GLOBAL PARTNERS DIGITAL

November 2016

Mapping the Cyber Policy Landscape: Kenya

WRITTEN BY **NANJIRA SAMBULI, JULIET MAINA AND TYRUS KAMAU**

Global Partners Digital
Second Home
68 - 80 Hanbury Street
London
E1 5JL
+44 (0)203 818 3258
info@gp-digital.org
gp-digital.org

Global Partners & Associates Ltd
Registered in England and Wales

Designed by SoapBox
Typeset by Erwin Yin
Cover image adapted from David Nagy under Creative Commons Licence 2.0.
https://www.flickr.com/photos/ndave/

Company Nº 520 1603
VAT Nº 840 1912 54

GLOBAL PARTNERS DIGITAL

Mapping the Cyber Policy Landscape: Kenya

WRITTEN BY NANJIRA SAMBULI, JULIET MAINA AND TYRUS KAMAU

gp-digital.org

Acknowledgements

This mapping study was made possible with the support of Global Partners Digital's Cyber Capacity Building Programme. Special thanks go to the Ministry of ICT - Kenya, Communications Authority of Kenya, Central Bank of Kenya, Article 19 East Africa, KICTANet, CIPIT - Strathmore University, TESPOK, Watoto Watch Network and Simba-Safe Kenya for their query responses that have been invaluable input to the study.

CONTENTS

KENYA'S CYBERSECURITY LANDSCAPE

Background

Kenya, like many other countries, has been prone to a varied range of cyber threats and challenges arising from the advancement and ubiquity of ICTs, with legal frameworks playing catch up with these developments. The government of Kenya recognises this, and is in the process of developing and reviewing a number of legislative frameworks and institutions to equip them with mechanisms for addressing cybersecurity in the country.

The inclusiveness of the ongoing policymaking processes in the country varies. In some instances, stakeholders from the private sector, academia and civil society have been engaged throughout the process. The general public is typically engaged with through a public consultation phase, which is enshrined as a national value and a mandatory step in the legislative process guaranteed by the Constitution of Kenya, 2010.[1]

This mapping study has been undertaken against the backdrop of the Freedom Online Coalition's recommended definition of cybersecurity;[2]

PREAMBLE: International human rights law and international humanitarian law apply online and well as offline. Cybersecurity must protect technological innovation and the exercise of human rights.

DEFINITION: Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality* and integrity* of information and its underlying infrastructure so as to enhance the security of persons both online and offline. *as defined by ISO 27000 standard.*

Laws, regulations and policies pertaining to cybersecurity in Kenya largely approach it from the perspective of curbing cybercrime, and to a much lesser extent safeguarding the rights of citizens as they translate to an increasingly interconnected and inescapable digital realm.

However, with the recently released draft review of the National ICT Policy (discussed below), rights-based language has been introduced. The same is observed with the 2016 Computer and Cybercrimes Bill, which states in its "Memorandum of Objects and Reasons" that it does not contain provisions limiting rights and fundamental freedoms. What remains to be seen is how adherence to human rights principles will be reflected in the enforcement of these legal frameworks.

1. Article 118 (2), Constitution of Kenya 2010.
2. https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1

This mapping study investigates the ways in which the Kenyan government and other actors have initiated or engaged in multistakeholder processes in order to address cybersecurity-related matters in the country. Based on this, it will identify best practices, gaps and missing links, as well as opportunities and recommendations for improving the cyber policy landscape in the country.

The assessment of Kenya's cybersecurity landscape in this report will identify actors within the government and civil society, as well as existing laws and frameworks, and address the proposed ones, based on the information that is currently available. Unless otherwise stated, all institutions and legislative documents listed here are existent and/or functional.

01

GOVERNMENT BODIES

i. Ministry of Information Communications and Technology (MOICT)

The ministry was created in 2004 with the responsibility of "formulating, administering, managing and developing the Information, Broadcasting and Communication policy", and regulating the Information Communication sector.[1]

Some of the ministry's core functions relevant to cyber issues are:

- to formulate and implement ICT policy;
- to facilitate the development of ICT infrastructure in Kenya.

Policy priority areas that are pertinent to this mapping exercise include:

- capacity building in the ICT sector;
- continually reviewing and amending the legal and regulatory framework;
- promoting regional and international cooperation in ICT issues;
- periodically reviewing and updating national ICT policy to facilitate the development of the ICT sector.

The Ministry of Information Communications and Technology (MoICT) can thus be considered to be leading the state's efforts in driving cybersecurity efforts.

ii. ICT Authority

Established in 2013, the Information and Communication Technology Authority (ICTA) is a state corporation under the Ministry of Information Communication and Technology (MoICT). The Authority is tasked with rationalising and streamlining the management of all government of Kenya ICT functions.

