Cybersecurity in Mozambique: Status and Challenges

Martina Jennifer Zucule de Barros[1] and Brett Van Niekerk[2]
[1]Universidade Pedagógica de Maputo, Maputo, Mozambique
[2]Durban University of Technology, KwaZulu-Natal, South Africa

martina.barros02@googlemail.com
brettvn@gmail.com

Abstract: Digital technologies became one of the most important components of societies day to day life. In Africa, they brought several benefits as well as challenges. For instance, the number of cyber-crimes and cyber-attacks are increasing. Yet, not all 54 African countries have implemented proper cybersecurity measures such as the adoption of national cybersecurity strategy, technical and organizational measures, development of cyber capacity and fostering national and engaging in regional and international cooperation. However, the adoption of these measures are vital and imperative. Mozambique is one of these countries where these measures are lacking. Therefore, the aim of this paper is to give an overview of the current state of cybersecurity in Mozambique considering all of the aspects mentioned above. Additionally, this paper also aims to present some best practices that Mozambique can adopt to improve and intensify its cybersecurity commitments. The proposed recommendations are based on internationally recognized frameworks and models developed by entities such as the European Union Agency for Cybersecurity (ENISA), International Telecommunication Union (ITU) and African Union (AU).

Keywords: cybersecurity, cyber- attacks, policy, standards, Mozambique

1. Introduction

Over the last years, developing countries, especially African countries have been experiencing a growth of their country's economy and social development due to their increasing reliance on the use of information and communications technologies (ICT) and cyberspace. These are considered as indispensable elements for governments, business and individuals and are viewed as crucial infrastructures of the 21st century. Despite all the benefits, they also bring several challenges. For instance, the number of cyber-attacks and cyber-crime is increasing globally. In Africa, Saeed and Osakwe (2021) state that many countries have been experiencing a rise of digital threats and malicious cyber activities for instance, sabotage of public infrastructure, national security breaches involving cyber-espionage and intelligence theft by militant groups, losses from digital fraud and illicit financial flows. Therefore, addressing these vulnerabilities requires a higher commitment to cybersecurity. This "requires enforceable policy safeguard, risk prevention and management approaches, along with technologies and infrastructure that can protect each country's cyber environment, as well as individual and corporate end-user assets" (Saeed & Osakwe, 2021). However, according to ITU's 2020 Global Cybersecurity Index (GCI) report, the level of African countries' commitments to cybersecurity remains low compared to other countries in other regions around the world (ITU, 2020).

In many African countries, cybersecurity is not viewed as a national priority as in developed countries. This is emphasized by Kshetri (2019) which states that in Africa, cybersecurity is considered to be a luxury and not a necessity. On the one hand, countries such as Mauritius and Tanzania stand out as regional leaders in cybersecurity. On the other hand, countries such as Mozambique, Lesotho and Madagascar continue to present lower levels of cybersecurity commitments (ITU, 2020). In Mozambique, cybersecurity has not yet been recognized by the government as a national priority. Only in 2021, the government of Mozambique approved the country's first national cybersecurity policy and the national cybersecurity strategy. Recently, the government of Mozambique officially published the policy (INTIC, 2021). Despite this there is no information regarding when the policy will come into effect i.e, will be implemented. In February 2022, a group of hackers attacked more than 30 web sites from the government of Mozambique.

According to the National Institute of Electronic Government (INAGE) despite the attacks, the problem was solved and no data breach was registered as well as loss of information. However, this was the first time that the country registered a cyber-attacks of this magnitude (Club of Mozambique, 2022). In the last three years, the Covid-19 pandemic has forced many people in developed as well as in developing countries to work remotely. This also contributed to an increasing number of cyber-attacks and has been considered as one of the world's biggest cybersecurity threats (Alawida et al., 2022). Therefore, this paper presents an overview of the cybersecurity environment in Mozambique. The paper addresses all issues related to the five pillars of the ITU global cybersecurity agenda (GCA). Frameworks such as the cybersecurity maturity model (CMM), the ITU global cybersecurity agenda (GCA) and the Cyber Readiness Index 2.0 were utilized to conduct this research. The rest

of this paper is organized as follows: Section 2 describes the cybersecurity environment in Mozambique. In section 3, an analysis of the state of cybersecurity is presented. The recommendations are outlined in section 4 and finally section 5 concludes the paper.

