Fight Cybercrime and Preserve Human Rights?" BBC News. www.bbc.com/news/business-32079748.

Kagwanja, P. and M. Karanja. 2014. "How Cybercrime Complicates War on Terror." *The East African*, August 18. www.theeastafrican.co.ke/news/How-cyber-crime-complicates-war-on-terror/-/2558/2422854/-/item/0/-/3ur4taz/-/index.html.

Kharouni, L. 2013. "Africa: A New Safe Harbor for Cybercriminals?" Trend Micro Incorporated Research Paper. www.trendmicro.co.uk/media/misc/africa-new-safe-harbor-for-cybercriminals-en.pdf.

Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi and B. Shiyayo. 2014. "Kenya Cybersecurity Report 2014." www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf.

Little, P. 2003. *Somalia: Economy without State*. Bloomington, IN: Indiana University Press.

Macharia, J. 2014. "Africa Needs a Cybersecurity Law But AU's Proposal Is Flawed, Advocates Say." http://techpresident.com/news/wegov/24712/africa-union-cybersecurity-law-flawed.

Makulilo, A. B. 2012. "Privacy and Data Protection in Africa: A State of the Art." *International Data Privacy Law* 2 (3): 163–78.

Mohamed, H. 2013. "Electronic Transfers Improve Somalia Economy." Aljazeera. www.aljazeera.com/indepth/features/2013/08/20138311416149256 82.html.

Mukinda, F. 2014. "Fraudsters Find Easy Cash in Mobile Banking, Report Says." *Daily Nation*, September 7. http://mobile.nation.co.ke/news/-/1950946/2444632/-/format/xhtml/-/10da2sbz/-/index.html.

Mwenesi, S. 2014a. "ICT Contribution to Kenya's GDP now at 12.1%." Human IPO, July 22. www.humanipo.com/news/46203/ict-contribution-to-kenyas-gdp-now-at-12-1/.

———. 2014b. "World Bank Allocates $12m for Kenya County for ICT projects." Human IPO, April 17. www.humanipo.com/news/42926/world-bank-allocates-12m-for-kenya-county-ict-projects/.

Nyambura-Mwaura, H. 2013. "Somalia's Hormuud Rings up Telecom Profits Despite Anarchy." Reuters, November 13. http://uk.reuters.com/article/2013/11/13/uk-somalia-hormuud-idUKBRE9AC0WQ20131113.

Nzwili, F. 2015. "China and Kenya at Odds over Suspected Chinese Cyber Criminals." *The Christian Science Monitor*, January 26. www.csmonitor.com/World/Africa/2015/0126/China-and-Kenya-at-odds-over-suspected-Chinese-cyber-criminals.

Otieno, J. 2014. "Worries over New Avenues of Cybercrime." *The East African*, September 22. www.theeastafrican.co.ke/news/Worries-over-new-avenues-of-cyber-crime/-/2558/2461630/-/vsn7k0z/-/index.html.

Otuki, N. 2014. "Beijing Says Runda Fraud Ring Likely Targeted China." *Business Daily*, December 5. www.businessdailyafrica.com/Beijing-says-Runda-fraud-ring-targeted-China/-/539546/2546306/-/item/0/-/v9hr5bz/-/index.html.

Quarshie, H. O. and A. Martin-Odoom. 2012. "Fighting Cybercrime in Africa." *Computer Science and Engineering* 2 (6): 98–100.

Penicaud, C. and F. McGrath. 2014. "Innovative Inclusion: How Telesom ZAAD Brought Mobile Money to Somaliland. GSMA Mobile Money for the Unbanked Programme.

Ploch, L. 2010. "Countering Terrorism in East Africa: The U.S. Response." CRS Report for Congress, Congressional Research Service.

Protalinski, E. 2012. "Former Pentagon Analyst: China has Backdoors at 80% of Telecoms." ZDNet, July 14. www.zdnet.com/article/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms/.

Rid, T. 2014. "Snowden, 多谢 多谢." Kings of War, March 23. http://kingsofwar.org.uk/2014/03/snowden-thanks-very-much/.

Stremlau, N. 2012. "Somalia: Media Law in the Absence of a State." *International Journal of Media and Cultural Politics* 8 (2,3): 159–74.

Stremlau, N. and R. Osman. 2015. "Courts, Clans and Companies: Mobile Money and Dispute Resolution." *Stability: International Journal of Security and Development* 4 (1).

UN Security Council. 2001. Resolution 1373, New York, September 28.

Yilma, K. 2014. "Developments in Cybercrime Law and Practice in Ethiopia." *Computer Law & Security Review* 30 (6): 720–35.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Vice President of Public Affairs	Fred Kuntz
Director of the Global Economy Program	Domenico Lombardi
Vice President of Finance	Mark Menard
Chief of Staff and General Counsel	Aaron Shull

Publications

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Vivian Moser
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Graphic Designer	Melodie Wakefield
Graphic Designer	Sara Moore

Communications

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org