SAIIA
SOUTH AFRICAN INSTITUTE OF INTERNATIONAL AFFAIRS

OCCASIONAL PAPER 275

JANUARY 2018

BALANCING CYBER SECURITY AND INTERNET FREEDOM IN AFRICA

YARIK TURIANSKYI

African perspectives. Global insights.

SOUTH AFRICAN INSTITUTE OF INTERNATIONAL AFFAIRS

The South African Institute of International Affairs (SAIIA) has a long and proud record as South Africa's premier research institute on international issues. It is an independent, non-government think tank whose key strategic objectives are to make effective input into public policy, and to encourage wider and more informed debate on international affairs, with particular emphasis on African issues and concerns. It is both a centre for research excellence and a home for stimulating public engagement. SAIIA's occasional papers present topical, incisive analyses, offering a variety of perspectives on key policy issues in Africa and beyond. Core public policy research themes covered by SAIIA include good governance and democracy; economic policymaking; international security and peace; and new global challenges such as food security, global governance reform and the environment. Please consult our website www.saiia.org.za for further information about SAIIA's work.

GOVERNANCE AND APRM PROGRAMME

SAIIA's Governance and African Peer Review Mechanism (APRM) programme aims to place governance and African development at the centre of local and global discussions about the continent's future. Its overall goal is to improve the ability of the APRM to contribute to governance reforms, institutions and processes. The programme focuses on: Enhancing meaningful and authentic participation of non-state actors in Country Self-Assessment Review (CSAR) and National Programme of Action (NPoA) processes; increasing knowledge among key decision-makers of the need for Country Level Institutions to be functional, have political support and enjoy legitimacy; increasing the capacity and functionality of official APRM institutions; and contributing to the identification of critical issues for governance reform in Africa through the APRM.

SAIIA gratefully acknowledges the Swedish International Development Cooperation Agency (Sida), which generously supports the Governance and APRM Programme.

PROGRAMME HEAD Steven Gruzd, steven.gruzd@wits.ac.za

Please note that all currencies are in US$ unless otherwise indicated.

ABSTRACT

This paper discusses the current state of cyber security and policies in Africa, with a specific focus on Kenya and South Africa as continental leaders in technology. Globally, Internet freedoms are on the decline and Africa is no exception. In 2016 at least 10 African states cut off access to the Internet, social media websites or messaging apps. This is happening as governments attempt to curtail the transparency, information-sharing and mobilisation potential of the Internet. At the same time, the rise in cybercrimes and the emergence of cryptocurrencies call for improved regulatory frameworks. Governments, not only in Africa but also worldwide, often seem to be a few steps behind, owing to the rapid development of new technologies. This paper analyses how technological advances could ultimately improve governmental accountability. It concludes by arguing for a middle ground in cyber policies, between the need for Internet freedoms, on the one hand, and policies that protect citizens and companies against crime, on the other.

ABOUT THE AUTHOR

YARIK TURIANSKYI is the Deputy Head of the Governance and African Peer Review Mechanism (APRM) Programme at the South African Institute of International Affairs. He has been studying and working on the APRM since 2006. He holds an MA in Political Science from the University of Pretoria and is the co-editor of *African Accountability: What Works and What Doesn't* (SAIIA, 2015).

Matebe Chisiza is thanked for her valuable research assistance in writing this paper.

ABBREVIATIONS AND ACRONYMS

EAC	East African Community
ECOWAS	Economic Community of West African States
ICT	information and communications technology
IGF	Internet Governance Forum
ISP	Internet service provider
ITU	International Telecommunication Union
MSI	multi-stakeholder initiative
SADC	Southern African Development Community
SDGs	Sustainable Development Goals
UNECA	UN Economic Commission for Africa

INTRODUCTION

Internet freedoms declined globally in 2016 for the sixth consecutive year, according to Freedom House.[1] The 'Twitter Revolutions' of 2011 during the Arab Spring made many governments fearful of the power of the Internet. While some researchers question social media's contribution to socio-political change in the region, they do nonetheless admit that it helped to amplify discontent.[2] The mobilisation potential of social media is enormous, allowing people to connect, discuss and rally with unprecedented ease. Unlike older forms of communication such as a telephone call, which usually connects one person to another, modern technology can bring together much larger groups of people simultaneously. Facebook posts and Tweets were shared across people's social media timelines, ultimately resulting in mass-scale protests in various countries in 2011, including Tunisia, Libya and Egypt. Officials expected to physically disperse protests before they got out of hand. Yet mobilisation in cyber space enabled protesters to organise spontaneously, quickly and efficiently, making it difficult for governments to respond in the same manner. According to Philip Howard, a Professor in Communications at the University of Washington,[3]

> Our evidence suggests that social media carried a cascade of messages about freedom and democracy across North Africa and the Middle East, and helped raise expectations for the success of political uprising. People who shared interest in democracy built extensive social networks and organised political action. Social media became a critical part of the toolkit for greater freedom.

