DEMOCRACY REPORT

By Frederico Links

Special Briefing Report No. 20

JANUARY 2018

TACKLING CYBER SECURITY/CRIME IN NAMIBIA – CALLING FOR A HUMAN RIGHTS RESPECTING FRAMEWORK

1. Introduction – A need for meaningful consultation

In February 2017, with the opening of parliament, the Minister of Information and Communication Technology (MICT) filed an unexpected motion to table the long-in-coming Electronic Transactions and Cybercrime Bill for debate and discussion, and eventual promulgation.

This happened despite the last meaningful consultations around the provisions of such a draft law having been conducted in 2010, in a process which formally began in 2005. The consultations culminated with the first substantial draft Bill that was put together with the assistance of International Telecommunications Union (ITU) experts in 2013, through the ITU's Harmonization of the Telecommunication and ICT Policies in Africa (HIPSSA) project. HIPSSA was started in 2008 and produced the Computer Crime and Cybercrime: SADC Model Law, which was also launched in 2013, the same year in which the first substantive draft of Namibia's Electronic Transactions and Cybercrime Bill made its appearance.

In June 2014, the African Union Convention on Cyber Security and Personal Data Protection was adopted by the 23rd Summit of Heads of State and Government at Malabo, Equatorial Guinea. This is significant because the AU Convention, while nowhere near perfect, nevertheless appears to set a much better standard against which to design and draft a cybersecurity framework than the ITU proposals did. One of the significant differences between the two instruments is that the AU Convention is said to have been the product of wide consultations across the continent, while the ITU proposals were constructed "prior to 2014 without public consultation".[1]

This is an important aspect to bear in mind, because while the last draft of the Electronic Transactions and Cybercrime Bill that appeared to have been publicly and widely circulated was the 2013 version, which in many respects was quite substantially flawed, the draft (with some minor textual changes and additions, and bearing the 2017 year date) that Namibia's

[1] https://www.accessnow.org/cms/assets/uploads/2016/12/RoomforImprovement_Africa.pdf

Democracy Report is a regular publication featuring analysis and commentary relating to the legislative agenda of the Parliament of the Republic of Namibia. It is produced by the Institute for Public Policy Research (IPPR), PO Box 6566, Windhoek, Namibia. Tel: +264 61 240514, Fax: +264 61 240516,info@ippr.org.na. The publication is also available as a PDF download from http://www.ippr.org.na Democracy Report is funded by the Embassy of Finland

EMBASSY OF FINLAND WINDHOEK

MICT minister announced for tabling in parliament in early 2017 was subject to only limited consultations, i.e. with the Namibian Police (NamPol), which officially created its cybercrime unit in 2014, the computing departments of the University of Namibia (UNAM) and the Namibia University of Science and Technology (NUST), and the United Nations Children's Fund (UNICEF) office in Namibia.

That said, cybercrime and cybersecurity are often conflated to mean or refer to the same thing. However, technically, cybercrime is merely one of the primary focus areas within the broader cybersecurity field.

In this context, the Electronic Transactions and Cybercrime Bill is clearly the first major and specific attempt at cybersecurity legislation in Namibia. And it is against this backdrop that relevant Namibian authorities' attention is herewith drawn to a statement by the UN Economic Commission for Africa (UNECA): "It is important to understand that no one person or institution can have the requisite capacity to deal with cybersecurity. Cybersecurity is not an event but rather a process. As a result, it is not simply a matter of passing legislation, or something that belongs to lawyers only. Members of Parliament, lawyers, the judiciary, intelligence/military, civil society, media, young people and members of the public as key stakeholders should all be involved in efforts to deal with cybersecurity at the earliest available opportunity. It is important to engage all stakeholders to ensure the necessary buy-in and that they understand the issues and processes involved."[2]

For its part, the Global Commission on Internet Governance (GCIG) recommends[3] that, at a minimum, any cybersecurity frameworks and solutions "should be derived through a multi-stakeholder process, broadly agreed, and must be subject to legal oversight, governed by principles of necessity, proportionality and avoidance of unintended consequences".

In light of these statements, the question must be asked whether Namibian cybersecurity proposals, as presented in the Electronic Transactions and Cybercrime Bill of 2017, meet such standards.

There are several lessons to be drawn from global and regional efforts in the cybersecurity space:

1. Although there is no one, precise definition of cybersecurity, it nevertheless is clear to most in or around the field what is broadly meant by the term. Namibian authorities would do well to engage various and all relevant sectors and actors to put forward, in the first instance, a credible, domestically subscribed to definition of the concepts falling under the cybersecurity umbrella.

2. Every serious actor in the cybersecurity space should recognise that cybercrime can only be effectively countered and cybersecurity mechanisms only efficiently implemented if such measures are approached, agreed to and designed in a cooperative, multi-stakeholder setting and framework that comprehensively includes the business, technology, and civil society sectors.

3. A fairly extensive body of literature and material that is freely available and easily accessible in the online public domain concerning cybercrime and cybersecurity (including against the backdrop of larger human rights concerns and considerations) already exists. This means that there would be no need for further local extensive studies on these topics. While Namibia does not need to reinvent the wheel in this context, legal drafters and decision and law makers should be encouraged to acquaint themselves, if not thoroughly, at least sufficiently with the themes, considerations and concerns in this field in order for law and policy making to reflect best practices as they already exist and continue to evolve.

4. Given the availability of such an extensive and growing body of literature on the topics of cybersecurity and cybercrime, and related matters, relevant authorities should take the time and opportunity to organise intensive consultations, with special emphasis on creating platforms for enhanced cooperation between state and non-state actors in this field, before rushing through legislation which would not be fit for purpose and could actually lead to human rights violations, condemning such a framework to unconstitutionality.

It is with these lessons in mind that we make the following recommendations.

Recommendations

1. The Namibian government and parliament should ratify the African Union Convention on Cyber Security and Personal Data Protection as a matter of urgency;

2. Once ratification of the AU Convention has been achieved, Namibian authorities should use the AU Convention, along with other more inclusively crafted instruments, such as the Budapest Convention on Cybercrime, as the guide for designing, drafting and implementing a cybersecurity-related regulatory framework;

3. In the process of coming up with such a framework, it is recommended that relevant Namibian decision and law making authorities, as well as legal drafters, as the first step, commence a review of the extensive existing body of literature and materials on cybercrime and other cybersecurity-related issues and measures in order to, firstly, acquaint themselves with the issues and the myriad voices on the constantly evolving cybercrime and cybersecurity landscape; and secondly, assess whether Namibia's proposed efforts are in line with emergent trends and best practices towards the installation of the best possible framework for the Namibian context;

[2] http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf

[3] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

4. In line with international best practice, we recommend that any cybersecurity law and institutional framework be the product of an extensive and meaningful cooperative multi-stakeholder consultative process and that the eventual framework make provision for some level of multi-stakeholder oversight involvement.

5. Finally, against the backdrop of everything stated in this paper, we call on Government to restart the law drafting process of a cybercrime/security law, while finalising the Electronic Transactions Bill as a matter of urgency.

