



Analysis of the Cybersecurity Threats in Botswana Using Publicly Available Data

Seth M. Sarefo, Botswana International University of Science and Technology, Botswana*

 <https://orcid.org/0000-0003-4789-6935>

Maurice E. Dawson, Illinois Institute of Technology, USA

Banyatsang Mphago, Botswana International University of Science and Technology, Botswana

 <https://orcid.org/0000-0002-9451-3119>

ABSTRACT

Online criminal and terrorist activities impact society at individual, organizational and national levels. This makes cybersecurity risk a society risk, one in which cyber-attacks affect the whole community. As such a government led cybersecurity response is important, where government, private entities, and individuals each have a part to play. In this study online discussions on cybersecurity in Botswana were analysed to assess the cybersecurity risks and activity in the country. A public cyber threats register is not available in Botswana and organizations do not benefit from shared knowledge on cybersecurity threats and their mitigations in the country. As such Open Source Intelligence data is used to analyse the threats in Botswana. This study concluded that Botswana could benefit more from nation-wide data publicized by the government as this will help support industries that are most affected.

KEYWORDS

Cyber-Attack, Cybercrime, Cybersecurity Strategies, Cybersecurity Threats, Cyberterrorism, National Cybersecurity, Open Source Intelligence, Vulnerabilities

INTRODUCTION

Botswana is one of Africa's most stable and peaceful democracies with a growing Gross Domestic Product (GDP) since independence in 1966. The country has an estimated population of 2,346,179 (Statistics Botswana, 2022) and a GDP of USD 20.36 billion (World Bank, 2022). Mining and quarrying are the major contributor to GDP followed by public administration & defense, wholesale & retail, and construction respectively (Statistics Botswana, 2023). As of 2023, the mobile penetration of Botswana was at 173% of the total population since one person can use multiple networks (Statista, 2024). Botswana as a model of democracy as well as a major diamond mining hub in Africa is threatened by the recent spike in criminal and terrorist activity on the internet (National Cyber Security Centre, 2020; African Union Commission, Symantec, 2016; Serianu Limited, 2018; Sarefo, Dawson,

DOI: 10.4018/IJICTRAME.344837

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

& Mphago, 2023). The ongoing cyber threat in Botswana has been displayed through social media manipulation, and attacks on essential services in nearby countries such as South Africa (Gallagher & Burkhardt, 2021). These services such as online banking, citizens of Botswana are dependent upon. In some cases, these attacks are enabled by outdated information technology systems where criminals can easily exploit vulnerabilities (Global Initiative Against Transnational Organized Crime, 2023). Financial-related cyber-attacks in the country include cryptocurrency attacks, social media impersonation of religious leaders to raise funds, and fake adverts that sell inexistent goods that defraud people of their money (Global Initiative Against Transnational Organized Crime, 2023).

Botswana is faced with a shortage of available workers in the field of cybersecurity and attracting foreign workers is still a problem (Serianu Limited, 2018; Maramwidze, Civil society in Botswana puts spotlight on cyber attacks, 2023). This is because Botswana has been mainly focused on investing in mining diamonds as this is the main contributor to GDP (World Bank, 2021). As such, in 2018 Botswana only had 250 professionals with certifications in the cybersecurity area (Serianu Limited, 2018). Implementing cybersecurity strategies at a national level is therefore still a priority. The ongoing Mozambican war which is linked to the Islamic State of Iraq and Syria (ISIS) is also a threat to cybersecurity in Botswana (British Broadcasting Corporation, 2021). With the ongoing geopolitical power wars, states also see the cyberspace as an opportunity to achieve such objectives using asymmetrical warfare tactics (Bradshaw, 2017). In this study, online (publicly available) statements from Information Technology (IT) professionals and government speeches are analyzed to investigate the national cybersecurity activity. The keywords “cybersecurity Botswana”, “cyber security Botswana”, “cyber Botswana”, “cyber risk Botswana” and “cyber threat Botswana” were used to search for such articles online. The terms “cyber” and “cyber security” were also replaced with “Information Technology”, “IT”, “computer” and “network” respectively, to broaden the search scope. The cybersecurity threat landscape is not well publicised in Botswana and IT professionals are reluctant to share threat landscape data. As such Open Source Intelligence (OSINT) data from popular cybersecurity providers is used in this study to investigate the threats in Botswana.