Since the events of 2011 many states, both democratic and authoritarian, have passed new security and cyber laws to limit Internet freedoms and authorise surveillance. Others have utilised older and outdated security laws and applied them to new technologies and social media. Governments have much to fear from the Internet: increased information, transparency, the ability to report on government abuses and irregularities in real time, and its mobilisation potential. Open and free Internet is increasingly under attack, with many governments trying to control all or at least certain parts of it. Furthermore, online surveillance is increasing, with more and more people being intimidated or detained because of their online activities.[4]

1 Freedom House, 'Freedom on the Net 2016: Silencing the messenger – communication apps under pressure', 14 November 2016, https://freedomhouse.org/article/freedom-net-2016-silencing-messenger-communication-apps-under-pressure, accessed 10 February 2017.

2 Radcliffe D, 'Five years after the Arab Spring, how does the Middle East use social media?', *The Conversation*, 24 February 2016, https://theconversation.com/five-years-after-the-arab-spring-how-does-the-middle-east-use-social-media-54940, accessed 18 October 2017.

3 See O'Donnell C, 'New study quantifies use of social media in Arab Spring', *University of Washington News*, 12 September 2011, http://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/, accessed 17 October 2017.

4 DW Akademie, *Internet Governance Guidebook: Top Resource for the Global South*, 2016, http://www.dw.com/en/internet-governance-guidebook-top-resource-for-the-global-south/a-19321335, accessed 16 October 2017.

The most concerning examples are found in authoritarian regimes, where governments use antiterrorism laws to prosecute users for simply writing about democracy, religion or human rights.[5] Such governments also cut Internet access to combat online protests before they materialise in front of government buildings. In 2016 at least 10 African countries – Burundi, Cameroon, Chad, the Democratic Republic of Congo, Ethiopia, Gabon, The Gambia, Mali, Uganda and Zimbabwe – shut down social media sites and/or messaging apps, or even cut off access to the Internet entirely before, during or after elections or in response to protests. Social media surveillance by authoritarian governments is also prevalent. In The Gambia, a Facebook post calling on young people to join peaceful protests disappeared and was replaced with a warning to abide by the law. The author of the post left the country, citing death threats.

Other African governments, some of which are usually considered more liberal, attempted to curtail Internet freedoms but backed down following pressure from citizens. For instance, Ghana announced it would shut down the Internet during the December 2016 elections, but later backtracked. Elections were peaceful and the opposition candidate won. Nigerian social media enthusiasts successfully lobbied against the proposed 2015 Frivolous Prohibition Bill, which sought to regulate messaging apps, including WhatsApp, BlackBerry Messenger and Facebook Messenger, and the government withdrew the bill. However, several bloggers who criticised then president Goodluck Jonathan were arrested.[6] Clearly, there are concerns across the political spectrum on how to deal with rapidly evolving technologies, in the Global South as well as the Global North. The legal battle between Apple and the US' Federal Bureau of Investigation over unlocking an iPhone belonging to a terrorist in the US, and the UK government's saying that security services must have access to encrypted messaging applications such as WhatsApp, are examples of this. Both liberal and authoritarian governments are thus attempting to exercise more control over the Internet, online content and digital communication. These technologies evolve at a rapid pace and tend to remain ahead of legislation. The difference between liberal and authoritarian regimes is how they approach this phenomenon. The former attempt to consult with relevant stakeholders and their citizens, following due processes established through precedents set by other regulatory issues in the past. The latter impose censorship and block content unilaterally, without any form of consultation. Yet the Internet challenges both approaches.

Governments need to adopt a careful balancing act to ensure that there are appropriate regulations that allow them to deal with cybercrime and terrorists without infringing on online freedoms or providing opportunities for security services to spy on their citizens

This paper argues that governments need to adopt a careful balancing act to ensure that there are appropriate regulations that allow them to deal with cybercrime and terrorists without infringing on online freedoms or providing opportunities for security services to spy on their citizens. 'Resolving these questions is about balancing a variety of rights, centrally media freedom.'[7] This will not be easy. The same technologies that enable

5 Freedom House, *op. cit.*

6 *Ibid.*

7 Bird W, 'Media freedom for all in our young democracy', *Daily Maverick*, 10 October 2017, https://www.dailymaverick.co.za/opinionista/2017-10-10-media-freedom-for-all-in-our-young-democracy/, accessed 16 October 2017.

increased transparency are also used by terrorists to carry out acts of terror and recruit converts. The international dimension of such crimes further complicates the situation. Domestic laws are insufficient – global Internet governance is needed too. Yet significant differences remain between countries on how the Internet should be governed, and it is unlikely that consensus will be reached any time soon.