Its broad mandate entails enforcing ICT standards in Government and enhancing the supervision of its electronic communication.[2] The Authority also promotes ICT literacy, capacity, innovation and enterprise in line with the Kenya National ICT Masterplan, 2017.[3]

Specific to cybersecurity, ICTA's mandate is to provide leadership in the cybersecurity management framework outlined in the aforementioned masterplan.

Along with the Communications Authority, the ICTA has been setting up the Public Key Infrastructure (PKI), a national system implemented by the government to provide digital certification services at the CAK. "The PKI includes the establishment of a Root Certification Authority (RCA) and a Government

1. Ministry of Information Communications and Technology's responsibility, core functions and policy priority areas retrieved from http://www.information.go.ke/?page_id=226
2. http://www.icta.go.ke/ict-authority/
3. http://www.icta.go.ke/national-ict-masterplan/

Certification Authority (GCA) for Kenya to provide citizens with digital certificates for online identification and e-commerce transactions."[4]

A special e-government program on National Cybersecurity is also being spearheaded and coordinated by the Kenya ICTA.

iii. Communications Authority of Kenya (CA)

The Communications Authority of Kenya (CA) is the regulatory authority for the information and communications sector in Kenya. It is responsible for facilitating the development of Information and Communications sectors including multimedia, telecommunications and electronic commerce.[5] The CA is further tasked with protecting consumer rights in the communications environment.

The Authority was established by the Kenya Communications Act of 1998, which has since been revised and amended into the Kenya Information and Communications (Amendment) Act, 2013 (KICA). With this law, the regulatory scope and jurisdiction of the Authority was enhanced; KICA now entrusts the CA with the power to work as an independent regulator. Therefore the CA is responsible for facilitating developments in the ICT, telecommunications, electronic commerce and transactions sectors in Kenya through licensing and regulations.

CA has also provided cybersecurity sector regulations, whose public consultation phase recently concluded in May 2016.[6]

As part of its consumer protection mandate, CA has also localised the ITU's Child Online Protection (COP) initiative as a two-year campaign, encompassing awareness-raising and direct stakeholder engagement (engaging students through various platforms and activities).[7] The Authority is also engaging various private sector and civil society stakeholders with the initiative. Various resources for parents and minors are provided, including on how one can report incidents (via the KE-CIRT/CC).

iv. National KE-CIRT/CC

This was established as a function of the Communications Authority in 2012. The Kenya Computer Incident Response Team Coordination Centre's (KE-CIRT/CC) role is to facilitate coordination and collaboration in response to cybersecurity incidents, in liaison with sector CIRTs and other local, regional and international cybersecurity management actors, among other cybersecurity-related activities.

KE-CIRT/CC's stated functions include:

- Offering advice on cybersecurity matters and coordinating cybersecurity incident responses in collaboration with relevant actors locally, regionally and internationally;
- Acting as the national trusted point of contact for information security matters;
- Gathering and disseminating technical information on computer security incidents;
- Capacity building in information security and creating and maintaining awareness around cybersecurity related activities;
- Putting in place Network Early Warning Systems (NEWS) in order to identify possible cybersecurity incidents in advance;
- Collecting, compiling and disseminating national statistics on cybersecurity incidents;
- Carrying out research and analysis on computer security;
- Facilitating the development of a National Public Key Infrastructure (NPKI), among others.

4. http://www.information.go.ke/?p=241
5. http://ca.go.ke/index.php/what-we-do
6. http://www.ca.go.ke/index.php/public-consultations
7. http://www.ca.go.ke/childonlineprotection/index.php/about-cop

The Authority's National KE-CIRT/CC also engages stakeholders through the National KE-CIRT/CC Cybersecurity Committee (NKCC) in the management of cybercrime. The NKCC membership includes members drawn from government agencies, law enforcement (DCI, Military, NIS), the banking sector, academia, the telecom sector, ISPs, public utility service providers and consumer advocacy groups, among others.[8]

v. Proposed National Cybersecurity Agency

This agency, proposed in the **Draft National ICT Policy**, is envisioned as a body that will be responsible for overseeing the mechanisms of protecting against advanced internet-based crimes.

The proposed functions of the Agency include:

- Protection of government communications and information systems against penetration of its databases and systems. This includes, but is not limited to detection, prevention and the management of cyber risks and data breaches in accordance with ISO 27001 series of standards and their successors;
- Decoding translation and information analysis.

vi. Other Government Actors

Kenya Law Reform Commission

The Commission has a statutory and ongoing role of reviewing all the laws of Kenya to ensure that they are modernised, relevant and harmonised with the Constitution of Kenya. They are part of the task force constituted to formulate legislation on cybercrime (**the Computer and Cybercrimes Bill, 2016**).