BACKGROUND

The rollout of Information Communications Technologies in Africa to compensate for inequalities and challenges faced by the continent has created an attractive environment for cyber threat agents (Gcaza, 2017; Pillay, 2017; Sutherland, 2018). In many instances, Africa has become the source of cyberattacks and it has at the same time become the target of cyberattacks (Kshetri, 2019). Losses due to cybercrime in Africa are estimated to be \$4 billion each year (Investment Monitor, 2022). Vulnerable systems and poor cybersecurity practices are the cause of the increasing cyberattacks on the continent (Kshetri, 2019). Other causes include a lack of cybersecurity expertise, insufficient legal provisions to combat cybercrime, and low priority placed on cybersecurity with many organizations investing very little of their budget towards cybersecurity (Sutherland, Digital privacy in Africa: cybersecurity, data protection & surveillance, 2018; Kshetri, 2019). At a national level some African countries like Botswana, Namibia, Zimbabwe, and Mozambique do not prioritize cybersecurity in their budgets (Renaud, 2018). However, the establishment of Computer Security Incident Response Teams (CSIRTs) by African countries indicates an awareness of cyber threats and the need for a multi-stakeholder model for a cybersecurity response (Pillay, 2017). Legislative frameworks for cybersecurity have also been established in Southern Africa with the help of the Southern African Development Community (SADC) through its Computer Crime and Cyber Crime Model Laws (Pillay, 2017).

Mauritius has been at the forefront, leading most African countries in adopting regional and international policies (Turianskyi, 2020). These policies include passing laws on cybercrime and data privacy, a data privacy regulator, and a public-private partnership for raising awareness of cyber risks (Turianskyi, 2020). In Kenya, a data protection bill for protecting the localization of data has been passed and payment service providers are required to submit their cybersecurity policies

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/analysis-of-the-cybersecurity-threats-in-botswana-using-publicly-available-data/344837

Related Content

Instructional Design and Technology Implications for Indigenous Knowledge: Africa's Introspective

Wanjira Kinuthia (2007). *Information Technology and Indigenous People* (pp. 105-116).

www.irma-international.org/chapter/instructional-design-technology-implications-indigenous/23540

Philosophers and the Press in the Collaborative Task of Demystifying Philosophy Through Increasing Public Awareness

Christiana Danjuma (2022). *Handbook of Research on Connecting Philosophy, Media, and Development in Developing Countries* (pp. 13-25).

www.irma-international.org/chapter/philosophers-and-the-press-in-the-collaborative-task-of-demystifying-philosophy-through-increasing-public-awareness/304258

Entrepreneurship Policy Framework: Understanding Cultural and Educational Determinants for Entrepreneurship

Raghubir Singh Chauhan and Rituparna Das (2017). *Global Perspectives on Development Administration and Cultural Change* (pp. 95-139).

www.irma-international.org/chapter/entrepreneurship-policy-framework/164744

Policy as a Bridge across the Global Digital Divide

Meena Chary and Stephen K. Aikins (2010). *Handbook of Research on Overcoming Digital Divides: Constructing an Equitable and Competitive Information Society* (pp. 40-56).

www.irma-international.org/chapter/policy-bridge-across-global-digital/38310

The Accessibility and Problems Associated with the Use of Information and Communication Technologies (ICTs) by Fish Farmers in Rural Areas of Ondo State, Nigeria

J. B. Ogunremi and P. Abraham (2012). *International Journal of ICT Research and Development in Africa* (pp. 45-52).

www.irma-international.org/article/the-accessibility-and-problems-associated-with-the-use-of-information-and-communication-technologies-icts-by-fish-farmers-in-rural-areas-of-ondo-state-nigeria/84485