There are few avenues to discuss these challenges globally. One of these is the Internet Governance Forum (IGF), a multi-stakeholder dialogue on key Internet governance issues, launched by the UN in 2006.[8] Respondents to a 2017 survey regarded the IGF as the most appropriate platform to discuss and learn about Internet content regulation.[9] However, the respondents felt that cybersecurity regulation issues were better addressed at the International Telecommunication Union (ITU) level, as well as by national governments. The ITU is a specialised agency of the UN, dealing with information and communications technologies (ICTs) and founded on principles of international cooperation between governments (member states) and the private sector (sector members, associates and academia).[10]

Both of these forums are examples of multi-stakeholder initiatives (MSIs) – voluntary partnerships between governments, civil society and the private sector. These are increasingly being used in multiple countries by citizens, businesspersons, public officials and politicians to collaboratively and holistically address formidable development challenges and strengthen legal frameworks. MSIs operate on the premise that, through the enactment of policy reform, increased transparency and enhanced stakeholder participation, they can facilitate improved governance outcomes.[11] Indeed, MSIs are very useful for bringing together different actors, with different perspectives, to discuss solutions to complex, multi-dimensional issues. This is certainly applicable in the case of Internet governance, given the various points of view, agendas and approaches. However, a major criticism of MSIs is that they are often used as talk shops and fail to achieve concrete, measurable progress. Research ICT Africa makes an important point in this regard, stating that 'Internet governance is not just about discussing internet issues and sharing ideas and opinions. Reaching an agreement in these fora is of paramount importance.'[12]

8 IGF (Internet Governance Forum), 'About IGF', https://www.intgovforum.org/multilingual/content/about-igf-faqs, accessed 17 October 2017.

9 Research ICT Africa, 'Findings of a Survey on Multi stakeholder Participation in Internet Governance from Africa', 28 June 2017, http://researchictafrica.net/2017/06/28/findings-of-a-survey-on-multistakeholder-participation-in-internet-governance-from-africa, accessed 17 October 2017.

10 ITU (International Telecommunication Union), 'About', http://www.itu.int/en/about/Pages/default.aspx, accessed 16 October 2017.

11 SAIIA (South African Institute of International Affairs), 'Literature Review on Multi-Stakeholder Initiatives', 2016 (unpublished).

12 Research ICT Africa, *op. cit.*

CYBER POLICIES IN AFRICA

Approximately 27.7% of Africa's 1.2 billion people had access to the Internet in 2017, compared to 54% in the rest of the world.[13] However, some countries, such as Kenya and South Africa, are ahead of the curve. Kenya is emerging as a technological hub, with the highest estimated Internet penetration in Africa. It is important to note that these estimates differ between various reports. For instance, the '2016 State of the Internet in Kenya' report estimates Internet penetration at 85.3%,[14] while the 'White Paper 2017: Trends from the Kenyan Smartphone and E-Commerce Industry' claims that 67% of the population have access to the Internet.[15] A growing number of young Kenyans have been using social media to raise critical issues in the governance sphere, such as the (mis)use of government funds and corruption charges against government officers. The country also houses numerous information technology start-ups and is home to Ushahidi. This company used geo-tagging (identification of where users are geographically) to report voting irregularities and political violence during the December 2006 elections, thereby determining hotspots and facilitating workable solutions. It is widely recognised that Ushahidi identified outbreaks of violence more quickly, and captured many more instances of violence, than traditional media. In a recent visit to Nairobi, Facebook founder Mark Zuckerberg stated that the country is a 'world leader in mobile money', in reference to M-Pesa, the mobile phone-based money transfer, financing and microfinancing service launched in 2007.[16]

However, Kenya's cyber policies are a mixed bag. While the country's Access to Information Act 2016 paves the way for citizens to seek information from government agencies, officials have also been abusing older laws to silence dissenting voices. Specifically, Kenyan authorities often utilised the 'improper use of licenced telecommunications gadget' under Section 29 of the Information and Communications Act. It criminalised publishing information online that was deemed unlawful by authorities. In a positive move, this section has recently been declared unconstitutional. Police also charge bloggers with 'undermining the authority of a public officer' for criticising government officials on social media, a charge under Section 132 of the Penal Code, enacted in 1948 under colonial rule. Kenya's government likewise threatened an Internet shutdown should there be instability during the August 2017 elections.[17]

13 Internet World Stats, 2017, http://www.internetworldstats.com/stats1.htm, accessed 11 December 2017.

14 BAKE (Bloggers Association of Kenya), *State of the Internet in Kenya*, Report, November 2016, http://www.ifree.co.ke/wp-content/uploads/2016/11/State-of-Internet-Report-Kenya-2016.pdf, accessed 28 February 2017.

15 Daily Nation Kenya, '*New study shows more Kenyans have Internet access*', 19 April 2017, http://www.nation.co.ke/news/Internet-access-grows-in-Kenya/1056-3895304-nsw0nnz/index.html, accessed 1 October 2017.