National Intelligence Services (NIS)

The NIS is a department under Kenya's Ministry of Interior, charged with identifying conditions which threaten Kenya's social, economic and political stability - and developing techniques and strategies to neutralise such threats. NIS works collaboratively with the Technology Service Providers of Kenya (TESPOK) and the ICT Authority in gathering intelligence based on existing or emerging threats.[9] They have a dedicated cybercrime unit which acts as a liaison between the NIS and other industry stakeholders. The unit reports to the Director General of the NIS, who sits on the National Security Council.

National Police Service (NPS)

The National Police Service is also a department under Kenya's Ministry of Interior. One of the police service's strategic priority areas is the application of ICT to policing work. Cybercrime has been identified as one of the most challenging crime categories for them. Cybercrime is investigated through the Directorate of Criminal Investigations. A specialised cyber forensics unit,[10] dubbed the cyberspace watchdog,[11] states the following as among its functions:

- Forensic examination of computers and mobile phones;
- Maintenance of lab processes, such as acquisition, archiving and analysis;
- Maintenance of inventories of digital evidence as per standards/ISO;
- Analysis of deleted and active files;
- Location and analysis of data in ambient data sources;
- Recovering deleted or encrypted data/emails, SMS, MMS, videos and websites;
- Uncovering of passwords;
- Forensic SIM card analysis;
- Extraction of data from mobile phones;
- Presentation of expert forensic evidence in court.

8. Efforts are underway to identify specific non-state actors who comprise the Committee.
9. http://www.interior.go.ke/?page_id=294
10. http://www.cid.go.ke/index.php/sections/specilizedunits/cyber-crime.html
11. http://www.interior.go.ke/?page_id=309

The National Police Service is listed as a member of the National KE-CIRT/CC Cybersecurity Committee (NKCC).

Office of the Director of Public Prosecutions (ODPP)

The ODPP is the National Prosecuting Authority in Kenya, mandated by the Constitution to prosecute all criminal cases in the country.[12] The office has previously led efforts that resulted in the Kenya Cybercrime and Computer-related Crimes Bill of 2014. These efforts, however, were halted, given that drafting bills is not part of the office's mandate.

The ODPP subsequently became a member of the taskforce constituted to formulate the **Computer and Cybercrimes Bill, 2016.**

Central Bank of Kenya (CBK)

The CBK is instrumental in shaping financial policies in the financial sector. One of the most significant cybercrime threats in the country pertains to the financial sector, requiring the leadership and engagement of CBK in the cyber policy landscape.

Until recently, CBK was always behind the curve when it came to policy enforcement as far as banking and outsourced services were concerned. This was remedied by the introduction of the CBK Prudential Guidelines.[13] However, the alignment of these guidelines is a far cry from what the Government is working on with regards to the National Cybersecurity Strategy.

Currently, the IT security experts in CBK seek to enforce industry standards so as to ensure that the security measures in place are adequate. A representative sits on ICT committees with the Kenya Bureau of Standards (KEBS) and influences the adoption of these industry standards from the banking sector perspective. Through this, they are able to ensure cybersecurity in the sector, without needing to rely on legal and regulatory frameworks.[14]

Presently, CBK collaborates with KE-CIRT/CC and is a member of the task force constituted to formulate the Computer and Cybercrimes Bill, 2016.

National Communications Secretariat

This is a policy advisory body to the government on matters relating to information and communication policy. Its duties include producing policy papers, sessional papers, country position papers and legislation on ICTs, as well as advising the government on the adoption of appropriate information and communication technologies.

The Secretariat was established through the Kenya Information and Communications Act of 1998, and its role as a policy advisory arm of the government on all matters pertaining to ICT has been reaffirmed in the recently revised 2016 Draft National ICT Policy.

12. http://www.odpp.go.ke/index.php/about-us/who-we-are.html
13. https://www.icpak.com/wp-content/uploads/2015/10/CBK-Prudential-Guidelines-for-Institutions-Licensed-under-the-Banking-Act.pdf.pdf
14. This insight was provided us by a CBK representative.

02

KEY DOCUMENTS: FRAMEWORKS AND LEGISLATION

i) Kenya National Cybersecurity Strategy

A National Cybersecurity Strategy was devised in 2014 to "defin[e] Kenya's cybersecurity vision, key objectives, and ongoing commitment to support national priorities by encouraging ICT growth and aggressively protecting critical information infrastructures."[1] It was envisioned as a guiding document for the management of cybersecurity issues in the country, to address loopholes in information security, and to provide the government with implementation plans to protect Kenya's ICT cyber assets.

