An Evaluation of Cyber Crime and Cyber Security Bill of Zimbabwe

Farai Francisco Madyira, Ramson Munyaradzi Nyamukondiwa and Cuthbert Tendaupenyu
University of Zimbabwe School of Technology
University of Zimbabwe
Harare, Zimbabwe
madyiraff@gmail.com, fmadyira@uz.edu.zw, nyamukondiwar@schooloftech.uz.ac.zw, tendaupenyuc@schooloftech.uz.ac.zw

Abstract

The recent radical digitalization of our societies through internet and the use of computer systems, gave rise to new cyber-crimes or cyber-security threats. Cyber security has thus became a general concern for all, citizens, professionals, politicians, and, more generally, all decision makers. The Cyber Security Bill was introduced to criminalize offences against computers and network related crime; to consolidate the criminal law on computer crime and network crime; to provide for investigation and collection of evidence for computer and network related crime; to provide for the admission of electronic evidence for such offences and to provide for matters connected with or incidental to the foregoing. With the Cyber Crime and Cyber Security Bill on the cusp of being promulgated, prosecuting Cyber Criminals in Zimbabwe finally became effective. The focus of this paper is to discuss issues around the introduction of the Cyber Crime and Cyber Security Bill in Zimbabwe and the likely impact it will have on the investigation and prosecution of cybercrime. This is achieved through the analysis of global cybercrime and cyber security legislation trends; factors influencing the success of the bill in the investigation and prosecution of cybercrime in Zimbabwe as well as the advantages and disadvantages of the Bill in question.

Keywords (12 font)
Cyber-crime, cyber security, cyber security bill, radical digitalization, cyber criminals

1. INTRODUCTION

The recent past has witnessed the world becoming more progressively connected coupled with expeditious technological transformations. This phenomenon has set an environment which promotes expansive and diversified ways for cyber criminals to launch cyber assaults. As a result, many expansive and complex attacks have been unleashed into the cyber world such as the ransomware WannaCry assault of May 2017 (Sherr, 2017) which crippled many computer systems, cyber terrorism, unlawful acquisition, interception and access of data, cyber bullying and harassment, transmission of data messages inciting violence and damage of property, cyber-fraud and extortion, and so on, thereby bringing the reality of cybercrime and cyber security to the world. This reinforced the need for national driven strategies aimed at regulating the cyberspace so as to identify and proactively contain the attacks of this magnitude through intercontinental strategies and partnerships. This can be achieved through the process of enacting laws that are related to cybercrime and cyber security (Sabillon, et al., 2016), improve cyber governance, and invest in computer security and cooperation among nations. Lastly, conclusion will be drawn.

2. GLOBAL CYBERCRIME AND CYBER SECURITY LEGISLATION TRENDS

The global trends on legislation with regards to cybercrime and cyber security indicate that most nations have national cyber security strategies and policies in place which they use to regulate the cyber environment. Top agenda issues has been in the establishment of legal framework for cyber security, improvements on user awareness and promotion of ICT educational programs, support for the creation of national CIRT/CSIRT and technical support for combating cyber threats. In the majority of the cases, there is the creation of joint partnerships amongst the governmental and private segments of the nation in order to control the transmission of data as well as the development of nationwide cyber space agencies, with the main thrust of coming up with mechanisms to handle the dangers of the cyber space as well as the enactment of laws that regulate cybercrime (Mendoza, 2017). These strategies and policies are constantly under review in order to cater for the changes that take place since technology constantly change as indicated by the modified frequent occurrences of cyber incidences.

According to (Yedaly & Wright, 2016) only 11 out of 54 Review countries in Africa have substantive laws that regulate cyber-criminal activities with Zimbabwe among the group of 54. It is a disappointing phenomenon however it is encouraging to note that there are efforts in some of the African countries to institute reforms with regards to cybercrime and cyber security laws and Zimbabwe is one of them.

3. CYBERCRIME AND CYBER SECURITY BILL OF ZIMBABWE

Recently, Zimbabwe has experienced a sharp increase in the rate of cybercrime and cyber security raptures. This is attributable to the rapid growth in the usage of the Internet in comparison to other African nations. This has prompted the Zimbabwean government to take the stance of regulating the cyber space by promulgating the Cybercrime and Cyber Security legislation (Canny & Pillay, 2017). The cyber-crime bill was crafted in 2017 along the provisions of the draft ICT policy and the SADC computer and cyber-crime model law. The main objectives of the bill are as follows:

a) To provide a legal framework for the criminalisation of computer and network related offences.
b) To criminalize certain illegal content in line with regional and international best practices,
c) To provide the necessary specific procedural instruments for the investigation of such offences and define the liability of service providers (Pierce, 2017).

