



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

to the government (Kshetri, 2019). Ghana has also issued a Cyber Security Directive for Financial Institutions, which requires the involvement of executive officials in cybersecurity initiatives, as well as the appointment of a Cyber and Information Security Officer (CISO) in all banks to advise senior management and formulate cybersecurity strategies (Kshetri, 2019). Nigeria also announced the development of a risk-based cybersecurity framework for banks and financial institutions (Kshetri, 2019). South Africa strengthened its law enforcement agencies (Kshetri, 2019) and has made the reporting of cybercrime incidents mandatory (Sutherland, 2017).

These cybersecurity efforts have been met with challenges and limitations in setting up telecoms regulatory authorities, data privacy authorities, and the development of cybersecurity centers for the collection of data on attacks and strategies (Sutherland, 2018). However, African countries have invested more in surveillance technologies than in cybersecurity initiatives. This is evidenced by the procurement of spying equipment and systems such as the International Mobile Subscriber Identity (IMSI) catcher, NSO Group's Pegasus, and the collection of customer data from telecom operators (Sutherland, Digital privacy in Africa: cybersecurity, data protection & surveillance, 2018; Jili, 2010; Roberts, Mohamed Ali, Farahat, Oloyede, & Mutung'u, 2021). These procurements are done in countries where CSIRTs are under-resourced, insufficient, and lack cyber-attacks and defense registers. In neighboring South Africa, the information regulator is not fully operational, and the cyber warfare strategy has not yet been finalized due to poor inter-ministerial coordination (Sutherland, Governance of Cybersecurity – The Case of South Africa, 2017). Other issues are weak oversight structures (e.g., parliament struggles to analyze cyber-related legislation hence the limited oversight) as well as counterproductive secrecy (Sutherland, Governance of Cybersecurity – The Case of South Africa, 2017). Additionally, private firms are not forthcoming in reporting data breaches due to the potential financial losses that they may incur. Van Niekerk (2017) identified six types of cyber impacts due to cyber-attacks in South Africa and these were data exposure, denial of service (DoS), financial, website defacement, data corruption, and system penetration. Some of the data exposure attacks were categorized as Advanced Persistent Threats (APT) and were attributed to China and Russia, respectively (Van Niekerk, 2017). The attacker group Anonymous also attacked the South African Police Service, the African National Congress Party, and the state broadcaster (Van Niekerk, 2017). In Zimbabwe, the cybercrimes that were reported included phishing, credit card fraud, identity theft, unauthorized access, hacking, and telecommunications piracy (Kabanda, 2018).

CYBERSECURITY IN BOTSWANA

With the penetration of Information Communications Technology (ICT) in Botswana, the government saw the need to develop a National Cybersecurity Strategy (NCS). The NCS was a response to the weaknesses in the cybersecurity posture of the country which included a lack of cybersecurity experts in the country (Ministry of Transport and Communications, 2016). Botswana also did not have a coordinated framework for the various stakeholders to engage on cybersecurity issues (Ministry of Transport and Communications, 2016). However, the strategy is still at a high-level concept and needs to be further developed so that the engineers can implement security controls into their systems. Therefore the Botswana NCS which was first released in 2016, should be reviewed considering the changes in the threat landscape that have been brought by factors such as the coronavirus pandemic and the Mozambican war. This is because cybersecurity is constantly evolving and as such the cybersecurity framework should be continually updated, to essentially make it a living document (Dawson, Bacius, Gouveia, & Vassilakos, 2021).

The recent Presidential Directive 30(B)/2020 by the Masisi administration to approve the strategy (Parliament of Botswana, 2021) is a move that will lead to the implementation of cybersecurity measures in the country. This has consequently led to the establishment of the national Computer Incidence Response Team (CIRT) and the Digital Forensic Lab (Parliament of Botswana, 2021). With these recent developments, it is expected that Botswana will be better positioned to stop cyber

threats. The CIRT team, which was set up in 2019 is responsible for identifying threats, responding to threats, and managing them. However, the government has not been able to implement most of the programs in the NCS although it was in the national development plan for the period of April 2017 to March 2023 (Ministry of Finance, 2017). This can be due to the government focusing on the major contributors of GDP and improving the livelihoods of Botswana citizens. Cybersecurity and resilience guidelines for financial institutions have also been established by the Central Bank of Botswana (Bank of Botswana, 2023). These guidelines are based on industry best practices and have been developed to improve the cyber resilience posture of financial institutions that are set up through the Banking Act. Financial institutions are required to send self-assessment reports to the central bank as well as incident reports within 48 hours of occurrence.