2. Overview – Cybercrime and Cybersecurity Threat Situation

The exponential rise in online criminal activity is hardly surprising, given the pervasive spread of technology, and especially of devices connected to the Internet (the Internet of Things), into all spheres of human activity. This has given rise to an increasing preoccupation – at political, institutional and individual levels – with cybersecurity and related concerns.

And so it has to be asked: just how serious is the cybercrime threat situation?

In a 2016 report, the Global Commission on Internet Governance states: "The IT security firm Kaspersky Labs has collected data on the number of web-based cyber-attacks from 2008 to 2014 and found a nearly consistent year-over-year increase in the total number of attacks, reaching as high as 1.7 billion attacks in 2013. Other IT security companies such as Norton Symantec collect data on the generally growing number of vulnerabilities in computer software and firmware. For example, according to Symantec's annual Internet Security Threat Report, the number of new vulnerabilities identified each year has grown from 5,562 in 2008 to 6,549 in 2014. Among a number of other speculative predictions of the costs of cybercrime, the IT security firm McAfee (a division of Intel), in collaboration with Center for Strategic and International Studies, contends that cybercrime costs the global economy somewhere between $375 and $575 billion per year."[4]

These assessments are echoed by others, such as US civil society organisation Public Knowledge, which stated recently that: "Cyberattacks continue to be on the rise and it is estimated that they could potentially cost the global economy US$3 trillion in productivity and growth by 2020 – a key area of concern for the digital economy."[5]

And no-one or nothing is safe, as explained by the DiploFoundation in its 2017 preview: "cyber-attacks continue to increase and move from mass frauds to sophisticated attacks targeting individuals, as well as hacking particular companies or institutions. Lead technology, financial, and government institutions have also become targets of cybercrime, which shows that no one is immune. The consequences of the attacks are increasingly geo-political rather than localised.

"This trend calls for increased efforts from governments, intergovernmental organisations, and private companies to work towards identifying and implementing more adequate responses. But the perspectives do not look very encouraging. While more countries are strengthening their law enforcement agencies, the general level of resources available to these agencies in developing countries remains small, mainly due to a limited political understanding of cybersecurity challenges."[6]

This dire threat situation prompted the former director of the US's Department of Homeland Security, Michael Chertoff, to remark during a talk at Oxford University at the end of 2016 that: "One of many challenges we are presented with today and into the future is that we need to try and keep intact the basic backbone of how the Internet has evolved, but we have to find ways in which to stay ahead of highly-skilled cybercriminals out there such as hackers, fraudsters and terrorists."[7]

Bearing all this in mind, it has to be said that Africa on the whole appears to be woefully underprepared to deal with cybercrime, as well as other cyber threats, and that criminals have taken notice. The UN Economic Commission for Africa (UNECA) states that: "Cybercriminals have long considered Africa as opportune to commit their criminal acts. Statistics from various sources indicate that Africa is very prone to cyber-related threats due to the high number of domains coupled with very weak network and information security. For example, according to the Norton Cyber-Crime Report, every second, 18 adults are victims of cybercrime, resulting in more than 1.5 million victims globally per day. In addition, South Africa (80 percent) has the third highest number of cybercrime victims in the world, after Russia (92 percent) and China (84 percent)."[8]

It is thus clear that many African states operate in the cybersecurity realm, and indeed in the technology space as a whole, with under-developed regulatory and security measures, which has had the effect in some instances of contributing to the appearance of unsavoury practices. The African situation should be viewed against a GCIG assessment of the global situation which found that: "Very few nations have adequate independent accountability mechanisms and judicial oversight, which are necessary to keep state power in check. Some states, governments and militaries are even known to actively stockpile vulnerabilities, develop malware or subvert security standards, which can then be used to conduct targeted or mass surveillance. Most of this activity was conducted in secrecy and left largely unregulated, posing threats not only to the ongoing security and stability of the Internet, but to freedom and democracy."[9]

While the above does not only apply to Africa, it needs to be

[4] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

[5] https://www.publicknowledge.org/cybersecurity-and-human-rights

[6] https://digitalwatch.giplatform.org/sites/default/files/GIP2016review.pdf#7

[7] https://sputniknews.com/science/201611231047747056-future-internet-geopolitics-security/

[8] http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf

[9] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

underscored that African states especially have started demonstrating the propensity to deploy cybersecurity measures to undermine and suppress legitimate political expressions. This goes to illustrate that while governments, intergovernmental bodies, business and civil society organisations have made immense strides in putting together measures and mechanisms to counter the surge in cybercrimes and related threats over especially the last decade or so, the threatening downside to such initiatives has also become increasingly apparent. The GCIG recently stated, with regard to dealing with cybersecurity threats of all sorts, and re-emphasising the point already made above, that "some governments are conducting surveillance for purposes and in ways that have a negative effect on fundamental human rights such as privacy, freedom of expression, and legitimate dissent and protest."[10]

In light of these developments, it is necessary to direct Namibia's relevant authorities' attention to these issues.

According to some sources, Namibia appears amongst the most vulnerable countries in the world with respect to cyber threats of all sorts[11]. In an article published in June 2016[12], a senior IT official at one of the country's major banks was quoted saying: "Well, it is as simple as the fact that we have a very good communications network and are well provisioned with internet services. This allows criminals access and a way for them to move information and money out of the country. Another reason is that our thriving banking sector with multiple points of presence throughout the country and internationally via ATM networks offers opportunity. Further, we have inadequate laws that focus on dealing with and bringing cyber criminals to justice. We also have limited capability of pro-actively monitoring and preventing such attacks as this requires huge investments in security infrastructure and systems."

For years now, Namibia has been in the process of crafting cybercrime fighting measures, but these processes have never actually been brought to meaningful fruition. And now that Namibian authorities are ready to legislate for cybersecurity and against cybercrime, they are in danger of installing an inadequate framework which could have a "negative effect on fundamental human rights such as privacy, freedom of expression, and legitimate dissent and protest".

Applicable lesson

It is for this reason that Namibian state authorities need to be reminded that: "Security cannot be treated as an afterthought, trailing technological innovation, nor is it an issue for governments alone. Personal freedom, economic growth and innovation, particularly in the IoT [Internet of Things], will be degraded if the digital space is not sufficiently secure and all actors do not practice better digital "hygiene".[13]

Cybersecurity: Challenges for Africa[14]

Africa is facing several Internet-related challenges in relation to security risk, intellectual property infringement and protection of personal data. Cybercriminals target people inside and outside their national boundaries and most African governments have neither the technical, nor the financial capacity to target and monitor electronic exchanges deemed sensitive to national security. These challenges are:

1. Low level of security provisions sufficient to prevent and control technological and informational risks.
2. Lack of technical know-how in terms of cybersecurity and inability to monitor and defend national networks, making African countries vulnerable to cyberespionage, as well as to incidences of cyberterrorism.
3. Inability to develop the necessary cybersecurity legal frameworks to combat cybercrime. In a survey of 21 countries conducted by ECA, it was found that while many countries had proposed legislations, the level of deployment of security systems in both the private and the public sectors to combat cybercrime was low.
4. Cybersecurity concerns are broader in scope than national security concerns. Yet, few major significant cybersecurity initiatives in Africa have been implemented. As ICTs are hailed as the end-all to the many pressing problems of Africa, cybersecurity is a critical issue that needs to be dealt with more comprehensively.
5. There is a need to build an information society that respects values, rights and freedoms and guarantees equal access to information, while encouraging the creation of authentic knowledge and that can build confidence and trust in the use of ICTs in Africa.
6. Generally limited levels of awareness of ICT-related security issues by stakeholders, such as ICT regulators, law enforcement agencies, the judiciary, information technology professionals and users.