16 *Forbes*, 'Africa will build the future says Zuckerberg, visits Kenya on first African trip', 1 September 2016, http://www.forbes.com/sites/tobyshapshak/2016/09/01/africa-will-build-the-future-says-zuckerberg-visits-kenya-on-first-african-trip/#5a077eb85214, accessed 15 March 2017.

17 BAKE, *op. cit*.

There are, however, positive developments as well, exemplified by how the Kenyan government is using new technologies to improve service delivery. For instance, it partnered with cell phone service provider Safaricom in launching subscription service Kipokezi,[18] which provides online chatting and email on previous-generation, non-smart phones. Within the e-government framework, this facilitates dialogue between authorities and citizens, especially those in remote areas. In addition, the Kenyan government is increasing ease of access to services and improving transparency. The former is done through eCitizen, which allows citizens to access important services electronically, such as issuing of marriage certificates, driver's licences, visas, immigration and civil registration services. Transparency is improved with an open data platform, introduced with the purpose of making public government databases more accessible.[19] These show that the Kenyan government is eager to utilise technology to improve access to services and ease the flow of information, but at the same time is overly sensitive to the accountability and civil liberty elements that technology brings.

The Kenyan government is eager to utilise technology to improve access to services and ease the flow of information, but overly sensitive to the accountability and civil liberty elements that technology brings

South Africa is another interesting case study. It has numerous innovative ICT companies, as well as one of the most liberal constitutions in the world. However, its new Cybercrimes and Cybersecurity Bill cannot be described in the same manner. The bill will be tabled in Parliament shortly, following its publication in August 2015. Numerous experts and civil society organisations have criticised its overly broad mandate. Yet the government has a very different interpretation of the bill, and claims that it will not give the State Security Agency the power to control the Internet or spy on users. The bill has been through a number of drafts, which have removed some of its more controversial aspects, but concerns still remain.

Worryingly, the bill does not contain a public interest defence clause. South African civil society activists Murray Hunter and Allison Tilley argue that[20]

> [t]here are some 'cybercrimes' that make society better: the leaking of secret government information that exposes human rights abuses, or the leaking of the Panama Papers that exposed money laundering and tax evasion, are clearly in the public interest.

There are numerous other criticisms. According to Michalsons law firm[21], the bill creates approximately 50 new offences related to data, messages, networks and computers, among others, the penalties for which range from one to 10 years in prison or a fine of up to ZAR[22] 10 million ($731,500). The offences include unlawful interception of data; fraud;

18 Cyclopedia, 'e-Government', 2017, http://kuliah-karyawan-up45.minyak.us/IT/en/cyclopedia-691/e-Government_18588_kuliah-karyawan-up45-minyak.html, accessed 25 March 2017.

19 Open Data Kenya, http://www.opendata.go.ke, accessed 15 March 2017.

20 Hunter M & A Tilley, 'Cybercrimes Bill makes cyberspace less secure,' *Daily Maverick*, 28 July 2017, https://www.dailymaverick.co.za/article/2017-07-28-groundup-cybercrimes-bill-makes-cyberspace-less-secure/#.WeCyN2hL82w, accessed 13 October 2017.

21 Michalsons, 'Cybercrimes and Cybersecurity Bill – Overview of the Cyber Bill,' https://www.michalsons.com/blog/cybercrimes-and-cybersecurity-bill-the-cac-bill/16344, accessed 13 December 2017.

22 Currency code for the South African rand.

infringement of copyright; harbouring or concealing a person who commits an offence; dissemination of a data message that advocates, promotes or incites hate, discrimination or violence; and computer-related espionage. Furthermore, '[T]he Cybercrimes and Cybersecurity Bill gives the South African Police and the State Security Agency extensive powers to investigate, search, access, and seize just about anything – like a computer, database, or network.'[23] A number of new institutions will also be established, including a National Cybercrime Centre, Cyber Response Committee, Cyber Command, Cyber Security Hub and a 24/7 Point of Contact, to deal with these matters.[24]

Under the provisions of the bill, South Africa's president may enter into agreements with foreign states to promote cyber security. This is disconcerting, given that the country was one of the few to side with China and Russia in voting against a landmark UN resolution on Internet freedoms in July 2016.[25] South Africa seems to want to follow Russia's lead on other cyber matters as well. Following comments by then South African state security minister David Mahlobo about contemplating the regulation of social media in the country, then communications minister Faith Muthambi met one of her Russian counterparts. After the meeting she talked about sharing 'best practices in the area of communications and media'.[26] In fact, Russia's example should be considered 'bad' or 'worst' practice. In June 2016 Russia passed a draconian antiterrorism law that requires all 'organisers of information online' – a very broad definition that could include Internet service providers (ISPs) and foreign social media companies – to provide the country's security services with tools to decrypt any information they transmit, essentially mandating backdoor access. ISPs are also required to keep the content of users' communications, including calls, texts, images, videos and other data, for up to six months.[27] Due to non-compliance LinkedIn was blocked in 2016 and Facebook was recently threatened with the same treatment.[28]

