**Commentary on the Cybersecurity and Cybercrimes Bill**

*Social media threat to cybersecurity?*

In his address during the opening of the 5th Session of the 8th Parliament, President Robert Mugabe expressed hope that Parliament would debate and finalise the three cyber law related Bills Zimbabwe has been working on since mid-2013.

Since then, developments in Zimbabwe's cyber law and policy landscape have been fast-paced with the recent one being the creation of the Ministry of Cybersecurity, Mitigation and Threat Detection. At face value, such actions give the impression that the Zimbabwean government is taking serious measures to combat any potential cyber threats.

However, this article seeks to show that current efforts by the government to secure cyberspace really have nothing to do with promoting cybersecurity, but are more focused on protecting the interests of the State.

**Government's intentions**

Government efforts in combatting online criminal activity have resulted in the passing of the National ICT Policy, the National Cyber Security Policy (both in 2016), and the updating of the draft Cybercrimes and Cybersecurity Bill, which is currently in its third draft. On paper, these policies are aimed at fighting cybercrime in Zimbabwe in a manner which purports to promote the fundamental rights enshrined in the Constitution.

For example, the draft Cybercrime and Cybersecurity Bill's main focus is to consolidate cyber-related offences with due regard to the Constitution's Declaration of Rights as well as the public and national interest. Furthermore, the Cybersecurity Committee to be established when this draft Bill is gazetted into law, has a mandate to produce annual reports on how national cybersecurity initiatives/activities impact on fundamental rights such as the right to privacy and the right to freedom of expression.

However, as Zimbabwe inches closer to the 2018 general elections, a gap is emerging between the proposed cybersecurity policies and the government's actual intentions. One example of this discrepancy came in the wake of remarks by presidential spokesperson George Charamba in clarifying the role of the Ministry on 10 October 2017.

Charamba was quoted saying:
*"… ndiyo riva redu kubata makonzo aya anoita mischief using cyber space [it is the trap to catch mischievious mice …..This is coming against the background of the abuse that we saw not too far back on social media, where the social media then causes some kind of excitement to the country, not on the basis of fact, but generation of copy which is in fact calculated to trigger a sense of panic in the economy, and that in itself suggests that it is indeed a major threat to State security."*

Charamba also revealed how President Mugabe had drawn lessons on controlling cyberspace from countries such as Russia, China and "the Koreans." This is a chilling admission given the fact that these three nations are notorious for clamping down on online rights and freedoms, with China going as far as setting up its own parallel internet network from the rest of the global internet.

President Mugabe has since confirmed these remarks. While officially opening the Nkulumane Community Information Centre in Bulawayo on 4 November 2017 he said:

*"We have set up the Cyber Security Ministry to build our own cyber systems to defend ourselves from cybercrime. We are aware that there are some people who use the internet to fight us and implement what they say is regime change.*
*"This is not a first, actually some nations are at an advanced stage in controlling this social media, which is why we thought that Minister Chinamasa as a lawyer can help in controlling our cyber space."*

In revealing the dual purpose of the Ministry of Cybersecurity in preventing abuse of social media, and protecting the State's interests, there has been no reference to the actual cybercrimes or cybersecurity threats faced by Zimbabwe. Summarily, these remarks have escalated free expression on social media to a cybersecurity threat which government took seriously enough to warrant the creation of the responsible ministry.

A few weeks after the creation of the Ministry of Cybersecurity, President Mugabe made additional remarks which show the potentially restrictive nature this new ministry will play in the governance of Zimbabwe's cyberspace.

Furthermore, the draft Bill's long title pays homage to the protection and promotion of fundamental rights. However, some sections of the draft Bill actually infringe on the same fundamental rights. Section 17 of the draft Bill criminalises the publishing of false statements, a provision similar to that contained under Section 31 of the Criminal Law Codification and Reform Act. The constitutionality of Section 31 was challenged in 2015 in the Constitutional Court in the case involving AMH journalist, Nqaba Matshazi but the State was quick to drop the charge, a gesture that in itself was a tacit

acknowledgement of the fact that the provision might not be able to meet the objective test of constitutionality.

It is trite to note that in 2015, the Constitutional Court found that this crime was inconsistent with the freedom of expression guaranteed by Section 20 (1) of the former Constitution. Incorporating the same crime in the current draft Bill is tantamount to revival of this unconstitutional act under a different guise.

**social media**

Social media is an umbrella term which describes internet based instant messaging platforms such as *Facebook, Twitter, WhatsApp,* and *Instagram.* As the prices of Internet enabled smartphones have steadily dropped, more Zimbabweans are connecting to the Internet via these mobile devices. This is reflected in the quarterly reports published by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), in the past two years.

By mid-2016, an estimated 92% of Zimbabweans accessing the Internet did so through mobile devices. Popular social media services in Zimbabwe are *Facebook*, and *WhatsApp.* Recently, the number of Zimbabweans who actively use *Twitter* and *Instagram*, has also risen.

In a country with high voice-call rates, coupled with a political environment where freedom of association is sometimes restricted, social media has provided affordable and relatively safe platforms for Zimbabweans with similar interests to “meet-up” and share their views. This has significantly improved the flow and accessibility of information in the country.

Unfortunately some of the information shared by citizens also reflects on governance issues, including important issues such as management of the current economic crisis.

For example, towards the end of September 2017, Zimbabwe experienced sporadic price increases, which citizens documented and shared on social media. The statements released by government after that spell of price increases blamed inaccurate social media posts for causing panic buying which then led to opportunistic retailers hiking their retail prices.

It is apparent that government is convinced that social media was used to induce panic buying in a bid to discredit its efforts in rebuilding the economy. It is these same narratives that government uses as examples of the abuse of social media by Zimbabweans for their own political gains.

The arrest of United States citizen, currently working in Zimbabwe, Martha O'Donovan on Friday, 3 November 2017, is one that should be viewed in that context. Martha was arrested in connection with a tweet which allegedly insulted the person of the President.

Martha is charged under Section 33 (2) of the existing Criminal Law (Codification and Reform) Act [*Chapter 9:23*] which criminalises the making of statements which undermine the authority of the President.

Her arrest is the first one to be effected in connection with online statements since the creation of the Ministry of Cybersecurity. The same section has over the years been used to restrict offline freedom of expression. Martha's arrest does serve as a warning on how closely state authorities are now monitoring statements made through social media.

**Conclusion and predictions**

If past trends are anything to go by, there is high probability that the Cybercrimes and Cybersecurity Bill will be selectively applied through the various State institutions to persecute any dissenting voices on online spaces.

As mentioned in the first instalment of these commentary series, existing laws are being stretched beyond their intended purpose. The Cybercrimes and Cybersecurity Bill provides convenient cover for government to use in the persecution of online activists and their supporters. This is likely to increase in the run-up to the 2018 general elections.

**Key summary points**

- The Cybercrime and Cybersecurity Bill is part of government efforts to secure Zimbabwean cyberspace against cyber attacks.
- There is risk that this piece of legislation will be used to shut down online space, especially for online social movements and other dissenting voices, all in the name of “protecting national interests”.
- There is need to hold government accountable on the democratic principles of cybersecurity governance as contained in the Cybersecurity Bill and National Cybersecurity policies.

**End////**