C3SA

Cybersecurity Capacity Centre for Southern Africa

Southern African Development Community Cybersecurity Maturity Report 2021

A C3SA Report

Cybersecurity Capacity Centre for Southern Africa (C3SA)
School of IT, Department of Information System, University of Cape Town.
Leslie Commerce Building, Upper Campus.
Rondebosch, Cape Town, Western Cape 7701
South Africa
Tel: +27 (0)21 650 4345
Email: c3sa@uct.ac.za
Web: http://www.c3sa.uct.ac.za/

ISBN

978-1-991228-00-0	Southern African Development Community Cybersecurity Maturity Report 2021 (PRINT)
978-1-991228-01-7	Southern African Development Community Cybersecurity Maturity Report 2021 (PDF)

Citation: C3SA (2022) *Southern African Development Community Cybersecurity Maturity Report 2021.* C3SA

Rights and permissions

Southern African Development Community Cybersecurity Maturity Report 2021

A C3SA Report

Table of Contents

Abbreviations & Acronyms

ACP	African Caribbean Pacific
ARIPO	African Regional Intellectual Property Organisations
AU	African Union
BYOD	Bring Your Own Device
C(S)IRT	Computer (Security) Incident Response Team
C3SA	Cybersecurity Capacity Centre for Southern Africa
CERT	Computer Emergency Response Team
CERT-MU	Computer Emergency Response Team of Mauritius
CI	Critical Infrastructure
CMM	Cybersecurity Capacity Maturity Model for Nations
CTO	Commonwealth Telecommunications Organisation
DCI	Digital Civility Index
DRC	Democratic Republic of the Congo
ECTA	Electronic Communications and Transaction Act
EU	European Union
GCI	Global Cybersecurity Index
GCSCC	Global Cyber Security Capacity Centre
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GFCE	Global Forum on Cyber Expertise
HIPSSA	Harmonization of ICT Policies in Sub-Saharan Africa
ICT	Information and Communication Technology
INTIC	The National Institute of Information and Communication Technologies
ISO	International Standards Organisation
ITU	International Telecommunication Union
MACRA	Malawi Communications Regulatory Authority
NCSI	National Cybersecurity Index
NUPI	Norwegian Institute of International Affairs
POPIA	Protection of Personal Information Act
SADC	Southern African Development Community
SSA	Sub-Saharan Africa
UNESCO	The United Nations Educational, Scientific and Cultural Organisation
WIPO	World Intellectual Property Organisations
WTO	World Trade Organisations

Glossary of Terms

Capacity building	The process of developing and strengthening the skills, instincts, abilities, processes and resources that organisations and communities need to survive, adapt, and thrive in a fast-changing world.[1]
Civil society	An ecosystem of organised and organic social and cultural relations existing in the space between the state, business, and family, which builds on indigenous and external knowledge, values, traditions, and principles to foster collaboration and the achievement of specific goals by and among citizens and other stakeholders.[2]
Critical Infrastructure	Assets and systems that are vital for the functioning of a country's economy, public health and national security, such as energy, telecommunications, banking/finance and government services.
Cross-sector regulator	A supervisory body whose remit spans several sectors; examples include data protection and competition regulators whose scope of work spans multiple sectors.
Cybercrime / Digital Crime	An act that violates the law and: – is committed through digital means (such as online fraud, identity theft, phishing) or, – is specific to the internet, such as attacks against information systems or phishing (e.g., fake bank websites to solicit passwords enabling access to victims' bank accounts) or – involves illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.
Cyber defence	National security and defence capability and strategic and tactical operations designed to identify/detect, prevent, disrupt and respond to cyber threats and risks aimed at harming citizens, destroying state assets or coercing states.
Cyber-insurance	Insurance cover for losses and liabilities from a variety of cyber incidents, including data breaches, business interruption, and network damage.
Cybersecurity	The practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting online users; or interrupting normal business processes.[3]
Cybersecurity awareness raising, education and professional	Refer to a structure of resources (e.g., Infrastructure, finance, people, information, etc.), processes, and deliverables established to support activities of cybersecurity awareness raising, education, and professional training in a country.

[1] See United Nations. (n.d.). *Capacity-Building*. Retrieved November 11, 2021, from https://www.un.org/en/academic-impact/capacity-building

[2] See Centre for Strategic and International Studies. (2017, June 30). *Concept and Definition of Civil Society Sustainability*. Retrieved March 17, 2022, from https://www.csis.org/analysis/concept-and-definition-civil-society-sustainability

[3] See Cisco Systems. (2022). *What is Cybersecurity?* Retrieved March 15, 2022, from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

training framework	
Cybersecurity culture	Refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies.[4]
Cybersecurity marketplace	Commercial dealings and platforms for commercial dealings in cybersecurity technology, cyber-insurance products, cybersecurity services and expertise, and the security implications of outsourcing.
Cybersecurity mindset	Cybersecurity awareness and mindset encompass knowledge, attitudes, practices, and behaviour to safeguard information and critical assets.
Cybersecurity policy	Refers to a statement of intent that sets a system of standards and guidelines to guide cybersecurity decision making and implementation that achieves rational outcomes.
Cybersecurity regulator	A supervisory body whose responsibility is to ensure that regulated entities comply with minimum cybersecurity standards set for a sector or type of organisation.
Cybersecurity standards and best practices	Refers to a level of quality attainment in a cybersecurity product, service, or related activity recognised or promoted by a standardisation organisation or is widely accepted within an industry.
Cybersecurity strategy	Refers to a plan of action designed to achieve long-term and overarching cybersecurity goals for a country
Digital rights	Digital rights are an extension of the Universal Declaration of Human Rights applied to the cyberspace, and usually pertaining to freedom of expression and privacy. They include universal and equal access, freedom of expression, information and communication, privacy and data protection, right to anonymity, right to be forgotten, intellectual property, protection of minors, protection of all against sexism, racism, and xenophobia.
Maturity model	A set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline.[5]
Model law	A template of legislation from which different countries may develop a law such that it is harmonised across jurisdictions that adopt the template.
Private sector	The part of the economy constituted by entities that are privately owned and controlled by individuals and other private companies for profit.
Public sector	The part of the economy constituted by entities that are owned or controlled by government, funded by the public purse, and deliver public programs, goods, or services to citizens of a country.
Regulatory framework	Laws, rules, directives, guidelines and codes of conduct which a government puts in place to ensure consumer welfare or achieve specific public policy objectives.

[4] See The European Union Agency for Cybersecurity. (2017). *Cyber Security Culture in Organisations*. Retrieved March 7, 2022, from https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

[5] See Caralli, R., Knight, M. & Montgomery, A. (2012). *Maturity Models 101: A primer for applying maturity models to smart grid security, resilience, and interoperability*. (p.3). Retrieved November 11, 2021, from https://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf

Responsible disclosure	The practice of communicating security vulnerabilities in a manner that minimises potential risks that can result from a public disclosure.
Sector-specific regulator	A government body that supervises a specific are of economic activity, such as banking and finance, energy, transport, or telecommunications.
Security controls	Measures aimed at protecting the confidentiality, integrity, and availability of computer systems and the information they process according to defined security requirements, best practices, and standards.
Software quality	A standard for applications indicating the extent to which software functions as intended.

Institutional Messages

Foreword C3SA

As a pillar of cybersecurity research and capacity building in Africa, the aim of the Cybersecurity Capacity Centre for Southern Africa (C3SA) is to empower countries to develop cyber resilience. Its mission is to inform policy through cybersecurity research as well as to improve national cyber resilience across Africa through capacity building. C3SA provides a single-entry point for cybersecurity capacity building and research activities in Africa and is hosted by the University of Cape Town. C3SA is part of the global constellation of regional cybersecurity capacity research centres, which includes the Global Cyber Security Capacity Centre (GCSCC) and the Oceania Cyber Security Centre (OCSC). C3SA is a consortium between Research ICT Africa (RIA), the Department of Information Systems (DIS) at the University of Cape Town (UCT), the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, and the Norwegian Institute of International Affairs (NUPI). We are a partner of the Global Forum on Cyber Expertise (GFCE).

Our core activities include deploying the Cybersecurity Capacity Maturity Model for Nations (CMM), developing initiatives to improve cybersecurity capacity and conducting cybersecurity research in Africa. Along with CMM deployments, we strive to increase cybersecurity awareness in the region. Our strength is in our cybersecurity experts, researchers, and partners who share the overarching goal of helping nations with cyber resilience.

This regional study is the first one conducted by C3SA. The study seeks to assess the level of preparedness of SADC countries to respond to emerging cyber threats, and their level of resilience to a growing number of digitally mediated risks. The outbreak of the COVID-19 pandemic in early 2020 not only revealed that digital infrastructures are a lifeline, but also how vulnerable our societies are to new and emerging online threats. With the increasing reliance on digital connectivity for various aspects of our lives, our economies and societies came under threat from different fronts. Not only have digital attacks to network and IT systems compromised confidentiality, integrity, and accessibility of data, but it has become evident that cyber-attacks to critical infrastructures can interrupt supply chains of basic necessities, including food, electricity, medicines, or disrupt the functioning of hospitals during periods of crisis.

As our economies and societies are becoming increasingly dependent on digital connectivity, it becomes a priority for policy makers in our region to protect the critical infrastructures and information infrastructures undergirding our business, educational, and social activities. Therefore, cybersecurity capacity has become a top priority in the political agendas of all governments, including in the SADC region.

Dr. Enrico Calandro

Prof. Wallace Chigona

C3SA Directors

Foreword ITU

In the upcoming years and even decades, technologies will become ever more pervasive and continue to evolve, resulting in ICTs expanding in all areas of our lives.

This digital transformation is clearly perceptible in Africa as well. Digital technologies bring transformative changes across all sectors in Africa. As a result, building trust is a must to ensure a smooth transition towards sustainable digital socio-economic development. The urge for cybersecurity relates to more complexity and interdependency of systems, increased risks, and growing sophistication of threats.

Committing to cybersecurity capacity development and implementation has become a very high priority for those embarking on their digital transformation journey to ensure infrastructure and services we depend on are trusted, safe, secure, and resilient.

In the SADC region, the cybersecurity commitment of members has accelerated in parallel with their digitalisation. According to the latest Global Cybersecurity Index (GCI) released in 2020, SADC member states are improving their response to cybersecurity challenges, with a regional GCI score of 36.42, which certainly counts as a significant achievement. As cyber risks are in constant evolution, so should the security posture of all SADC members be.

Furthermore, the region needs to reinforce harmonisation in the level of cybersecurity maturity of its members. Considering the growing transnational interdependencies of digital infrastructure and services, having a good level of cybersecurity capacity in place is key to efficiently managing risks and building resilience, and the effort in this direction should continue, even more vigorously.

SADC and ITU work closely to improve cybersecurity readiness in the region through capacity building activities, during which countries from the region have demonstrated a strong commitment, adaptability, and determination to strengthen cooperation with relevant stakeholders.

This first study is setting the baseline and the level of maturity of SADC as a region and the included recommendations give indications to SADC secretariat of the priorities to embark towards a harmonized, scalable, and sustainable cybersecurity cooperation and collaboration in the region with an aim to create a safer cyberspace for all.

SADC's aim to go *"towards a common future",* states undoubtedly that the region wants to keep and strengthen its unity, but this unity also comes with a well-expressed interdependency. An incident in one country in the region can easily escalate or replicate its impact on the other countries due to strong regional and economic interdependencies. Clear cybersecurity strategies on national levels can set goals to create harmonised frameworks and set a minimum level of security required in countries and the region. When achieving that, SADC members will develop a common shield, equally strong and evenly forged, that can be implemented well and effectively protect all.

Furthermore, common regional guidance on cybersecurity strategies can target the regional specifics and set shared objectives that can have a long-term impact in terms of socio-economic development and growth benefits for the region.

Hence, an evolving cybersecurity maturity at the national level is required to address national specifics to meet the target cybersecurity maturity level. SADC member states should continue applying good practices with a view to improving the use of cybersecurity standards.

Integrating collaboration with the private sector, critical information infrastructure protection (CIIP) operators and civil society to develop frameworks or national policies addressing technical security monitoring is key to desired levels of protection in the region and to long-lasting partnerships for a sound and effective digital transformation.

Anne-Rachel INNE

ITU Regional Director for Africa

Acknowledgements

First and foremost, C3SA would like to thank the researchers who showed tremendous commitment and enthusiasm while conducting the research and interviews in selected SADC countries. We also thank our senior researchers at C3SA, Dr Karen Sowon, Dr Shallen Lusinga, and Dr Laban Bagui, who actively produced this research output in addition to coordinating the research project. We would like to thank also Ms Nthabiseng Pule for her active participation as a researcher as well as coordinator of the production of this study. In addition, we would like to thank the researchers from our partner organisations Dr Patricia Esteve-González from the Global Cyber Security Capacity Centre at the University of Oxford and Mr Erik Kursetgjerde and Ms Claudia Aanonsen from the Norwegian Institute of International Affairs for their support and research capacity. We would like also to thank members of the technical review board Professor Bassie Von Solms, Professor Michael Goldsmith, Dr Willan Dutton, Dr Jamie Saunders. We are also grateful to Ms Elizabeth Orembo and Mrs Carolin Weisser Harris from the University of Oxford and Dr Niels Niels Nagelhus Schia from the Norwegian Institute of International Affairs for their support in the production of the Report.

Moreover, we are grateful to the respondents from SADC countries who took time to respond to our questions. A special thanks goes to Mr Graig Rosewarne from Wolfpack Information Risk (Pty), and to Mr Adilson Gomes from Communications Regulatory Authority of Mozambique, and to Mr Blaise Azitemina from the Post, Telecommunications and ICT Ministry of the Democratic Republic of Congo.

Additionally, we are very grateful to our project partners, specifically the Mr. Orhan Osmani and Mr. Serge Valery Zongo from the ITU and Ms Ida Mboob from the World Bank for their inputs into the study, and Dr Ah-Thew from the SADC Secretariat to providing support in identifying stakeholders in SADC countries and in providing feedback and suggestions to strengthen the study.

Finally, we would like to express our appreciation for the funding received from our donors, The Norwegian Ministry of Foreign Affairs, who trusted us in carrying out this project.

C3SA is confident that the dissemination of this report will be invaluable in raising awareness of the need to improve cyber capacity at all levels and across all dimensions of the Cybersecurity Capacity Maturity Model for Nations. Further, C3SA is confident that these findings and recommendations from the report will contribute towards the design of cyber strategies and policies to make the digital environment safe for all SADC countries and their citizens.

Please contact C3SA at c3sa@uct.ac.za with any comments or inquiries in respect to this publication.

About this Report

Cybersecurity has become a priority area in the digital age. The need for well thought-out cybersecurity policies has become even more apparent in a post COVID-19 pandemic world, where the internet is considered a critical resource for almost all aspects of life. Users, organisations, and governments access and offer services and products online and more than ever before. For this reason, there is need to ensure that information and users are safe online. To contribute to having a digital space that promotes the well-being and prosperity of all, it is important for countries to understand their cyber risks, threat, and vulnerability landscape before they can improve on their capacity to deal with cybersecurity. While there are various national and regional reports examining the cybersecurity status of various territories, understandings of regional cybersecurity capacity landscapes are lacking Sub-Saharan Africa.