The strategy also affirms Kenya's commitment to multistakeholder engagement by stating that cybersecurity is a shared responsibility, and that the government "will continue to partner with government bodies, private sector, academia, and other non-government entities to implement [the] Strategy in the most efficient and effective way possible."[2]

Although it is an exhaustive document, the strategy does not explicitly acknowledge the importance of protecting human rights. However, it does make mention of privacy considerations in the strategy's implementation, which is accompanied by a cybersecurity master plan.

ii. Kenya Information Communications Act (KICA), Chapter 411A

A cybersecurity framework for the country is presently articulated under the Kenya Information Communications Act (KICA), Chapter 411A of the Laws of Kenya, in a bid to facilitate and promote electronic transactions. In recognition of the rapid changes and developments in technology, there have been a number of amendments since its enactment.

The Act currently covers the following:

- Privacy protections
- The use of, and requirements for, electronic signatures
- Unauthorised access to or modifications of information systems and data
- The legal recognition of digital documents, records, and signatures. This enables digital evidence to be admissible in court proceedings
- Specific details of computer crimes and associated punishments:
    - Malicious tampering with or unauthorised access to systems, networks or source code
    - Hacking
    - Publishing obscene information
    - Using electronic signatures for fraudulent purposes
    - Interfering with mobile device identity or operations

1. http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cyber security-strategy.pdf
2. ibid

There is a need for reform of this Act, as it fails to incorporate a number of other offences that occur in the cyber environment. However, with the introduction of the Computer and Cybercrimes Bill, 2016, the requisite amendments would need to factor in the latter bill. Ultimately, the enactment of the Computer and Cybercrimes Bill 2016 will exist as a standalone piece of legislation for cybercrime, which will lead to the amendments of a number of laws, which include KICA (2013).

iii. Draft National ICT Policy (2016)

The National ICT Policy of 2006 has recently come under review in order to streamline it with emerging developments in the ICT sector. The public participation phase of the policy review concluded in July 2016.

The principles and values enshrined in the Constitution of Kenya, 2010 are referenced in the revised National ICT Policy; in particular, the policy's commitment to upholding the constitution and respecting essential values of human rights, equality, freedom, democracy, social justice and the rule of law. The policy also acknowledges that "the privacy, security of the person and property shall be paramount in the deployment of information and communications technologies."[3]

The document outlines key policy objectives for cybersecurity, which include:

- Establishing cybersecurity as a key objective of national security and creating a sufficiently empowered agency or office to cover it.
- Supporting the development of a new generation of technologies that will lead to measurable, available, secure, trustworthy, and sustainable computing and communications systems, as well as associated management and policy tools that enable successful utilization of the new technologies;
- Recognising vulnerable populations such as children, who will require special focus to ensure that they are safe and derive value from cyberspace;
- Providing for the development of best practice information security standards for the ICT sector;
- Balancing the efficient mitigation of cyber threats in order to promote trust and confidence with the objective of preserving the openness of the internet as a platform for innovation and new sources of growth;
- Developing appropriate legal and regulatory frameworks, technical solutions and law enforcement strategies for the appropriate detection and prevention of cyber threats, given the dynamic nature of cyber threats.

It also touches on key issues of capacity building, awareness, broader cooperation, and other approaches that will enhance cybersecurity.

iv. Computer and Cybercrimes Bill (2016)

The Computer and Cybercrimes Bill, 2016[4] has been formulated through a taskforce of state actors, chaired by the **Kenya Law Reform Commission**. The bill borrows heavily from the Council of Europe Convention on Cybercrime CETS (Budapest Convention) with the aim of adhering to international standards and streamlining international cooperation efforts. The bill can therefore broadly be categorised into four main categories: jurisdiction, offences, forensic procedures and international cooperation, which constitute some of the key problem areas that have been faced in the fight against cybercrime.

3. http://www.information.go.ke/wp-content/uploads/2016/06/Draft-National-ICT-Policy-20June2016.pdf
4. http://www.mygov.go.ke/wp-content/uploads/2016/07/MOICT-PUBLICATION-READY-COMPUTER-AND-CYBERCRIMES-BILL-2016-1-1-1.pdf

Offences

- The bill highlights a number of offences, some of which are already housed under the KICA.
- It addresses access-related offences, and also looks to incorporate more content-related offences such as cyberstalking and cyberbullying, not previously covered in existing laws.
- The bill also assigns fines and jail terms for these offences.

Investigation and handling procedures

- This constitutes one of the biggest gaps in the fight against cybercrime, as a lack of law and provisions in this area has complicated prosecution processes. The bill now seeks to provide clear protocols and approaches for the investigation and retention of data in the face of cybercrime through data collection, interception of data, and other various technical mechanisms.
- There is provision for authorised officials in the investigative procedures, who require official court orders before such investigations can be carried out.
- And the bill also lays out clear requirements for the officials carrying out such orders to do so in a manner that will be admissible in court. The bill, in this section, also provides for the obstruction and misuse of the powers granted to officials, and creates offences and penalties for all who are found to be abusing their conferred rights.

