

Review of Namibia's National Cyber-security Strategy & Awareness Raising Plan 2022-2027

**A SUBMISSION BY THE NAMIBIA MEDIA TRUST
SEPTEMBER 2021**





Executive Summary

In September 2021, the Namibia Media Trust reviewed the Namibia National Cybersecurity Strategy & Awareness Raising Plan 2022-2027: A Step towards Cyber Resilience & Digital Security, which is currently being discussed in Namibia, for its compliance with regional and international human rights standards.

Our analysis shows that the strategy is well thought through and informed by some of the best models on the issue of cybersecurity. Its provisions are informed by critical core principles and clearly it is a product of a multi-stakeholder endeavour that brought together state agencies, academia, civil society and multilateral agencies like the World Bank, and Commonwealth Secretariat. The strategy is apparently modelled after relevant international standards. The six pillars are well defined and broad enough with attendant strategies.

However, at the general level, the strategy could benefit from some refining of the strategies under some of the pillars. It could also benefit from the finalisation of the implementation plan to ensure it has clear priorities, resources allocated (costing) and timeframes. The Monitoring and Evaluation Plan must equally be completed and the specific data to be collected periodically clearly stated.

Key among the specific changes we propose are that the Strategy:

- Must define or adopt a clear conceptualisation of cybersecurity
- Define the scope of the strategy
- Identify four strategic objectives that the strategy seeks to fulfill and develop the framework, pillars and the implementation plan around them
- Incorporate the centrality of a multi-stakeholder approach to cybersecurity and ensure that one of the objectives identified above addresses the issues of an ordinary Namibian.

We undertake an analysis of Part One and Part Two and suggest some of the specific recommendations that could be included to make the good strategy better.

1.0 Introduction

Cybercrime is a growing concern to countries at all levels of development, and affects both buyers and sellers. It affects both public and private sectors. It can unduly affect and compromise the growth potential of a country. This is because cybercrime can be highly volatile and massive in dysfunctional impact.

With improved connectivity that has resulted from mobile revolution and the increased capacity of the submarine fibre-optic cables connecting Africa in general and Namibia in particular to the cyberspace, the country must urgently have a trustworthy legislative, institutional, administrative framework to regulate activities conducted online.

As it expands its information, communication and technology sub-sector so does its risks to cybersecurity incidents grow. It is therefore prudent that a comprehensive strategy is developed, adopted and roll out without further delay.

Although no international standard on cybercrime exists some regional instruments in Africa and Europe are worth looking drawing lessons from. There are also models and guides on how to design a working and comprehensive cybersecurity programme and strategy. A good strategy lays out comprehensive legislative, technical, institutional and administrative measures necessary for its effective implementation.

According to UNCTAD, 39 member states of the African Union have comprehensive legislations. Namibia is one of the 12 countries with no legislation.

In January 2019 Namibia became a party to the African Union Convention on Cyber-Security and Data Protection (AU Cyber Security Convention/Malabo Convention), not yet in force.¹ The AU Convention stresses the importance of protecting of fundamental human rights including the right to privacy and data protection and the freedom of expression. In the same year, a draft Cybercrime Bill was developed. The ratification of the AU Cyber Security Convention and the development of a draft legislation come nearly six years after a draft Data Protection Bill was developed and nearly a decade after the overarching ICT policy was adopted.

1. The African Union Convention on Cyber Security and Personal Data Protection, adopted on Malabo, 27 June 2014. The Malabo Convention has not yet entered into force. It has been ratified by 8 states and signed by 14 countries.

2.0 Part One

Part One is quite elaborate and is organised in 13 subsections.

2.1 The Context

We first look at the first five subsections. The Introduction and the Background subsections provide some clear information on the status of the ICT sector.

The two subsections situate the Strategy under the Vision 2030 Plan and the Ministry of ICT Strategic Plan 2017-2022.

The background (subsection 2) and the methodology (subsection 3) redraws the steps taken by the government and other agencies to arrive at the current version of the strategy.