3. First, the issue of definitions

Against the backdrop of the threats lurking both on the Internet and of some state authorities increasingly using cybersecurity laws and regulations to justify clampdowns on the freedoms of expression and association, to limit access to information and to violate the privacy of individual and group communications through the deployment of aggressive surveillance measures and other invasive espionage techniques that go beyond ensuring the stability and reliability of the Internet and the safety and security of individuals, organisations and states, it first and foremost becomes necessary to understand what is meant by cybersecurity (and cybercrime).

This is exactly where some of the opacity in discussions in the cybersecurity realm first becomes apparent, for it appears that there actually is no standard or precise definition of the term cybersecurity or what is or should be understood by it.

[10] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

[11] http://www.itnewsafrica.com/2016/01/namibia-still-a-top-target-for-cybercriminals/

[12] https://www.newera.com.na/2016/07/05/namibia-top-african-destination-cyber-criminals/

[13] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

[14] http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf

The tendency has thus been to couch it in broad terms and concepts that makes liberal use of buzz-words in an effort to lump as much as possible under the term as could be credibly accommodated.

The numerous (and increasing) definitions of cybersecurity prompted the Internet Society (ISOC) to remark: "As a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and "solutions" ranging from the technical to the legislative. While buzzwords like cybersecurity may make for good headlines, serious discussions of security and the Internet require a shared understanding of what is meant by cybersecurity."[15]

"Cybersecurity is a broad term that has evolved over time with no clear consensus on its exact meaning. Public awareness of the status of cybersecurity is colored by the often-sensational lapses in security that occupy the media. The exposure of personal information, stolen financial data, and spread of malware and viruses all give the impression of danger and chaos, of the imminent collapse of the Internet. In fact, the sky is not falling, but there could be storms on the horizon."

In light of this, following are just a few definitions of the term cybersecurity, to underscore the lack of universally subscribed to definitions, even though all the available definitions roughly subscribe to similar phrasing and broadly reference the same terms and concepts:[16]

> The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. -— **The Oxford English Dictionary, 2014**
>
> The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence. -— **France, Information Systems Defence and Security: France's Strategy, 2011, p. 21**
>
> Translation: A set of conditions under which all components of cyberspace are protected from the maximum number of threats and impacts with undesirable consequences. -— **Russia, Concept Strategy for Cybersecurity of the Russian Federation**
>
> Cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers. It is important to remember that cyber security is not an end in itself. It should not discourage the use of new technologies. The Government's Digital Britain Strategy aims to make the UK the leading major economy for innovation, investment and quality in the digital and communications industries. The Government's ultimate goal is to enable the full benefits of cyber space for the UK. -— **United Kingdom, Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyber space, 2009, p. 9**

The ability to protect or defend the use of cyberspace from cyber attacks. -— **United States of America, Committee on National Security Systems National Information Assurance Glossary, 2010, p. 22**

The process of protecting information by preventing, detecting, and responding to attacks. -— **United States of America, Framework for Improving Critical Infrastructure Cybersecurity, 2014, p. 37**

Our vision is to secure the Critical National Information Infrastructure (CNII) and make it resilient, and for Ghana to be self-reliant in securing its cyber space by infusing a culture of security to promote stability, social well being and wealth creation of our people. All actors in law enforcement, national security, network security practitioners in government and business, and the public will take part in the vision. -— **Ghana, Making our Cyber Space Safe, 2014, p. 14**

Policies, security arrangements, actions, guidelines, risk management protocols and technological tools designated to protect cyberspace and allow action to be taken therein. -— I**srael, Resolution No. 3611: Advancing National Cyberspace Capabilities, 2011, p. 1**

Japan aims to construct a "world-leading," "resilient" and "vigorous" cyberspace, and incorporate this cyberspace as a social system to realize a "cybersecurity nation" as a society that is strong against cyber attacks, full of innovations and of which its people will be proud. -— **Japan, Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace, 2013, p. 19**

The processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. -— **Kenya, Cybersecurity Strategy, 2014, p. 12**

Protection of data and systems connected to the Internet. -— **Norway, Cyber Security Strategy for Norway, 2012, p. 28**

The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them. -— **New Zealand, New Zealand's Cyber Security Strategy, 2011, p. 12**

The ability to protect or defend the use of cyberspace from cyber-attacks. -— **Saudi Arabia, Developing National Information Security Strategy for the Kingdom of Saudi Arabia, 2013, p. A-2**

[15] https://www.internetsociety.org/sites/default/files/bp-deconstructing-cybersecurity-16nov-update.pdf

[16] https://na-production.s3.amazonaws.com/documents/compilation-of-existing-cybersecurity-and-information-security-related-definitions.pdf

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protected the cyber environment and organization and user assets. Organisation and user's assets include connecting computing devices, personnel, infrastructure, applications, services, telecommunication systems, and a totality of transmitted and/or stored information in the cyber environment. -— **South Africa, Notice of Intention to make South African National Cybersecurity Policy, 2010, p. 12**
>
> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, and confidentiality. [in force] -— **International Telecommunication Union, ITU-T X.1205 (04/2008), 2008, 3.2.5**

When considering these and other definitions of cybersecurity, perhaps it is best to reflect on the following: "The term "cybersecurity" is used by different stakeholders to reference many different subjects often depending upon context, ranging from national security, to data security, to critical infrastructure security, and beyond."[17]

That said, while the definitions above are just some of those available out there it's important to note the following:

1. Most of these definitions, some quite clearly more extensively formulated than others, have been crafted from a systems perspective and broadly speak more to securing state or organisational level data/information and systems that could face cyber threats;

2. At this stage there does not appear to be a Namibia-specific definitional articulation of cybersecurity, which is problematic, as law initiators and drafters should operate against a clear definitional backdrop – to illustrate to stakeholder communities that they fully understand the nature of the realm they're attempting to legislate in – when provisioning for cybersecurity. If they have a definition, then it does not appear to have been made public.

While most of the definitions above reflect official or state-driven positions or perspectives, there are also several good civil society definitions to consider for guidance. With this in mind, as a starting point, maybe Namibian authorities could be persuaded to consider definitions along the lines of the following:

1. "Public Knowledge defines cybersecurity as the preservation – through policy, law, technology, best practices, cooperation, and education, both in the civilian and military fields – of the availability, confidentiality, and integrity of information and its underlying infrastructure, so as to preserve the security of networks and ultimately people both online as offline."[18]

2. "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."[19]

With regard to the latter definition, the following:

"The definition includes three core elements:

1. The ultimate goal of cybersecurity: "to enhance the security of persons both online and offline";

2. Articulation of how this ultimate goal and the dimensions of cybersecurity translate into technical terms: "cybersecurity is the preservation…of the availability, confidentiality and integrity of information and its underlying infrastructure";

3. The means through which this goal is being achieved: "through policy, technology, and education" with the understanding that "policy" includes the law."