2. Cybersecurity environment in Mozambique

The ITU states that cybersecurity is built upon five strategic pillars such as: legal, technical, organizational measures, capacity development and international cooperation (ITU, 2017). These pillars measure countries' commitments to cybersecurity. Thus, this section discusses the state of these pillars in Mozambique.

2.1 Legal measures

In Mozambique, the government does not view cybersecurity as a critical issue. Indeed, only in 2016 the Mozambican government started to address issues related to cybersecurity with the development of the country's first national cybersecurity strategy draft. The process was conducted by the National Communications Institute of Mozambique (INCM) and supported by the ITU and Europe Union (EU). Also in 2016, the first national cybersecurity strategy draft was released. The document states that Mozambique aims to be "a nation with a safe, secure, and resilient cyberspace that enables a knowledge based and digital society economy" (INCM, 2016). However, this strategy has never come into effect.

In 2017, the Mozambican assembly approved the country's first Electronic Transaction Law (GovMZ, 2017). Also by 2017, the government of Mozambique designated the INTIC as the new entity to oversee all the cybersecurity issues at national level. In 2020, the country's first national cybersecurity policy and the national cybersecurity strategy were approved by the Mozambican government and in 2021, both documents were officially published (INTIC, 2021). Beyond that there is no other legislation or regulation related to cybersecurity. For instance, there is no specific regulation to deal with, data protection, cyber-terrorism, cyber-activism, cyber-espionage and cyber threats targeting national security. Furthermore, Mozambique does not have any mechanisms related to child online protection. In 2018, the Mozambican government ratified the AU convention on cybersecurity and data protection (Club of Mozambique, 2018). However, aspects related to cybersecurity and data protection are still not being incorporated in national laws. In addition, there is no awareness of cybersecurity standards and regulations in Mozambique.

2.2 Technical measures

In this pillar, Mozambique also lacks comprehensive plans. Despite this, institutions such as INGAE and the Mozambique research and education networks (MoRENET) have established their computer security incident response teams (CSIRTs). The CSRITs from INAGE covers the government institutions (INAGE, 2021) whereas the CSIRT from Mozambique research and education networks (MoRENET) covers the academic institutions i.e., public and private (MoRENET, n.d.). However, these centers need to be strengthened to be able to give appropriate responses. In 2021, the INAGE announced that the Mozambican government will establish an electronic platform to track cyberterrorists. The aim of this platform is to protect the websites of state institutions and other entities from cyber-attacks. According to INAGE, digital service providers and other operators of essential services should notify the Mozambican entities in charge of cybersecurity issues about cybersecurity incidents. (Club of Mozambique, 2021). It is also not clear if the country has effective cybersecurity monitoring measures to control its critical national information infrastructures. For instance, a study conducted by Vumo et al (2018), shows that several public and private websites in Mozambique do not follow basic security measures. The majority of them are not audited and many people responsible for managing them lack knowledge regarding the security aspects (Vumo et al., 2018).

2.3 Organizational measures

According to ITU, this pillar ensures that "cybersecurity is sustained at the highest level of the executive and assigning relevant roles and responsibilities to various national entities, and making them accountable for the national cybersecurity posture" (ITU, 2020). In Mozambique, the first entity overseeing national cybersecurity issues was the INCM (Symantec, 2016). However, in 2017, the government of Mozambique designated the INTIC as the new entity in the government responsible for overseeing all cybersecurity issues (INTIC, 2021). According to ENISA (2016), there are three types of governance structures to govern cybersecurity: centralized approach, decentralized approach and institutional cooperation with the private sector such as public-private partnerships. In Mozambique, it is not clear which structure is being implemented. On one hand, INTIC, INAGE, INCM and

MoRENET continue to work on issues related to cybersecurity independently. On the other hand, there is no clear cooperation among them.