The Strategy also re-echoes the intention of the of the country to accede to the Council of Europe Cybercrime Convention (the Budapest Convention), ² but says nothing about the Malabo Convention which the country ratified in January 2019. It would be desirous for the Strategy to mention the Malabo Convention and how Namibia plans to show leadership in the realisation of its objectives.

While the background mentions in broad terms the current mobile subscribers and internet and 3G users, it does not specifically speak to the contribution of the ICT sector to the Namibian economy and what are the prospects in the next six years. It is our considered view, that such a mention would help in making a cost-benefit analysis and justify the subsequent investments.

The information and data on the current digital landscape is spread in three different subsections (the background, the current situation, and the digital landscape). Some of the information is equally dated. It refers to 2018. It must be updated with the current and latest data on the sector. Three of the subsections could easily just be titled the context.

Recommendations

- Include data on the real contribution of the ICT sector to the Namibian economy and if possible show how the sector is rated in relation to all other revenue earners for the country;
- Merge, update and reorganise data on the digital landscape (drawing from the background [2], the current situation [4], the digital landscape [5], and cyber threats and attack vectors [10]) so that it is not scattered over in different subsections; and
- Delete the current situation subsection as it is repetitive and redundant.

2. Namibia National Cybersecurity Strategy & Awareness Raising Plan 2022-2027: A Step towards Cyber Resilience & Digital Security, Page 10

2.2 High-Level Statement

The Strategy in subsection 6 provides for a vision, mission, strategic goal and guiding principles. It is our considered view that the vision and the mission could be recast so that they capture the intentions clearly. They should be formulated at a sufficiently high level and consider the dynamic nature of the digital environment.

For example, on the one hand, the vision “A secured cyberspace to enable an innovative Namibia and achievement of social and economic growth” could be stated as follows:

A secure Namibian cyberspace that fosters cutting-edge innovation and deployment of technologies for socio-economic growth.

On the other hand, the mission “Establish resilient infrastructure, legislations, and increase cybersecurity capabilities in Namibia” could be restated as “*Establish world-class counter cybercrime systems supported by progressive legislations and highly competent personnel in Namibia.*”

The strategic goal is intended to clearly capture what is to be accomplished. The Strategy just repeats the mission. Having reformulated it as above, we suggest that the Strategy introduces four strategic/ specific goals namely:

1. To effectively and efficiently tackle cybercrime and make Namibia one of the most secure places in Africa to do business;
2. Transforming Namibia to a more secure and resilient state to cyber attacks and better able to protect our interests in cyber space;
3. All Namibians are aware of cyber risks, secure their computers and take steps to protect sensitive personal data (identities, privacy and finances) online
4. Building Namibia’s cross-cutting knowledge, skills and capability to underpin all cybersecurity objectives.

The Namibia Media Trust welcomes that the guiding principles refer to governance, fundamental human rights and inclusivity. As such the guiding principles are well stated and all encompassing. We, however, think that there is clear need for it to refer to the fact that the strategy is for the whole Namibian ICT ecosystem. It is led by the government but it seeks to work with and for the private, public and non-state actors - thus, the whole society.

The protection and safeguarding of the fundamental human rights are best in the legal and regulatory framework (which is provided for under Pillar 3). However, there is need to mention other international and regional binding and soft law human rights instruments. These instruments reiterate the need to have access to a secure and affordable internet and also the issue of protection of personal data and the right to due process. They caution against cate blanche surveillance. They also highlight the need to protect women, marginalised and vulnerable groups of society.

Recommendations

- The strategy should in section 6.4, briefly mention specific regional human rights instruments like the African Charter on Human and People Rights, the African Declaration on Internet Rights and Freedoms ³ and the Declaration of Principles on Freedom of Expression and Access to Information,⁴
- The vision, mission and the strategic goals/objectives be reformulated as recommended above.

2.3 National cybersecurity strategy Framework and Strategic Pillars

The strategy has developed a clear framework that stands on six strong pillars. While the framework is clear, we fear that it may be over-ambitious and not realisable in a six-year period. This is because the development of the strategy has already taken over 3 years and the development of some the requisite legal framework has been under consideration for over 8 years.