Ethiopia is a more extreme example of an authoritarian government that tries to control the Internet. The country's online penetration level is only 12%, but following months of clashes between the police and the Oromo and Amhara ethnic communities in 2016 the government blocked access to the Internet. Social media networks such as Facebook, LinkedIn and Twitter remained blocked at the time of writing.[29] Citizens have been jailed for Facebook posts deemed 'radical blogging' and the country has blocked access to all

23 Michalsons, *op. cit*.

24 *Ibid.*

25 *Daily Maverick*, 'SA votes against internet freedoms in UN resolution', 4 July 2016, https://www.dailymaverick.co.za/article/2016-07-04-sa-votes-against-internet-freedoms-in-un-resolution/#.WR2bz2h97b0, accessed 18 May 2017.

26 Gerber J, 'Muthambi looks to draconian Russia for social media policy', *City Press*, 7 March 2017, http://city-press.news24.com/News/muthambi-looks-to-draconian-russia-for-social-media-policy-20170306, accessed 10 March 2017.

27 Freedom House, *op. cit*.

28 Khrennikov I, 'Russia threatens to shut Facebook over local data storage laws', *Bloomberg*, 26 September 2017, https://www.bloomberg.com/news/articles/2017-09-26/russia-threatens-to-shut-facebook-over-local-data-storage-laws, accessed 18 October 2017.

29 Freedom House, *op. cit*.

social media following the wave of anti-government protests in 2016.[30] Its overly broad definitions of terrorism also resulted in a blogger, who had merely facilitated a course on digital security, being sentenced to five years in prison.[31] Even worse off is its neighbour, Eritrea. It is reportedly the most censored country in the world,[32] and this repressive climate extends to the Internet, which is highly restricted. The only telecommunications company, EriTel, is state-owned. It restricts the number of websites that citizens can visit, and less than 1% of people are able to go online.[33]

Monitoring citizen activity online and using it as evidence to act against dissenting voices represents the dark side of technology. Thus it is important to guard against a naïve view of technology being only a liberating tool for citizens globally. While technology does have the potential to promote transparency, it can also be used for control, spying and propaganda by authoritarian governments. Some do it intentionally and others unintentionally, but many governments are trying to control the technology that has produced the greatest advance in human communication and free speech since the telephone. Given the Internet's decentralised nature, this is proving difficult, especially with the emergence of cryptocurrencies, which are easily transferred across borders with a few clicks of a mouse. While moderate regulation in the cybersphere can be justified, attempts to control the Internet, by governments that often have little understanding of the technologies that underpin it and are threatened by the freedom of speech that it brings, need to be discouraged.

A 2016 UN Human Rights Council resolution was passed condemning Internet shutdowns, and the UN General Assembly has declared the Internet a human right.[34] There have, however, been debates on what this means practically. Indra de Lanerolle compares the right to access the Internet with the right to freedom of expression, both of which are 'enabling rights'. Freedom of expression enables or allows citizens to access or defend other rights. Similarly, the Internet enables citizens to participate in social, economic and political life.[35] It is also increasingly seen as being crucial to development. The Sustainable Development Goals (SDGs) contain commitments to increase affordable access to the

30 Jeffrey J, 'Ethiopia's internet crackdown hurts everyone', *Irin News*, 17 November 2016, https://www.irinnews.org/analysis/2016/11/17/ethiopia%E2%80%99s-internet-crackdown-hurts-everyone, accessed 19 February 2017.

31 Freedom House, *op. cit.*

32 Committee to Protect Journalists, '10 most censored countries', 2015, https://cpj.org/2015/04/10-most-censored-countries.php, accessed 20 February 2017.

33 Winter C, 'Eritrea's communications disconnect', *Bloomberg*, 26 June 2014, https://www.bloomberg.com/news/articles/2014-06-26/eritrea-worlds-least-connected-country-tech-wise, accessed 12 February 2017.

34 UN, Human Rights Council, 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development', 27 June 2016, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf, accessed 20 October 2017.

35 De Lanerolle I, 'Internet freedom: Why access is becoming a human right', *The Conversation*, 1 June 2016, https://theconversation.com/internet-freedom-why-access-is-becoming-a-human-right-59125, accessed 16 October 2017.

Internet in least-developed countries,[36] as well as targets on proportions of schools with computer and Internet access, youth and adults with ICT skills, mobile network coverage and individuals using the Internet.[37] The SDGs contain a total of seven ICT indicators covering six targets, under SDGs 4, 5, 9 and 17.[38]

GOVERNMENTS AND TECHNOLOGY: NOW AND IN FUTURE

The Internet threatens many governments with public criticism of policies and officials, and as an outlet to publish exposés of corruption, incompetence and maladministration. Further to this is its potential for mass mobilisation that can quickly manifest as street protests. As the influence of technology increases and starts to challenge central financial authorities through unregulated cryptocurrency flows across borders, more governments are likely to try to either invoke outdated legislation or pass new draconian laws to silence dissenters and establish greater control.