ISIS Threat

The United States (US) military campaigns and its allies continue to have success against the extremist group ISIS. However, there are growing concerns over the ISIS propaganda that is being pushed through the internet and social media (Speckhard, Shajkovci, & Ahmet, 2016). The extremist group uses the internet and social media campaigns to direct and inspire its militant jihadi wannabes globally (Speckhard, Shajkovci, & Ahmet, 2016; Awan, 2017; Piazza & Guler, 2021). Recent research shows that ISIS has been successful at using online platforms and social media to radicalize recruits (Piazza & Guler, 2021). This is done through the use of viral professionally edited images and videos that are impressionable to the youth (Awan, 2017). For ISIS radicalization to take place there must be a pre-existing condition that is represented by distress such as an identity crisis or grievances (Mahood & Halim, 2016). Unemployment has been identified as one of those conditions that enable radicalization (Sardarnia & Safizadeh, 2019). With issues such as the high unemployment rate and idleness in Botswana, the youth may fall for the ISIS Caliphate. This can be done through online campaigns that are propagated through social media (Speckhard, Shajkovci, & Ahmet, 2016; Awan, 2017; Piazza & Guler, 2021). As an example, foreign recruits posing as tourists sometimes flow through countries such as Turkey to Syria where they join ISIS (Speckhard, Shajkovci, & Ahmet, 2016). Such recruits may later declare themselves dead and return to their countries without their original passports and continue to live there undetected, where further attacks may be launched (Speckhard, Shajkovci, & Ahmet, 2016). With the ongoing war in Mozambique, such a threat may exist in Botswana as well as the threat of home-grown terrorists.

Chinese Threat

Between 2018 and 2020 it was reported that the African Union (AU) headquarters were under espionage attack by the Chinese (Meservey, 2020; Reuters, 2020; Carrozza, 2018). However, African officials and China denied both claims (Meservey, 2020; Reuters, 2020; Carrozza, 2018). China and Chinese companies have built government buildings and donated computers in Africa. This has given it surveillance capabilities more than anywhere else since these companies are legally obligated to help the Chinese Communist Party (CCP) collect intelligence (Meservey, 2020). This gives China the ability to recruit intelligence and exert influence on the continent. Huawei also poses a threat to African states since the telecoms giant has built more than 70% of the 4G telecom networks in Africa, including military and police installations (Meservey, 2020). Plans are also underway to roll out 5G networks based on Huawei technology. The US House of Representatives has openly declared the Chinese telecom giants Huawei and ZTE as cyber threats to national telecoms infrastructure (McGuffin & Mitchell, 2014). With developed states such as the US, Germany, and Japan fearing that they cannot adequately protect against the Huawei threat, it is unlikely that Botswana can (Meservey, 2020). A recent study has also found out that cybersecurity is still underdeveloped in Botswana and its importance is undervalued (Vassilakos & Martin, 2023). With cybersecurity undervalued and the economic inducement of African leaders, Botswana may have accepted the risk posed by China and its companies and may even fear defying Beijing (Meservey, 2020). In Botswana, there are at least

two government buildings that were built by the Chinese government, and these include the Botswana High Court and Court of Appeal, and the Botswana Police Service Forensic Science Laboratory (Meservey, 2020). Botswana has also engaged Huawei to install over 500 cameras for its Safe City Project in Gaborone and Francistown which are the two biggest cities in the country. The project is used to fight crime by keeping streets and buildings safe and counter-terrorism (Xinhua Net, 2020). Huawei partnerships have also grown in Botswana to include different sectors of the economy such as telecommunications, mining, and higher education (BoFiNet, 2021; Xinhua, 2019; Mining Technology, 2023; Maramwidze, Huawei launches a skills transfer project in Botswana, 2023).

Analysis of Online Reports and Speeches

A few speeches where the Minister of Transport and Communications addressed the issue of cybersecurity were uncovered online. The first was delivered to the Committee of Supply and laid the foundation for discussions on the issue of cybersecurity from both the ruling and opposition political parties (Parliament of Botswana, 2021). The key cybersecurity strategies that were identified by the minister included cybersecurity professionals' recruitment and training, the national CIRT, and the delivery of the Digital Forensics Laboratory. The national CIRT coordinates the national cybersecurity response and sectoral CIRTs. Additionally, the ministry is collaborating with third parties such as the European Union Cyber Resilience for Development (EU Cyber-4-Dev) and E-Botho to develop cybersecurity laws and cybersecurity professionals' training respectively. Despite these initiatives, a Member of Parliament from the opposition party highlighted that these strategies have not been successful at mitigating social media manipulation and cyberbullying online as these criminals go unpunished. The Member of Parliament also highlighted that cybercrimes on social media, such as the use of fake accounts for impersonating others on Facebook, and cyberbullying are on the rise (Parliament of Botswana, 2021).