"The definition supports the view that security and freedom (as well as cybersecurity and human rights) are deeply interrelated and synergistic, rather than zero-sum, and that cybersecurity and human rights protection are mutually reinforcing, interdependent, and both essential to promoting freedom and security."

This last consideration is arguably, at least in our view, very significant, because in defining cybersecurity within the Namibian context, it is important not to lose sight of the immensely important human rights aspects in this discussion.

At the very least, considering the above statements should give Namibian authorities pause to reflect, firstly, on their understanding of cybersecurity and, secondly, on the process for arriving at a workable and domestically widely acceptable definition of the concept. In this vein, attention is drawn to the following:

> "Both cybersecurity problems specifically and other criminal activity carried out using the Internet are not going to be solved with technology alone, but rather via close cooperation and coordination by all Internet stakeholders, including business, organizational and individual users, governments and law enforcement agencies, and policy makers world-

[17] https://freeandsecure.online/definition/

[18] https://www.publicknowledge.org/cybersecurity-and-human-rights

[19] https://freeandsecure.online/definition/

> wide. This must be combined with active efforts aimed at Internet literacy for all Internet users, including parents, children, and educators. The social component of cyber-crime cannot be fixed without user engagement.” [20]

What this excerpt points to, and ultimately what our recommendation in this regard is, is the following:

That any process seeking to formulate and formalise a cybersecurity framework proceed with/from the intent to first and foremost define the concept of cybersecurity, as well as what should be understood as cybercrime(s) and what should be secured or protected, and that such a process be extensively consultative and multi-stakeholder.

Applicable lesson

Although there is no one, precise definition of cybersecurity, it is, nevertheless, clear to most in or around the field what is broadly meant by the term. Namibian authorities would do well to engage, as suggested above, various and all relevant sectors and actors to put forward, in the first instance, a credible, domestically subscribed to definition of the concepts falling under the cybersecurity umbrella.

To end off this section, it seems appropriate to conclude with the following quote: “Cyber policy is a policy field in the making. Thus, there is still a lot of terminological confusion, ranging from rather benign differences such as the interchangeable use of prefixes (cyber/e/digital/net/virtual) through to core differences, when the use of different terms reflects divergent policy approaches. In policy and political discussions about cybersecurity, different organisations and governments use different terminology, but they also view cybersecurity concepts differently.” [21]

4. Injecting the human rights perspective into cybersecurity discussions

The purpose of this section is to briefly spotlight some of the numerous perspectives on cybersecurity and human rights in order to draw attention to the fact that it is universally recognised that the discussions around cybersecurity and cybercrime have to be cognisant of the wider and long term implications these measures have or could have on freedoms within a democratic framework. It is against the backdrop of these perspectives that a brief discussion of the provisions of Namibia’s Electronic Transactions and Cybercrime Bill will ensue in the next section (5).

The statements, declarations and recommendations that follow are self-contained and clear and need no further explanation.

“Considering that the establishment of a regulatory framework on cyber-security and personal data protection takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and Peoples’ Rights;”[22]
– *Preamble: AU Convention on Cyber Security and Personal Data Protection*

“Governments have the responsibility to ensure that the Internet policies they pursue are consistent with fundamental human rights and the rule of law. At the same time, they have a duty to address threats from both state and so-called “non-state” actors such as terrorists and criminals of all kinds. However, it is sometimes difficult for law enforcement officials to indict and prosecute national and transnational criminal activity without having assistance from intelligence agencies and their powerful tools of digital intelligence gathering.”
“Some governments are conducting surveillance for purposes and in ways that have a negative effect on fundamental human rights such as privacy, freedom of expression, and legitimate dissent and protest”.[23]
– *Global Commission on Internet Governance (GCIC)*

“In order to create a balanced and constructive multi-stakeholder dialogue and action to deal with cybersecurity threats, there is an imperative need to ensure that human rights lie at the core of a balanced and comprehensive view of cybersecurity.”[24]
– *Public Knowledge*

“While it is true that numerous definitions relating to cybersecurity already exist, it is difficult to find any cybersecurity definitions that include clear commitments to and respect for human rights.”[25]
– *Free And Secure*

“It is critical for civil society actors to deepen their knowledge and develop skills, including technical skills and understanding, to actively engage in policy discussions and measure appropriate responses. Civil society is uniquely positioned to advocate for cybersecurity policies based on a human rights approach and can play an important role by monitoring and documenting government and business practices, identifying knowledge gaps, and providing analysis to inform policies and relevant discussions.
In order to increase civil society’s engagement in shaping cybersecurity strategies and influencing regional and international norms, information sharing and collaboration with other stakeholders is key.”[26]
– *Public Knowledge*

“Everyone has the right to benefit from security, stability and resilience of the Internet. As a universal global public resource, the Internet should be a secure, stable, resilient, reliable and

[20] https://www.internetsociety.org/sites/default/files/bp-deconstructing-cybersecurity-16nov-update.pdf
[21] https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf
[22] http://au.int/en2/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
[23] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf
[24] https://www.publicknowledge.org/cybersecurity-and-human-rights
[25] https://freeandsecure.online/definition/
[26] https://www.publicknowledge.org/cybersecurity-and-human-rights

trustworthy network.
Different stakeholders should continue to cooperate in order to ensure effectiveness in addressing risks and threats to security and stability of the Internet.
Unlawful surveillance, monitoring and interception of users' online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the Internet."[27]
– African Declaration on Internet Rights and Freedoms

"Human rights communities have also tried to offer a definition of cybersecurity, which suggests that it should be about people rather than about systems: it is a matter of individual security rather than national security. The Working Group of the Freedom Online Coalition – a partnership of 30 governments working to advance Internet freedom – has codified a similar perspective, defining cybersecurity as protecting information and the Internet infrastructure for the sake of enhancing the security of individuals, both online and offline."[28]
– DiploFoundation

"State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments."[29]
– Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

The Human Rights Council (HRC) has addressed human rights issues online in its Resolutions on The Promotion, Protection and Enjoyment of Human Rights on the Internet. In 2012, the HRC affirmed "that the same rights that people have offline must also be protected online, in particular freedom of expression". In 2014, the HRC importantly outlined how governments should respond to cybersecurity threats, calling on States to "address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet."[30]
– UN Human Rights Council (HRC)

The UNGA Resolution on The Right to Privacy in the Digital Age notes similarly, that "the same rights that people have offline must also be protected online, including the right to privacy".[5] The UNGA Report A/68/98 also established that international humanitarian law applies online as offline, stating that "efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments." The same Resolution also calls on States to "encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs."[31]
– UN Human Rights Council (HRC)

The London Process Seoul Framework document also noted that it "is important to maintain an open environment that supports the free flow of information, research, innovation, entrepreneurship and business transformation, to ensure the protection of personal information in the online environment and to empower consumers and users in online transactions and exchanges." The Chair's statement from the (London Process) GCCS meeting in The Hague also urged stakeholders "to ensure that cyber security policies are, from their inception, rights-respecting and consistent with international law and international human rights instruments."[32]
– Global Conference on Cyber Space (GCCS)

Recommendations for human rights based approaches to cybersecurity[33]

These recommendations are a first step towards ensuring that cybersecurity policies and practices are based upon and fully consistent with human rights – effectively, that cybersecurity policies and practices are rights-respecting by design.