The goal of this study is to evaluate the cybersecurity status of countries in the Southern African Development Community (SADC), and determine the capacity maturity of the region in light of emerging vulnerabilities, threats, and risks. SADC is one of the least explored regions concerning cybersecurity capacity. The study used the Cybersecurity Capacity Maturity Model for Nations (CMM) as an analytical and a benchmarking tool by means of which to evaluate the status of cybersecurity maturity in the region. The granular assessment of the CMM allows for specific regional policy recommendations for the different dimensions of the model with the aim of informing countries, with empirical evidence to take the necessary steps to increase the scale and effectiveness of cybersecurity capacity-building initiatives.

This study used both published and unpublished previous CMM assessments conducted by C3SA partners, including the GCSCC, the World Bank, the International Telecommunications Union (ITU), and the Commonwealth Telecommunications Organisations (CTO), which were available at various repositories. In addition, we reviewed other existing metrics and reports on the status of cybersecurity maturity in the region. The reports we reviewed include the NCSI by the e-governance academy foundation, the GCI by the ITU, academic literature such as published papers and grey literature, including regional reports and news articles. To fill any gaps on missing data, subject matter experts were identified and approached to provide more information through semi-structured interviews. The collected data was synthesised according to the relevant dimension for each country, which consequently allowed for a regional analysis based on the five dimensions of the model. Based on these findings, the report makes specific policy recommendations targeted at helping countries in the SADC region to improve their cybersecurity capacity.

This report was compiled by C3SA researchers in collaboration with researchers from the GCSCC and NUPI.

Executive Summary

This study is a review of the maturity of cybersecurity capacity in the 16 countries of the SADC conducted by the Cyber Security Centre for Southern Africa (C3SA). This review was carried out in collaboration with the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford and the Norwegian Institute of International Affairs (NUPI), with an aim to provide an empirical analysis of cybersecurity capacities in the region.

The result is an in-depth analysis of the status of cybersecurity maturity at a regional level, analysed across the five dimensions of the Cybersecurity Capacity Maturity Model for Nations (CMM) (See Appendix 1 for more details):

1. Cybersecurity Policy and Strategy
2. Cybersecurity Culture and Society
3. Building Cybersecurity Knowledge and Capabilities
4. Cybersecurity Legal and Regulatory Frameworks
5. Cybersecurity Standards and Technologies

Factors in the CMM dimensions allowed us to consider aspects relevant to cybersecurity capacity by grouping together related indicators, which describe steps and actions that, once observed, define the stage of cyber maturity of that aspect in each country. The maturity stages range from start-up to dynamic, creating an overview of dimensional strengths and gaps through cross-country comparisons.

The review of 16 SADC countries found that the region as a whole is at a lower maturity level compared to the rest of the world on all dimensions. While this is not good news, these findings provide a clear basis for prioritizing the building of cybersecurity capacity across the region. SADC countries find themselves predominantly at start-up or formative levels of cybersecurity maturity. The major differences in maturity between the SADC region and the rest of world were in the trust and confidence in online services (Dimension 2), the legal frameworks of cybersecurity (Dimension 4), and in national incident response (Dimension 1).

In summary, the main findings on cybersecurity maturity in SADC can be described as follows:

Dimension 1: Cybersecurity Policy and Strategy

Effective national cybersecurity policies and strategy is a crucial pillar for securing countries' digital infrastructure. Dimension 1 explores the capacity of a country to develop and deliver a cybersecurity strategy to enhance its cybersecurity resilience by building incident response, cyber defence and critical infrastructure (CI) protection capabilities. The maturity level for this dimension is based on a review of the following factors: national cybersecurity strategies, incident response and crisis management, CI protection and cybersecurity in national security and defence.

The gap between the SADC and the rest of the world remains large. There are few comprehensive and overarching national cybersecurity strategies, incident response routines and CI protection measures in the region. Although some countries (for example Mauritius and South Africa) are found to have initiated or implemented national policies or strategies, there is a need for streamlining efforts across countries; with rapid digitalisation comes increased interdependency between the digital economies and critical national infrastructures of the region. It is therefore in the interests of the region as a whole for member states to improve their cybersecurity maturity. Actors such as the African Union (AU) and the SADC can play an important role. Most of the SADC countries reviewed in the present study are at the start-up phase. Donor activity to raise awareness, strengthening capabilities through

education and the development of new standards to protect CI are evident in raising levels of cybersecurity maturity in the region.

To improve the cybersecurity capacity maturity of members, the SADC Secretariat should establish a programme aimed at encouraging member states to develop and implement national cybersecurity strategies (NCS) or policies and regulatory frameworks for addressing emerging threats and risks to CI and Human Rights. The SADC should consider including regional collaboration on cybersecurity within national security and defence in the Protocol on Politics, Defence and Security Co-operation.

Dimension 2: Cybersecurity Culture and Society

As cybersecurity is a shared responsibility among users and other actors in society, a responsible cybersecurity culture is evident. Dimension 2 assesses the following factors: cybersecurity mindset, trust and confidence in online services, users understanding of online personal information protection, reporting mechanisms and social media.

Most countries in SADC have a low level of maturity in this dimension. This means that the awareness of risks in the region's general public remains low and incentives to raise awareness are uncoordinated. Nonetheless, a few governments have pursued cybersecurity awareness-raising and there is evidence of an increasing level of cybercrime prioritisation such as protecting private data through legislative developments. Currently, however, the private sector is taking the lead in prioritising cybersecurity in most SADC countries, and much more work needs to be done to instil values, attitudes, and beliefs that will support a safe and vital internet across the region.

To cultivate a responsible cybersecurity culture among citizens of the region, the report recommends that the SADC Secretariat should encourage member states to include digital literacy and cyber risk awareness in their ICT policies or NCS and allocate funding for implementation. Member states should collaborate with the private sector in the development and implementation of strategies and programmes for digital literacy and cybersecurity awareness. The media should be capacitated to cover cybersecurity incidents appropriately.

Dimension 3: Building Cybersecurity Knowledge and Capabilities

Dimension 3 assesses the following factors: initiatives to build cybersecurity awareness, cybersecurity education, cybersecurity professional training, as well as cybersecurity research and innovation. From the assessment it emerged that SADC countries have protocols and strategic plans in place, implying aspirations to develop cybersecurity skills and capacity.

Nevertheless, cybersecurity awareness-raising in SADC is estimated to have remained low between the start-up and formative stages of maturity. Except for South Africa, Mauritius, Namibia, and Botswana, only a few initiatives to raise awareness about cybersecurity were found. Cybersecurity awareness-raising initiatives have been limited in regularity, scope, and scale across the SADC region, despite a little upsurge in activities since the start of the COVID-19 pandemic restrictions. The situation of cybersecurity education in the SADC is concerning, taking into account the emerging sophistication of cyberthreats and risks, and the fact that Africa has become a serious target for cybercriminals, especially since the COVID-19 pandemic restrictions were imposed. Additionally, the provision of cybersecurity professional training is barely commencing in the region. Except for South Africa, Mauritius, Namibia, and Botswana, all the other countries offer very few to no cybersecurity professional training programs. Further, the factor "cybersecurity research and innovation" is at a start-up stage in the SADC region.

This report recommends that the SADC secretariat calls for a prioritisation of cybersecurity awareness-raising by all member states, where governments in the SADC should collaborate with public sector and civil society to develop and deploy targeted, relevant, and regular countrywide cybersecurity awareness-raising campaigns. They should also collaborate to develop and implement national cybersecurity education frameworks including cybersecurity qualifications in secondary and tertiary education, as well as professional training so as to fill up gaps in skills and competencies. Additionally, they should also promote cybersecurity research and innovation, allowing for a better understanding of local contexts, and thereby the generation of locally relevant solutions.

Dimension 4: Cybersecurity Legal and Regulatory Frameworks

The purpose of cybercrime legislation is to ensure ability to combat digital criminal activities. Dimension 4 examines governments' capacity to design and enact national legislation related to cybersecurity. Countries' capacity to enforce such laws are examined through an overview of cyber-related law enforcement, prosecution, regulatory bodies and court capacities. Dimension 4 assesses the following factors: legal and regulatory provisions; related legislative frameworks; legal and regulatory capability and capacity; and formal and informal co-operation frameworks to combat cybercrime.

On average, SADC countries are showing progress in the development of substantive legislation on cybercrime. Most countries have passed specific cybercrime laws or amended their criminal law so that they can address cybercrime. However, as a collective, the capacity of the region to effectively investigate and prosecute cybercrimes is hampered by inadequate criminal and procedural legislation for cybercrimes and crimes involving digital evidence. Moreover, few countries have regulatory bodies in place to protect private data and CI, particularly in consideration of Human Rights. Although nearly half of SADC countries have enacted data protection legislation, implementation of the laws is not evident in most of them. When it comes to the capacity of law enforcement to investigate cybercrimes, most SADC countries fall under the start-up stage, with the exception of a few countries at formative and established levels of maturity.

Since cybercrimes often involve multiple jurisdictions, SADC countries need to ratify international treaties in order to facilitate cooperation in the investigation and prosecution of cybercrimes. However, only Angola, Mauritius, Mozambique and Zambia have ratified the African Union Convention on Cyber Security and Personal Data Protection, whose aim to harmonise is legislation in the area of cyber security among African Union member states and thus enable cooperation. Overall, there remains a need for SADC countries to review criminal and procedural legislation and regional/international cooperation to adequately cover cybercrimes.

Dimension 5: Cybersecurity Standards and Technologies

In an effort to combat cybercrime and ensuring a healthy digital environment, compliance to cybersecurity standards and best practices is indispensable. Dimension 5 addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure through an assessment of the following factors: adherence to standards, security controls, software quality, communications and Internet infrastructure resilience, and the cybersecurity marketplace.

SADC countries are generally assessed to be at *start-up to formative* stages on the CMM scale in adherence to ICT security standards. Countries such as Tanzania, Namibia and

Botswana have adopted some ICT standards, while other member states have acknowledged the importance of it. ICT standards are nonetheless most prevalent in private sector organisations such as the banking and telecommunication sectors. Despite the fact that several countries have procurement processes to ensure transparency and accountability, few have standards that include cybersecurity as a requirement for all products and services.

Many SADC countries are not actively involved in the development of ICT security standards yet. On a positive note, more than half of SADC countries have in fact reached a *formative to established stages* on the CMM scale in the assessment of technological security controls, such as software updates, anti-malware and firewall systems in both the public and private sector organisations. The same number of countries also have cryptographic controls such as digital authentication and certificates in place, and recognize the value of such controls. Nonetheless, software quality is considered low in maturity in SADC countries, with few exceptions. When it comes to internet infrastructure reliability, nearly half of SADC countries find themselves at the *start-up stage* on the CMM scale due to limited access to affordable and reliable internet services. The other half stand at the *formative* stage on the CMM scale because they have obtained reliable internet services and infrastructures but still lack the capacity to withstand disasters with minimal disruption. Three countries in the SADC showed an established maturity stage in certain aspects of this dimension. However, most countries lack ICT standards and solid procurement practices.

Although there is improvement in the use of cybersecurity standards and technologies, governments in SADC need to do more to promote and encourage the use of cybersecurity standards and technologies in the region. This study also recommends SADC countries to adopt frameworks or national policies to handle technological security controls, including cryptographic controls, and that governments collaborate with the private sector and civil society in the process. Crucially, SADC governments should promote cybersecurity research and protect the work of cybersecurity researchers by not unduly criminalising things like the use, development, possession, or distribution of tools created to test or compromise the security of an application for research purposes.

Introduction and Background

Cybersecurity is becoming a rising concern in a world that is increasingly dependent on the internet. As a region, Africa is plagued by some of the highest numbers of cybercrime that negatively impact its socioeconomic development.[6] The number of unprotected computers for cybercrimes to be launched on, lack of budgets for cybersecurity expenditure, limited cybersecurity awareness, lack of cybersecurity regulations and few cybersecurity professionals are some of the commonly identified challenges in the region.[7, 8, 9] Subsequently, African economies are increasingly becoming important sources and, victims of cyberthreats that have a worldwide effect. Unfortunately, the situation may be expected to become more alarming post-pandemic as internet and mobile penetration continues to rise.

An increase in cybercrimes are bound to negatively affect the economies that are already taking a hit from the pandemic. While various developed countries have made strides in understanding their cybersecurity landscape, in Africa, a budding economy, this is still less understood. Some initial work on Sub-Saharan Africa (SSA) offers useful insights to some of the challenges that the region faces such as the lack of cybersecurity awareness.[10] However, there are gaps in understanding the cybersecurity landscape in a systematic and substantive way. Africa is vast. Cyberattacks do not happen equally across its landscape. Some countries have been reported to receive much more attention from cybercriminals than others due to differences that may be attributed in part to the varied digital maturity and economic growth. With rapid digitalisation and increased interdependency, it is in the interests of the region to improve cybersecurity maturity with an approach that will raise all countries while taking account of their differences in digital maturity, economic growth and political culture.

Within the sub-Saharan region of Africa, there are various regional groupings:

- The West African Economic and Monetary Union (WAEMU),
- Economic Community of West African States (ECOWAS),
- Economic and Monetary Community of Central African States (CEMAC),
- Common Market for Eastern and Southern Africa (COMESA),
- East African Community (EAC),
- Southern African Development Community (SADC), and
- Southern African Customs Union (SACU).

---

[6] See Bada, M., Von Solms, B., & Agrafiotis, I. (2018). Reviewing national cybersecurity awareness in Africa: an empirical study. *Proceedings of the Third International Conference on Cyber-Technologies and Cyber-Systems, Cyber 2018, Greece,* 78-83. https://www.thinkmind.org/index.php?view=instance&instance=CYBER+2018

[7] See Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity, 2012*, 1.

[8] See Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77-81.

[9] See Serianu. (2016). *Africa Cyber Security Report*. Retrieved December 11, 2021, from http://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[10] See Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness for Users and Executives in Africa. *arXiv preprint arXiv:1910.01005*.

This report seeks to offer a cybersecurity landscape of the SADC. The SADC is the largest regional group, with 16 member states. For this reason, the findings of this report will provide a starting point to understand the Sub-Saharan African cybersecurity landscape. A generalised understanding of the landscape would be an important pre-requisite to more targeted studies which explore specific aspects of cybersecurity. Additionally, improving awareness of the cybersecurity maturity will hopefully help SADC countries to work together and collaboratively as part of an interconnected ecosystem for an open, safe, secure, resilient, and peaceful cyberspace.

Cybersecurity capacity building is the foundation for countries to boost their resilience against cyber threats. While there are several frameworks available for capacity building initiatives, the Cybersecurity Capacity Maturity Model (CMM) for Nations from the Global Cyber Security Capacity Centre (GCSCC) is the most comprehensive one (See Appendix 1 for more details). This model indicates that the five main dimensions as crucial steps to building a country's cybersecurity capacity:

1) developing policy and strategy;
2) encouraging responsible cyber culture within society;
3) developing cybersecurity knowledge and capabilities;
4) creating effective legal and regulatory frameworks; and
5) adopting standards and technologies that help to control risks.