A statement on the Ministry of Transport and Communications official Facebook page showed remarks that were made by the Minister at a Virtual Cybersecurity Symposium, that was hosted by the Botswana International University of Science and Technology (BIUST) (Ministry of Transport and Communications, 2021). The Minister talked about the Smart Botswana Strategy which aims to promote digitalization of public services. Some of the government digital projects identified by the Minister included the development of the National Biometric Identity Card, the integration of government systems, online visa applications, and e-learning. The Minister also observed the impact of the Coronavirus pandemic on the ICT landscape citing contact tracing applications and other digital initiatives by the government. However, the downside, he observed, has also been increased cyber-attacks. In his speech, the minister also commended efforts by both private and public tertiary institutions for raising awareness of cybersecurity issues. Among other things, the Minister also touched on the issue of capacity building and the need for a multi-stakeholder cybersecurity response and emphasized the importance of academia in cybersecurity initiatives. The Ministry has demonstrated awareness of the cyber threats and has mentioned government efforts to mitigate against them. However, the Ministry has not been successful at providing empirical data on threats in the country.

Attacks on journalists have also been reported as increasing not only in Botswana but the world over (Mnyobe, 2021). This is not surprising since journalists sometimes carry out work that threatens those in positions of power. To protect journalists from cyber-attacks, one of the measures has been identified as teaching journalists hacking skills (Mnyobe, 2021). With deep fakes being used to lure journalists into publishing fake content, journalists should also use best practice approaches such as fact-checking before publishing. With a highly contested national election coming up in 2024, journalists and media houses in Botswana are at risk of these cyber-attacks. While Botswana needs to produce 1000 cyber professionals annually to combat cyber threats (Churu, 2019), about 20 – 30 new professionals join the market each year. It has also been reported that banks are not keen on reporting cybersecurity incidences for fear of losing customers. Another reason for silence on cyber-attacks by organizations is that some attacks are carried out by insiders and organizations feel embarrassed

to report about that. In another article, ASC Botswana (2021) predicted that the technological changes brought by the Corona pandemic such as remote work are here to stay. Hackers are already taking advantage of the weak security measures in home networks and systems, and these are being compromised to access organizations. The article identified ransomware as a dominating threat in the world of IT security (ACS Services Botswana, 2021). Cybercriminals have also used COVID-19-themed phishing tactics to lure victims. As such modernization of data protection is a critical factor for ensuring business continuity and countering ransomware (ACS Services Botswana, 2021). Cloud volume backup is another countermeasure to protect against unauthorized encryptions (locking) on data. Other recommended solutions include software-defined solutions and using an Air Gap (tape storage) to make backup inaccessible.

An online article by Botswana Guardian (2019) indicated that there was a national gathering for cybersecurity stakeholders in Botswana in the year 2019 where the progress on cybersecurity initiatives as well as the NCS was discussed. Based on the report, the Botswana Police Service (BPS) registered 143 cybercrime cases between 2015 and 2018. BPS is also faced with the challenge of a shortage of digital forensic examiners which limits the prosecution of criminals (Botswana Guardian, 2019). By 2018, 80% of the 30 certified practicing digital forensic examiners were employed by law enforcement agencies in Botswana (Botswana Guardian, 2019). This also means that there is a shortage of certified digital forensic investigators in the private sector and government. In addition to the shortage of cybersecurity professionals, a lack of cybersecurity integration in some of the local institutions has also been identified as one of the challenges in Botswana (The Patriot on Sunday, 2019). A cybersecurity company in Botswana, also indicated that the cybersecurity posture of Botswana is weak and indicated that a lot of damage was done during the 2019 election period (The Patriot on Sunday, 2019).

The Director of Public Prosecution (DPP) was interviewed at the Internet, Cyber Security, and Information Systems (ICISIS) conference (Goitsemodimo, Cybercrime activities real in Botswana - DPP Director, 2016). The DPP mentioned that cybercrime is a serious threat in Botswana and gave the example of an incident in which ICT was used to steal money from Central Medical Stores. For the solution part, the DPP talked about building technical capacity in ICT and establishment of legal frameworks. Still, in 2016, another article was published on cyberbullying and interviewed the Botswana Communications and Regulatory Authority (BOCRA) Deputy Director of Corporate Communications (Goitsemodimo, BOCRA intensifies awareness on cyberbullying, 2016). The Deputy Director stated that BOCRA always undertakes initiatives to raise awareness on the safe use of the internet. According to the report the regulator has some annual activities educating the public on cyberbullying. Table 1 shows a summary of the threats and mitigations identified from the web sources analyzed in this study.

Table 1. Threats and mitigations identified from online sources analyzed in this study

Threats	Mitigations
Ransomware	Cloud and offline backup (ACS Services Botswana, 2021)
Malware	Cybersecurity awareness (Goitsemodimo, BOCRA intensifies awareness on cyberbullying, 2016)
Cyberbullying	Cybersecurity awareness (Goitsemodimo, BOCRA intensifies awareness on cyberbullying, 2016)
Shortage of cybersecurity professionals	Professional training (Botswana Communications Regulatory Authority, 2021)
Cyber-attacks (and deep fakes) on journalists	Hacking skills training, cybersecurity awareness, and traditional fact-checking to protect against deep fakes (Mnyobe, 2021).