While it is too early to worry about singularity,[39] significant breakthroughs in the development of artificial intelligence are predicted by 2040. These will raise entirely different ethical and moral questions. As discussed above, technology can be used as tool for control as well as for openness. Physicist Stephen Hawking notes that while technological advances have helped humanity achieve seemingly impossible feats, they may also lead to its demise. Better global controls may therefore be needed.[40] At the moment, there are too few collective efforts on regulating the Internet, cryptocurrencies and artificial intelligence. Critics note that this will lead to a widening gap between the frontiers of technology and the mechanisms of global governance.[41]

Some governments are starting to embrace technology. The Kenyan government's actions to facilitate access to government services and information were mentioned earlier. But there are other examples too. Namibia pioneered electronic voting in Africa. This has

36 DW Akademie, *op. cit.*

37 UNECA (UN Economic and Social Council), 'Report of the Inter-Agency and Expert Group on Sustainable Development Goal Indicators', 19 February 2016, https://unstats.un.org/unsd/statcom/47th-session/documents/2016-2-IAEG-SDGs-Rev1-E.pdf, accessed 16 October 2017.

38 ITU, *op. cit.*

39 While different definitions of the term 'singularity' exist, it is commonly understood to mean the point at which non-biological intelligence will match the depth and subtlety of human intelligence.

40 Bowerman M, 'Stephen Hawking: Technological advances may destroy us all', *USA Today*, 7 March 2017, http://www.usatoday.com/story/tech/nation-now/2017/03/07/stephen-hawking-technological-advances-may-destroy-us-all/98841862/, accessed 25 March 2017.

41 Evanoff K & M Roberts, 'A Sputnik moment for artificial intelligence geopolitics', Council on Foreign Relations, blog post, 7 September 2017, https://www.cfr.org/blog/sputnik-moment-artificial-intelligence-geopolitics?utm_medium=social_earned&utm_source=tw&utm_campaign=blog&utm_term=sputnik-moment&utm_content=091017, accessed 8 September 2017.

proved successful despite some teething problems, and also seems to attract a larger-than-normal youth vote. It has simplified counting and prevented obvious forms of vote rigging and ballot-box stuffing. However, some opposition parties have been critical of the innovations, meaning that greater voter education and sensitisation about new technologies need to take place.

In Morocco the government has established online forums that allow the general public to make suggestions on establishing electronic government services, submit ideas on simplifying administrative tasks and provide input on improving administrative issues. It is also possible to comment on draft legislation and decrees.[42] Liberia has made great strides in using technology to ease the flow of information, and has created laws that ensure all citizens have the right to access public information. In 2010 it became the first country in West Africa to pass legislation on comprehensive freedom of information, although years of civil war have left the government with limited capacity to effectively put it into practice.

Yet a government's use of technology should not be mistaken for Internet freedom, as the arrests in Kenya, discussed earlier, show. In Morocco, YouTube footage of a man lifting asphalt barehanded from a local road led to his arrest for allegedly defaming the official responsible for the poor construction.

With almost 200 million people in Africa aged between 15 and 24, the continent has the world's youngest population.[43] The eagerness of this demographic to embrace social media, online services and technology for political and social activism has already been demonstrated by the Arab Spring uprisings and recent demonstrations at South African higher education institutions during the #RhodesMustFall and #FeesMustFall campaigns. Increasingly affordable Internet and other technologies make it possible for citizens to express themselves, communicate with each other, seek information and use these as tools for mobilisation. Yet these positive developments and opportunities exist side by side with more troubling ones, including online surveillance, both poorly worded and intentionally draconian cyber security laws, harassment and a lack of awareness of digital rights.[44]

Governments are aware of their citizens' willingness to embrace social media and technology as tools in demanding social and political change, and are trying to find a way to deal with these. Indeed, regulatory laws are important, unless we want to enter a world of cyber anarchy. It is also important to recognise that such laws are important for combatting cybercrime, which is a growing global phenomenon. According to a 2013 report by Symantec Corporation, cybercrime is increasing at a more rapid rate in Africa than in any other area. Statistics from various sources indicate that many African countries

42 Kingdom of Morocco, 'e-Participation', http://www.egov.ma/en/e-participation, accessed 15 September 2016.

43 African Economic Outlook, http://www.africaneconomicoutlook.org/en/theme/youth_employment/, accessed 2 February 2017.

44 IDRC (International Development Research Centre), 'Protecting digital rights in Pakistan', 13 February 2017, https://www.idrc.ca/en/article/protecting-digital-rights-pakistan, accessed 12 March 2017.

are more prone to cyber-related threats owing to the high number of domains combined with weak network and information security.[45] Research from McAfee[46] shows that South Africa is losing approximately $550 million per year to cybercrime, while research by Serianu[47] shows that Kenya loses $146 million per year. The May 2017 WannaCry ransomware attack, which encrypted data on at least 200 000 computers in over 150 countries, highlighted the vulnerability of both government agencies and big commercial enterprises.[48] Once a computer was infected, a new browser tab opened, demanding $300 in Bitcoin to unfreeze the data. The scale of the attack caught governments and companies unprepared. While anti-virus and malware software has since been updated, new ways of extorting and stealing money are undoubtedly being devised by hackers.