This report uses the CMM as a basis for providing insights on the cybersecurity capacity status for SADC.

An Overview of SADC

Established in 1992, SADC is a development community of 16 Southern African member states: Angola, Botswana, Union of the Comoros, Democratic Republic of the Congo (DRC), Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic of Tanzania, Zambia, and Zimbabwe (Figure 1). As of 2018, the total population of the region was 345 million with a Gross Domestic Product (GDP) of approximately USD $721.3 Billion (Southern African Development Community [SADC], 2018).

Figure 1: SADC member states (Source: SADC website[11])

The SADC treaty stipulates policies that aim to promote sustainable and equitable economic growth and socio-economic development that will enhance the standard and quality of life of the citizens of the member states. The policies also aim to stimulate a self-sustaining development based on a collective self-reliance as well as the interdependence of the member states as well as to promote the development, transfer, and mastery of technology.[12] To support and facilitate deeper regional integration, the SADC's Vision 2050 has set out as one of its objectives to have efficient and effective, technologically driven cross-border infrastructure services and

[11] See Southern African Development Community (SADC). (n.d.). *About SADC*. https://www.sadc.int/about-sadc/

[12] Ibid.

networks.[13] It is in light of this goal that the Regional Indicative Strategic Development Plan (RISDP) 2020–2030[14] recognises the importance of an enhanced collective defence and security system anchored upon having regional cybersecurity strategies among other defence strategies to safeguard the territorial integrity of the region. To this end, one major achievement of the region between 2015 – 2020 was the establishment of Computer Incident Response Teams. However, by September 2021 out of the 16 member states, seven countries had established CIRTs (Computer Incident Response Teams) (Botswana, Malawi, Mauritius, Mozambique, South Africa, Tanzania, and Zambia), while six member states (Angola, the Democratic Republic of the Congo, Eswatini, Lesotho, Namibia, and Zimbabwe) had either enacted legislation to operationalise their national Computer Emergency Response Teams or were in the process of drafting the relevant legislation (See Appendix 4).

The Economic Context

It is estimated that Africa's information and communications technology (ICT) sector grew by 7,000% between the years 2000 and 2016, with internet penetration increasing to nearly 28%. Over and above economic development, these technologies also improve productivity, efficiency, and innovation across the continent, and encourage the free flow of ideas and information. The use of ICT, and in particular the internet, has therefore become a matter of strategic importance. Africa has experienced sudden growth in ICTs and especially mobile technologies. After Europe and Asia Pacific, SSA is the world's third largest mobile market when ranked by unique subscribers.[15] Developments that have accompanied the growth in mobile technology can be seen in areas like e-commerce, banking and mobile money services which have subsequently resulted to cybercrimes that target African economies being mostly concentrated in the financial sector.[16, 17]

In Africa, the use of e-commerce has increased exponentially with the growing internet penetration rates and technology affordability.[18] Of the top 20 countries in the world that lead in use of mobile money services, 15 countries are in Africa.[19] The mobile money services are integrated to other platforms such as banking, insurance, and e-commerce, with unfortunately low security controls. In South Africa, one of the biggest economies in Africa, and the largest in SADC, online banking utilisation rates

[13] See SADC. (2022). *Southern African Development Community Vision 2050*. Retrieved February 20, 2022, from https://www.sadc.int/files/9316/1470/6253/SADC_Vision_2050.pdf

[14] See SADC. (2020, October). *SADC Regional Indicative Strategic Plan (RISPD) 2020-2030*. Retrieved February 2, 2022, from https://www.sadc.int/files/4716/1434/6113/RISDP_2020-2030_F.pdf

[15] See Serianu. (2016). Africa Cyber Security Report 2016. https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[16] See Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity, 2012*, 1.

[17] See Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77-81. https://doi.org/10.1080/1097198x.2019.1603527

[18] See Serianu. (2016). *Africa Cyber Security Report.* https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[19] Ibid.

approximate at 86%.[20] The continent is also characterised by a unique use of other financial outfits such as Savings and Credit Cooperatives (SACCO) that have gained traction and greater transactional amounts. While the adoption of such services affords customers and bank various benefits including customer convenience and low operating costs, it also creates increased opportunities for cybercriminals who exploit mobile devices and other online banking systems to intercept financial transactions. As a result of such increased avenues for cybercrimes, the financial sector experiences 300% more cyber-attacks than any other industry.[21]

Other important sectors that drive the African economy such as hospitality and telecommunications have equally been affected. Here, cybercrimes mainly target the sensitive and confidential customer data.

Cybersecurity and the Socio-economic Context

Some of the key economic and social characteristics of African countries include low level of human development index, high unemployment rate, high degree of income inequality, low level of education, and weak democratic institutions[22] (UNDP, 2006). These characteristics bear critical implications and consequences for cybersecurity[23] for example, low levels of education may be associated with inexperienced internet usage and practices due to low digital literacy skills.[24, 25] The use of English as the main language to deliver security related instructions and information may also be a contributor to alienating many African internet users. Further, even when users are generally educated, many internet users in the region may still not be aware of cyber dangers as there is little citizen awareness and training.[26] In addition, the limited number of cybersecurity professionals may also exacerbate the cybersecurity vulnerabilities both within SADC and the African continent at large. Of a population of approximately 1.24 billion people, it is estimated that there are only about 7000 certified security professionals in Africa. This translates to one for every 177,000 people. This severe shortage in cybersecurity professionals may severely affect defensive mechanisms and response to the increasing cybercrimes in the region. The additional lack of cybersecurity orientation by consumers, businesses and policymakers creates more opportunities for cybercrime to thrive.

---

[20] See Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77–81. https://doi.org/10.1080/1097198x.2019.1603527

[21] See Raytheon. (2015). *2015 industry drill-down report financial services*. Retrieved March 6, 2022, from http://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf

[22] See United Nation Development Programme. (2006). *Country evaluation: Assessment of development results: Honduras.* Retrieved February 12, 2022, from http://web.undp.org/evaluation/documents/ADR/ADR_Reports/ADR_Honduras.pdf

[23] See Kshetri, N. (2016). Cybersecurity and development. *Markets, Globalization & Development Review, 1*(2). https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1012&context=mgdr

[24] See Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity, 2012*, 1.

[25] See Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313-338.

[26] See Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness for Users and Executives in Africa. *arXiv preprint arXiv:1910.01005*.

Cultural preferences also impact the extent of cybersecurity success by influencing uptake of some cybersecurity practices both among institutions and individuals.[27, 28] Most African societies tend to emphasize social harmony and human relationships. This aspect may limit cybersecurity procedures such as security checks that may be considered 'undignified' and encourage practices such as password sharing[29] For purposes of cybersecurity, different aspects of culture may necessitate a change of behaviour and the extent to which people are willing to change[30,31] an extensive use of mobile devices (smartphones) to access the internet among others may increase the susceptibility of users to cybercrimes.

With regards to the economy, the service sector, like most other economies, contributes to half of SADC's GDP.[32] These sectors which include financial services, government services, manufacturing and insurance are marked with increased cyberattacks.[33] With the technological advancements taking place at a rapid and unprecedented rate in the African space, the continent has become a hub for cybercrime activities as the emerging economies provide low-hanging fruit for cybercriminals. In 2017, cybercrimes cost African economies an estimated total of over US$ 3.5 billion. While the figures are much lower than the US economy which lost between US$ 57 billion and US$109 billion in 2016 from malicious cyber activity, the African figures represent approximately 0.12 percent of the total GDP. As reported by the South African Banking Risk Information Centre (SABRIC), South Africa alone, one of the largest economies in Africa, lost ZAR309,563,109 (approximately US$21.3 million) to digital crime in 2020 alone.[34] Although population density and the basis for calculating losses differ, other top economies in the continent are facing similar challenges with losses having soared to US$550 million for Nigeria and US$175 million for Kenya.[35, 36]

---

[27] See Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313-338.

[28] See Bada, M., Von Solms, B., & Agrafiotis, I. (2019, October 2). Reviewing national Cybersecurity awareness for users and executives in Africa. *International Journal on Advances in Security,12*(1&2), 108-118. https://arxiv.org/abs/1910.01005

[29] See Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313-338.

[30] See Bada, M., Von Solms, B., & Agrafiotis, I. (2019, October 2). Reviewing national Cybersecurity awareness for users and executives in Africa. *International Journal on Advances in Security 12*(1&2), 108-118. https://arxiv.org/abs/1910.01005

[31] See Marler, W. (2018). Mobile phones and inequality: Findings, trends, and future directions. *New Media & Society, 20*(9), 3498-3520.

[32] See SADC. (2012). *SADC overview*. from https://www.sadc.int/about-sadc/overview

[33] See Serianu. (2019). *African Cyber Security Report Kenya 2019/2020: Local Perspective on Data Protection and Privacy Laws Insights from African SMEs*. https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

[34] South African Banking Risk Information Centre. (2020). Annual Report 2020. Retrieved March 3, 2022, from https://www.sabric.co.za/media/lejmweri/sabric_annual-report_2020.pdf

[35] See Serianu. (2016). *Africa Cyber Security Report 2016*. https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[36] See Bada, M., Von Solms, B., & Agrafiotis, I. (2018). Reviewing national cybersecurity awareness in Africa: an empirical study. *Proceedings of the Third International Conference on Cyber-Technologies*

ICT Access and Use in Sub-Saharan Africa

In 2001 there were 400 million internet users worldwide, and by the end of 2019, the number was 3.7 billion.[37] The most considerable increase in users has been in the growing economies, especially on the African continent. In 2000, 0.5% of the population in the Sub-Saharan Africa region was using the internet, while in 2017, this had increased to 19%.[38] There are also significant regional differences in the type of electric communication. For broadband subscribers, there is one subscriber for every 1,000 inhabitants in Africa, while in Europe the corresponding figure is 200. In SADC, there has equally been an increasing number of internet users (Figure 2).

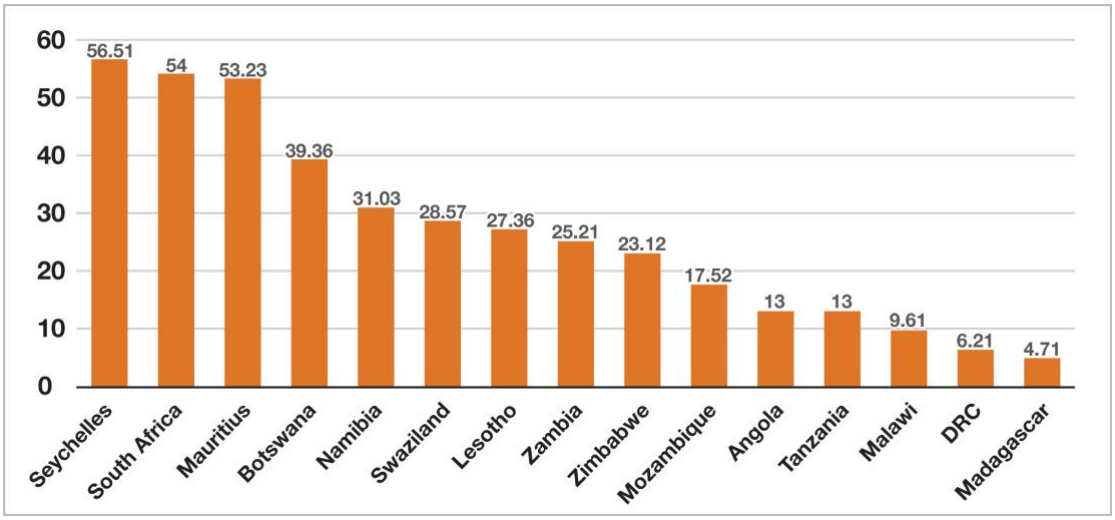

Figure 2: Percentage of individuals using the internet in SADC (2019)[39]

Most internet usage in sub-Saharan Africa is through mobile services, and nearly 500 million people have subscriptions[40], where 272 million connect to the internet on their phones. It is forecasted that the region will be surpassing 130 million new subscribers by 2025, where half of which will come from Nigeria, Ethiopia, Democratic Republic of Congo (DRC), Tanzania and Kenya.[41] There is a big difference in internet access in

and Cyber-Systems, Cyber 2018, Greece, 78-83. https://www.thinkmind.org/index.php?view=instance&instance=CYBER+2018

[37] See Kathuria, Vinish & Oh, Keun Yeob. (2018). ICT access: Testing for convergence across countries. *The Information Society, 34*(3), 166–182. https://doi.org/10.1080/01972243.2018.1438549

[38] See The World Bank. (2022). *Individuals using the Internet (% of population) - Sub-Saharan Africa | Data*. Retrieved March 6, 2022, from https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZG

[39] See Calandro, E., & Berglund, N. (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC case. *In GIGAnet annual symposium. Berlin.* https://researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf

[40] See GSM Association. (2021). *The Mobile Economy Sub-Saharan Africa 2021*. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf

[41] See Connecting Africa. (2020, September 30). *Strong mobile growth predicted for sub-Saharan Africa - GSMA*. Retrieved February 22, 2022, from https://www.connectingafrica.com/author.asp?section_id=761&doc_id=764310

areas outside capital cities. These areas tend to be far behind – with lack of infrastructure, especially electricity, as the main issue for internet access among poor Africans.[42]

Africa is one of the least connected regions globally. Its connectivity is growing rapidly, and the number of ICT users is increasing at an unprecedented pace. The GSM Association (GSMA) forecasted that sub-Saharan Africa will have more than 600 million by 2025.[43] Furthermore, the digital economy is expected grow significantly and could account for 5,2% of the region's GDP by 2025.[44] However, the transition to a digital economy comes with several challenges, as most countries in the region have a minimal institutional framework to ensure a sustainable transition to gain the desired effects of digitalisation.[45] With limited cyber-security, legislative measure, and awareness – several of the countries in the region are attractive to cybercriminals as digital services are thriving.

The current effects of COVID-19 on ICT access and use statistics is still unclear as the development is still fairly recent. Still, preliminary research shows a further dependence on digital infrastructure and increasing digitalisation of services. In 2020 McKinsey & Company[46] highlighted that "[...] the crisis-driven action currently underway contains the seeds of a large-scale reimagination of Africa's economic structure, service-delivery systems, and social contract. The crisis is accelerating trends such as digitisation, market consolidation, and regional cooperation, and it is creating important new opportunities [...]".