OSINT FINDINGS

An OSINT investigation was carried out between February and March 2024. Most of the data was obtained from Kaspersky (2024), However, some of the data was obtained from Imperva (2024) and Checkpoint (2024) but these sources were narrowed in terms of the data they provided. Data obtained on different days from Imperva (2024) showed that the only attack vector was an automated threat with attacks originating from countries such as Russia, China, and the Netherlands targeting the lifestyle industry. The occurrence of automated attacks however was very minimal. Kaspersky's "On Access Scan" averaged 4483 daily attacks during the month of February, while "On-Demand Scan" averaged 1405 daily attacks over the same period. On the other hand, "Botnet Activity Detection", and "Ransomware" statistics from Kaspersky showed very low numbers. On the global scale, Checkpoint (2024) regularly ranked the Education, Healthcare, and Government sectors as the top targeted industries worldwide with the highest rate of attacks.

Kaspersky revealed that for On-Access Scan, Trojans were the most common type of attack used to infiltrate systems and that most attacks targeted the Win32 platform. Some of the Trojans used AutoIt which has the capability to download and install other harmful programs and make changes to browser settings (Kaspersky, 2024). Trojans were also seen to use links to install malicious programs. Other Trojans detected have different capabilities categorized in the MITRE ATT&CK framework such as TA0001 Initial Access, TA0002 Execution, TA0003 Persistence, TA0004 Privilege Escalation, TA0005 Defense Evasion, TA0006 Credential Access, TA0007 Discovery, TA0008 Lateral Movement, TA0009 Collection, TA0010 Exfiltration, TA0011 Command and Control, and TA0040 Impact (Kaspersky, 2024; Mitre Corporation, 2024). Email worms were also detected and these can distribute themselves through malicious links or as an attachment to an email. The use of Trojans was also prevalent in web-based attacks as indicated by the Kaspersky Web Anti-virus. The presence of Trojan.PDF.Badur.gen which has the capability to booby-trap a Portable Document Format (PDF) file with malicious links indicated that some PDF files downloaded online were being used to lure users into clicking links that can install harmful programs to their systems. Other Trojans such as Trojan-Clicker.Script.Generic were also being used to perform illegitimate traffic redirection to malicious sites.

Intrusion Detection Scans also revealed attacks that targeted the Server Message Block (SMB), and Remote Desktop Protocol (RDP) in Windows. Bruteforce attack was being used to target RDP login/password pair (Kaspersky, 2024). A successful brute force attack would give the attacker remote access to the targeted host. The presence of Intrusion.Win.MS17-010 indicated that SMB-based attacks targeted a known vulnerability in the Windows operating systems known as EternalBlue (Kaspersky, 2024). This vulnerability allows the attacker to execute code with the highest level of permissions. Denial of Service (DoS) was also using the SYN (synchronize) flood attack by overloading the target server with SYN messages. Port scanning activity on both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) was also detected which could be used by adversaries as an initial step of an attack. However, port scanning can be used for both legitimate and illegitimate purposes to determine which ports are open. Other attacks target improperly configured applications such as command prompt in Windows.

Kaspersky Vulnerability Scan uncovered some exploits that target the Android operating system that may enable an attacker to gain access to the targeted system. Exploits that target HTTP service take advantage of vulnerabilities in some versions of Apache Struts 2. Other exploits detected targeted the vulnerabilities in Microsoft Office. The HEUR:Exploit.Linux.Enoket.a also showed the presence of exploits that target the Linux operating system. This exploit typically installs other malware in the system without the user's knowledge.

Mitigations

Trojans were commonly used to install other programs to further compromise the target and Windows was the most commonly targeted operating system. Some of the mitigations for these attacks are listed below.

Trojans and Other Malware

The best way to protect against malware is to use a defense-in-depth strategy. This can be done through four steps described as follows (National Cyber Security Center, 2021):

- Regular backups
- Prevent malware infection
- Prevent malware execution
- Prepare for an incident

Encrypted backups should be created using both cloud and offline solutions and these should be regularly tested for integrity and availability in case of an incidence of attack (Cybersecurity and Infrastructure Security Agency, 2024). Backup solutions should also be regularly patched to avoid attackers exploiting known vulnerabilities (National Cyber Security Center, 2021). Using multi-vendor cloud solutions will also help prevent vendor lockout (Cybersecurity and Infrastructure Security Agency, 2024). Malware prevention can be done by following the use of mail filtering, internet security gateways, and safe browsing (National Cyber Security Center, 2021). Preventative measures include enforcing malware preventative policies such as scanning devices from outside the organization, preventing the sending and receiving of executable files, and restricting the use of removable media (Souppaya & Scarfone, 2013). This measure should be applied together with staff awareness, vulnerability mitigation, threat mitigation, and defensive architecture. The use of device-level security such as AppLocker, the use of trusted stores, and ensuring that antivirus definitions are some of the measures that will prevent malware from being executed. In the eventuality that malware has already infected devices, incident response steps should be executed (Cybersecurity and Infrastructure Security Agency, 2024). These steps should be defined in advance in an incidence response plan.