1. Cybersecurity policies and decision-making processes should protect and respect human rights;
2. The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design;
3. Cybersecurity-related laws, policies and practices should enhance the security of persons online and offline, taking into consideration the disproportionate threats faced by individuals and groups at risk;
4. The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law;
5. Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy;
6. Responses to cyber incidents should not violate human rights;
7. Cybersecurity-related laws, policies and practices should uphold and protect the stability and security of the Internet, and should not undermine the integrity of infrastructure, hardware, software and services;
8. Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy;
9. Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights;
10. Cybersecurity-related laws, policies, and practices at national, regional and international levels should be

[27] http://africaninternetrights.org/articles/
[28] https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf
[29] http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98
[30] https://www.article19.org/data/files/Internet_Statement_Adopted.pdf
[31] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
[32] https://www.gccs2015.com/themes/security
[33] https://freeandsecure.online/recommendations-for-human-rights-based-approaches-to-cybersecurity/

developed through open, inclusive, and transparent approaches that involve all stakeholders;

11. Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights;
12. Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders;
13. Cybersecurity capacity building has an important role in enhancing the security of persons both online and offline; such efforts should promote human rights respecting approaches to cybersecurity.

Source: Freedom Online Coalition

Collaborative Security: An approach to tackling Internet Security issues[34]

People are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for the Internet's prosperity and potential.

Collaborative Security is an approach that is characterized by five key elements:

1. Fostering confidence and protecting opportunities: The objective of security is to foster confidence in the Internet and to ensure the continued success of the Internet as a driver for economic and social innovation.
2. Collective Responsibility: Internet participants share a responsibility towards the system as a whole.
3. Fundamental Properties and Values: Security solutions should be compatible with fundamental human rights and preserve the fundamental properties of the Internet — the Internet Invariants.
4. Evolution and Consensus: Effective security relies on agile evolutionary steps based on the expertise of a broad set of stakeholders.
5. Think Globally, act Locally: It is through voluntary bottom-up self-organization that the most impactful solutions are likely to reached.

Source: Internet Society (ISOC)

13 International Principles on the Application of Human Rights to Communication Surveillance[35]

LEGALITY: Limits on the right to privacy must be set out clearly and precisely in laws, and should be regularly reviewed to make sure privacy protections keep up with rapid technological changes.

LEGITIMATE AIM: Communications surveillance should only be permitted in pursuit of the most important state objectives.

NECESSITY: The State has the obligation to prove that its communications surveillance activities are necessary to achieving a legitimate objective.

ADEQUACY: A communications surveillance mechanism must be effective in achieving its legitimate objective.

PROPORTIONALITY: Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Proportionate communications surveillance will typically require prior authorization from a competent judicial authority.

COMPETENT JUDICIAL AUTHORITY: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.

DUE PROCESS: Due process requires that any interference with human rights is governed by lawful procedures which are publicly available and applied consistently in a fair and public hearing.

USER NOTIFICATION: Individuals should be notified of a decision authorizing surveillance of their communications. Except when a competent judicial authority finds that notice will harm an investigation, individuals should be provided an opportunity to challenge such surveillance before it occurs.

TRANSPARENCY: The government has an obligation to make enough information publicly available so that the general public can understand the scope and nature of its surveillance activities. The government should not generally prevent service providers from publishing details on the scope and nature of their own surveillance-related dealings with the State.

PUBLIC OVERSIGHT: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS: Service providers or hardware or software vendors should not be compelled to build surveillance capabilities or backdoors into their systems or to collect or retain particular information purely for State surveillance purposes.

SAFEGUARDS FOR INTERNATIONAL COOPERATION: On occasion, states may seek assistance from foreign service providers to conduct surveillance. This must be governed by clear and public agreements that ensure the most privacy-protective standard applicable is relied upon in each instance.

[34] http://www.internetsociety.org/collaborativesecurity

[35] https://www.eff.org/files/2014/01/05/13p-onepagerfinal.pdf

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS: There should be civil and criminal penalties imposed on any party responsible for illegal electronic surveillance and those affected by surveillance must have access to legal mechanisms necessary for effective redress. Strong protection should also be afforded to whistleblowers who expose surveillance activities that threaten human rights.

Extremist Content and the ICT Sector[36]

Summary of Recommendations

1. Governments must protect and respect human rights when developing, implementing, and enforcing laws and policies meant to address extremist content online.
2. Government legal demands to restrict content for the purpose of protecting public safety must be pursuant to the rule of law. They should respect and protect freedom of expression and privacy, and be directed at creators of content, rather than intermediaries, whenever possible.
3. Governments must not impose liability—directly or indirectly—on intermediaries on the basis of content sent or created by third parties. Intermediaries must not be required to monitor third-party content that they host or transmit.
4. Governments should not pressure companies to change their terms of service (TOS). Companies develop TOS in order to deliver user experiences that are appropriate for the nature or type of service, and the user community of the service.
5. When governments refer content to companies for removal under companies' TOS, governments should guard against the risks that such referrals may set precedents for extra-judicial government censorship without adequate access to remedy, accountability, or transparency for users and the public. If governments make such referrals, they should be transparent about, and accountable for, such referrals.
6. Companies should be transparent with their users when required by governments to remove or restrict content, unless prohibited by law.

Source: Global Network Initiative

Manila Principles on Intermediary Liability[37]

All communication over the Internet is facilitated by intermediaries such as Internet access providers, social networks, and search engines. The policies governing the legal liability of intermediaries for the content of these communications have an impact on users' rights, including freedom of expression, freedom of association and the right to privacy.

With the aim of protecting freedom of expression and creating an enabling environment for innovation, which balances the needs of governments and other stakeholders, civil society groups from around the world have come together to propose this framework of baseline safeguards and best practices. These are based on international human rights instruments and other international legal frameworks.

Principles:

1. Intermediaries should be shielded from liability for third-party content.
2. Content must not be required to be restricted without an order by a judicial authority.
3. Requests for restrictions of content must be clear, unambiguous, and follow due process.
4. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.
5. Laws and content restriction policies and practices must respect due process.
6. Transparency and accountability must be built into laws and content restriction policies and practices.