2.4 Cybersecurity capacity development

This area is considered a crucial factor in cybersecurity. The ITU states that "securing the cyber domain through cybersecurity capacity building activities is key as it contributes to reducing issues such as digital divide and cyber risks" (ITU, 2020). In Mozambique there is a lack of plans and programs in this regard. A study conducted by Symantec (2016) states that there is a lack of awareness raising campaigns as well as development of digital literacy and skills among the public in Mozambique. Primary and secondary schools do not have e-safety programs promoting good practices. Nevertheless, the recent cybersecurity policy approved by the Mozambican government mentions cybersecurity capacity building, research and innovation as one of its key principles (INTIC, 2021). The Ministry of Science and Technology and Higher Education in Mozambique has neither developed nor launched a program or initiatives to encourage cybersecurity education and applied research at academic institutions as well as cybersecurity awareness in all parts of society. To date, the only available information related to the existence of courses related to cybersecurity is related to one private academic institution, the Higher Institute of Transport and Communications (ISUTC) which offers a course related to cybersecurity focusing on firewalls. This course is offered in partnership with the Palo Alto Networks Cybersecurity Academy (ISUTC, 2020).

2.5 Cooperation

In relation to international cooperation, it is not clear if the government of Mozambique considers cybersecurity as a top issue of its foreign policy or international negotiations. There is a lack of information related to the engagement of Mozambique in fostering international cooperation. However, international cooperation is viewed as an important factor in cybersecurity. According to ITU (2018), establishment of national and international cooperation is very important "to facilitate a constructive dialogue, developing trust and cooperation mechanisms, finding mutually acceptable solutions to common challenges, and creating a global culture of cybersecurity" (ITU, 2018). Despite this in 2018, the government of Mozambique ratified the AU convention on cybersecurity and data protection (Club of Mozambique, 2018). Recently, the government of Mozambique announced a partnership with Brazil to establish a national certification authority i.e., Mozambique Digital Certification System. According to the Ministry of Science and Technology and Higher Education this system will allow the integration of the public and private sector such as registration and identification systems of the members of the academic and scientific community in Mozambique through the use of emerging technologies for electronic identity (MCETS, 2022).

3. Findings and Discussion

The ITU states that cybersecurity is built upon five pillars such as: legal, technical, organizational measures, capacity building and international cooperation (ITU, 2017). From the analysis of the cybersecurity environment in Mozambique one can see that the country's cybersecurity commitments are still at its start-up stage. In 2017, Mozambique was classified as an initiating stage i.e., a country that has started to make commitments in cybersecurity and ranked one hundred and nine globally (ITU, 2017).

In 2018, the overall country commitments remained the same as in 2017 (ITU, 2018). Recently, the ITU published an updated version of its GCI, the 2020 ITU's GCI report. This report states that Mozambique presents two areas of relative strength: technical and legal measures (ITU, 2020). However, technical and legal measures present elements such as data protection regulation, critical infrastructure regulations, active CIRTs, regional cooperation and child online protection mechanisms. South Africas as well as Tanzania have enacted legislation related to cyber crime. To date, Mozambique has not enacted any of them. Furthermore there is no official information covering how the government of Mozambique will act to establish them. For instance, despite the existence of national CIRTs, there is a lack of information related to activities that are being carried out by these centers. Nevertheless, Hathaway et al (2015) state that "a well established national CSIRT provides reactive services above all else...the ability to respond to incidents by containing and mitigating incidents as they occur" (Hathaway et al., 2015).

In relation to national cybersecurity policy and strategy, the government of Mozambique approved in 2021, the country's first national cybersecurity policy and its implementation strategy. From the capacity building dimension, the score is low. There is no information related to the development of a national plan for growth

science and innovation in cybersecurity. In addition, there is a lack of investments in cybersecurity basic and applied research and development (R&D). In relation to cyber awareness initiatives there is also a lack of these initiatives. To date, there is no information related to the establishment, for instance, of a national campaign related to cybersecurity targeting the general public, business as well as the government. For instance, South Africa is one of the African countries participating in the Safer Internet Day (SID). SID is an awareness program from the EU which aims to make the internet safer, particularly for young people (Bada et al., 2018). Mozambique is one the countries in the sub-saharan which is still not participating in this campaign. The development of national cybersecurity industries is also lacking in Mozambique. As well as other developing countries, Mozambique heavily relies on the information technologies (IT) products developed by developed countries.