SMB, RDP, and Brute Force Attacks

By applying the patch fix for the vulnerability in SMB protocol, users should be protected from EternalBlue exploit. However, since the fix requires for it to be installed in many Windows versions it has not been possible for many users to fix this vulnerability worldwide (Avast, 2024). Unpatched versions of RDP provide vulnerabilities that adversaries take advantage of to install malware and gain control of remote hosts (National Security Agency, 2019). To mitigate these kinds of exploits patching and upgrading Windows can help as well as using supported versions. Other measures include blocking port 3389 which is associated with RDP and using a custom port as well as disabling RDP when not in use (National Cyber Security Center, 2021; National Security Agency, 2019). Other measures include enabling multifactor authentication (e.g. enabling network-level authentication). Multifactor authentication will also protect against brute force which is commonly used to attack RDP. In addition to this, account lockout policy should also be implemented. However, account lockout alone is not effective against a well-resourced adversary. As such multiple countermeasures should be used including device cookies and using CAPTCHAS (The OWASP Foundation, 2024). Other exploits that target other operating systems and application software can also be mitigated by patching and updating software to the latest version.

SYN Flood Attack

SYN flood attacks have been around for a long time and a number of mitigations developed against this type of attack include increasing backlog queue of half-open TCP connections, recycling the

oldest half-open TCP connection, the use of SYN cookies, and deploying firewalls and proxies (Imperva, 2024; CloudFlare, 2024).

RECOMMENDATIONS

This study found that the government engages different stakeholders on cybersecurity issues in Botswana. However, the discussions are still at a preliminary stage and the cybersecurity activity of the government is not well publicized. As such for these discussions to reach an advanced stage, public reports by the government should include strategies on how the government protects different sectors of the economy. These strategies should also include strategies for protecting key national processes such as the national elections and democracy from cyber-attacks. The OSINT investigation also revealed some vulnerabilities and attacks that are prevalent in Botswana. Publication of empirical data on threats by the national CIRT can reveal which sectors of the economy are mostly affected and will enable security engineers to better protect their systems.

CONCLUSION

This work analyzed the cybersecurity discussions publicly available in Botswana. The articles analyzed in this study discussed cyber threats at a high level without mentioning the damage done by cyber-attacks in Botswana since there is limited government information on cyber threats and their mitigations. The mitigations mentioned in the articles mostly included cybersecurity awareness and professional training. While the government is aware of the cybersecurity threats in the country, a focus on improving the livelihoods of Botswana may have resulted in limited investments in cybersecurity initiatives. In recent years, however, the government has made efforts to stop cyber threats through the establishment of the national CIRT team and the Digital Forensics Lab. This is a commendable step as this study has revealed through the OSINT investigation that Botswana is under constant pressure from cyber-attacks. However, the activity of the government to stop cyber threats is not well publicized. As such limited information on cybersecurity may slow down national coordinated cybersecurity efforts. While AI is used by the police in the Safe City Project to improve processes in stopping crime, it is not clear whether those responsible for these AI systems have been resourced on how to defend themselves from cyber-attacks. It is therefore important to improve the publication of empirical data on cyber threats in the country by the government.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

FUNDING STATEMENT

No funding was received for this work.

FUNDING

No funding was received for this work.

CORRESPONDING AUTHOR

Correspondence should be addressed to Seth Sarefo (Botswana, 202207468@ub.ac.bw)