Source: https www.manilaprinciples.org

OECD Internet Policy Making Principles[38]

1. Promote and protect the global free flow of information
2. Promote the open, distributed and interconnected nature of the Internet
3. Promote investment and competition in high-speed networks and services
4. Promote and enable the cross-border delivery of services
5. Encourage multi-stakeholder cooperation in policy development processes
6. Foster voluntarily developed codes of conduct
7. Develop capacities to bring publicly available, reliable data into the policy making process
8. Ensure transparency, fair process and accountability
9. Strengthen consistency and effectiveness in privacy protection at a global level
10. Maximize individual empowerment
11. Promote creativity and innovation
12. Limit Internet intermediary liability
13. Encourage cooperation to promote Internet security
14. Give appropriate priority to enforcement efforts

Source: www.oecd.org

Applicable Lessons

It should be patently clear by now from the quotes, statements, declarations and recommendations briefly introduced here, as well as most of those not even mentioned here, is that just about every serious actor in the cybersecurity space recognises that cybercrime, and other illegal online activities, can only be effectively countered and cybersecurity mechanisms only efficiently implemented if such measures are approached, agreed to and designed in a cooperative, multi-

[36] http://globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-ICT-Sector.pdf

[37] "https www.manilaprinciples.org

[38] https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf

stakeholder setting and framework that comprehensively includes the business, technology, and civil society sectors.

Furthermore, the fact that there exists a fairly extensive and growing body of literature and material that is available in the online public domain concerning cybercrime and cybersecurity (including against the backdrop of larger human rights concerns and considerations) means that there probably would be no need for further local extensive studies on these topics. While Namibia does not need to reinvent the wheel in this context in any sense, legal drafters and decision and law makers should rather be encouraged to acquaint themselves, if not thoroughly, at least sufficiently with the themes, considerations and concerns in this field in order for law and policy making to reflect best practices as they already exist and continue to evolve.

That said, given the availability of such an extensive body of literature on the topic of cybersecurity and related matters, relevant authorities might wish to take the opportunity to organise intensive consultations, with special emphasis on creating platforms for enhanced cooperation between state and non-state actors in this field.

5. Electronic Transactions and Cybercrime Bill

When parliament opened in February 2017, one of the first motions tabled in the new session was for the consideration of the Electronic Transactions and Cybercrime Bill, which was placed on the parliamentary agenda by Minister of Information and Communication Technology, Tjekero Tweya. However, as quickly and unexpectedly as it made an appearance on the parliamentary agenda, just as quickly it was removed again. It is unclear why it was pulled and when it would be placed back on the parliamentary agenda again, but by end 2017 indications were that Namibian authorities were intent to push ahead, and by the sound of it urgently so, in 2018 to pass some sort of a cybersecurity law.

This would have followed a period of 'consultations', the outcomes of which were still unknown by end 2017. These 'consultations' on the draft Bill basically amounted to a month-long call for submissions and inputs, starting in mid-May and closing on 16 June 2017, which was followed by two one-day 'consultation' workshops on 29 August and 12 September 2017, organised by officials in the Ministry of Information and Communication Technology's ICT Development Directorate. On 18 August 2017 the Access to Information in Namibia (ACTION) Coalition also hosted a closed-door roundtable 'consultative' meeting with MICT officials, as well as select government and private sector stakeholders, around the provisions of the Bill.

It has to be noted though that these ministerial 'consultations' appeared to be merely procedural in nature and before, during and after this exercise it was clearly implied that there would be no substantial changes made to the Bill text dated April 2017, and such should not be expected.

That said, the draft Electronic Transactions and Cybercrime Bill, the April 2017 version, appears to have been crafted without substantial multi-stakeholder input before the abovementioned 'consultations'. The 2013 version, which was nowhere near ready for discussion in parliament, and certainly not for passing into law, was the last version that was apparently widely and publicly circulated for comment.

Despite this, the ACTION Coalition submitted substantial critiques, proposals and recommendations at each stage of this 'consultation' process. These submissions were drafted by this author for the Institute for Public Policy Research (IPPR), on behalf of the ACTION Coalition (submitted on 16 June 2017); Henry Maina of Article 19 Eastern Africa, on behalf of the ACTION Coalition (following the 18 August 2017 meeting); and Prof. Justine Limpitlaw, for the Namibia Media Trust, on behalf of ACTION (submitted on 12 September 2017). These submissions are attached to this paper as annex 1, 2 and 3, respectively.

The issue of stakeholder consultation and public inputs is a significant one in the context of cybersecurity, as this paper has attempted to demonstrate throughout.

It is our overarching contention and recommendation that the Electronic Transactions and Cybercrime Bill be subjected to wider stakeholder and public consultations, and possible extensive redrafting, before being tabled in parliament again.

That said, the following discussion will briefly look at some of the more striking aspects of the April 2017 version of the draft Electronic Transactions and Cybercrime Bill.

General Observations:

The ITU's Harmonization of the Telecommunication and ICT Policies in Africa (HIPSSA) project, which started in 2008, culminated with the Computer Crime and Cybercrime: SADC Model Law, which was launched in 2013, the same year as the first proper draft of the Electronic Transactions and Cybercrime Bill first made an appearance. Since the launch of the HIPSSA project a number of African countries have passed cybersecurity laws.

The 2013 draft of the Electronic Transactions and Cybercrime Bill is a direct result of the ITU led process. In fact, ITU consultants assisted with the drafting of the proposed legislation.

That said, the HIPSSA SADC Model Law and the Namibian Electronic Transactions and Cybercrime Bill came almost a year before the adoption of the African Union Convention on Cyber Security and Personal Data Protection at the 23rd Summit of Heads of State and Government at Malabo, Equatorial Guinea, on 27 June 2014.

Internet rights advocates have since called for African countries to rather use the AU Convention to guide the crafting of cybersecurity laws rather than the ITU proposals. AccessNow has identified an "overbroad interpretation" of the ITU guidelines as having contributed to highly flawed and human rights violating laws having been promulgated across the continent.

AccessNow warns that the ITU guidelines were "carried out prior to 2014 without public consultation. Unlike the ITU model regulations, this Convention was adopted after multi-stakeholder input, with the African Charter on Human and People's Rights as a reference. For this reason, governments should not pass the suggested ITU regulations into law, but should follow the AU Convention instead."[39] While the AU Convention has its own serious flaws, this is a position we recommend should be supported.

Following is a brief spotlighting of some of the key aspects of the latest available draft of the Electronic Transactions and Cybercrime Bill. However, before going there, it needs to be pointed out that the 2017 draft is a cleaned-up version of the 2013 one, and while MICT sources have indicated that the 2017 version gives more than a nod to the African Union Convention on Cyber Security and Personal Data Protection in its provisions, the drafts do mirror each other greatly in many respects, suggesting that the 2017 version is just a thin reworking of the 2013 draft.

Concerning Aspects:

1. Inappropriate two-in-one law making

The Electronic Transactions and Cybercrime Bill (2017) is in essence the Electronic Transactions Bill with cybercrime provisions tagged on towards the end. This goes against best practice in legislating for cybersecurity, or against cybercrime, which mostly is addressed in comprehensive standalone cybersecurity and cybercrime laws. The Electronic Transactions and Cybercrime Bill (2017) is not an example of a modern cybersecurity framework proposal. A separate cybercrime/cybersecurity Bill should be crafted around what is captured in chapter 8 of the Bill. The lumping together of two related but different topics in such a significant statutory instrument is the consequence of using a flawed and outdated standard as guide. It is proposed that Namibian authorities separate the two topics and go back to the drawing board to construct a much-improved cybersecurity/cybercrime framework, while pushing ahead with the promulgation of the Electronic Transactions Bill.