Trends Affecting Cybersecurity in Africa

As both opportunities and threats have increased parallel to the use of internet throughout the world, policy makers are called to put in place measures to secure the cyberspace domain. Cybercrime has significantly affected the African continent, with several of the Sub-Saharan countries being mentioned as most affected countries in international reports on cybercrime.[47] However, not only developing economies find it difficult to effectively protect cyberspace from malicious activities. Developed countries as well are struggling with securing their digital infrastructure. Considering the

---

[42] See Mahler, D., Montes, J., & Newhouse, D. (2019). *Internet Access in Sub-Saharan Africa. World Bank Group. Poverty & Equity Notes*. Retrieved March 5, 2022, from https://documents1.worldbank.org/curated/en/518261552658319590/pdf/Internet-Access-in-Sub-Saharan-Africa.pdf

[43] See GSM Association. (2019). *The Mobile Economy Sub-Saharan Africa 2019*. Retrieved February 20, 2022, from https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=45121567&file=2794-160719-ME-SSA.pdf

[44] See International Finance Corporation. (2020). *e-Conomy Africa 2020 - Africa's $180 Billion Internet Economy Future*. Retrieved March 6, 2022, from https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/google-e-conomy

[45] See Schia, N. N., & Gjesvik, L. (2018). *Managing a Digital Revolution - Cyber Security Capacity Building in Myanmar*. NUPI Report. http://hdl.handle.net/11250/2563201

[46] See McKinsey & Company. (2020). *How the COVID-19 crisis can catalyze change across the continent*. https://www.mckinsey.com/featured-insights/middle-east-and-africa/reopening-and-reimagining-africa

[47] See Interpol. (2021). *African cyberthreat assessment report*. Retrieved March 4, 2022, from https://www.interpol.int/en/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

transnational nature of cybercrime, the problem has both an international and a regional dimension. Since the internet is an interconnected network of networks, all elements linked to the internet are dependent of each other, and one is “only as strong as the weakest link”.[48]

Certain trends have influenced cybersecurity in the African space.[49] The rapid diffusion of mobile technologies resulting from increased affordability have spurred access to the internet and the number of services offered over mobile platforms. The growing adoption of these technologies has led to the exposure of novice users to cybercrimes and has created new vulnerabilities that directly impact both users, low-cost devices and services designed with little attention to security standards. Other technological trends that have emerged such as internet of Things (IoT) complicate the situation further due to their insecure implementation and configuration of these internet connected devices.

At an organisation level, certain practices and their potential trade-offs may need to be considered. African companies have increasingly embraced a ‘bring your own device’ (BYOD) culture and have started to set up policy to support it.[50] Since devices may not be adequately secured, and usually have lower security policy in personal devices, they become easy targets for cybercriminals. While the use of cloud-based solutions has the potential to help companies to reduce expenditure on ICT infrastructure, they can also carry a loss of control over the security of business-critical systems on the cloud if the transition is done incorrectly.

At the national level, the laxity in implementing cybersecurity laws, as well as local challenges such as high poverty and unemployment rates, tend to contribute to cybercrime because of the lack of any credible deterrence.

Cybersecurity Vulnerabilities

Cybersecurity vulnerabilities target and affect individuals, organisations and the state/government.

Individuals

It is quite clear that attackers tend to focus their efforts on "weak links". These include individuals who lack the awareness and who do not adopt proper "cybersecurity hygiene", security habits and practices, that would safeguard them as well as their organisations.[51]

---

[48] See Schia, N. N., & Gjesvik, L. (2018). *Managing a Digital Revolution - Cyber Security Capacity Building in Myanmar*. NUPI Report. http://hdl.handle.net/11250/2563201

[49] See Serianu. (2016). *Africa Cyber Security Report*. http://www.Serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[50] See Africa *Cyber Security Report - Kenya 2019/2020. Local Perspective on Data Protection and Privacy Laws: Insights from African SMEs*. https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

[51] See Cybersecurity Tech Accord. (2020). *Cybersecurity Awareness of Commonwealth Nations.* https://cybertechaccord.org/uploads/prod/2020/03/TechAccord-awareness-06.pdf

In Sub-Saharan Africa mobile phones are typically used for connectivity, but also many use them for banking and financial transactions. In most of Sub-Saharan Africa mobile money is actually more popular than banking.[52] In a survey from 2020[53] with 900 respondents from Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria, and South Africa – 48% were concerned about cybercrime but were still conflicted about necessary steps to secure their digital presence. The need for awareness-raising is still clearly evident, with individuals taking huge risks with a lack of understanding of what constitutes a threat and how their mobile devices can be compromised.

Organisations

In African organisations there is a lack of cybersecurity professionals, general awareness of cyber issues, lack of benchmarking of international standards such as ISO, and limited spending and resources on cyber security. As experiences of cybercrime within the African region are increasing both in organisations and individuals this can be troublesome. It is critical for organisations to increase training of employees around security best practices and various methods used by cybercriminals.[54] Further, when individuals are BYOD, they are putting themselves and their organisation at risk, as mentioned earlier.

Financial institutions are regular targets, which has had major losses of billions of USD. A survey by the Moroccan company Dataprotect indicated that more than 85% of financial institutions interviewed in Sub-Saharan Africa had been the victim of cyber threats that had resulted in damage.[55]

State/Government

In Sub-Saharan Africa, one sees a general shortage of cybersecurity personnel, making it demanding to build frameworks to secure digital infrastructure. In the meantime, the region is characterised by weak legislation and law enforcement, which provides a fertile ground for cybercrime activities.[56] The states are experiencing increasing amounts of cyberthreats and are seeing a broad range of actors, everything from individuals to nation-states, with varied capabilities and goals.[57]

Most of cyberspace infrastructure is owned by private actors, and critical infrastructure is distributed between public and private stakeholders making it more complex and

---

[52] See International Monetary Fund (IMF). (2019). *Fintech in Sub-Saharan Africa: A Potential Game Changer.* https://blogs.imf.org/2019/02/14/fintech-in-sub-saharan-africa-a-potential-game-changer/

[53] See KnowBe4 Africa. (2020). *2020 African Cybersecurity Research Report*. https://www.knowbe4.com/hubfs/2020%20African%20Cybersecurity%20Research%20Report.pdf?hsCtaTracking=9de8b71e-3443-4b75-a7df-ccdc81607b89%7C3ac45c4f-3fac-404d-8b48-59c0c204d07f

[54] See Serianu. (2016). *Africa Cybersecurity Report*. https://www.cybersecurityhub.gov.za/cyberawareness/images/pdfs/AfricaCyberSecurityReport20161.pdf

[55] See Data Protect. (2019). *La cybersécurité dans le secteur financier africain*. https://www.sciencetech.com/fr/wp-content/uploads/2021/01/Afrique_Faits-saillants_12sep19.pdf

[56] See Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77-81.

[57] See Africa Center for Strategic Studies. (2021). *Africa's Evolving Cyber Threats. https://africacenter.org/spotlight/africa-evolving-cyber-threats/*

which gives a shared responsibility between different type of actors and interests.[58] As the telecom-infrastructure overall is poorly secured, in combination with the increased pressure from COVID-19 affecting the patterns of the use of digital infrastructure of both private and public services – the demands for a safe, effective and resilient internet are becoming more evident in the region.

[58] See Cybersecurity Observatory. (2020). *Cybersecurity Risks, Progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Status of CMMs in SADC

With regards to the Cybersecurity Capacity Maturity Model for Nations (CMM) deployments, the cybersecurity capacity-building space in Southern Africa is a confederation between the member states and diverse regional, multilateral organisations and partnerships from all over the world. These organisations have played various roles in SADC ranging from providing cybercrime courses, funding capacity building projects and strengthening legal frameworks among others.[59] Some of the common players in the region include NUPI, GCSCC at the University of Oxford, CTO, ITU, World Bank and NEPAD. In 2019, the Norwegian Ministry of Foreign Affairs funded the establishment of the Cybersecurity Capacity Centre for Southern Africa (C3SA). Table 1 shows the list of SADC countries, reporting those that have completed a CMM review, when the review was completed and the collaborating institution.

Table 1: Current CMM status for SADC countries as of June 2021[60]

Country	CMM completed by	Year	Publicly available?
Angola	-	-	-
Botswana	World Bank	2019	No
Union of the Comoros	-	-	-
Democratic Republic of the Congo	-	-	-
Eswatini	CTO/ITU	2017	No
Lesotho	World Bank/GCSCC	2019	No
Madagascar	GCSCC/ITU	2016	Yes
Malawi	CTO and World Bank	2016 and 2020	No
Mauritius	World Bank/GCSCC	2019	No
Mozambique	CTO	2016	No
Namibia	World Bank	2019	No
Seychelles	-	-	-
South Africa*	GCSCC	2020	No
United Republic of Tanzania	CTO	2016	No
Zambia	GCSCC/World Bank	2017	No
Zimbabwe	-	-	-
*A desktop study A blank indicates no CMM available			

[59] See Calandro, E., & Berglund, N. (2019). Calandro, E., & Berglund, N. (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC case. In *GIGAnet annual symposium. Berlin.* https://researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf

[60] See Global Cyber Security Capacity Centre. (2022). *CMM Reviews around the World*. https://gcscc.ox.ac.uk/cmm-reviews#/

From Table 1, it is possible to observe that by 2021, eleven countries had a CMM review. Of those, only one country published its national CMM report. Therefore, it is difficult to find and access to information and data on cybersecurity in the region. The main organisation having supported the deployment of CMM is World Bank with six studies conducted between 2016 and 2020. Published and unpublished national CMM reports were used as a starting point to conduct this regional analysis, always respecting the confidentiality and anonymity of those unpublished CMM reports.

The following section analyses the results of this study and Appendix 2 describes in detail its methodological approach.

Regional Analysis

In this section of the report, we present the findings of the regional analysis using the CMM as a framework. The CMM considers broad topics of cybersecurity by including five different but inter-connected dimensions of cybersecurity capacity and allows to measure the maturity of nations in each one of these cybersecurity aspects (see Appendix 1). The methodology used in this regional study consists of a broad document review of more than 200 documents (including the CMM reports of those SADC countries reviewed)[61], using thematic analysis based on CMM themes, in-depth interviews with key informants of cybersecurity in the SADC, and descriptive statistics (see Appendix 2). This methodology allowed to gather enough evidence to gauge the national maturity stage of the SADC countries in the different dimensions of the CMM. This analysis anonymises the SADC countries' maturity in each cybersecurity aspect and describes the cybersecurity capacity landscape in the region.

Due to the limitations explained in Appendix 2, this regional study did not conduct national CMM reviews to SADC countries which include in-country discussion groups with national key stakeholders. Appendix 1 explains the methodology used in CMM reviews where the focus of study is a nation, and Appendix 2 details the methodology used in this study that focusses on the SADC region.

This section follows the structure of the CMM 2021 Edition (Global Cyber Security Capacity Centre, 2021). The analysis describes how the region is performing in each factor within a cybersecurity dimension, drawing recommendations for nations within the region and for the SADC Secretariate on what steps could be taken towards improving the cybersecurity maturity in the SADC region.

Most internet usage in sub-Saharan Africa is through mobile services, and nearly 500 million people have subscriptions[62], where 272 million connect to the internet on their phones. It is forecasted that the region will be surpassing 130 million new subscribers by 2025, where half of which will come from Nigeria, Ethiopia, Democratic Republic of Congo (DRC), Tanzania and Kenya.[63] There is a big difference in internet access in areas outside capital cities. These areas tend to be far behind – with lack of infrastructure, especially electricity, as the main issue for internet access among poor Africans.[64]

Africa is one of the least connected regions globally. Its connectivity is growing rapidly, and the number of ICT users is increasing at an unprecedented pace. The GSMA

[61] As mentioned previously, ten SADC countries were reviewed under the CMM and have the corresponding national CMM report (Botswana, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, the United Republic of Tanzania, and Zambia). For more information, see https://gcscc.ox.ac.uk/cmm-reviews, Retrieved November 10, 2021.

[62] See GSM Association. (2021). *The Mobile Economy Sub-Saharan Africa 2021*. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf

[63] See Connecting Africa. (2020). *Strong mobile growth predicted for sub-Saharan Africa – GSMA*. http://www.connectingafrica.com/author.asp?section_id=761&doc_id=764310

[64] See Mahler, D. G., Montes, J., & Newhouse, D. L. (2019). *Internet access in sub-Saharan Africa* (No. 135332, pp. 1-4). The World Bank. https://documents1.worldbank.org/curated/en/518261552658319590/pdf/Internet-Access-in-Sub-Saharan-Africa.pdf

forecasted that sub-Saharan Africa will have more than 600 million by 2025.[65] Furthermore, the digital economy is expected grow significantly and could account for 5,2% of the region's GDP by 2025.[66] However, the transition to a digital economy comes with several challenges, as most countries in the region have a minimal institutional framework to ensure a sustainable transition to gain the desired effects of digitalisation.[67] With limited cyber-security, legislative measure, and awareness – several of the countries in the region are attractive to cybercriminals as digital services are thriving.

The current effects of COVID-19 on ICT access and use statistics is still unclear as the development is still fairly recent. Still, preliminary research shows a further dependence on digital infrastructure and increasing digitalisation of services. In 2020 McKinsey & Company[68] highlighted that "[...] the crisis-driven action currently underway contains the seeds of a large-scale reimagination of Africa's economic structure, service-delivery systems, and social contract. The crisis is accelerating trends such as digitisation, market consolidation, and regional cooperation, and it is creating important new opportunities [...]".

D.1 Cybersecurity Policy and Strategy in SADC

Cybersecurity Policy and Strategy is the main pillar for securing a country's digital infrastructure. Dimension 1 explores a country's capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience, through improving its incident response, cyber defence, and critical infrastructure protection capacities. This Dimension considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business, and society in general.[69]

Figure 3 below depicts how many SADC countries had a start-up, formative, established, and strategic maturity stage in each aspect within Dimension 1 at two points in time: when the national CMM reviews were conducted (ten SADC countries had a CMM report during the period 2016-2020); and when this SADC regional report was completed (2021). The four aspects included in factor D1.1 - National Strategy development, content, implementation and review, and international engagement. Identification and categorisation of incidents, organisation, and integration of cyber into national crisis management are the three aspects that form factor D1.2 incident response and crisis management. Identification, regulatory requirements, and operational practice are the three aspects within factor D1.3 critical infrastructure protection. Finally, defence force cybersecurity strategy, defence force cybersecurity

[65] See GSMA. (2019). *The Mobile Economy Sub-Saharan Africa*. https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=45121567&file=2794-160719-ME-SSA.pdf

[66] See IFC. (2020). *e-Conomy Africa 2020 - Africa's $180 Billion Internet Economy Future.* https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/google-e-conomy

[67] See Schia, N. N., & Gjesvik, L. (2018). *Managing a Digital Revolution - Cyber Security Capacity Building in Myanmar*. NUPI Report. http://hdl.handle.net/11250/2563201

[68] See McKinsey & Company. (2020). *How the COVID-19 crisis can catalyze change across the continent*. https://www.mckinsey.com/featured-insights/middle-east-and-africa/reopening-and-reimagining-africa

[69] See Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

capability, and civil defence coordination are the three aspects that form factor D1.4 cybersecurity in defence and national security.

To interpret Figure 3, consider, for example, the first aspect on the strategy development. The information from the CMM reports in 2016-2020 (labelled CMM 2016-20 in Figure 3) showed that a high proportion of the reviewed countries had a start-up maturity stage, and that there was a country with an established maturity stage that was leading the regional capacity building in this particular aspect. However, this regional study (labelled C3SA 2021 in Figure 3) found that, in 2021, there was actually three countries in the region with an established maturity stage for their strategy development. This regional analysis had certain limitations in finding evidence on all the aspects in Dimension 1 for all the SADC countries, although it has extended the available information on cybersecurity capacity in the SADC. The results of 2021 shows that there were some leading countries with an established and even strategic maturity stage in all aspects of this dimension, except those related to defence and national security. Moreover, this study has detected that some countries are no longer considered established in the identification of critical infrastructure protection, according to the new requirements of the CMM 2021 Edition. The next subsections describe the regional level of maturity in the different factors included in Dimension 1.