REFERENCES

- ACS Services Botswana. (2021, February 11). *Counter ransomware attacks with HPE data protection solutions*. (ACS Services Botswana) Retrieved July 20, 2021, from ASC Botswana: <https://acs.co.bw/2021/02/11/ransomware-attacks/>
- African Union Commission. (2016). *Symantec. Cyber Crime & Cyber Security Trends in Africa*.
- Avast. (2024). *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* Retrieved from Avast Website: <https://www.avast.com/c-eternalblue>
- Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, 138–149.
- Bank of Botswana. (2023). *Guidelines on Cybersecurity and Resilience*. Bank of Botswana. Retrieved from Bank of Botswana.
- BoFiNet. (2021, 08 06). *BoFiNet in partnership with Huawei Botswana donate ICT equipment and internet to Gaborone Secondary School*. Retrieved from BoFiNet Website: <https://www.bofinet.co.bw/news/article/bofinet-in-partnership-with-huawei-botswana-donate-ict-equipment-and-internet-to-gaborone-secondary-school>
- Botswana Communications Regulatory Authority. (2021, June 24). *Draft Guidelines on Electronic Mail (E-mail) Security*. Retrieved June 24, 2021, from Botswana Communications Regulatory Authority: <http://www.bocra.co.bw>
- Botswana Guardian. (2019, January). *Cyber security stakeholders introspect*. (Botswana Guardian) Retrieved July 20, 2021, from www.botswanaguardian.co.bw/news/item/3945-cyber-security-stakeholders-introspect.html
- Bradshaw, S. (2017). *Global Commission on Internet Governance*. Center for International Governance Innovation.
- British Broadcasting Corporation. (2021, August 6). *Mozambique insurgency: Rwanda leads the fightback*. (BBC) Retrieved August 28, 2021, from British Broadcasting Corporation Website: <https://www.bbc.com/news/world-africa-58079510>
- Carrozza, I. (2018). China's African Union Diplomacy: Challenges and Prospects for the Future. *LSE Global South Unit Policy Brief Series*, (2), 1–8.
- Check Point Software Technologies LTD. (2020). *Cyber Security Report*.
- Checkpoint. (2024, March 1). *Live Cyber Threat Map*. Retrieved from Checkpoint Website: <https://threatmap.checkpoint.com/>
- Churu, J. (2019, October 7). *Cyber security professionals: Botswana's headache*. (BizTech Africa) Retrieved July 19, 2021, from <https://www.biztechafrika.com/article/cyber-security-professionals-botswana-headache/15072/>
- CloudFlare. (2024). Retrieved from CloudFlare Website: <https://www.cloudflare.com/en-gb/learning/ddos/syn-flood-ddos-attack/>
- Cybersecurity and Infrastructure Security Agency. (2024, April 4). *Stop Ransomware Guide*. Retrieved from Cybersecurity and Infrastructure Security Agency Website: <https://www.cisa.gov/stopransomware/ransomware-guide>
- Dawson, M., Bacias, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*, XXVI(1).
- Gallagher, R., & Burkhardt, P. (2021, July 29). *'Death Kitty' Ransomware Linked to South African Port Attack*. (Bloomberg) Retrieved August 31, 2021, from <https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports>
- Gcaza, N., & von Solms, R. (2017). A Strategy for A Cybersecurity Culture: A South African Perspective. *The Electronic Journal on Information Systems in Developing Countries*, 80(6), 1–17. doi:10.1002/j.1681-4835.2017.tb00590.x
- Global Initiative Against Transnational Organized Crime. (2023). *Global Organized Crime Index Botswana*. Global Initiative Against Transnational Organized Crime.

- Goitsemodimo, K. (2016, November 4). *BOCRA intensifies awareness on cyber-bullying*. (Mmegi) Retrieved July 19, 2021, from <https://www.mmegi.bw/index.php?aid=64387&dir=2016/november/04>
- Goitsemodimo, K. (2016, May 20). *Cyber crime activities real in Botswana - DPP Director*. (Mmegi) Retrieved July 19, 2021, from <https://www.mmegi.bw/index.php?aid=60139&dir=2016/may/20>
- Imperva. (2024, February 29). *Cyber Threat Attack Map*. Retrieved from Imperva Website: <https://www.imperva.com/cyber-threat-attack-map/>
- Imperva. (2024). *TCP SYN Flood*. Retrieved from Imperva Website: <https://www.imperva.com/learn/ddos/syn-flood/>
- Investment Monitor. (2022, June 16). *Africa faces huge cybercrime threat as the pace of digitalisation increases*. Retrieved from Investment Monitor Website: <https://www.investmentmonitor.ai/features/africa-cyber-crime-threat-digitalisation/#:~:text=Cybercrime%20is%20estimated%20to%20cost%20Africa%20%244bn%20a,%24570m%20a%20year%2C%20Nigeria%20%24500m%20and%20Kenya%20%2436m>
- Jili, B. (2010, December 11). *The Spread of Surveillance Technology in Africa Stirs Security Concerns*. (Africa Center for Security Studies) Retrieved November 27, 2021, from <https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/>
- Kabanda, G. (2018). A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organisations. *Asian Journal of Management [AJMECS]. Engineering & Computer Sciences*, 3(4), 17–34.
- Kaspersky. (2024, March 1). *Cyber Threat Real-Time Map*. Retrieved from Kaspersky Website: <https://cybermap.kaspersky.com/stats#country=138&type=OAS&period=m>
- Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, 22q(2), 77–81. doi:10.1080/1097198X.2019.1603527
- Mahood, S., & Halim, R. (2016). Islamist narratives in ISIS recruitment propaganda. *Journal of International Communication*, ●●●, 15–35.
- Maramwidze, A. (2023, May 30). *Civil society in Botswana puts spotlight on cyber attacks*. Retrieved from ITWeb: <https://itweb.africa/content/mYZRXv9g8QZMOgA8>
- Maramwidze, A. (2023, November 22). *Huawei launches a skills transfer project in Botswana*. Retrieved from ITWeb Website: <https://itweb.africa/content/Kjlyr7wBbpGvk6am>
- McGuffin, C., & Mitchell, P. (2014). On domains: Cyber and the practice of warfare. *International Journal (Toronto, Ont.)*, 69(3), 394–412. doi:10.1177/0020702014540618
- Meservey, J. (2020). Government Buildings in Africa Are a Likely Vector for Chinese Spying. *BACKGROUNDERS. The Heritage Foundation*, (3476), 1–23.
- Mining Technology. (2023, March 1). *Debswana partners with Huawei to launch 5G smart diamond mine project*. Retrieved from Mining Technology Website: <https://www.mining-technology.com/news/debswana-huawei-5g-diamond/?cf-view&cf-closed>
- Ministry of Finance. (2017). *National Development Plan II*. Government of Botswana.
- Ministry of Transport and Communications. (2016). *National Cybersecurity Strategy*. Government of Botswana.
- Ministry of Transport and Communications. (2021). *Ministry of Transport and Communications-Botswana Facebook Page*. (Ministry of Transport and Communications) Retrieved July 20, 2021, from <https://m.facebook.com/>
- Mitre Corporation. (2024, April 1). *Enterprise tactics*. Retrieved from Mitre Corporation Website: <https://attack.mitre.org/tactics/enterprise/>
- Mnyobe, L. (2021, June 24). *Latest News*. (Rhodes University) Retrieved July 19, 2021, from <https://www.ru.ac.za/latestnews/cybersecurityexpertswarnofcyberattacktargetedatjournalists.html>
- Nagar, D., & Paterson, M. (2013). *Peace and Security; SOUTH AFRICA IN SOUTHERN AFRICA*. Centre for Conflict Resolution.