3.1 Benefits of Cybercrime and Cyber Security Bill

The promulgation of this bill enables Zimbabwe to solve the problem of cybercrime jurisdiction since some of the offenders reside in other nations as was with the case of WannaCry ransomware attack. The solution emanates from the bill's ability to ready Zimbabwe for collaboration and partnership with other countries within region, continent and the world at large (Segal, 2017).

In addition, the bill will be able to police crimes that are perpetrated in the cyber world. The regulation is required since some of the actions of cyberspace users require governing as witnessed in the cyber bulling case of a Durban teenage student. From this and other cases, it can be seen that it is imperative to have legislations such as those proposed in the bill which defines criminal activities with regards to cyberspace utilisation and impose stiff penalties for those obscene activities. These stiff penalties will act as a deterrence mechanism for both individuals and groups to commit cyber offenses (Khan, 2017).

Furthermore, the bill instils the sense of responsibility with regards to data protection and disclosure of breaches. The bill ensures that negligence is eliminated on the account of institutions who generate, store and transmit private data of individuals and organisations by exercising due diligence in all aspects of cyber security as failure attracts stiff penalties. This ensures that cyber security levels are improved to match global standards hence increased privacy protection and the ability to receive restitution when the need arises (Hogan Lovells, 2017).

3.2 Drawbacks of Cybercrime and Cyber Security Bill

One of the major concerns raised about the misgivings of this bill is invasion of privacy. It is feared that the bill will give the government excessive power as it can be able to control the freedom of speech and as well as the independence of the cyberspace. This entails that the government will be able to access information about anyone and there by controlling the activities of the cyberspace including those that are not criminal (ParlyReportSA, 2017).

In addition, enactment of cyber laws will not guarantee behavioural change. This can be evidenced by traffic laws in which offenders are always there even if the laws are in place. It can be noted that in most of the cases people who commit offenses are repeat offenders. Furthermore, the majority of the victims of cyber assaults are reluctant to report the incidences in order to protect their image in the eyes of their stakeholders as well as the perception that the cost of the investigation is greater than the loss incurred. This notion will hamper the effective investigation and prosecution of cybercrime (Solomon, et al., 2011).

3.3 Factors Influencing the Success of the Bill in the Investigation of Cybercrime in South Africa

According to (Pillay, 2017) the bill provides for the establishment of central points in every sector of the economy with the mandate of informing of any cybercrime occurrences. In this regard, the bill also creates other structures such as the Cyber Response Committee which are mandated to promote and enforce cyber security in South Africa (Canny & Pillay, 2017).

In addition, the bill empowers the state security agents which include the police to be able to enforce, investigate and prosecute cybercrimes. This is as a result of the requirement of organisations such as financial institutions, telecommunication service providers and banks to co-operate with these state agents in providing information and assistance required in prosecution and investigation (Hofmeyr, 2017).

4. CONCLUSION

It is the obligation of the government to ensure that its citizenry is secured in all aspects of security. One way of guaranteeing this is by proclaiming laws. The proclamation of legislation with regards to cyber security indicates the significance of putting into place extensive governing frame of reference. This has a positive impact of contributing to the contraction of security occurrences. It also improves and institutes an acceptable cyber security culture. In spite of all these dividends that such enactments may convey to the security of digital resources, the real world scenario is that there is the existence of a number of conflicts, positions and contradictions implying that the process of implementing these enactments is a mammoth task.

In this regard, the Cyber Crime and Cyber Security Bill being promulgated for the Republic of Zimbabwe will go a long way in supporting the investigation and prosecution of cybercrime as this sets a legal framework on which the cyber space can be regulated. It lays the foundation on what is expected of those who harbor sensitive digital data of individuals and business organizations thereby contributing towards increased cyber security. It also empowers the agents of the government concerned with investigations, monitoring and prosecution of cybercrime to carry out their duties effectively within the confines of the law and hence the reduction in cybercrime instances.

In addition, the bill allows for the creation of alliances with other nations as this helps in tackling cases where the perpetrator is not within the jurisdiction of the Republic of Zimbabwe laws. This

partnership although complicated will enable investigation and prosecution of perpetrators who reside beyond the borders of Zimbabwe.

REFERENCES

Canny and Pillay (2017) Cybercrime *and Cybersecurity Bill was tabled in Parliament on 21 February 2017*. [Online] Available at: https://www.lexology.com/library/detail.aspx?g=9a2a3dd6-b722-461e-895f-67459f808760 [Accessed 22 September 2017].