In relation to international cooperation, the government of Mozambique has not defined cybersecurity as a part of its foreign policy. Moreover, Mozambique is not participating in many international forums related to cybersecurity, for instance the Forum of Incident Response and Security Teams (FIRST), on the contrary to its neighboring countries such as South Africa, Zambia and Tanzania, Mozambique is not a member of this forum. Nevertheless, Mozambique is one of the few African countries who have ratified the AU convention on cyber security and personal data protection. Figure 1 below, shows the country's current score of cybersecurity commitments according to ITU's 2020 GCI report (ITU, 2020).

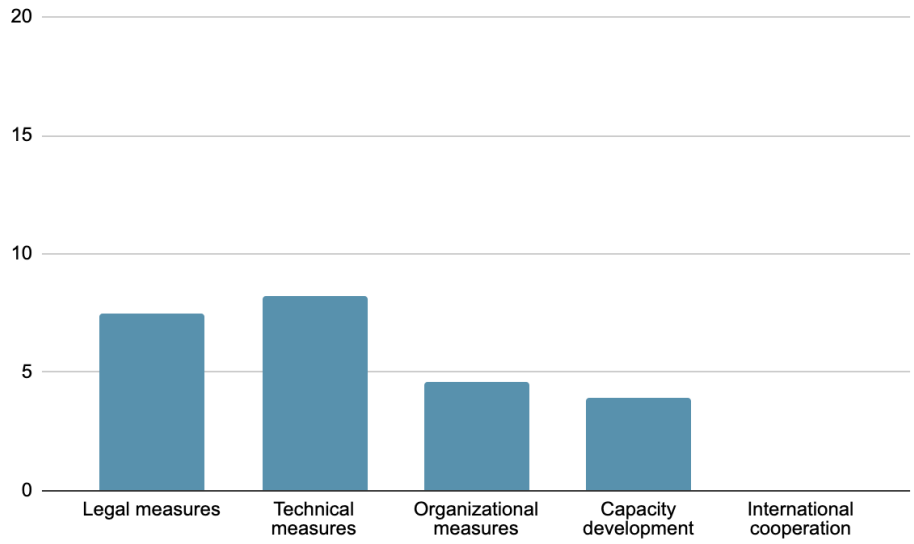

Figure 1: Mozambique's cybersecurity commitments level (ITU, 2020)

The score starts from 0 to 20 points (0.200) in each pillar. Thus, Mozambique's current overall score is 24.18 points. The GCI is the result of the total score of all five pillars and starting from 0 to 100 points. According to ITU, countries are ranked according to their final score. Therefore, Mozambique ranks 123 globally and regionally ranks 23 (ITU, 2020). On the other hand, the e-governance academy (eGA) states that Mozambique's national cybersecurity index (NCSI) is 9.09 points from (0 to 100 points) and ranks 151 globally. The NCSI "is a global live index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents" (e-GA, 2018). This index focuses on cybersecurity elements such as existing legislation, established units, cooperation formats and outcomes implemented by local governments.

4. Recommendations

After the analysis of the country current situation and based on our findings we proposed that, the government of Mozambique should:

- Enhance governmental coordination: Governments play a crucial role in managing cybersecurity issues. The ITU guide on developing a national cybersecurity strategy states that "cybersecurity should be promoted and sustained at the highest levels of government" (ITU, 2018). On the other hand, the recently published AU digital transformation strategy recommends member states to establish national cybersecurity governance structures involving actors such as policy makers,

technical, economic, educational and business communities, legal, law enforcement, military, academia and diplomacy (AU, 2020). Therefore, Mozambique should define cybersecurity as a national priority and improve its national governance structure.