International cooperation

- The bill looks to complement the already existing Mutual Legal Assistance Act (2011)[5] which serves to increase international cooperation between countries. Stemming from this Act, a Central Authority is to be established which is mandated to assist any foreign bodies with investigations upon request.
- This section of the bill on international cooperation creates a point of contact for other jurisdictions – necessary due to the cross-border nature of cybercrime. It emphasises immediate assistance for the purpose of investigations and proceedings concerning criminal offences related to computer systems and data. This will then facilitate trans-border access to stored computer data with consent - or if the data is publicly available – as well as real time collection of data and the interception of content data as and when necessary.

Jurisdiction

- Again, due to the cross border nature of cybercrime, there is a need for clear parameters with regards to jurisdiction. The bill addresses this by ensuring that jurisdiction can be established even where the crime does not happen in one particular country. It holds that an act or omission committed constitutes an offence under the bill if committed by a citizen of Kenya, or by a person who is ordinarily resident in Kenya.
- Additionally, it is provided that an act constitutes an offence if it is committed against a citizen of Kenya; against property belonging to the government of Kenya outside Kenya; or if it compels the Government of Kenya to do, or refrain from doing, any act. An offence also occurs if the person who commits the act or omission is, after its commission or omission, present in Kenya.
- However, one of the scenarios that this bill does not consider is when a cyberattack is launched and routed through a third country.

There are a number of existing laws that would need to be amended with the enactment of this legislation as they already have elements of cybercrime embedded in them. This would eliminate duplication and ensure that the law is clear.

5. http://www.kenyalaw.org/lex//actview.xql?actid=CAP.%2075A

v. Kenya Information and Communications Act (Cybersecurity regulations) 2016

Stemming from the provisions in KICA, the regulations aim to provide a framework for boosting security in the cyber environment.

More specifically, the regulations have the following objectives:[6]

- To promote and facilitate the efficient management of critical internet resources;
- To develop a framework for facilitating the investigation and prosecution of cybercrime offences;
- To make provisions for criminalizing offences relating to computer systems and information communication technologies;
- To provide for the investigation, collection, and use of electronic evidence and for matters related therewith;
- To develop a safe, secure and effective environment for consumers, businesses and the government to conduct and use electronic communications, electronic transactions and electronic commerce;
- To ensure efficient use and management of the .KE domain name space;
- To promote legal certainty and confidence with respect to electronic communications, electronic transactions and electronic commerce.

Currently, the regulations have undergone public participation, with stakeholder comments awaiting amalgamation with the zero draft before they can be put into law.

vi. Other Laws, Conventions and Frameworks

Budapest Convention

This is the first international treaty covering crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in its preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. The Convention therefore provides helpful guidance on how to draft cybercrime legislation in accordance with human rights standards. It incorporates offences against confidentiality, integrity and availability of computer systems and computer data. Additionally, the Convention includes procedural measures for the investigation and prosecution of cybercrimes.

Currently, Kenya is not a signatory to the Convention. Nevertheless the cybercrime legislative framework under KICA reflects a number of similar provisions as those in the Convention, and the Computer and Cybercrime Bill, 2016 borrows heavily from it.

African Union Convention on Cybersecurity and Personal Data Protection

The AU Convention[7] embodies the existing commitments of African Union Member States at sub-regional, regional and international levels to build Information Societies.

Its provisions seek to boost electronic commerce and address a range of issues, which include:

6. http://ca.go.ke/index.php/public-consultations
7. http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf

- The gaps affecting the regulation of legal recognition of data communications and electronic signatures;
- The absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems;
- The absence of e-services and telecommuting legislations;
- The application of electronic techniques to commercial and administrative acts;
- The probative elements introduced by digital techniques (time stamping, certification, etc.);
- The rules applicable to cryptology devices and services;
- The oversight of online advertising;
- The absence of appropriate fiscal and customs legislations for electronic commerce.

Although not ratified by Kenya, the AU convention prompted the creation of cybercrime laws by a number of African states, including Kenya, South Africa and Tanzania.

Data Protection Bill

The Constitution of Kenya guarantees the right to privacy, including the right to not have information relating to one's family or private affairs unnecessarily revealed, and to not have the privacy of one's communications infringed.[8]

The Data Protection Bill, 2013[9] was formulated to give effect to this constitutional provision. It articulates requirements for electronic personal information collection, storage, protection/security, access, disclosure, and misuse.

While a crucial legislative provision, the bill has been awaiting adoption, and it remains unclear when this will happen.

