
Trudging Down the wrong path

Introduction

The purpose of this brief is to advocate for an approach to cybercrime and cyber security in Zimbabwe that protects individuals, devices and networks and guards against arbitrary infringement of human rights in the name of national security. The Ministry of Information Communication Technology and Cyber Security spearheaded drafting of the draft Cyber Crime and Cyber Security Bill (2017)\(^1\) (the “draft Bill”).

The Bill seems to borrow from the Budapest Convention. Its main objective, as set out in the 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. However, the ICT landscape is evolving and there is need to move on with the times to reflect the new realities.

There is no information on when the draft Bill will be formally presented before Parliament for debate and subsequent gazetting as an Act. Speculation is that the Bill might be signed into law before Zimbabwe’s elections which are expected to be held anytime between July and August 2018.

This is a unique moment in Zimbabwe’s legislative history which presents opportunity for the government to implement fundamental rights enshrined in the country’s current constitution. Unfortunately, the current draft Bill falls short of protecting important rights such as the right to privacy, access to information, and freedom of expression.

The government should address deficiencies in the draft bill and align it with international standards that ensure strong protections for the people’s privacy and security online.

---

Currently, the draft Bill does not reflect these globally accepted privacy and freedom of expression principles. This brief outlines how the Zimbabwean government misinterprets cyber security by conflating it with restrictive control of Zimbabwe’s online space. The brief goes on to state why the current approach will fail to improve security of Zimbabwe’s online space. Lastly, the brief concludes with recommendations on how to improve the draft Bill.

When drafting this type of legislation, the government must ensure that the envisioned legislation reflects and embodies constitutional principles as well as Zimbabwe’s international obligations to protect human rights.

Unfortunately, the current Bill encroaches on fundamental rights such as the right to privacy and the right to freedom of expression. This places the draft Bill at loggerheads with the Constitution.

The government drafted a law which criminalises various forms of online behaviour which at times do not respond to actual online threats which prevail in Zimbabwe. A reading of the draft gives an impression that the Bill’s focus is more on policing social media, in an attempt to shield government from criticism as opposed to protecting the public from actual harm associated with online crime.

Government’s focus seems to be on silencing dissent on social media. The priority should be on developing a data protection framework, which will go a long way in protecting the public from cybercrime. With so much work still to be done on Zimbabwe’s cyber security framework, we recommend halting passage of the draft Bill as it undergoes proper consultation with technical experts, industry and civil society.

We therefore recommend the following:

1. **Revise Zimbabwe’s approach to cyber security.**

   Good cyber security policies and practices put people and their rights at the centre, and seek to strengthen and protect basic human rights rather than curtail them. Good cyber security is about addressing the root causes of insecure systems, identifying vulnerabilities and
protecting critical infrastructure so that individuals, devices and networks are protected from data breaches and falling victim to cyber crime. Legislation should be underpinned by globally accepted human rights safeguards.

Government’s current approach ignores human rights principles related to cybersecurity and instead focuses on criminalising the use of ICTs. The preferred approach to regulating Zimbabwean cyberspace should have been one that ensures secure use of ICTs by tackling the root cause of insecure systems and increasing protections and safeguards.

If government does not take steps to address the draft Bill’s deficiencies, this may result in the negation of the cybersecurity principles enshrined in Zimbabwe’s National ICT Policy, as well as the country’s Cybersecurity Policy which were both adopted in 2016.

Controlling social media is not cyber security, but this seems to be the government’s priority. The ruling party and government views social media as a national security threat ever since the appearance of Baba Jukwa, a phantom Facebook character in 2013, who tormented the ruling Zanu PF party by leaking party secrets.

In February 2016, then Zanu PF spokesperson Simon Khaya Moyo, told journalists that his party’s politburo had resolved that members stop using social media to discuss party business. This move was meant to silence dissent from within the party which was facing growing discord. In the same month, then Police Commissioner-General Augustine Chihuri, said social media had the ability to destabilise the country.

In June 2017, the Minister of ICTs, Supa Mandiwanzira, admitted that the Cyber Crimes and Cyber-security Bill, was in response to social media which is seen as having adverse political consequences. He said: “It is important that we have this law as of yesterday, not tomorrow and not today because our people are being abused. They are vulnerable and we need to protect them.”

---

2 https://www.herald.co.zw/politburo-bans-social-media-abuse/
3 http://www.chronicle.co.zw/chihuri-deplores-social-media/
Government’s position on social media as a threat, was further revealed when the government announced its reasons for creating a Ministry of Cyber Security, Threat Detection and Mitigation. Presidential spokesperson, George Charamba, explained then that the ministry was created to catch mischievous elements using social media. He further stated that Zimbabwe had looked to China, Korea, and Iran for insights on how to regulate local cyberspace.\(^4\)

The draft Bill restricts access to information which government also views as another threat to national security. The public has a right to access to information held by the government or private entities that deal with the public. The public has a right to know of any surveillance programmes being run by the government. Governments should not withhold any information concerning violations of human rights. Governments should also not persecute whistleblowers or journalists who obtain access to such information. Where governments feel that disclosing certain information may compromise national security, such information must be narrowly defined and justified.

In short, the government of Zimbabwe is currently labouring with what can only be viewed as a misguided perception of cyber security. This is dangerous because this stance will disadvantage citizens who may not necessarily be aware of the real threats and how they can protect themselves. Such an approach may also muzzle the growth of the ICT sector as intended by the ICT policy. This must be rectified.