- Implement a national cybersecurity strategy: Hathaway et al (2015) states that a national cybersecurity strategy should not only be articulated, it should also be actionable. Therefore, Mozambique should implement its recently approved national cybersecurity policy.
- Establish cyber response capabilities: The existence of national entities to exchange threat and vulnerability assessment and address operational cybersecurity challenges is very important (ITU, 2020). Moreover, cyber incident response capabilities play an important role in coordinating incident management at national level (ENISA, 2016). Therefore, Mozambique should establish national cyber incident response capabilities to oversee these issues.
- Strengthen public-private partnership (PPP): PPP plays a crucial role in cybersecurity efforts "from sharing actionable intelligence, exchanging good practice and communicating R&D needs and priorities" (ITU, 2020). Therefore, the government of Mozambique should establish effective partnership with other public and private entities.
- Invest in cybersecurity capacity building: The development of a stronger cybersecurity workforce is considered a crucial issue to decrease risks for business and society in general. According to ENISA (2016), increasing the level of skills and knowledge is an indispensable element in building society's resilience to cyberspace threats. Moreover, the AU digital transformation strategy recommends member states to conduct capacity building of policy makers and law enforcement to strengthen cybersecurity (AU, 2020). Thus, Mozambique should: i) develop a national plan covering cybersecurity across primary and secondary schools, ii) integrate cybersecurity courses in computer science, IT programmes and other related programmes, iii) develop dedicated undergraduate and graduate post-graduate programs in cybersecurity and iv) invest in research in cybersecurity.
- Implement awareness raising campaigns: Raising awareness is very important because "end users play a crucial role in ensuring the security of networks and information systems" (EU, 2013). Thus "they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them" (EU, 2013). South Africa has been carrying out several awareness initiatives developed by academic institutions as well as the public and private sector. The University of South Africa (UNISA) has developed a cyber awareness campaign to contribute towards the creation of a cybersecurity culture targeting school children. The University of Pretoria (UP) runs a project called PumaScope targeting rural schools, churches and orphan homes (Dlamini & Modise, 2012). Therefore, Mozambique should develop and implement national cybersecurity awareness campaigns targeting the general public, business and the government.
- Develop and align cybersecurity legislation and regulation: The need for strong and effective legislation for instance, to tackle cybercrime is crucial. The AU's digital strategy recommends the development and adoption of regulations and legislation related to personal data protection, cybercrime, cybersecurity standards and governance (AU, 2020). Mozambique should adopt or create laws in the area of cybercrime, child online protection and data protection. Moreover, Mozambique should intensify activities aimed at implementing standards related to cybersecurity.
- Engage in international cooperation: Cybersecurity plays a key role in many areas of international relations such as human rights, economic trade, security, stability, peace and conflict resolution, commerce and arms controls (ITU, 2018). Mozambique should develop and improve its national, regional and international cooperation to foster knowledge exchange and learning.

5. Conclusion

African economies as well as other economies around the world are facing increasing cyber-attacks. This underscores the need to strengthen cybersecurity measures as well as investment in human capital. However, in Africa, on the contrary to developed countries, many countries are still lagging behind. Therefore, this paper has examined the cybersecurity environment in a developing country, in the SADC region, Mozambique. Data was collected from international organizations such as the ITU - GCI, the e-GA - NCSI and the Symantec report on cyber crime and cyber security trends in Africa. The findings show that despite some efforts, cybersecurity is still a challenging process in Mozambique. To date, Mozambique still presents lower levels of cybersecurity commitments in almost all the five pillars of the GCA. However, with the upsurge of cyber-attacks, the need to adopt measures to deal with it became a priority. Therefore, the paper made some recommendations for the

government of Mozambique in order to improve the country's current scenario. With these recommendations we believe that Mozambique will gradually start making positive signs to improve its cybersecurity commitments. On the other hand, this can also help other African countries in the SADC region as well as in other regions on the continent.

References

Alawida, M., Omolara, A. E., Abiodun, O., & Al-Rajab, M. (2022, August 11). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *ScienceDirect*, (34), 8176-8206.