Critical Infrastructure Protection Bill

The Critical Infrastructure Protection Bill, 2015[10] proposes the establishment of a Critical Infrastructure Protection Unit whose functions include, inter alia;

- Implementing strategies and measures for the protection of critical infrastructure
- Establishing an integrated database of information on critical infrastructure;
- Maintaining a register of all the assets and locations declared as critical infrastructure
- Coordinating the planning, development and implementation of security measures and strategies for the protection of critical infrastructure
- Preparing and implementing critical infrastructure programmes
- Deploying relevant security measures for the protection of critical infrastructure
- Advising and making recommendations to the Committee on matters relating to critical infrastructure

The purpose of the bill is therefore to establish a cross-sector initiative aimed at improving the resilience of the critical infrastructure in all sectors of the economy, so that critical infrastructure assets are afforded continued security surveillance and protection against, inter alia, "cybercrime or crime targeted at information transmitted by means of Critical Infrastructure Assets".[11]

This is another significant bill in the cybersecurity landscape, but it is unclear what the progress towards enacting it is, since the public consultation process was conducted in late 2015.

8. Article 31, Constitution of Kenya 2010
9. http://www.cickenya.org/index.php/legislation/item/download/299_b3de9506b20338b03674eacd497a6f3a
10. http://www.icta.go.ke/downloads/critical-bill.pdf
11. Section 27(d), Critical Infrastructure Protection Bill, 2015

03

CIVIL SOCIETY/NON-STATE ACTORS

In the draft National ICT Policy (whose review process is currently ongoing), civil society is acknowledged as playing an important role in the ICT sector. More specifically, the government sees civil society informing the policymaking process by making relevant contributions to various thematic areas within the broad ICT spectrum.

i. Kenya ICT Action Network (KICTANet)

The Kenya ICT Action Network (KICTANet) is a multistakeholder platform for people and institutions interested and involved in ICT policy and regulation. The network aims to act as a catalyst for reform in the ICT sector in support of the national aim of ICT enabled growth and development.[1]

Some of the key activities that KICTANet has undertaken in addressing cybersecurity issues include:

- Participation in discussions that led to the drafting and passing of the National Cybersecurity Strategy (2014)
- Convening engagement sessions with civil society organisations and various government entities on various issues in the ICT sector
- Coordinating public participation/consultation processes, such as Kenyan input into the 2014 African Union Convention on Cybersecurity

KICTANet has also hosted discussions on the draft National ICT policy and the Computer and Cybercrimes Bill, 2016.[2]

Being a discussion group, KICTANet is open for everyone to contribute. It currently doesn't operate in an organisational capacity (i.e. not a registered entity), but is perhaps the biggest virtual convener of ICT stakeholders in Kenya.

ii. Article 19 East Africa

Article 19 East Africa works on ensuring plurality and diversity in the media and campaigning to place information at the centre of development policies and practices.[3]

The organisation works on promoting human rights in the digital sphere including through policy advocacy, litigation and capacity development.

They engage with:

- Government, by providing legal analyses of laws being developed, such as the 2014 Kenya Cybercrime and Computer Related Crimes Bill.[4]

1. https://www.kictanet.or.ke/
2. http://www.mygov.go.ke/wp-content/uploads/2016/07/MOICT-PUBLICATION-READY-COMPUTER-AND-CYBERCRIMES-BILL-2016-1-1-1.pdf
3. https://www.article19.org/pages/en/east-africa.html
4. https://www.article19.org/resources.php/resource/37652/en/kenya:-cybercrime-and-computer-related-crimes-bill

- Corporates, by sharing analysis with them and by meeting them to influence their policies to respect human rights standards
- Human Rights Defenders (HRDs) by training them about their rights, particularly how to promote and protect them.

iii. Centre for Intellectual Property and Information Technology Law (CIPIT)

CIPIT is a research institute hosted at the Strathmore Law School, Nairobi, which focuses on intellectual property and information technology, and how they relate to African law and human rights. The institute conducts academic research, legal and policy analysis on ICT related topics and laws and information management training and events.

Their Jadili ICT Platform[5] is emerging as an instrumental database for aggregating relevant ICT legislative frameworks and allowing multiple viewers to comment and engage in policy debates.

iv. Watoto Watch Network

Watoto Watch Network[6] is an NGO that focuses on child online protection (internet safety for children). They have trained over 20,000 children, parents, teachers, members of the judiciary, police and children's department staff on how to deal with cybersecurity issues facing children in Kenya.

v. Telecommunications Service Providers of Kenya (TESPOK)

TESPOK[7] is a non-profit organization that was established in 1999 to represent the interests of technology service providers in Kenya. It has since widened its base to represent the interests of software and hardware developers, as well as ICT hubs, defining itself as an all-inclusive body. TESPOK's main objectives are:

- To influence ICT policy and regulations by engaging government at the relevant levels;
- To address challenges faced by technology stakeholders and provide guidance on resolution mechanisms;
- To provide a forum for the exchange of ideas amongst industry stakeholders and to foster the development of white papers;
- To manage the Kenya Internet Exchange Point[8] in line with internationally accepted best practices.