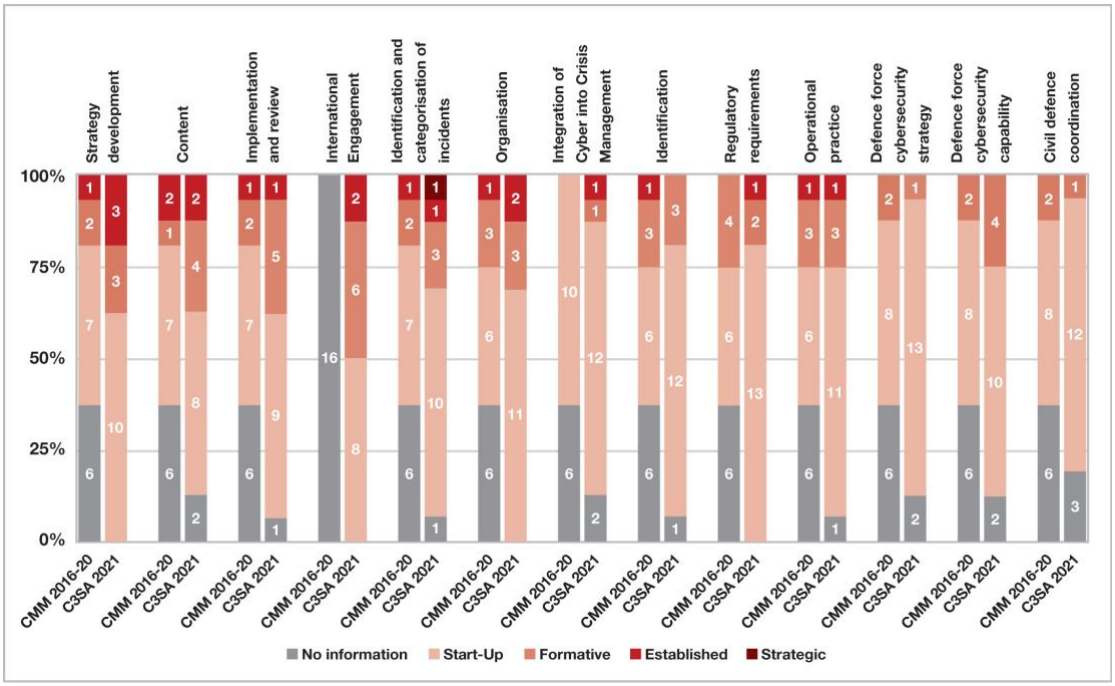

Figure 3: Number of SADC countries within each maturity stage for the CMM aspects of Dimension 1 "Cybersecurity Policy and Strategy".

Source: C3SA (C3SA 2021) & GCSCC (CMM 2016 – 2020)

D1.1 National Cybersecurity Strategy

A cybersecurity strategy is necessary to be able to mainstream a cybersecurity agenda across government branches, as it helps to prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key actors, and directs allocation of resources to the emerging and existing cybersecurity issues and

priorities.[70] To manage both internal and external cyber threats, there is an evident need for cybersecurity strategies in the SADC countries. Unfortunately, the study found few national cybersecurity strategies in the region, although some countries have initiated or implemented these strategies (see Table 2).

Table 2: Development of Cybersecurity Strategy/Policy in the SADC

Country	National Cybersecurity Strategy / Policy	Year Adopted
Angola	-	-
Botswana	National Cybersecurity Strategy[71]	2020
Comoros	-	-
DRC	Draft	-
eSwatini	Eswatini National Cybersecurity Strategy 2020 -2025[72]	2020
Lesotho	-	-
Madagascar	-	-
Malawi	National Cybersecurity Strategy (2019 - 2024)[73]	2019
Mauritius	National Cybersecurity Strategy (2014-2019)[74]	2014
Mozambique	Estratégia Nacional de Segurança Cibernética de Moçambique - (Proposta) Versão 2[75,76]	2021
Namibia	-	-
Seychelles	-	-
South Africa	National Cybersecurity Policy Framework	2015
Tanzania	-	-
Zambia	National Cybersecurity Policy 2021[77] and Implementation Plan (2021 – 2015)[78]	2021
Zimbabwe	-	-

NB: "-" means no evidence could be found

[70] See Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. https://gcscc.ox.ac.uk/files/cmm2021editondoc.pdf

[71] See Republic of Botswana. (n.d). *National Cybersecurity Strategy*. Retrieved March 3, 2022, from https://www.bocra.org.bw/sites/default/files/documents/approved%20botswana-national-cybersecurity-strategy.pdf

[72] See Kingdom of eSwatini. (2020). *Eswatini National Cybersecurity Strategy 2025*. http://www.gov.sz/images/ICT/Eswatini-National-Cybersecurity-Strategy-NCS-2025.pdf

[73] See Government of Malawi. (2019). *Malawi National Cybersecurity Strategy (2019-2024)*. https://api.pppc.mw/storage/160/National-Cybers-col.pdf

[74] See Republic of Mauritius. (2014). *Republic of Mauritius National Cybersecurity 2014-2019*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Mauritius_2014_National%20Cyber%20Security%20Strategy%20-%202014%20-%20EN.pdf

[75] See Government of Mozambique. (2017). *Estratégia Nacional de Segurança Cibernética de Moçambique - (Proposta) (2017-2021) Versão*. https://www.oam.org.mz/wp-content/uploads/2017/06/Draft_National_Cyber_Security_Strategy_Mozambique_PT_GT_24052017FINAL.pdf

[76] See The National Institute of Information and Communication Technologies (INTIC). (2021). Government approves national cybersecurity policy and strategy. Retrieved January 5, 2022 from https://www-intic-gov-mz.translate.goog/?p=979&_x_tr_sl=pt&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

[77] See Republic of Zambia. (2021). *National Cybersecurity Policy 2021*. Retrieved January 5, 2022, from https://www.mtc.gov.zm/wp-content/uploads/2021/06/National-Cybersecurity-Policy2_compressed.pdf

[78] See Republic of Zambia. (2021). *National Cybersecurity Policy Implementation Plan 2021-2025*. Retrieved March 4, 2022 from https://www.mtc.gov.zm/wp-content/uploads/2021/06/National-Cybersecurity-Policy-Implementation-Plan-2021-2025.pdf

Source: C3SA (C3SA 2021) & GCSCC (CMM 2016 – 2020)

Of the 16 SADC countries reviewed, most are in the start-up phase. Although five countries are past the start-up phase, there is reason for concern, as these countries are digitalising rapidly, whilst their economies are emerging. The highest-rated country, Mauritius, has had a national cybersecurity strategy since 2014, and is at the end of its five-year cycle of implementation, with no other country close to this status. The ITU Global Cyber Security Index[79] for 2020 supports the claim that most Sub-Saharan countries, with the exception of Mauritius, Rwanda and South Africa, have low levels of cyber maturity. This covers the full spectrum of the index, from governance levels to responsiveness and development. Cyber security below the poverty line corresponds to a scarcity of resources relative to the scale of the threat. Most countries in this regional analysis demonstrated some fragments of national policies or strategies that referred to somehow to cybersecurity but were not overarching and lacked comprehensiveness. Please refer to Table 2 above for the summarisation of the development of cybersecurity strategy and policies in the SADC.

D1.2 Incident Response and Crisis Management

Incident Response and Crisis Management as a factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systemic way, while at the same time reviewing a government's capacity to organise, co-ordinate, and operationalise incident response, and whether cybersecurity has been integrated into the national crisis management framework.[80]

For this factor, the region is at a *start-up level* of maturity. Most of the countries that lack national cybersecurity strategies also have little or no routines for computer incident response and crisis management. Organisations for national-level cyber incident response are mostly lacking, as well as frameworks for national level crisis management. There are only four countries[81] at a *formative level* of maturity or higher in this factor. The regional study has observed that most SADC governments are lacking capacity to identify and determine characteristics of national level incidents in a systemic way.

In terms of organisation for incident response and crisis management, as depicted in Table 3, seven countries in the region have a national CSIRT/CSERTs in place, but coordination is minimal between them. For some of the CSIRT/CSERTs in place, it was hard to determine whether they are operational at all. As the countries are experiencing rapid development in digitalisation, they are also seeing a significant increase in cybercrime launched both externally and internally. The lack of tools for response and incorporating cybersecurity as a part of national crisis management makes the region increasingly vulnerable to bad actors. This is in line with previous findings in earlier CMM reviews, which demonstrate that government response is lacking.

[79] See ITU. (2020). *Global Security Index*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[80] See GCSCC. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[81] Malawi (avg. 2), Zambia (avg. 2), Mauritius (avg. 3,5), South Africa (avg. 3,5).

Table 3: Status of National CIRT/CERT/CSIRT by Country in the SADC

SADC Country	National CIRT/CERT/CSIRT
Angola	No CIRT
Botswana	https://www.cirt.org.bw
Comoros	No CIRT
Democratic Republic of the Congo	No CIRT
Eswatini	No CIRT
Lesotho	No CIRT
Madagascar	No CIRT
Malawi	https://mwcert.mw
Mauritius	http://www.cert-mu.org.mu
Mozambique	https://csirt.gov.mz
Namibia	No CIRT
Seychelles	No CIRT
South Africa	https://www.cybersecurityhub.gov.za
Tanzania	http://www.tzcert.go.tz
Zambia	http://www.cirt.zm
Zimbabwe	No CIRT

Source: AfricaCERT,[82] retrieved 19/10/2021

D1.3 Critical Infrastructure (CI) Protection

Critical Infrastructure Protection as a factor assesses a government's capacity to identify CI assets, the regulatory requirements specific to the cybersecurity of CI, and the implementation of good cybersecurity practices by CI operators.[83] As shown in Table 4, most SADC countries lack formal categorisation of CI assets. Cross-sector regulatory requirements for CI protection are also mostly lacking, except for in South Africa, Zambia and Zimbabwe, as well as good cybersecurity practices among CI-operators.

There are only three countries[84] in the *formative stage* of maturity or higher on average in this factor. This is cause for concern, as a disruption may have dire consequences across other sectors, as seen during the ransomware attack on the South African port and railway in 2021.[85] This risk continues to grow as traditional infrastructures

[82] See AfricaCERT. (n.d.). *African CSIRTs*. Retrieved March 5, 2022, from https://www.africacert.org/african-csirts/

[83] See GCSCC. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[84] Botswana (avg. 2), Mauritius (avg. 3), Malawi (avg. 2).

[85] See Gallagher, R. & Burkhardt, P. (2021, July 29). '*Death Kitty' Ransomware Linked to South African Port Attack*. Bloomberg. Retrieved March 5, 2022, from https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports

increasingly rely on digital infrastructures, both with regards to dependency and an increase of vulnerable surfaces to attack.

Table 4: Categorisation of Critical Infrastructure Assets in the SADC

Country	CI assets, sectors and operators	Cross-sector regulatory provisions for CI operators
Angola	-	-
Botswana	**Sectors:** finance, communications, energy, water, emergency services, food, public safety, health, public services and e-government[86]	-
Comoros	-	-
DRC	-	-
eSwatini	Critical information infrastructure[87]	-
Lesotho	-	-
Madagascar[88]	-	-
Malawi	**Proposed sectors:** Energy ICT Tourism Finance Mining Manufacturing & Industry Defence & Security Transport Government Research & Development Water Health Food & Agriculture Education Environment[89]	-
Mauritius	**Proposed sectors:** Financial services, tourism, ICT & broadcasting, health, government services, manufacturing, transport & logistics, sugar and customs[90]	-
Mozambique	-	-
Namibia	-	-

[86] See Republic of Botswana. (n.d). *National Cybersecurity Strategy*. Retrieved March 3, 2022, from https://www.bocra.org.bw/sites/default/files/documents/approved%20botswana-national-cybersecurity-strategy.pdf

[87] See ITU. (2020). *eSwatini National Cybersecurity Strategy 2020 – 2025*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Eswatini%20NCS%202020.pdf

[88] See GCSCC. (2016). *Cybersecurity Capacity Review of the Republic of Madagascar*. https://gcscc.ox.ac.uk/files/cmmrapportfinalcybersecuritemadagascarpdf

[89] See Koyabe, M. (2019). *Critical Information Infrastructure Protection: Commonwealth Perspective.* https://www.torchlightgroup.com/media/CTO-FCO-Critical_National_Information_Infrastructure_Protection.pdf

[90] See Republic of Mauritius. (2014). *National Cybersecurity Strategy 2014 – 2019.* https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Mauritius_2014_National%20Cyber%20Security%20Strategy%20-%202014%20-%20EN.pdf

Table 1 continued

Country	CI assets, sectors and operators	Cross-sector regulatory provisions for CI operators
Seychelles	-	-
South Africa	**Assets:** referred to as "National Key Points"[91] identified and listed[92]	National Key Points Act, 1980[93]to be replaced by Critical Infrastructure Protection Act 8 of 2019[94]
Tanzania	**Proposed sectors**: ICT, emergency services, energy, banking & finance, agriculture & livestock, manufacturing, trade & industry, transport, water, health, government & public services, tourism, education, research & innovation, culture, environment & natural resources, land & settlements, public, legal order and safety[95]	-
Zambia	Critical Information Infrastructure assets (not yet listed)	The Cyber Security and Cyber Crimes Act, 2021
Zimbabwe	-	-

NB: "-" means no evidence could be found

Source: C3SA (C3SA 2021) & GCSCC (CMM 2016 – 2020)

D1.4 Cybersecurity in Defence and National Security

Cybersecurity in Defence and National Security as a factor explores whether the government has the capacity to design and implement a strategy for cybersecurity within national security and defence. Further it also reviews the level of cybersecurity capability within the national security and defence establishment, and the collaboration arrangements on cybersecurity between civil and defence entities.[96] From this review, it emerged that there is only one country which, on average is at the formative level of maturity or further in this factor.[97]

---

[91] See National Key Points Act of the Republic of South Africa. (1980). *Government Gazette*. (No. 7134). https://www.gov.za/sites/default/files/gcis_document/201503/act-102-1980.pdf

[92] See De Wet, P. & Benjamin, C. (2015, January 22). National key points: The list you weren't meant to see. *Mail & Guardian*. Retrieved March 4, 2022, from https://mg.co.za/article/2015-01-22-national-key-points-the-list-you-werent-meant-to-see

[93] See National Key Points Act of the Republic of South Africa. (1980). *Government Gazette.* (No. 102). https://www.gov.za/documents/national-key-points-act-24-mar-2015-1016

[94] See Critical Infrastructure Protection Act of the Republic of South Africa. (2019). *Government Gazette*. (No. 8). https://www.gov.za/documents/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019-0000

[95] See Koyabe, M. (2019). *Critical Information Infrastructure Protection: Commonwealth Perspective.* https://www.torchlightgroup.com/media/CTO-FCO-Critical_National_Information_Infrastructure_Protection.pdf

[96] Botswana (maturity level 2), Mauritius (maturity level 3), Malawi (maturity level 2).