2. Problems with key definitions

The definitions section of the draft Bill is incomplete and does not contain definitions of key concepts. In fact, amongst others, neither cybercrime nor cybersecurity are defined in the proposed law. Such significant omissions certainly indicate that this draft is not a proposed cybersecurity/cybercrime framework. Other key definitions missing are those for "functionary" and "forensic tools", while basic concepts such as "access", "data", "privacy" or "seize" are also not included in the definitions. The list goes on. Some of these terms, including "child pornography", only come up for definition in chapter 8, which feeds into the notion that this bill is actually two draft laws unsatisfactorily melded into one.

Not only are key concepts not defined, but others, such as "computer system" are either woefully under-defined or outdated in their definition. The definitions section needs to be updated and expanded considerably, especially given the specialised and technical nature of the field that is being legislated for.

Against this backdrop, although there is no single, precise definition for cybersecurity or cybercrime, it nevertheless is clear to most in or around the field what is broadly meant by the term. As noted earlier, Namibian authorities would do well to engage various and all relevant sectors and actors to put forward, in the first instance, credible, domestically subscribed to, but universally understood, definitions for the concepts falling under the cybersecurity umbrella.

3. Confusing arrangement of cybersecurity related provisions

Unlike cybersecurity laws the world over, the Electronic Transactions and Cybercrime Bill's (2017) cybersecurity provisions are a mish-mash and do not deal in a structured and substantially consequential way with the necessary aspects of combatting cybercriminal activities. The Bill lacks coherence. To view what a coherent contemporary cybersecurity law proposal looks like, Namibian authorities are requested to view the Cybercrimes and Cybersecurity Bill (2017) of South Africa.[40]

4. Unauthorised access, secret warrants and warrantless search & seizure

Of utmost concern is that various sections of the Bill appear to enable warrantless search and seizure operations, while other sections seem to allow for a system of secret warrants and unauthorised access by state agents. In this regard, chapter 5, in sections 43 (2) and (3), seems to enable unauthorised access and access without notification by CRAN and others to computer systems, which would amount to government hacking of private computer systems. The legality of these provisions is highly questionable.

Similarly, in chapter 7, in section 61 (6), (7) and (8), a "Computer Security Inspector", which can be anyone, is also authorised to access computer systems without giving notification or seeking legal authorisation. At the same time, sections of chapter 8, in sections 70 (2) and all of section 72, allow for a system of secret warrants while vaguely defining the conditions under which such secret warrants can be sought. These provisions open the door to pervasive communications surveillance and interception without appropriate oversight mechanisms to monitor the conduct of those carrying out such surveillance or interception activities. It seems clear that unauthorised access by state agents and interception of communications is under-regulated, especially when viewed against the body of available literature on these topics.

[39] https://www.accessnow.org/cms/assets/uploads/2016/12/RoomforImprovement_Africa.pdf

[40] http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

It has to be further pointed out, in relation to secret warrants, that unlike South Africa's Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) which provides for a "designated judge" to hear intercept applications, this Bill makes no provision for even the most basic of accounting for such requests. Although RICA's provisions on accounting standards are significantly flawed, they do present some measure of transparency and do provide the public with basic insight, by way of a publicly released annual report by the designated judge into state surveillance and interception. No Namibian law, including this Bill, allows for such transparency or insights.

A system of secret warrants and warrantless accessing of private data and communications and computer systems basically means that "the target of an interception order is never granted the opportunity to test whether the intrusion was lawfully approved – and on the basis of a reasonable suspicion"[41] . This is because the judicial process of applying for and granting such warrants is not adversarial.

In this regard, the following should be borne in mind: "Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Proportionate communications surveillance will typically require prior authorisation from a competent judicial authority." And also: "States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions."[42]

While some of the Bill's draft provisions are similar to sections of the Communications Act of 2009, it has to be pointed out that the constitutionality of some of these provisions, along with those of concern in the Communications Act, is highly debatable and challengeable.

5. Lack of data and privacy protections

The Electronic Transactions and Cybercrime Bill (2017) is worryingly thin on personal data and privacy protections, and the little that is there comes across as severely under- developed. The draft law does not adequately provide for personal data protection or proscribe the rights of data subjects, in line with international best practice. In this regard: "To assure the public that their data is being appropriately protected, states that do not already have comprehensive personal data protection legislation and a privacy enforcement authority with legal enforcement powers should take steps to create such regimes." [43]

Related to the issue of absent or under-developed privacy and data protection safeguards, as well as the concerns sketched in point 4 above, is that the Bill is silent "on the correct procedure to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from the interceptions".[44]

In the same vein, and in this context of invasion of privacy, this is highly problematic, as the "target of the interception order is never informed of the order, even after the period of interception has ended and even after any investigation has been concluded."[45] When it comes to informing or notifying targets, after the fact, of invasive surveillance and interception, perhaps Namibian authorities should look at frameworks used in the US, Japan, Austria and Chile, which seem to be the countries with user notification legal dispensations that can be emulated.

Given that the right to privacy is explicitly enshrined in the Namibian Constitution, the absence of substantive personal data and privacy protections in the draft law raises serious constitutional alarm, especially in relation to the concerns sketched in point 4 above.

Against this backdrop, Namibian authorities are thus encouraged to formulate a comprehensive data protection framework and can look to such countries as Singapore[46] for guidance, as well as to the EU and South Africa.

6. Undermining of encryption and anonymity

Chapter 5 (Accreditation of Security Services or Products) of the draft law deals with the regulation of encryption devices and technologies. This chapter seeks to introduce a rather onerous and intrusive registration regime, and appears to enable state agents to establish and open "backdoors" in encryption technologies.

These provisions should be tested against best practice and brought up to date. In this regard, the Global Commission on Internet Governance states[47] : "Anonymity-granting technologies and end-to-end encryption provide the security and privacy necessary for exercising fundamental human rights online and for individuals, businesses and governments to engage in activities that support economic growth and social progress."

And it recommends that: "Governments should not compromise or require third parties to weaken or compromise encryption standards, for example, through hidden "backdoors" into the technology as such efforts would weaken the overall security of digital data flows and transactions." The proposed provisions of the 2017 draft should be measured against such assertions, with particular and appropriate input from the technical community, as well as other stakeholders.

In our analysis, provisions in the Bill seeking to regulate the use of encryption technologies do seem to be aimed at weakening such technologies, and thus would open the door to such technologies being infiltrated by criminal and other malignant actors.