TESPOK also houses a Computer Security Incident Response Team, dubbed i-CSIRT,[9] which tracks cyber threats and issues periodical reports on the same, as well as providing advice.

vi. TripleOKLaw Advocates, LLP

TripleOKLaw is a leading Kenyan law firm practicing in Nairobi, Kenya. The firm was established in 2002. The firm has a practice area dedicated to Telecommunications, Media and Technology (TMT), and it is through this that the issue of cybersecurity became a core concern for the practitioners. Based on this growing concern, the firm actively creates synergies with key players in the technology sector, so as to contribute towards the fight against cybercrime. Beyond advising clients on the current position of the law in this area, the firm also participates in the creation of laws in this area, a right afforded to members of the public by the Constitution of Kenya. The firm therefore continually acts as a bridge between the law and technology. TripleOKLaw have experts who are well versed in ICT and the formulation of policy and regulation in this area.

5. http://jadili.ictpolicy.org/
6. http://watotowatchnetwork.org
7. www.tespok.co.ke
8. http://www.tespok.co.ke/?page_id=11648
9. http://www.tespok.co.ke/?page_id=11674

vii. Euclid Consultancy Services Limited

Euclid Consultancy Services LTD is a private firm which offers cybersecurity services which include, but are not limited to, Penetration Testing and Vulnerability Assessment, Cybersecurity Training and Awareness, Compliance, Fraud Forensics in collaboration with the Directorate of Criminal Investigations (DCI) and Research and Development. Euclid also houses the AfricaHackOn brand which is a collective of cybersecurity practitioners drawn from diverse professions. This brand is responsible for outreach in learning institutions to nurture young minds for an understaffed profession. Euclid Consultancy Services Ltd has partnered with TESPOK, Jomo Kenyatta University of Agriculture and Technology (JKUAT) and Safaricom Ltd in areas of research, training and capacity development. Under the AfricaHackOn, Euclid hosts an annual cybersecurity conference which attracts players from across the industry.

viii. Serianu Limited

Serianu is an IT consultancy firm that offers Information Security and Risk services to a range of clients. More specifically, they cover Risk and Compliance; Security operations; Governance and Strategy; Technology Implementation Support; Enterprise Threat Management, and Cyber Intelligence Monitoring.

Serianu publishes annual Kenya Cybersecurity Reports, and issues 'Cyber Threat Vulnerability Alerts.'[10]

ix. Simba-Safe Kenya

Simba-Safe Kenya[11] is a personal safety education program for children and youth. Online Safety is a major component of their education and outreach; they train and provide educational material regarding online safety to parents, teachers and children. The initiative is a key champion for child online safety within KICTANet.

x. Hivos Regional Office East Africa (HIVOS ROEA)

HIVOS East Africa, through its Freedom of Expression program,[12] engages with bloggers, journalists, human rights defenders, activists and civil society organisations working on internet freedom. They do so through grant-making for policy and advocacy, as well as meetings and trainings.

Specific to cybersecurity, they are supporting work addressing the safety and protection of online activists, journalists and human rights defenders, as well as online violence against women.

xi. S.K.I.R.T.S Foundation

The Socially Keen Individuals Redefining Tech Spaces (S.K.I.R.T.S.) foundation works specifically on creating safe online spaces for women, and amplifying the voices of women against online discrimination and harassment. They offer digital security training in universities, colleges, and for civil society organisations, to build awareness around cybersecurity threats. They also facilitate conversations about online harassment and violence as an internet governance issue. S.K.I.R.T.S also collect evidence (through research and data collection) on the different types of online violations and to what extent they exist in Kenya's cyberspace.

S.K.I.R.T.S. is also leading engagement around the Computer and Cybercrimes Bill from a public interest perspective, and is pursuing a partnership with the National Police Service to bridge the gap on collecting digital evidence on online harassment and violence.

10. http://www.serianu.com/resources.html
11. http://www.simbasafekenya.com/
12. https://east-africa.hivos.org/freedom-expression

CHALLENGES, PRESSING ISSUES AND RECOMMENDATIONS

Kenya is in the nascent stages of establishing a holistic and multistakeholder engagement process as far as cyber policy is concerned. The outlined bodies and instruments need to be synchronised to ensure that the resulting cyber policy and legislative environment is in accordance with the recommendations for human rights based approaches to cybersecurity developed by the Freedom Online Coalition.[1]

There are a range of actors, both state and non-state, as well as legal instruments in Kenya's cyber policy landscape. Roles, functions and scope are still shaping up, as cybersecurity gains wider prominence in the country.