WannaCry brought public attention to the issue of cybercrime and cryptocurrencies, and highlighted the need for joint action. In many cases existing national legislation and methods to combat cybercrime are outdated or ambiguous. Security laws and how they define national security give governments too much latitude to claim they are acting within the law. Overly broad laws result in convictions based on alleged defamation or insult, while they in fact aim to suppress information that is in the public interest. The governments that crack down on physical protests are attempting to do the same in the digital space, as well as conduct online surveillance of their citizens. Such extremes in policymaking – of either no regulation or over-regulation – must be avoided. The UN Economic Commission for Africa (UNECA) recently conducted a survey of 21 African countries that found that while many countries had proposed legislation, the level of deployment of security systems in both the private and the public sectors to combat cybercrime was low. This needs to be prioritised, as UNECA's research also shows that in major African cities, including Cairo, Johannesburg, Lagos and Nairobi, fraudulent financial transactions and child kidnappings, facilitated through the Internet, doubled between 2011 and 2014.[49]

South Africa and Kenya are the only two countries in Africa with complete Internet freedom, according to a 2016 report by Freedom House

Interestingly, in spite of some the concerns outlined above, South Africa and Kenya are the only two countries in Africa with complete Internet freedom, according to a 2016 report by Freedom House. The same report also states that two-thirds of all Internet users worldwide (67%) live in countries where criticism of the government, the military or

45 Symantec Corporation, *Internet Security Threat Report 2013*, 18, 2013, www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf, accessed 3 March 2017.

46 *BusinessTech*, 'The cost of cyber crime in South Africa', 10 June 2014, https://businesstech.co.za/news/internet/60021/the-cost-of-cyber-crime-in-south-africa/, accessed 12 March 2017.

47 Serianu, *Kenya Cyber Security Report 2015: Achieving Enterprise Cyber Resilience through Situational Awareness*, 2015, http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf, accessed 10 March 2017.

48 Wall M & M Ward, 'WannaCry: What can you do to protect your business?', *BBC News*, 19 May 2017, http://www.bbc.com/news/business-39947944, accessed 19 May 2017.

49 UNECA, 'Tackling the Challenges of Cybersecurity in Africa', Policy Brief, NTIS/002, 2014, https://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf, accessed 19 October 2017.

ruling family is subject to censorship.[50] It also mentions that censorship of social media and messaging apps is increasing, for two reasons. Firstly, these apps are able to spread information quickly and to large groups of people at the same time. Some of them, such as WhatsApp, also use encryption, which protects users from government surveillance. These restrictions are thus often imposed during protests or owing to national security concerns. Secondly, messaging apps such as Viber and audio-visual calling apps such as Skype are eroding the business models and profit margins of traditional telecommunications companies (in which many governments have a large stake).

Uniformity in cyber policies and their implementation may be necessary not only on the continental but also on the global level

Policymakers furthermore rarely understand how the Internet – and technology – works. This often results in cybersecurity laws that are poorly worded and unfeasible in practice. Potentially, governments could outsource work related to cyber security to experts in the field. However, this would be difficult in authoritarian states, whose cyber policies tend to protect those in power. More research is therefore needed on cyber policies in Africa – not only on the policies of individual countries but also on how regional blocs and continental bodies are addressing the situation. SAIIA's preliminary research shows little to no regional or continental input or guidance. The only continental document publicly available at this point is the AU's Convention on Cyber Security and Personal Data Protection,[51] which was adopted in 2014 as part of Agenda 2063, the continent's 50-year development vision. However, as of July 2017 only nine countries had signed it and only one (Senegal) had ratified and deposited it. While the reasons for this need to be researched further, one possibility is that the convention's provisions contain unclear terms that give too much room for interpretation.

Regionally, as far as data privacy protection is concerned, ECOWAS is the first and only subregional grouping in Africa to develop a concrete framework for data privacy legislation: the Supplementary Act on Personal Data Protection within ECOWAS of 2010. The East African Community (EAC) has established two instruments related to data privacy: the Bill of Rights for the EAC (passed in 2012) and the draft EAC Legal Framework for Cyber Laws of 2011. A model law for SADC, known as the SADC Model Law on Data Protection, was created in 2012, but little appears to have been done since then to make it binding on member states. However, implementation in member states is a challenge. The main reason is that none of these instruments, with the exception of the ECOWAS framework, are binding, but instead are viewed as templates for developing national legislation.[52] More consistency is therefore needed, especially at the continental level. Uniformity in cyber policies and their implementation may be necessary not only on the continental but also on the global level.