National Cyber Security Center. (2021, September 9). *Mitigating malware and ransomware attacks*. Retrieved from National Cyber Security Center: <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

National Cyber Security Centre . (2020). *Annual Review 2020, Making the UK the safest place to live and work online*.

National Security Agency. (2019, June 4). *NSA Cybersecurity Advisory: Patch Remote Desktop Services on Legacy Versions of Windows*. Retrieved from National Security Agency Website: <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/>

Parliament of Botswana. (2021). *SECOND MEETING OF THE FIFTH SESSION OF THE ELEVENTH PARLIAMENT*. Gaborone: Prliament of Botswana.

Piazza, J. A., & Guler, A. (2021). The Online Caliphate: Internet Usage and ISIS Support in the Arab World. *Terrorism and Political Violence*, 33(6), 1256–1275. doi:10.1080/09546553.2019.1606801

Pillay, K. (2017). Guest Editor's Introduction: AJIC Focus Section on Cybersecurity. [AJIC]. *The African Journal of Information and Communication*, 20, 79–82.

Renaud, K. (2018, August 26). It's time for governments to help their citizens deal with cybersecurity. *The Conversation*.

Reuters. (2020, December 16). *Exclusive-Suspected Chinese hackers stole camera footage from African Union - memo*. (Reuters) Retrieved September 1, 2021, from <https://www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idINKBN28Q1DB>

Roberts, T., Mohamed Ali, A., Farahat, M., Oloyede, R., & Mutung'u, G. (2021). *Surveillance Law in Africa: a review of six countries, Senegal country report*. Institute of Development Studies. doi:10.19088/IDS.2021.059

Sardarnia, K., & Safizadeh, R. (2019). The Internet and Its Potentials for Networking and Identity Seeking: A Study on ISIS. *Terrorism and Political Violence*, 31(6), 1266–1283. doi:10.1080/09546553.2017.1341877

Sarefo, S., Dawson, M., & Mphago, B. (2023). An exploratory analysis of the cybersecurity threat landscape for Botswana. *Procedia Computer Science*, 219, 1012–1022. doi:10.1016/j.procs.2023.01.379

Serianu Limited. (2018). *Africa Cybersecurity Report - Botswana*. Serianu Limited.

Souppaya, M., & Scarfone, K. (2013). *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-83r1

Speckhard, A., Shajkovi, A. S., & Ahmet, Y. (2016). Defeating ISIS on the Battle Ground as well as in the Online Battle Space: Considerations of the “New Normal” and Available Online Weapons in the Struggle Ahead. *Journal of Strategic Security*, 9(4), 1–10. doi:10.5038/1944-0472.9.4.1560

Statista. (2024, February 26). *Dermographics & Use*. Retrieved from Statista Website: <https://www.statista.com/statistics/1155134/number-of-mobile-connections-botswana/#:~:text=As%20of%20the%20fourth%20quarter,person%20can%20use%20multiple%20networks>

Statistics Botswana. (2022, May 10). *2022 Population and Housing Census Preliminary Results V2*. Retrieved from Statistics Botswana: <https://www.statsbots.org/bw/sites/default/files/2022%20Population%20and%20Housing%20Census%20Preliminary%20Results.pdf>

Statistics Botswana. (2023). *Gross Domestic Product: First Quarter of 2023*. Statistics Botswana. Retrieved from StatsBots Website.