As highlighted in the Draft National ICT Policy, 2016 and echoed by the stakeholders engaged for this mapping exercise, Kenya's cybersecurity framework faces a number of challenges. These include:

- Inadequate skills in the cybersecurity sector;
- Insufficient awareness of cybersecurity issues among various stakeholders;
- An unconducive legal framework, and lack of related institutional infrastructure for ICT development and application;
- Inadequate regulatory capacity, especially in the face of the convergence of networks and services;
- Inadequate capacity for research into ICT-related legal and regulatory issues;
- Absence of a culture that fosters the adoption of internet security standards in various sectors;
- A lack of specific and effective legislative instruments on privacy, security, cybercrimes, ethical and moral conduct, encryption, digital signatures, copyrights, intellectual property rights and fair trade practices;
- Inadequate capacity for research in ICT related legal and regulatory issues.

As noted previously, discourse and efforts in the cybersecurity space are quite fragmented, with a disproportionate focus on cybercrime. This compromises the pursuit of a holistic approach to effectively managing and governing Kenya's cyberspace.

There also is an emerging risk of over-regulation, especially in the context of various legal instruments that are not synchronised.

The participation of civil society organisations could be deemed insufficient. While civil society and multistakeholder engagement are acknowledged by the state, the facilitative avenues and mechanisms are unclear. Some progress has been made, with the government availing itself of pertinent instruments for public consultations. However, the window for consultation, as well as mechanisms for

1. https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf

announcing the process, require further work.

In addition, the seeming lack of a systematic process for enacting cyber policies and legislative frameworks has led to an asynchronous and disjointed policy process. For instance, the Cybersecurity Regulations[2] preceded the Computer and Cybercrimes Bill; and this bill was in turn unveiled hot on the heels of the draft National ICT Policy. Additionally, a Cybersecurity and Data Protection Bill (2016) has recently been introduced at the Senate; its justification or motivations in light of the existing bills and policy revision process is unclear. This duplication of efforts and lack of harmonisation risks stalling the enforcement of viable legislative frameworks for the country. However, this is a widely acknowledged challenge that the state is keen to address.

The cyber policy environment also requires that other crucial pieces of legislation, such as the Data Protection Bill and the Critical Infrastructure Protection Bill, are put in place. Their status remains unclear. With the current interest and focus on the cyber policy landscape, it is hoped that progress will be made on this legislation, and that these bills will address cybersecurity issues in a manner which is synchronised with existing and proposed bills.

The amendment of other laws to accommodate the Computer and Cybercrime Bill, 2016 will also be required. These laws include:

- KICA (Cap 411 A)
- The Evidence Act (Cap 80) – which currently recognises electronic records as admissible in court
- The Mutual Legal Assistance Act, No. 36 of 2011
- The Penal Code (Cap 63) - which has recent amendments touching on crimes related to electronic devices
- The Proceeds of Crime and Anti Money Laundering Act, No. 9 of 2009
- The Criminal Procedure Law (Cap 75)
- The National Payment Systems Act, 2011
- The Sexual Offences Act, 2006

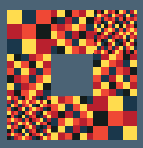
It remains to be seen how these and other laws will relate to the Computer and Cybercrimes Bill, 2016.

The roles and scope of various state actors also requires urgent streamlining – which is expected to go hand in hand with changes to legislative instruments.

Other elements which could be established both in law and at the practitioner's level to improve accountability in cyber policy include:

- The formalization of a Responsible Disclosure framework.[3] This needs to be part of a culture of innovation, where companies and the government alike should welcome discoveries arising from vulnerable systems. This would not only improve the security of products but would also allow more public participation.
- The reworking of curricula in universities in Kenya covering ICT and cybersecurity to reflect realities in the job market. More often than not, academia is left behind by innovation – which can mean students leave university with skills which are already obsolete. In turn, this means that businesses need to spend more time training graduates on the job.

2. From engagement with relevant actors, the prevailing sentiment is that the Cybersecurity regulations are quite flawed, as they seem to duplicate the Computer and Cybercrimes Bill 2016's provisions. This may be the case since the draft regulations were issued in the absence of an overarching bill and guiding policy, all of which are currently under review. Based on this, it is anticipated that the regulations will need to be re-drafted to better align themselves to other legislative documents.
3. https://securityintelligence.com/the-responsible-disclosure-policy-safeguard-or-cybercriminal-siren-song/



GLOBAL PARTNERS DIGITAL

Human rights in a connected world

GLOBAL PARTNERS DIGITAL
Second Home
68 - 80 Hanbury Street
London E1 5JL
+44 (0)20 3 818 3258
gp-digital.org