[97] Malawi (maturity level 2).

Most SADC countries have reflected upon the potential impact of cybersecurity on national security and defence, but impact assessments have not been formally articulated. The lack of impact assessments of cybersecurity on national security and defence is, of course, connected to the lack of cybersecurity strategies, as most countries lack such frameworks for handling cybersecurity. This becomes a structural issue with lack of professionals and competence on the thematic, as evident in limited specialist cybersecurity capability within the national security establishment. Further to this, the collaboration on cybersecurity between civil and defence entities is also limited.

RECOMMENDATIONS

Following the information presented during the study of the maturity of Cybersecurity Policy and Strategy, C3SA has developed the following set of recommendations for consideration by governments of member states and the secretariat of the SADC.

National Cybersecurity Strategy

R1.1 The SADC Secretariate should develop a programme that encourages and promotes the development of National Cybersecurity Strategies (NCSs) for nations in the SADC.

R1.2 The SADC Secretariate should develop, promote, manage, and measure the efforts put forth by the nations in the SADC to develop and uphold the proposed NCSs.

R1.3 Part of the promotion of the development of NCSs should include nations in the SADC prioritising the involvement of stakeholders from all sectors in the development of the NCSs.

R1.4 Furthermore, the nations should be encouraged to set aside budgets for the development, promotion, implementation, and monitoring of NCSs.

R1.5 Active funders in the cybersecurity capacity building community with high digitalisation competence and presence in the region should act as relevant partners for developing cybersecurity strategies but also raising awareness amongst decision-makers to understand the importance of such strategies.

R1.6 As most countries already have fragments of national policies or strategies, there is a need for streamlining efforts across countries, where actors such as the SADC Secretariat can be a relevant actor in fulfilling the aims/goals of all the nations in the SADC.

Incident Response and Crisis Management

R1.7 All nations should develop mechanisms for incident reporting that are regularly evaluated for effectiveness and establish a central registry of

national-level cybersecurity incidents to keep a record of cybersecurity incidents in both public and private sectors.

R1.8 The SADC Secretariat should also develop an organisation within itself to monitor the development and subsequent management of the cybersecurity incident registries for all SADC member nations.

R1.9 The SADC Secretariat should also budget and invest in the development of this organisation and further cyber capabilities through technical education and research.

Critical Infrastructure (CI) Protection

R1.10 To handle CI-assets, there is a need for each nation within the SADC to take internal steps in increasing capabilities, although it takes more than just using expertise and practices from abroad, each nation needs to develop new standards relevant to the cultural context in the region.

R1.11 All nations in the SADC official critical infrastructure asset lists which combine both private and public sector CIs. The list should be developed in consultation between government ministries and owners of CI assets.

R1.12 All nations should develop and implement the standards of the critical infrastructures that should be listed and those that require cybersecurity protection.

Cybersecurity in Defence and National Security

R1.13 The SADC Secretariat should coordinate with all member states to establish cybersecurity in national security and defence capability for the region.

R1.14 The SADC Secretariat should encourage and support the police and military forces of all the nations to develop cyber defence strategies and cyber defence infrastructures.

R1.15 The SADC Secretariat should include regional collaboration on cybersecurity within national security and defence in the Protocol on Politics, Defence and Security Co-operation

R1.16 Each nation should develop their own cyber defence strategies and cyber defence infrastructures and corporate with these to the SADC Secretariate to evaluate and assist in upholding these strategies and infrastructures.

D.2 Cybersecurity Culture and Society in SADC

With ever more users on the internet, cybersecurity must be considered a shared responsibility among users and other actors in society.[98] As described in the 2021 version of the CMM, Dimension 2 reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in internet services, e-government and e-commerce services, and users' understanding of personal information protection online. It also explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this *Dimension* reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.[99]

Figure 4 below depicts how many SADC countries had a start-up, formative, established, and strategic maturity stage in each aspect within Dimension 2 in two points in time, when the national CMM reviews were conducted (i.e.: 10 SADC countries had a CMM report during the period 2016-2020) and when this SADC regional report was completed (2021). Awareness of risks, priority of security, and practices are the three aspects included in factor D2.1 cybersecurity mindset. Digital literacy and skills, user trust and confidence in online search and information, disinformation, user trust in e-government services, and user trust in e-commerce services are the five aspects that form factor D2.2 trust and confidence in online services. Finally, we have three factors, with only one aspect in each factor: D2.3 user understanding of personal information protection online (whose aspect is named personal information protection online), D2.4 reporting mechanisms, and D2.5 media and online platforms (whose aspect is named media and social media).

To interpret Figure 4, consider, for example, the first aspect on the awareness of risks. The information from the CMM reports in 2016-2020 (labelled CMM 2016-20 in Figure 4) showed that all countries reviewed had a start-up maturity stage, except one which was formative. However, this regional study (labelled C3SA 2021 in Figure 4) found that, in 2021, the region was more mature in its awareness of risks. While eight countries had a start-up maturity stage, seven countries had a formative maturity stage, and there was a leading country with an established maturity stage. Although this regional analysis had limitations in finding evidence on all the aspects in Dimension 2 for all the SADC countries, the number of countries with no information has been reduced compared to the available information only from national CMM reports in the SADC. The analysis shows that, in 2021, the region had a low proportion of countries with start-up maturity stages specially in cybersecurity aspects related to reporting mechanisms and the role of media and social media in informing users on cybersecurity. Moreover, while those ten SADC countries reviewed previously (CMM 2016-20) had had formative or start-up maturity stages in the past, the results of this regional study show that, in 2021, the SADC region had more mature countries in all aspects included in Dimension 2 except digital literacy and skills, disinformation, and user trust in e-government services. The next subsections describe the regional level of maturity in the different factors within Dimension 2.

[98] Dutton, W. H. (2017). Fostering a cyber security mindset. *Internet Policy Review, 6*(1). https://doi.org/10.14763/2017.1.443

[99] See Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM).* https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

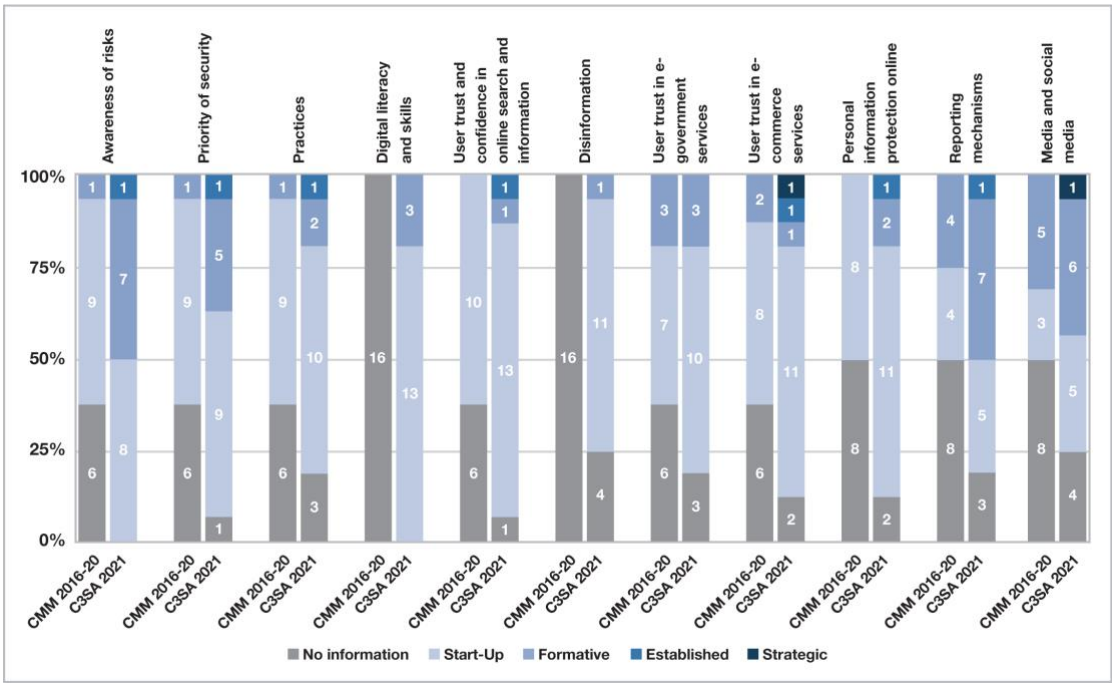

Figure 4: Number of SADC countries within each maturity stage for the CMM aspects of Dimension 2 "Cybersecurity culture and society".

Source: C3SA (C3SA 2021) & GCSCC (CMM 2016 – 2020)

D2.1 Cybersecurity Mindset

The cybersecurity mindset "evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society at large […] that increases the capacity of users to protect themselves online."[100] A strong mindset entails being aware of risks, prioritising cybersecurity and following safe cybersecurity practices, as a matter of routine.[101] Thus, cybersecurity awareness not only refers to the knowledge that users have about these cyberthreats, but also their ability to habitually put them in practice to recognise and avoid them, and knowing where and how to report suspicious activity when it occurs. A majority 95% of all cybersecurity breaches are linked to one or another form of human error.[102] In most SADC countries, the awareness of risks in the general public remains low and initiatives to raise awareness are uncoordinated. The urban areas as expected have a higher level of awareness compared to their rural counterparts. In the private sector, there is greater awareness in high-risk sectors such as finance/banking-related institutions. Though a few governments[103] have started to pursue cybersecurity awareness campaigns and initiatives that target their citizens, these efforts are mainly sporadic with few countries showing evidence of having initiatives such as a

[100] *See* Global Cyber Security Capacity Centre (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf.

[101] Ibid.

[102] See IBM Global Technology Services. (2014). *IBM Security Services 2014 Cyber Security Intelligence Index.* https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

[103] See Cybersecurity Tech Accord. (2020). *Cybersecurity Awareness in the Commonwealth of Nations*. https://cybertechaccord.org/uploads/prod/2020/03/TechAccord-awareness-06.pdf

cybersecurity awareness month. For instance, during the cybersecurity awareness month, Botswana developed a nationwide campaign to educate young people on cyber hygiene, which is mandated to protecting young people on how they can safely conduct themselves online.[104] Other countries, for instance Zambia, through the Zambian Cyber Security Initiative Foundation (ZCSIF), shared posts on social media[105] in raising awareness during their cybersecurity awareness month. In addition to these local initiatives, the SADC secretariat has in the recent past conducted some initiatives such as the SADC Regional Cyber Drill in Ebene, Republic of Mauritius to enhance the cyber-threat preparedness of SADC Member States. Such initiatives have also had the aim of intensifying awareness on the importance of cyber security at household and organisational levels.

The recent cybercrime legislations being developed by various member states in SADC is evidence of increasing level of prioritisation of cybersecurity in the respective countries' governments. Governments are engaging with laws like European Union's (EU) General Data Protection Regulation (GDPR) and ratification of the Malabo Convention and the SADC model law to address data protection[106] and computer crime and cybercrime,[107] engaging stakeholders to develop legislations around protection of internet users including minors and modifying various existing legislations to address various cybercrimes. In July 2021, South Africa's Protection of Personal Information Act (POPIA) came into effect. Within organisational settings, prioritisation of cybersecurity is unequally observed in the private sector and in specific sectors like within banking, finance and telecommunications. In general, however, the private sector is taking a lead in prioritising cybersecurity in most SADC countries.

Few amongst the general public are able to recognise security concerns.[108, 109] As a result, there is generally a low adoption of safe cybersecurity practices.[110] With the increased mobile adoption that is prevalent in not only SADC but across the wider SSA, practices related to mobile technology use are important in determining cybersecurity trends. Most phone users tend accept default settings when using mobile

---

[104] See Churu, J. (2021, October 6). *Network of Young Cybersmart Champions launched in Botswana*. https://www.biztechafrica.com/article/network-young-cybersmart-champions-launched-botswa/16811/

[105] See Zambian Cyber Security Initiative Foundation. (2021, December 8). *Home* [Facebook page]. Facebook. Retrieved March 25, 2022, from https:////www.facebook.com/ZCSIF/

[106] See ITU. (2013). Data Protection: *SADC model law on data protection.* https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[107] See ITU. (2013). *Data Protection: SADC model law on data protection*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[108] See Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing national cybersecurity awareness in Africa: An empirical study.

[109] See Calandro, E., & Berglund, N. (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC case. *In GIGAnet annual symposium. Berlin*. https://researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf

[110] See Zucule de Barros, M. J., & Lazarek, H. (2018). Comparative study of cybersecurity policy among South Africa and Mozambique. *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*, *2018-March*, 521–529.

technology apps, and rarely adjust settings for improved security.[111] However, in leading government agencies and large multinationals, there is generally better cybersecurity practices.[112] This may be linked to the availability of resources to invest in cybersecurity. With the changes taking place in the 4IR, including the pervasiveness of IoTs and BYOD trends, one of the challenges facing organisations is the lack of best practice policies to guide the use of such technologies, which may be increasing the susceptibility of organisations as targets for perpetrating cybercrime attacks in the SADC region.

D2.2 Trust and Confidence in Online Services

Internet users in SADC largely have a blind trust and do not critically assess the information that they see online.[113] Although countries in the SADC region acknowledge the issue of disinformation[114] as a crime, it is not clear in what way these are provisioned for in law. Currently, due to COVID-19 pandemic, disinformation is a pointed concern of most of the countries in the SADC region.[115] Countries for instance, South Africa and Zimbabwe prosecutes anyone sharing misinformation about the pandemic.[116, 117] However, the region shows limited evidence of initiatives that would be useful to curb disinformation.

While countries in SADC have implemented certain online services, such as e-government and e-commerce, there is lack of information about security and breaches, and no metrices to show the extent to which users trust such services. In general, the adoption of e-government and e-commerce is still very low in most SADC countries,[118] with varied levels of sophistication between the countries, and few used by any significant number of people.[119] For example, the wider form of payments for e-commerce that exists in SADC are related to financial transactions, including mobile

[111] See Markowitz, C. (2019). Harnessing the 4IR in SADC: Roles for Policymakers Occasional Paper 303. *South African Institute of International Affairs*, *October*, 1–47. https://media.africaportal.org/documents/Occasional-Paper-303-markowitz.pdf

[112] See Jenalda, M., & Kurebwa, J. (2020). Multilateral Responses to Cybercrimes in the SADC Region: *The Case of Zimbabwe and South Africa*. https://doi.org/10.3968/11946

[113] See Munyoka, W., & Maharaj, M. S. (2019). Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries. *SA Journal of Information Management*, *21*(1), 1–9. https://doi.org/10.4102/sajim.v21i1.983

[114] See Mawarire, T. (2020). "Things will never be the same again". *Covid-19 effects on freedom of expression in Southern Africa.* https://internews.org/wp-content/uploads/2021/02/Internews_Effects_COVID-19_Freedom_of_Expression_Southern_Africa_2020-12.pdf

[115] See Nganje, F. (2021). *Building Anticipatory Governance in SADC: Post-COVID-19 Governance Outlook.* https://media.africaportal.org/documents/Occasional-Paper-324-nganje.pdf

[116] See South African Government. (n.d.). Fake news-Coronavirus COVID-19. Retrieved March 6, 2022, from https://www.gov.za/covid-19/resources/fake-news-coronavirus-covid-19

[117] See Mutsaka, F. (2020, December 7). Zimbabwe arrests 2 men for selling fake COVID-19 results. Retrieved March 5, 2022, from https://apnews.com/article/arrests-zambia-zimbabwe-coronavirus-pandemic-6d8fc1964f5a152c5a0d1b71d4f5f9b0

[118] See Munyoka, W., & Maharaj, M. (2017, May). Understanding eGovernment utilisation within the SADC. In *2017 IST-Africa Week Conference (IST-Africa)* (pp. 1-10). IEEE.