Sunday Standard. (2017, August 28). *Botswana is the cyber crime capital of Africa*. (Sunday Standard) Retrieved July 20, 2021, from Sunday Standard Website: <https://sundaystandard.info/botswana-is-the-cyber-capital-of-Africa>

Sutherland, E. (2017). Governance of Cybersecurity – The Case of South Africa. [AJIC]. *The African Journal of Information and Communication*, 20(20), 83–112. doi:10.23962/10539/23574

Sutherland, E. (2018). Digital privacy in Africa: cybersecurity, data protection & surveillance.

- The OWASP Foundation. (2024). *Blocking Brute Force Attacks*. Retrieved from OWASP Website: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
- The Patriot on Sunday. (2019, September 11). *Botswana: 'Botswana Has Huge Cyber Security Skills Gap*. (All Africa) Retrieved July 19, 2021, from <https://allafrica.com/stories/201909111000.html>
- Turianskyi, Y. (2020). *Africa and Europe: Cyber Governance Lessons*. South African Institute of International Affairs.
- Van Niekerk, B. Brett Van Niekerk. (2017). An analysis of cyber-incidents in South Africa. [AJIC]. *The African Journal of Information and Communication*, 20(20), 113–132. doi:10.23962/10539/23573
- Vassilakos, A., & Martin, R. (2023). A PHENOMENOLOGICAL STUDY OF THE LIVED EXPERIENCES OF IT AND CYBERSECURITY PROFESSIONALS IN BOTSWANA: INVESTIGATING THE PERCEIVED LEADERSHIP EFFECT ON SUPPLY CHAIN CYBERSECURITY. *Military Art and Science*, 179-191.
- World Bank. (2021, April 1). *The World Bank in Botswana*. (World Bank) Retrieved August 28, 2021, from <https://www.worldbank.org/en/country/botswana/overview#1>
- World Bank. (2022). *GDP (Current US\$)*. Retrieved from The World Bank.
- Xinhua. (2019, 11 08). *Huawei offers telecom equipment to Botswana university*. Retrieved from XinhuaNet: http://www.xinhuanet.com/english/2019-11/08/c_138539884.htm
- Xinhua Net. (2020, February 20). *Safe city project in Botswana's two major cities operational*. (Xinhua Net) Retrieved August 1, 2021, from http://www.xinhuanet.com/english/2020-02/20/c_138799621.htm

Seth Sarefo has an MSc in Computer Science from the Botswana International University of Science and Technology. For his Masters thesis, he conducted an exploratory investigation of the cybersecurity threat landscape for Botswana. Seth also holds a BSc (Hons) in Computer Systems Engineering from the University of Sunderland and has worked in government as an IT professional.

Maurice Dawson is an Assistant Professor of Information Technology and Management within the College of Computing at Illinois Institute of Technology. Additionally, he serves as Director and Distinguished Member of the Center for Cyber Security and Forensics Education (C2SAFE). Before joining academia, he was an engineering manager for unmanned air systems and senior program manager for rotary-wing aircraft. Dawson completed a postdoctoral study in Systems and Information Technology (IT) at University Fernando Pessoa. He has a Doctor of Computer Science from Colorado Technical University and a Doctor of Philosophy in Cyber Security from the Intelligent Systems Research Centre at London Metropolitan University. Dawson has recently received his fourth Fulbright Scholar Grant to teach and conduct research at the Botswana International University of Science and Technology. Additionally, he is the co-editor of Developing Next-Generation Countermeasures for Homeland Security Threat Prevention and New Threats and Countermeasures in Digital Crime and Cyber Terrorism, published by IGI Global in 2017, and 2015 respectively. The United States (US) Department of Defense (DoD) 8140 recognized him for the roles of Information Assurance Manager (IAM) Level II & III, Cyber Security Service Provider (CSSP) Manager, and Information Assurance Systems Architect and Engineer (IASAE) I & II. His research areas are cyber operations, software assurance, cyber strategy, and cyber-terrorism.

Mphago is a lecturer and a researcher of cyber security with Botswana International University of Science and Technology (Biust). He worked in the academic industry for over 14 years as a teaching assistant, demonstrator, teaching instructor and then lecturer. He received his BSc. (Computer Science) degree from the University of Botswana in 2006, MSc. (Information Security) degree from Lulea University of Technology (Sweden) in 2011, and Ph.D. (Computer Science) from Botswana International University of Science and Technology in 2020. His research interests include honeypots security, Web application security, networks and systems security, banking security, and security in IoT. He also finds fun in being engaged in systems and application penetration testing. In addition to his academic work, he also holds several cyber security professional certifications including CEH, OSCP and others.