Hofmeyr (2017) *Cybercrime and Cybersecurity Bill (extension of date for comments).* [Online] Available at: https://www.lexology.com/library/detail.aspx?g=679aab75-81df-4ade-84aa-d7c1e55148b1 [Accessed 20 September 2017].

Lovells(2017) *The Cybercrime and Cybersecurity Bill and POPIA: Prioritising data protection.* [Online] Available at: https://www.hoganlovells.com/publications/the-cybercrime-and-cybersecurity-bill-and-popia [Accessed 26 September 2017].

Khan (2017) *Cybercrime Law in South Africa.* [Online] Available at: http://www.labourguide.co.za/most-recent/2178-cybercrime-law-in-south-africa [Accessed 25 September 2017].

Mendoza (2017) *Challenges and implications of cybersecurity legislation.* [Online] Available at: https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/ [Accessed 20 September 2017].

ParlyReportSA (2017) *Cybercrime and Cybersecurity Bill invokes suspicion.* [Online] Available at: http://parlyreportsa.co.za/communications/cybercrime-cybersecurity-bill-invokes-suspicion/ [Accessed 25 September 2017].

Pierce (2017) *Articles: The South African Cybercrimes & Cybersecurity Bill, 2017...Much Better!.* [Online] Available at: https://www.bdo.co.za/en-za/insights/2017/cyber/the-south-african-cybercrimes-and-cybersecurity-bill-2017-much-better [Accessed 20 September 2017].

Pillay (2017) The Cybercrime and Cybersecurity Bill and POPIA: Prioritising data protection. [Online] Available at: https://www.hoganlovells.com/publications/the-cybercrime-and-cybersecurity-bill-and-popia [Accessed 22 September 2017].

Sabillon et al (2016) *National Cyber Security Strategies: Global Trends in Cyberspace. International Journal of Computer Science and Software Engineering, May, 5(5), pp. 67-81*.

Segal (2017) *South Africa Introduces Revised Cybercrime Legislation, Acknowledging Criticism.* [Online] Available at: https://www.cfr.org/blog/south-africa-introduces-revised-cybercrime-legislation-acknowledging-criticism [Accessed 22 September 2017].

Sherr (2017) *WannaCry ransomware: Everything you need to know.* [Online] Available at: https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/ [Accessed 20 September 2017].

Solomon et al (2011) *Computer Forensics Jump Start. 2nd ed. Indiana: Wiley Publishing.*

Yedaly and Wright (2016) *Cyber Crime and Cyber Security: Trends in Africa, s.l.: Symantec.*

Biography / Biographies

Farai Francisco Madyira is an Engineering Instructor at the University of Zimbabwe specializing in Network Engineering. He has earned a Master of Business administration from University of Zimbabwe, Bachelor of Business Management and Information Technology from Catholic University of Zimbabwe, Certificate in Cyber Security and Certificate in Digital forensics both from University of Johannesburg and ITIL Foundation Certificate in IT Service Management. Currently, he is pursing PhD qualification in Engineering Management at the University of Johannesburg. He has also co-authored journal papers. His research interests include cloud computing, digital forensics, cyber security, ICT investments, systems thinking and IoT.

Ramson Munyaradzi Nyamukondiwa is a seconded Senior Research Scientist at Zimbabwe National Geospatial Agency (ZINGSA), lecturer of the University of Zimbabwe (UZ) and member of Zimbabwe Institute of Engineers (ZIE). He earned BSc in Electronics Engineering at the University of Tlemcen (Abou Bekr Belkaid) in Algeria, MEng Electronics Engineering from Chonbuk National University in South Korea. Currently, he is pursuing PhD studies in Space Engineering at Kyushu Institute of technology in Japan as the main engineer of the satellite (CubeSat) communication subsystem and subordinate member of the store and forward mission and antenna deployment mechanism. He has published a Journal, conference paper and posters. His research interests include space systems, software defined radios, big data and AI.

Cuthbert Tendaupenyu is a Lecturer in ICT who specializes in Network Engineering at the department of Electronics and Telecoms under the faculty of Computer Engineering Informatics and Communications. He is also the Managing Director at Fast Matters Technologies, a company that offers ICT consultancy services and technological solutions in Zimbabwe. He obtained his MSc in Electronic Engineering specialized in Networks, Telecoms, Computer Vision and Multimedia at the University of Science and Technology of Oran in Algeria. Engineer Tendaupenyu also earned a BSc in Electronic engineering specialized in Telecoms at the University of Science and Technology of Oran in Algeria. He is the Vice President of ZIMNOG, an organization that holds labs and training events both online and physically to help people in the field of ICT enhance their skills and knowledge to match up with current technological trends. He has written papers and co-authored in publications in the field of Information and Technology.