[119] See Munyoka, W., & Maharaj, M. S. (2019). Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries. *SA Journal of Information Management*, *21*(1), 1–9. https://doi.org/10.4102/sajim.v21i1.983

banking and mobile money,[120] thereby necessitating institutions to consider trust in online payments and mobile money solutions. Few economies like South Africa, and Mauritius are leading the park and showing a higher and wider usage of e-government and e-commerce. Although transparent metrics on usage were not available for most countries, the UN e-government 2020 Index and the UNCTAD B2C e-commerce Index provide some insights. The 2020 e-government Index indicates that, while Africa has made progress in e-government in the last 10 years, nine of the sixteen SADC countries are still ranked in the last third of the countries worldwide,[121] with Mauritius being ranked as the best-performing country in SADC at rank 63, followed by Seychelles and South Africa ranking at 76 and 78, respectively. The UNCTAD B2C e-commerce index also ranks South Africa and Mauritius among the few top-ranked economies in Africa[122] with regards to e-commerce, with most of the other nations ranking yet again in the last third worldwide.

While a variety of factors may influence use of internet services, access to internet itself may be a major barrier to use, and a pre-requisite for a more nuanced understanding of why people may not be using services when they are readily accessible. The B2C e-commerce Index Report[123] notes that less than a third of the population in Africa uses the internet, compared to three quarters in Western Asia. And while seven out of 10 users access internet through mobile broadband, internet usage in most of SSA is still low at only 21%, compared to 80% in Europe.[124] In Mauritius, Seychelles, and South Africa, the three countries that also rank high in e-government and e-commerce use, the internet penetration stands at 64%, 59% and 56%, respectively (Figure 5).

[120] See Nyimbiri, B. A. (2021). The Impact of the Mobile Money on People's Use of Financial Services in Sub-Sahara Africa. *Management Dynamics in the Knowledge Economy*, *9*(1), 137-146.

[121] See United Nations. (2020). *E-Government Survey 2020: Digital Government in Decade of Action for Sustainable Development.* Retrieved February 11, 2022, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

[122] See United Nations Conference on Trade and Development. (2020). *The UNCTAD B2C e-commerce index 2020 Spotlight on Latin America and the Caribbean*. Retrieved from https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf

[123] Ibid.

[124] See GSM Association. (2021). *The Mobile Economy Sub-Saharan Africa 2021*. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf

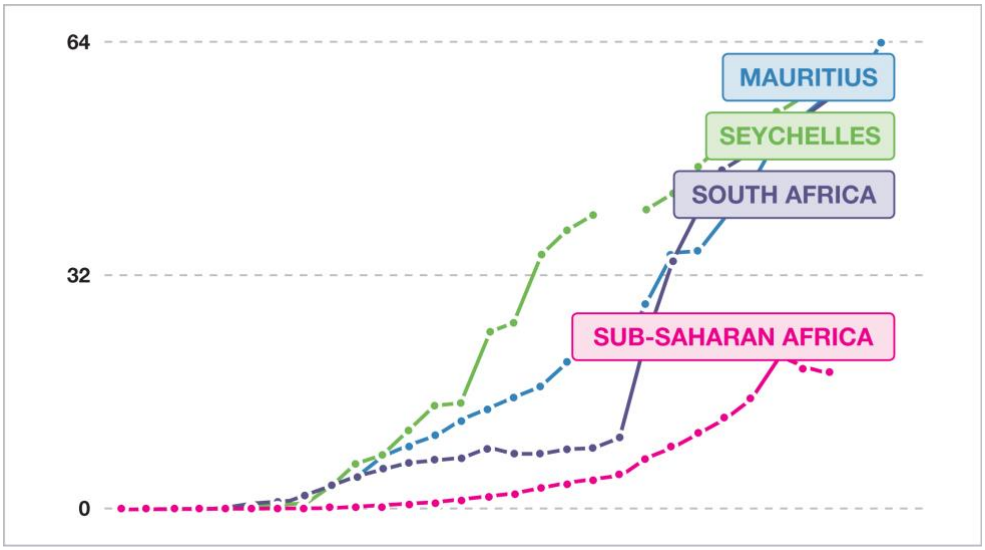

Figure 5: Individuals using the internet (% of population). (Source: World Bank)[125]

The factors that have been attributed to this low use include high cost of equipment and internet and lack of digital literacy skills (Figure 6). Digital literacy is generally low in SADC region. Unfortunately, with the exception of a few academic programs/courses that are not a privilege of all, there is no evidence of any programmes to support digital literacy.

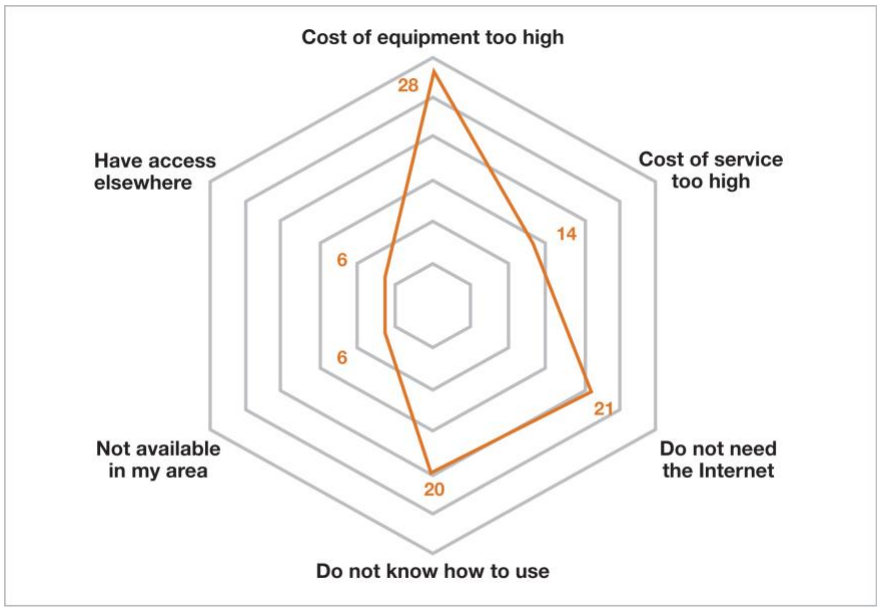

Figure 6: Barriers to the use in households
Source: RIA After Access Report[126]

[125] See World Bank Group. (2022). *Individuals using the internet (% of population)*. Retrieved March 5, 2022, from https://data.worldbank.org/indicator/IT.NET.USER.ZS

[126] Ibid.

Together with other specific measures, SADC will therefore need to overcome these challenges in order to promote and encourage the use of e-government and e-commerce. The trends in the low adoption, albeit not ideal, may be consistent with the observed trends on digital literacy and skills, the cost of accessing the internet for most users, as well as the lack of prioritisation of these areas, both in terms of creating a secure legal environment, as well as other enabling environments. “In order to flourish, e-commerce requires an accessible, predictable, safe and transparent trading environment, which operates across territorial borders and jurisdictions”.[127] Another major impediment to the adoption of e-commerce is linked to trust, where most users lack a fundamental trust in e-commerce.[128] Specifically, there is a higher level of distrust of online information among those who have not used or experienced the technology.[129] Since internet penetration is still low in developing countries, the low levels of trust and confidence observed in online services in SADC may not be unusual.[130] Together with measures to promote internet access and increasing digital literacy to empower users on best practices for using the internet, increasing the level of trust and confidence will be crucial to the increased use of online services.

Other reasons why and whether trust is influenced by cultural issues may need to be further studied in order to inform the formulation of context-specific policies and initiatives that will improve trust. It is, however, encouraging that most stakeholders in the region are cognisant of the need for e-commerce security in order to increase adoption.[131]

D2.3 User Understanding of Personal Information Protection Online

“This *factor* looks at whether internet users and stakeholders within the public and private sectors recognize and understand the importance of protecting personal information online, and whether they are sensitive of their privacy rights” (p. 21).[132] While it is encouraging to see that governments in SADC are increasingly acknowledging the need for different laws and policies to promote protection of personal data (Table 4), the slow pace of such laws coupled with a lack of understanding on the need for protecting personal information among users, is encumbering developments in the SADC, and thereby creating an enabling environment for cybercrimes that target users’ information.

Some of these laws have not yet been fully implemented and though there are legislations that mandate regulators to be on the lookout for infringements, their

---

[127] See ITU. (2012). Draft Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce. Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA). https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/electronic%20transaction.pdf

[128] See Verkijika, S. F., & De Wet, L. (2018). A usability assessment of e-government websites in Sub-Saharan Africa. *International Journal of Information Management*, *39* (September 2017), 20–29. https://doi.org/10.1016/j.ijinfomgt.2017.11.003

[129] See Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology. *Information, Communication & Society*, *9*(4), 433-451.

[130] See Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. *Personal and Ubiquitous Computing*, 1-15.

[131] See Mannion, C. (2020). Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets. *Vanderbilt Law Review, 53,* 685.

[132] See GCSCC. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM).* https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

adoption and enforcement may still be weak and lacking. Others may yet to be adapted for the online environment.

The *Data Protection: Southern African Development Community (SADC) Model Law*[133] was developed with the aim of ensuring that the region has a regionally and globally harmonized data protection legislation. One important feature of the of the model law was the establishment of data protection authorities entrusted with a responsibility to combat the violation of users' data privacy rights.[134] The extent to which the model law has been beneficial is not clear as the pace of promulgation and implementation has been slow. However, the SADC Secretariat has embarked on a process to revise and modernized it.[135]

Countries like Angola, Mozambique, and Zimbabwe have no specific data protection law and therefore rely on various laws to impose privacy obligations. Zimbabwe's Access to Information and Protection of Privacy Act offers partial regulation; only governing the use of personal data by public bodies. Inevitably, this implies that use of data by private bodies is not governed legally, thus creating potential loopholes for cybercrime. The draft Data Protection Bill which has been under consideration by the Zimbabwean Cabinet since 2015, is said to address the gaps on the part of governing both private and public bodies.

Countries that have a specific data protection law include Botswana, DRC, Swaziland, Lesotho, Madagascar, Mauritius, Seychelles, South Africa, and Zimbabwe. However, while most of the member states have passed these laws, some do not yet enforce them. For example, Lesotho has had a data protection act since 2013, to provide for principles for the regulation of processing of personal information. To date, the law has not been enforced nor has the commission that the law envisaged been established.[136] Similarly, in the Seychelles, the Data Protection Act that was enacted in 2003 has not yet come to effect. Among those that have enacted the laws, Mauritius and South Africa are ahead of the park. The Data Protection Act of 2017 (DPA) for Mauritius is aligned with the EU's GDPR and the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data.[137] It is also one of the few countries in SADC together with Angola, Mozambique, and Namibia that has ratified the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). Other SADC countries that have signed but not yet ratified the convention as of June 2020 are Comoros and Zambia.[138] In South Africa, POPIA came into effect

---

[133] ITU. (2013). *Data Protection: Southern African Development Community (SADC) Model Law.* Retrieved March 5, 2022, from https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[134] Ibid.

[135] SADC. (2022). Consultancy for revision and modernisation of the SADC data protection model law. Retrieved March 7, 2022, from https://www.sadc.int/files/8216/4400/4803/CONSULTANCY_FOR_THE_SADC_DATA_PROTECTION_MODEL_LAW_04022022.pdf

[136] See Mudavanhu, E. (2021, April). *Lesotho - Data Protection Overview*. Retrieved February 10, 2022, from https://www.dataguidance.com/notes/lesotho-data-protection-overview

[137] See Oozeer, A. (2021, April). *Mauritius - Data Protection Overview*. Retrieved February 10, 2022, from https://www.dataguidance.com/notes/mauritius-data-protection-overview

[138] See African Union (2014, June 27). *African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/sites/default/files/treaties/29560-sl-

on 1 July 2020, and all organisations that collect personal data were required to comply as of 1 July 2021.

Zambia, Malawi, Comoros, and Namibia do not have a data protection law, and therefore regulate data privacy and protection issues through the Electronic Transactions and Cybersecurity/Communications Act (ECTA). In Malawi, the ECTA law will be superseded by the Data Protection and Privacy Bill, whose drafting was announced in 2019.[139] Namibia has not enacted a comprehensive data privacy legislation, and, therefore, relies on sector-specific laws to protect client information.[140]

While these efforts for ratification and enforcement of laws need to be fast-tracked, they need to be combined with efforts to educate users on some of the already promulgated laws and on the importance of their information being protected. Such steps will empower the users/citizens to demand stakeholders to provide the necessary legal environment. The data revealed that there is some awareness of the risks of sharing personal information online among a few savvy internet users. In countries like South Africa, that are leading regionally in adoption and use of internet, a growing proportion of users have the skills to manage their privacy online, and protect themselves from intrusion, interference, or unwanted access of information by others.[141] However, a majority of users from the general public have minimal or no knowledge about how their personal information is handled online.[142] Users also tend to give away their personal details too easily, and do not read terms and conditions or critically assess websites and associated risks.[143] Those who know about data protection do not believe that adequate measures have been established nationally to ensure the protection of their personal information online.[144] This may be attributed to the slow progress in enforcement of the existing laws.

D2.4 Reporting Mechanisms

Reporting mechanisms that function as channels for users to report internet-related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other cyber-related incidents, are an important step to building cybersecurity capacity. A cybersecurity report[145] noted that 90% of cybercrime cases were not reported, and metrics of reported incidents are scarcely available in

AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

[139] See Kainja, J. (2021, June 22). *Data Protection Law on the Horizon in Malawi*. CIPESA. Retrieved March 16, 2022, from https://cipesa.org/2021/06/data-protection-law-on-the-horizon-in-malawi/

[140] See DL Piper. (2021, December 7). *Global Data Protection Laws of the World – Namibia*. DLA Piper Global Data Protection Laws of the World. Retrieved March 6, 2022, from https://www.dlapiperdataprotection.com/index.html?t=law&c=NA&c2=

[141] See ITU. (2021). Digital Trends in Africa 2021. *Information and communication technology trends and developments in the Africa region 2017-2020*. https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf

[142] See Ilori, T. (n.d.). Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions. 1–18.