[41] https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1/

[42] https://www.eff.org/files/2014/01/05/13p-onepagerfinal.pdf

[43] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

[44] https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1/

[45] https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1/

[46] https://www.pdpc.gov.sg/legislation-and-guidelines/overview

[47] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

7. Lack of transparency and access to information

The draft law suffers from a lack of transparency-inducing measures, and does not compel government authorities, law enforcement or private companies to account for their actions openly. In this regard, the emerging trend is that: "Private companies should publish transparency reports that reveal the amount of content being restricted or blocked in response to requests by governments, for what purposes and by what means. Governments must allow companies to publish aggregate information about what they have requested and how the company responded."[48]

Such measures would allay fears of the abuse of secret warrants, amongst others, and would give the public confidence that the law is not being used gratuitously to violate individual privacy and the integrity of private data systems.

Further, the draft law does not appear to explicitly encourage access to information. This appears to be inconsistent with ongoing access to information legislating in Namibia and current and emergent global best practice trends.

8. Excessive and unaccountable ministerial power

Related to the point above about a lack of transparency, is the vesting of what appears to be excessive discretionary decision-making and appointing powers in the minister. No oversight or accountability measures are included with regard to ministerial conduct under the provisions of this draft law. In this regard, the AU Convention on Cyber Security and Personal Data Protection calls on states to: "Establish clear accountability in matters of cyber security at all levels of government by defining the roles and responsibilities in precise terms."

It has to be questioned to what extent the relevant draft provisions that vest various powers in the minister, and those he empowers, would be in line with Namibia's emerging access to information legislation and current best practice, which points to the emergence of more collaborative systems of accountability in dealing with cybersecurity issues. It would seem that the Electronic Transactions and Cybercrime Bill (2017) would not be compatible with such emergent legal and best practice dispensations.

9. Too lenient an approach to service provider or intermediate liability?

While the law incorporates provisions in Chapter 6 (Liability of Service Providers for Unlawful Material) to protect service providers who merely serve as hosts or conduits for third-party content, concerning such provisions AccessNow states that: "This type of legal protection enabled the growth of the internet and allows the smooth functioning of the global web at scale, so these provisions must be retained."[49]
Whether the provisions of the Electronic Transactions and Cybercrime Bill (2017) are up to standard in terms of intermediate liability is open to question, and should be further investigated through a process of open and extensive consultation. Intermediate liability needs to be weighted against end-user data and privacy protections, as well as net neutrality considerations. In this regard, it can be argued that the Electronic Transactions and Cybercrime Bill (2017) takes too lenient an approach to intermediate or service provider liability.

10. Online child protections

As with the inappropriate melding together of electronic transactions and cybercrime provisions, the Electronic Transactions and Cybercrime Bill also seems to be an inappropriate place to deal with child online protections and safeguards. Chapter 8, section 66, of the Bill deals with child pornography, while section 67 deals with online harassment.

While such safeguards are highly and urgently necessary, child online protections should be comprehensively dealt with through amendments to the Child Care and Protection Act of 2015.

11. General concerns

The Electronic Transactions and Cybercrime Bill (2017) is substantially weak on adequate and appropriate judicial, legislative and public oversight mechanisms, to especially prevent abuse of potential communications surveillance and interception provisions and mechanisms. To put it bluntly, this draft law makes no provision for multi-stakeholder oversight mechanisms and, given the Namibian state's acknowledged capacity limitations, this could make for strained implementation of any cybersecurity regulatory framework ultimately promulgated.

Conclusions

With the provisions of the draft Electronic Transactions and Cybercrime Bill not having been crafted in an extensively consultative process, it is concerning that the draft managed to make it onto the parliamentary agenda in early 2017 (even though it has since been removed indefinitely). It appears that over the years, very few stakeholders would have had an opportunity to make inputs into its provisions. If this is in fact the case, then the most recent draft might very well be significantly flawed and outdated in some of its provisions.

In this regard, it is worth reiterating Privacy International's remarks that: "Cyber policy and law making is in its infancy and requires the input of different stakeholders. Truly effective security must be done as a collaboration and no one actor can claim to have the solution. This requires trust and efforts to understand different stakeholder perspectives."[50]

It is against this backdrop that we make the following recommendations.

[48] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

[49] https://www.accessnow.org/cms/assets/uploads/2016/12/RoomforImprovement_Africa.pdf

[50] https://www.privacyinternational.org/sites/default/files/CyberSecurity_2017.pdf

Recommendations

1. Namibia should ratify the African Union Convention on Cyber Security and Personal Data Protection as a matter of urgency;

2. Once ratification of the AU Convention has been achieved, Namibian authorities should use the AU Convention as the guide for designing, drafting and implementing a cybercrime/security regulatory framework;

3. In the process of coming up with such a framework, it is recommended that relevant Namibian decision and law making authorities, as well as legal drafters, as the first step, commence a review of the extensive existing body of literature and materials on cybercrime/security related issues and measures in order to, firstly, acquaint themselves with the issues and the myriad voices on the constantly evolving cybercrime and cybersecurity landscape, and secondly, assess whether Namibia's proposed cybersecurity efforts are in line with emergent trends and best practices towards the installation of the best possible framework for the Namibian context;

4. In line with international best practice, we recommend that any cybercrime/security law and institutional framework be the product of an extensive and meaningful cooperative multi-stakeholder consultative process and that the eventual framework make provision for some level of multi-stakeholder oversight involvement;

5. Finally, against the backdrop of everything that has been stated in this paper, we call for the restarting of the law drafting process of a cybercrime/security law, while finalising the Electronic Transactions Bill (separately from a cybercrime law) as a matter of urgency.

Submissions on the draft provisions of the electronic transactions and cybercrime bill 2017

The ACTION submission of 13 September 2017 can be accessed at the following link:

http://wordpress.p426669.webspaceconfig.de/wp-content/uploads/2017/10/ACTION-Submission-E-Transactions-CybercrimeBill2017-Sept2017.pdf

The ACTION submission of June 2017 can be accessed at the following link:

http://wordpress.p426669.webspaceconfig.de/wp-content/uploads/2017/10/ACTION-IPPR-Submission-on-ETC-Bill-June2017.pdf

About the Author

Frederico Links has been an IPPR Research Associate since 2009. He has focussed on democracy and elections, party political finance, empowerment policies, internet governance, and public procurement. He has previously worked as a journalist for a range of Namibian newspapers and is a former editor of Insight Namibia magazine. He is the current Chairperson of the ACTION Coalition which campaigns for greater access to information in Namibia.

About Democracy Report

Democracy Report is a project of the IPPR which analyses and disseminates information relating to the legislative agenda of Namibia's Parliament. The project aims to promote public participation in debates concerning the work of Parliament by publishing regular analyses of legislation and other issues before the National Assembly and the National Council. Democracy Report is funded by the Embassy of Finland.

About IPPR

The Institute for Public Policy Research (IPPR) is a not-for-profit organisation with a mission to deliver independent, analytical, critical yet constructive research on social, political and economic issues that affect development in Namibia. The IPPR was established in the belief that development is best promoted through free and critical debate informed by quality research.

Incorporated Association Not for Gain Registration Number 21/2000/468
Directors: M M C Koep, D Motinga, M Humavindu, N Nghipondoka-Robiati, J Ellis, G Hopwood

PO Box 6566, Ausspannplatz, Windhoek, Namibia · Tel: +264 61 240514/5 Fax +264 61 240516
info@ippr.org.na · www.ippr.org.na