2. Policy objectives of the 2016 ICT Policy.

Zimbabwe has an ICT policy which is supposed to inform the Cyber crime and Cyber Security Bill, which seems to have been forgotten. Zimbabwe’s 2016 ICT Policy\(^5\) sets out a vision of a vibrant ICT sector, based on improved infrastructure and inclusivity. It acknowledges the absence of a “cyber security framework”\(^6\) and the need to

---

\(^4\) George Charamba explains functions of Cybersecurity ministry: https://youtu.be/Z_iTNf6Taks
\(^6\) Ibid p14
“implement cyber laws and ICT legislative provisions”, including identifying the need to “adopt data protection and privacy”.

This should be the priority. The current proposed Cyber Security and Cyber Crime Bill appears to contradict objectives set out in the ICT policy. There is need for the two documents to speak to each other.

3. Development of a data protection framework

Data protection is the cornerstone of cyber security as outlined in the African Convention for Cybersecurity and personal data protection. Article 8 of the African Convention on Cyber Security and Personal data says that member states must commit to establishing a legal framework designed to strengthen fundamental rights and public freedoms, particularly the protection of physical data and punish any violation of privacy without prejudice to the principle of free flow of personal data. Article 11 compels states to establish independent data protection committees but the current cyber security bill does not conform to these requirements.

Data protection legislation and policies ensure that citizens’ and consumers’ right to privacy. Some big corporate companies commercialise personal data without the consent of the data owners and this may have repercussions on privacy especially with regards to medical records or the security of citizens. Data protection should go hand in hand with initiatives to grow a country’s ICT sector. ICT strategies will fail if people don’t trust the systems they are expected to use.

Data protection helps to build and maintain that trust. The ICT policy of 2016 provides for the establishment of a national data centre which allows Zimbabwe to centralise her

---

7 Ibid p32  
8 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_unionConvention_on_cyber_security_and_personal_data_protection_e.pdf  
information storage, management and protection. The national data protection centre is to be managed by government entities as well as private business interests. No mention is made of the involvement of citizens. The cybercrime and cyber security bill is silent on this national data protection centre. It is not advisable to set up the National Data centre without any comprehensive data protection laws.

Absence of adequate data protection legislation is a problem, particularly for countries which are attempting to grow their economies, or introduce initiatives like biometric voter registers, which Zimbabwe already has. Using systems which rely on the collection and sharing of data without basic protections which underpin the collection, storage and sharing of such data, leaves data subjects vulnerable to their data being stolen.

Citizens are already speculating that their data will be used to expose their electoral choices and victimise them. The government can allay those fears by gazetting adequate data protection laws. This is one major reason why the Zimbabwean government is urged to finalise the drafting of the Data Protection Bill which has been in the pipelines since 2013.

The draft Bill suffers due to the lack of data protection regulation, and makes the provisions in handling data seem careless.

3. Proper threat assessment and prioritise what needs to be protected

As the country invests in ICT infrastructure, security considerations must be built in from the start. For example, the draft Bill references the importance of protecting critical data but has not identified what critical data actually is. There is need for the bill to define personal data that must be protected, but also not to unnecessarily keep away data from citizens by governments.

Part II of the draft Bill discusses the establishment of a Cybersecurity Centre, including a representative from civic society on the Committee. This committee however, is dominated by the commanding officers from State controlled intelligence and security units whose

http://www.veritaszim.net/node/1818
understanding of cyber security is sometimes questionable. There must be balance within the committee to ensure that the interests of a cross section of stakeholders are factored in.

4. **Highlight real cyber security issues and raise awareness, show people how they can protect themselves.**

The ruling Zanu PF politburo has made at least four resolutions which sought to stop use of social media or regulate use in a bid to silence internal dissent. There is need for public education campaigns which raise awareness on real/more urgent online threats, such as online scams which has been rife with mobile money platform **Ecocash**. Ecocash fraud involving identity theft is on the rise for example.\(^\text{11}\) Not enough has been done to educate vulnerable citizens especially the elderly about the threats in the cyber space.

4. **Underpin any future legislation with Zimbabwe’s constitution and international obligations to protect human rights.**

The draft bill has been re-written three times and still falls short of international standards. These include the Tshwane Principles on National Security and the Right to Information, the Necessary and Proportionate Principles and the provisions of the African Charter of Human and People’s Rights as well as the internal constitutional provisions.

The Constitution of Zimbabwe guarantees the right to access to information. The right to privacy is also guaranteed and fundamentally the constitution offers protection to journalists not to reveal their sources. These safeguards are not considered or made meaningful in the draft Bill.

The Tshwane Principles on National Security and Right to Information, addresses the legitimate right that citizens have to access information held by the government and the need for national security. Key state actors view activities on the internet as a threat to national security and the proposed bill seeks to repel these perceived real or imagined threats.

---

\(^{11}\) [http://www.chronicle.co.zw/new-wave-of-ecocash-fraud/]
Zimbabwe has ratified the United Nations International Covenant on Civil and Political Rights as well as the African Charter on Human Rights which places obligations on the country to craft policy and laws that respect the requirements of these covenants. These are very clear that government policy and laws must promote and uphold fundamental human rights.

5. Separate cyber security and cyber crime in any future legislation.

Cybercrime criminalises behaviour while cyber security is focused on protecting the individual, devices and networks. Having both in the same legislation leads to confusion about what cyber security is. Government must therefore consider separating the two in order not to create confusion.

Conclusion

The government of Zimbabwe needs to consider whether the proposed Cyber Crime and Cyber Security Bill meets modern international standards as well as whether it is consistent with the national constitution and other international human rights treaties.

We would like to thank the Ministry for taking the time to consider these comments. We are available to discuss any further aspects or questions on the matter at hand.

Written by Malvern Mkudu\textsuperscript{12} with generous support from:

\begin{center}
\textbf{PRIVACY INTERNATIONAL} \quad \textbf{MISA ZIMBABWE}
\end{center}

\textsuperscript{12} Contact Malvern on mmkudu@gmail.com or +263 778 194 939