Pillar 1: Privacy and Personal Data Protection

That the pillar seeks to focus on the review and finalisation of the Draft Data Protection Bill (2013) is welcome. Given that the adoption of the proposed law has taken inordinately long, we must prioritise it in the first two years of the strategy. Lack of such a comprehensive law continues to deter other countries from engaging in trade with Namibia especially on services that may require transfer of personal data.

Secondly, we note that the second strategy under this pillar is extremely generic and does not endear itself to periodic measurement. We make a few recommendations:

Recommendations

- All the strategies must be stated with a clear timeframe within which they must be accomplished.
- Develop a comprehensive policy on data protection for Namibia by June 2022;
- Adopt a progressive Data Protection law by October 2022;
- Establish a well-resourced and effective data protection commission or office of the data protection commissioner by December 2022.

3. African Declaration on Internet Rights and Freedoms, available at <file:///tmp/mozilla_henry0/African-Declaration-English-FINAL.pdf> Accessed on 5th Sept 2021.

4. Declaration of principles on Freedom of Expression and Access to Information, available at <file:///tmp/mozilla_henry0/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf> Accessed on 5th Sept 2021.

Pillar 2: Building National Capacity on Cybersecurity

This pillar rightly seeks to establish an agency responsible for detection, response and recovery (restoration) -the National Cybersecurity Incident Response Team. The team is to be charged with addressing operational cybersecurity challenges. This is to say the specialised team must be able to provide a set of both proactive and reactive functions, as well as preventive and educational services. It also speaks on the issue of enhancing skills and capacities. However, the explanation about the pillar does not clearly speak to the issue of building technical capabilities of respective government agencies to be able to fully understand that they be exposed to and develop requisite risk-management capabilities that enable them to manage them effectively. It also does not speak of the time frame within which each strategy shall be fulfilled.

We recommend that the strategies under this pillar include the following:

Recommendations

- All the strategies must be stated with a clear timeframe within which they must be accomplished. e.g. Establish a national cybersecurity Incident Response Team for Namibia by March 2022
- Build the technical capabilities of respective government agencies to be able to prevent, detect cyber threats and effectively respond to cyber attacks by June 2022;
- Establishing a scheme for certifying the competence of information assurance and cybersecurity professionals and certifying specialist training by September 2022.

Pillar 3: Enabling Legal Framework

The pillar underscores the centrality of having a robust cybercrime law and data protection law. However, the strategy does not elaborate on why the laws and what may constitute good cybercrime and data protection laws.

Recommendations

We recommend that the section be developed further to incorporate the suggestions below.

A progressive cybercrime law would serve six main functions namely:

1. Setting clear standards of behaviour for use of computer devices;
2. Deterring perpetrators and protecting citizens;
3. Enabling law enforcement investigations while protecting individual privacy;
4. Providing fair and effective criminal justice procedures;
5. Requiring minimum protection standards in areas such as data handling and retention; and
6. Enabling cooperation between countries in criminal matters involving cybercrime and electronic evidence.

Similarly, a progressive cybercrime law must criminalise acts against confidentiality, integrity and accessibility of computer systems.

A data protection law must also meet certain thresholds. Key among them is the entrenchment of fair data protection principles. These are:

1. Collection limitation principle
2. Data quality principle;
3. Purpose specification principle;
4. Use limitation principle;
5. Security safeguards principle;
6. Openness principle;
7. Individual participation principle; and
8. Accountability principle.

The above principles are drawn from the Malabo Convention and other relevant regional and international instruments.

Further, clear timelines for the adoption of the laws must be indicated.

Pillar 4: Cybersecurity Awareness

This pillar and the strategies are well stated. It covers initiative to conduct education and awareness raising activities to promote a culture of cyber security amongst all Namibian ICT users.