50 Freedom House, *op. cit.*

51 AU, 'Convention on Cyber Security and Personal Data Protection', 2014, https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection, accessed 15 February 2017.

52 Makulilo A, 'Myth and reality of harmonisation of data privacy policies', *Africa Computer Law & Security Review*, 21, 1, February 2015, pp. 78–89.

CONCLUSION

Citizens are increasingly using technology to communicate with their governments. The Internet is being utilised to increase governmental transparency, by making relevant documents available online and even making information about government processes publicly available. An example of this is Ukraine's ProZorro platform, an online public procurement platform that was created to make government tenders transparent. This initiative received the first prize at the Open Government Partnership Summit awards in Paris in December 2016.[53] There are numerous other platforms that are intended to improve communication between governments and citizens, but most of them are not widely known or used, at least not to the same extent as WhatsApp, Gmail or Instagram. Becoming mainstream is crucial for the success of a technological platform. This is why the most effective way for governments to communicate with their citizens, eg, to provide updates about service delivery or solicit inputs on policies, is through the use of existing mainstream platforms such as Facebook and Twitter.

The global dimension is another crucial factor. The Internet is able to transcend borders and connect citizens. According to Ronald Deibert, a leading expert on digital technology, '[cyberspace] is global commons … Something like the environment that we need to work together to steward and protect.'[54] This argument becomes particularly important as many governments try to adopt data localisation laws, intended to keep citizens' personal data in-country and subject to local regulation. This is why more intra-government efforts are needed, not only in regulating technology and cyberspace but also in promoting common platforms to increase governmental transparency.

With Internet freedoms on the decline and more governments targeting social media and messaging apps to halt rapid flows of information, stifling dissent and increasing surveillance of citizens, research and advocacy on cyber policies become crucial

As noted earlier, consensus on global Internet and artificial technology governance is unlikely to be achieved any time soon. This is owing to differing ideologies, as well as to the extent to which different governments want to control the World Wide Web. In the Global South, 'it is not difficult to find weak regulators and state actors, but powerful (often global) private sector actors in conflict with each other over the Internet's future direction'.[55] De Lanerolle points to recent conflicts in India and Africa regarding net neutrality and zero-rating of Internet services. Protection of data is another case that shows divergent government views. Laws governing data can range from the very specific (government data in Nigeria and health data in Australia) to all encompassing (such as in Russia, where LinkedIn is now blocked, as noted earlier, because all data collected from Russians must be stored and processed on servers located within the country).

The rise of the Internet goes hand in hand with new technologies, mobile apps and ways of doing business. The 'Fourth Industrial Revolution', defined by combining technologies

53 Prozorro, https://prozorro.gov.ua/en, accessed 16 October 2017.

54 IDRC, 'Canada's cyber steward on digital espionage, democracy and protecting the Internet', 16 December 2016, http://idrc.canadiangeographic.ca/blog/cyber-stewards-network-project.asp, accessed 24 October 2017.

55 De Lanerolle I, 'Book Review: Reimagining how to govern the Internet', *Information Technologies & International Development*, Special Issue, 12, 2, https://www.academia.edu/27796356/Reimagining_How_to_Govern_the_Internet, accessed 16 October 2017.

and blurring the space between the physical, digital and biological spheres, provides new opportunities and challenges for Africa. Entrepreneurial activities, creative solutions, information sharing and communication are now easier than ever before. But these often go hand-in-hand with governments' desire to control the activities of their citizens. Given the exponential rates of technology change and growth, most of these governments struggle to keep up with the latest advances. In order to ensure that restrictions and surveillance activities do not result in a crisis of democracy, meticulously planned and implemented legal and policy changes are required. With Internet freedoms on the decline and more governments targeting social media and messaging apps to halt rapid flows of information, stifling dissent and increasing surveillance of citizens, research and advocacy on cyber policies become crucial.

SAIIA'S FUNDING PROFILE

SAIIA raises funds from governments, charitable foundations, companies and individual donors. Our work is currently being funded by, among others, the Bradlow Foundation, the UK's Department for International Development, the Konrad Adenauer Foundation, the Royal Norwegian Ministry of Foreign Affairs, the Swedish International Development Cooperation Agency, the World Bank, the Swiss Agency for Development and Cooperation, the Open Society Foundations, the Organisation for Economic Co-operation and Development, Oxfam South Africa and the Centre for International Governance and Innovation. SAIIA's corporate membership is drawn from the South African private sector and international businesses with an interest in Africa. In addition, SAIIA has a substantial number of international diplomatic and mainly South African institutional members.

African perspectives.
Global insights.

Jan Smuts House, East Campus, University of the Witwatersrand
PO Box 31596, Braamfontein 2017, Johannesburg, South Africa
Tel +27 (0)11 339–2021 • Fax +27 (0)11 339–2154
www.saiia.org.za • info@saiia.org.za