AU. (2020, May 18). *The Digital Transformation Strategy for Africa (2020-2030)*. Retrieved August 23, 2022, from https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

Bada, M., Von Soms, B., & Agrafiotis, I. (2018). Reviewing National Cybersecurity Awareness in Africa: An Empirical Study. *repository.cam*, 78-83. htpps://doi.org/10.17863/CAM.40856

Club of Mozambique. (2018, July 25). *Mozambican government approves resolution on cybersecurity*. Club of Mozambique. Retrieved October 06, 2022, from https://clubofmozambique.com/news/mozambican-government-approves-resolution-on-cybersecurity/

Club of Mozambique. (2022, February 21). *Mozambique: State portals are back online after cyberattack- Noticias*. Club of Mozambique. Retrieved September 19, 2022, from https://clubofmozambique.com/news/mozambique-state-portals-are-back-online-after-cyberattack-noticias-210067/

Dlamini, Z., & Modise, M. (2012). *Cyber Security Awareness Initiatives in South Africa: A Synergy Approach*. Proceedings of ICIW.

e-GA. (2018). *National Cyber Security Index*. https://ncsi.ega.ee.

ENISA. (2016, November 14). *NCSS Good Practice Guide*. Retrieved July 20, 2022, from https://www.enisa.europa.eu/publications/ncss-good-practice-guide

EU. (2013, February 07). *Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace*. EU. Retrieved August 24, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

GovMZ. (2017). *Lei de Transacoes Electronicas*. Retrieved September 19, 2022, from https://www.portaldogoverno.gov.mz/por/Media/Files/Lei-de-Transaccoes-Electronicas

Hathaway, M., Demchak, C., McArdle, J., & Spidalieri, F. (2015, November). *Cyber Readiness Index 2.0*. Retrieved August 15, 2022, from https://www.potomacinstitute.org/academic-centers/cyber-readiness-index

INAGE. (2021). *CSIRT GOV*. Retrieved September 19, 2022, from https://csirt.gov.mz/?page_id=3486#quem_somos

INCM. (2016). *1 Reuniao sobre Estrategia Nacional de Seguranca Cibernetica*. INCM. Retrieved September 19, 2022, from https://www.ciberseguranca.org.mz/

INTIC. (2021, September 1). *Governo aprova Politica e Estrategia Nacional de Seguranca Cibernetica*. INTIC. Retrieved September 19, 2022, from https://www.intic.gov.mz/?p=979

ISUTC. (2020). *Academia Palo Alto Networks do ISUTC*. Retrieved September 05, 2022, from https://www.isutc.ac.mz/wp-content/uploads/2020/11/Certificações-Academia-Palo-Alto_ISUTC_20.pdf

ITU. (2017). *Global Cybersecurity Index*. ITU. Retrieved August 08, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU. (2018). *Global Cybersecurity Index*. Retrieved August 10, 2018, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU. (2020). *Global Cybersecurity Index 2020*. ITU. Retrieved August 11, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology*. 10.1080/1097198X.2019.1603527

MCETS. (2022). *Mocambique trabalha na operacionalizacao do SIstema de Certiicacao Digital*. Retrieved September 20, 2022, from https://www.mctes.gov.mz/mocambique-trabalha-na-operacionalizacao-do-sistema-de-certificacao-digital/

MoRENET. (n.d.). *who we are*. Retrieved September 10, 2022, from https://csirt.morenet.ac.mz/en/who-we-are/

Saeed, M., & Osakwe, S. (2021, September 1). *Are African countries doing enough to ensure cybersecurity and Internet safety*. ITU. Retrieved October 06, 2022, from https://www.itu.int/hub/2021/09/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/

Symantec. (2016, November). *cyber Crime & Cyber Security Trends in Africa*. Retrieved June 28, 2022, from https://thegfce.org/initiatives/cybersecurity-and-cybercrime-trends-in-africa/

Vumo, A., Spillner, J., & Koepsell, S. (2018). Analysis of Mozambican websites: How do they protect their users? *IEEE*, 8. 10.1109/ISSA.2017.8251780