We would add that Namibians use ICT for a wide variety of purposes and at an ever-increasing rate. In order to ensure their personal and financial information and their identity and privacy is protected, it is essential that they maintain an awareness and an understanding of the cyber environment and its risks. We therefore recommend a few more strategies:

Recommendations

- All the strategies must be stated with a clear timeframe within which they must be accomplished.
- Establish a single authoritative website for cyber security information for Namibian home users and small business including those with cyber security knowledge and skills by June 2022. The website should have plain language alerts and advisories for the public including information on new cybersecurity risks and how to address them;
- Develop practical tools on issues like spam, bots and others that address growing problems of spam etc by December 2022
- Develop cyber security education modules for Namibian primary and secondary schools by June 2022. This strategy would equally add value to Pillar 2 above.

Pillar 5: National and International Collaboration

The framework under this pillar is well developed. To bolster it we recommend the following:

Recommendations

- Establish a functional command and control centre for cybersecurity by August 2020; and
- Broader engagement with the commercial internet industry, including working with industry on the development of a voluntary Internet Service Providers (ISP) Code of Practice to promote best practice approaches to deal with cybersecurity issues by December 2022.

Pillar 6: Critical National Infrastructure (CNI)

This section is well developed but could be refined further. For instance, the definition of critical national infrastructure.

Recommendations

- Review the definition of critical infrastructure to those physical facilities, assets, systems, supply chains, information and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the socio-economic well-being of the nation or affect Namibia's ability to ensure national security.
- Clearly define what may constitute critical infrastructure and critical National Information Infrastructure by April 2022,
- Broader engagement with the business industry via the Trusted Information Sharing Network for Critical Infrastructure Protection to promote integrated, best practice approaches to cybersecurity and critical infrastructure protection, including working with industry on the development of a voluntary Internet Service Providers (ISP) Code of Practice to promote best practice approaches to deal with cybersecurity issues by Sept 2022.

It is our considered view that subsections 9,10 and 11 are important but they ought not be included in the strategy. They should inform other sections of the Strategy in general and the implementation plan (subsection 12) in particular.

2.4 Notional Implementation Plan and Monitoring and Evaluation Plans and Costs

The subsections are incomplete. They must be fully completed. It is our considered view that the implementation plan must be organised around the four strategic objectives highlighted above and not the pillars as is the case now. Further, the implementation plan and the monitoring plan must have clear timeframes within which certain milestones will be gauged. It must have clarity of what are the short-term and long-term deliverables and how they will best be recorded and captured.

2.0 Part Two

The cybersecurity awareness raising campaign is well articulated.

The campaigns outputs are well elaborated on page 33. We must however note that the message and the audience both play a part in determining the medium. Certain communication media are inherently suitable for transmitting certain types of information of specified audiences.

While the Strategy clearly identifies school teens, out of school young adults and youth, parents and teachers as targets, ⁵ it does not mention who has the power to make the changes desired happen.

Further, while the broad categories may be seen to include most of the vulnerable members of the community it leaves out women -especially those 18-45, as a special group that may suffer disproportionate cyber-violence.

Further, the strategy does not clearly identify key allies and stakeholders. The action plan does spell out how to move parents and general public, children, employees and employers and what would constitute the key messages. But the strategy must of necessity equally target to reach policy-makers and leaders in both the public and private sector.

However, the Strategy misses out on how it will protect the drivers and ambassadors of the campaign from risks.

The Strategy could also speak of the different communication approaches and message choices that the campaign would deploy. For instance, messages choices can seek to make an emotional or rational appeal, it can be mass or individual, it can be positive or negative, it can be serious or humorous. But in a nutshell, a good message must be specific, accurate, simple, appealing, attractive, timely, clear and concise, action-oriented, appropriate to the channel selected, directed to designated audiences, and be compatible with social, physical, economic and emotional capacity of the audience.

In sum, the Strategy is a novel start for Namibia and when complete and implemented, it will ensure the cyberspace is secure and trustworthy to unleash the innovation prospects of the country

5. Ministry of ICT, Namibia National Cybersecurity Strategy & Awareness Raising Plan 2022-2027, pages 39-40