[143] See Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on Facebook social media: Facebook. *South African Journal of Sciences*, *114*(5), 1–5. http://www.sajs.co.za

[144] See Munyoka, W., & Maharaj, M. S. (2019). Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries. *SA Journal of Information Management*, *21*(1), 1–9. https://doi.org/10.4102/sajim.v21i1.983

[145] See Serianu. (2018). Cyber security Report-Lesotho. *Cyber security skills gap.* https://www.serianu.com/downloads/LesothoCyberSecurityReport2018.pdf

SADC. Indeed, most people do not know to whom, and how they ought to report cybercrime.[146] The general lack of knowledge on how to deal with cybercrime occurrences means that many cybercrime cases go unreported.[147] Some users do not report cybercrime because they may feel that an incident is not serious enough to warrant reporting, or that the process is a waste of time since there is little chance of a successful prosecution.[148] While the former may be the result of the lack of knowledge, the latter may be attributed to the lack of faith in law enforcement and other agencies that are supposed to attend to cybercrime cases.[149]

There are scarcely any centrally dedicated mechanisms to enable citizens to report computer-related or online incidents and crimes. The study also revealed that reporting structures and mechanisms are limited, and uncoordinated. In fact, most of initiatives identified are used in an ad-hoc manner for example, in Mozambique, MoRENet, Mozambique Research and Education Network, established by the Ministry of Science and Technology in 2005 provides channels for students and teachers to report cybercrime. Zambia CIRT provides a reporting page on their website. In Swaziland and Zimbabwe, the police force provides channels for reporting cyber-crimes. However, once cyber incidents are reported through existing channels, the requisite stakeholders do not take any preventive or supporting actions. In general, whether and what mechanisms exist for reporting cybercrime in SADC could not be sufficiently accessed through this study and would require further research.

Thus, the lack of knowledge on reporting structures and on how to deal with cybercrime issues both by the users and law enforcement actors, coupled with the vague and inadequate reporting channels, a lax cybersecurity legal environment, and inaction by the requisite stakeholders in taking any preventive or supporting actions may be creating an enabling environment for cybercriminals to continue to thrive.

D2.5 Media and social media

Internet penetration has improved with rates exceeding the 50% mark in at least seven of the SADC countries, viz.: Eswatini, Mauritius, Namibia, Seychelles, South Africa, Zambia and Zimbabwe.[150] However, the cost of the internet, especially in most SADC countries, is high, and has generally hampered internet usage.[151] Among those who use internet in Africa, social media (Facebook, WhatsApp and Twitter) is the main driver of use. Thus, a large percentage of individual internet users spend most of their

[146] See Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of cybersecurity: A South African context. *Acta Criminologica: African Journal of Criminology & Victimology*, *31*(3), 111-131.

[147] Ibid.

[148] See Choo, K.K.R. 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

[149] See Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of cybersecurity: a South African context. *Acta Criminologica: African Journal of Criminology & Victimology, 31*(3), 111-131 https://sahs.ukzn.ac.za/wp-content/uploads/2019/07/PUBLIC-PERCEPTIONS-OF-CYBERSECURITY-A-SOUTH-AFRICAN-CONTEXT.pdf

[150] See Kubatana. (2020, October 2). *An analysis of Social Media use in the SADC region 2014 – 2020*. Retrieved February 10, 2022, from https://kubatana.net/2020/10/02/an-analysis-of-social-media-use-in-the-sadc-region-2014-2020/

[151] Ibid.

time on social media.[152] A report by Media Institute for Southern Africa Zimbabwe (MISA)[153] shows that social media contributes to the creation and circulation of news. About 37% of social media users in SADC either create comment on news or share it with others.

With regards to cybersecurity, however, there are limited discussions on social media about cybercrime matters. A small number of private organisations and NGOs in SADC run ad-hoc campaigns on social media for people to be aware of certain types of cyber risks.[154, 155] However, it would appear that the spectrum of cybersecurity issues covered is narrow. In countries like Zimbabwe, where mobile money is popular, most of the campaigns are related to mobile money scams[156] of which others ought to be aware.

While there are no specific laws that solely address data protection on social media use in the region,[157] social media use does not operate in a legal vacuum. SADC model laws addresses social media use concerning aspects related to electronic transaction,[158] cybercrime[159] and data protection.[160] The general use of social media for whistleblowing, however, may still be hampered by the limiting environment related to freedom of speech and expression. Some governments, notably Zambia, Zimbabwe, Angola, and the DRC, have threatened to shut down media or regulate it heavily and increase surveillance whenever there has been disparaging news, or during sensitive and political events such as the elections process.[161]

---

[152] See Research ICT Africa. (2018). *After Access*. Retrieved February 17, 2022, from https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

[153] See Kubatana. (2020, October 2). An analysis of Social Media use in the SADC region 2014 – 2020. Retrieved February 10, 2022, from https://kubatana.net/2020/10/02/an-analysis-of-social-media-use-in-the-sadc-region-2014-2020/

[154] See Zambian Cyber Security Initiative Foundation. (2021, December 8). *Home* [Facebook page]. Facebook. Retrieved March 25, 2022, from https://www.facebook.com/ZCSIF/

[155] See Cyber4Dev. (2020, November 18). *Young people of Botswana find creative ways to promote Cyber Resilience.* Retrieved February 16, 2022, from https://cyber4dev.eu/2020/11/18/young-people-of-botswana-find-creative-ways-to-promote-cyber-resilience/

[156] See Kwaramba, M. (2020, October 14). *Zimbabwe's restrictions on mobile money punish the users, not the offenders*. Retrieved March 10, 2022, from https://www.theafricareport.com/45825/zimbabwes-restrictions-on-mobile-money-transfers-punish-the-users/

[157] Ibid.

[158] See ITU. (2012). Draft Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce. *Support for Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA)*. https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/electronic%20transaction.pdf

[159] See ITU. (2013). *Data Protection: Southern African Development Community Model Law*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[160] See ITU. (2013). *Data Protection: Southern African Development Community Model Law*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[161] See Kubatana. (2020, October 2). *An analysis of Social Media use in the SADC region 2014 – 2020*. https://kubatana.net/2020/10/02/an-analysis-of-social-media-use-in-the-sadc-region-2014-2020/

With regards to general media, almost all SADC countries, with the exception of Mauritius and South Africa, show limited and ad-hoc coverage of cybersecurity issues. Where present, media mainly covers sensational cyber-related issues.

RECOMMENDATIONS

Following the information presented during the study of the maturity of *Cybersecurity Vulture and Society,* C3SA has developed the following set of recommendations for consideration by governments of member states and the secretariat of the SADC.

Cybersecurity Mind-set

R2.1 Cybersecurity practices need to be communicated widely, and prioritised. Governments and organisations may use incentive mechanisms, such as providing tax rebates, based on cybersecurity parameters or including cybersecurity standards as part of contracts to encourage private and public sector actors to prioritise the dissemination of good cybersecurity practices within their structures and processes.

R2.2 Create and deliver cybersecurity risks and threats webinars and workshops to all government ministries and organise more of such workshops within SADC region, providing guidance on good practice.

R2.3 Establish teams across governments who can answer questions about and advocate for cybersecurity standards and practices.

R2.4 Prioritise national surveys to assess attitudes and behaviour in public and private sectors to guide the implementation of cybersecurity measures, in order for the SADC countries to know where the gaps can be found.

R2.4 Given the critical mass of the internet and social media users across the region, governments should utilise traditional and social media channels more intensively to share information on incidents and best practices and to promote a proactive cybersecurity mind-set across different sectors and covering the diverse online vulnerabilities beyond financial scams.

Trust and Confidence in Online Services

R2.5 Encourage internet service providers (ISPs) to establish programmes that promote trust in their services, and that promote protection of user data online.

R2.6 With the increased dependence on the internet to access products and services necessitated by the COVID-19 pandemic, SADC countries needs to prioritise both national and regional e-government and e-commerce.

R2.7 Countries need to facilitate more inclusive e-commerce and e-government, SADC countries would benefit from exploring measures to reduce the cost of access to the internet and to provide access to remote areas.

R2.8 Countries and stakeholders also need to prioritise research that is aimed at understanding trust and confidence in the internet, as well as other relevant attitudes, values, and behaviour of users with respect to cyber security, such as privacy.

R2.9 SADC countries should increase and prioritise digital literacy initiatives aimed at educating internet users on threat detection and navigation on online platforms to minimise risks.

User Understanding of Personal Information Protection Online

R2.10 Operationalise the legal environment on data protection, including ratifying the Malabo Convention, adapting the SADC model law on data protection to a given country's needs, and tightening the law enforcement frameworks.

R2.11 SADC countries should prioritise the establishment of the independent data protection commissions as envisaged by the various data protection laws and ensure these laws are adapted to the online environment.

R2.12 The SADC Secretariat ought to coordinate the establishment of awareness raising initiatives in collaboration with civil society and the private sector to promote users' understanding on the importance of protecting personal information online. Such initiatives need to be both region-targeted, so that countries can learn from each other, and country-specific, to address national specific needs.

Reporting Mechanisms

R2.13 SADC countries ought to prioritise the establishment of national incident response teams.

R2.14 SADC secretariat should improve SADC states' coordination of reporting mechanisms and track reported incidents.

R2.15 SADC secretariat should develop standard metrics to report incidents to CSIRTs.

R2.16 SADC countries should work with stakeholders from the private sector, from civil society, and from academia to prioritise the establishment of centralised reporting mechanisms with clear channels that target users with and without internet access. These may include a telephone hotline, a website and, if possible, a localised mobile app for reporting and addressing cyber incidents.

R2.17 The SADC Secretariat should promote cybercrime knowledge sharing as a means to increase awareness, by learning from the experiences of different SADC countries. Countries can do this by collaborating with private organisations and other civil societies to provide channels that encourage people to speak up and share their experiences in a safe, free environment protected by the requisite legal laws.

R2.18 SADC countries ought to exploit mass media as well as social media for threat-reporting and to raise awareness of cybersecurity.

R2.19 SADC countries ought to use social media for education and awareness of cybersecurity related issues in the general public. Media institutions, news generators and other cybersecurity experts should be encouraged to use social media to engage with the general public and to conduct various campaigns to create awareness and share safe cyber practices.

R2.20 Governments, private and civil society organisations ought to work together to ensure digital rights and promote responsible social media use by creating advocacy against freedom of expression violations and accompanying laws and litigation to protect citizens from potential harms to each other that are propagated on social media.

D.3 Building Cybersecurity Knowledge and Capabilities in SADC

Dimension 3 relates to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, professional training programmes, and research and innovation. This *Dimension* reviews the availability, quality, and uptake of programmes for various groups of stakeholders, including the government, private sector, and the population as a whole.

Figure 7 displays how many SADC countries had a start-up, formative, and established maturity stage in each aspect within Dimension 3 in two points in time, when the national CMM reviews were conducted (ten SADC countries had a CMM report during the period 2016-2020), and when this SADC regional report was completed (2021). Awareness-raising initiatives by the government, the private sector, and civil society, joint with executive awareness raising, are the four aspects included in Factor D3.1-Building Cybersecurity Awareness. Provision and administration are the two aspects that form factor D3.2-Cybersecurity Education. Provision and uptake are the two aspects within factor D3.3-Cybersecurity Professional Training. Finally, 'Cybersecurity Research and Development' is the only aspect that forms factor D3.4-Cybersecurity Research and Innovation.

In order to interpret Figure 7, consider for example the first aspects on awareness-raising initiatives driven by government, the private sector, and civil society. The previous editions of the CMM do not distinguish between initiatives by these different actors but offer an overall picture of programmes by means of which to raise cybersecurity awareness. The information from the ten SADC countries reviewed between 2016 and 2020 (labelled CMM 2016-20 in Figure 7) showed that six countries were start-up in awareness raising while four countries were formative. This regional study (labelled C3SA 2021 in Figure 7) found that, in 2021, there were some countries with even established maturity stages in awareness raising initiatives, and that the region had a higher proportion of start-up countries in initiatives driven by governments than in initiatives driven by the civil society or the private sector. Although this regional analysis had limitations in finding enough evidence on all the aspects in Dimension 3 for all the SADC countries, some changes over time can be observed. While those ten SADC countries reviewed previously (CMM 2016-20) had had formative or start-up maturity stages in the past, this regional study shows that, in 2021, there was a minority of SADC countries with an established maturity stage in the aforementioned aspects related to awareness-raising initiatives and, moreover, in the provision of education, the uptake of professional training, and cybersecurity research and development. The next subsections describe the regional level of maturity in the different factors within Dimension 3.

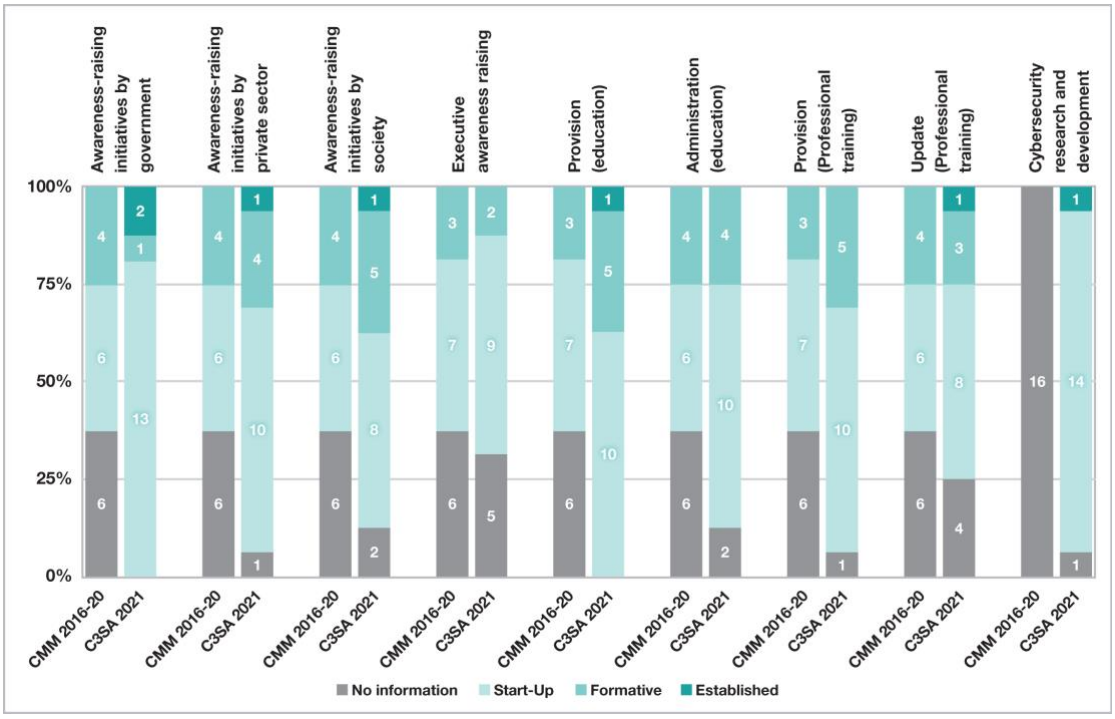

Figure 7: Number of SADC countries within each maturity stage for the CMM aspects of dimension 3 "Building cybersecurity knowledge and capabilities".

Source : C3SA (C3SA 2021) & GCSCC (CMM 2016 – 2020)

The SADC has aspirations to join in the 4th Industrial revolution as implied by its Protocol on Transport, Communications and Meteorology,[162] e-SADC Strategic Framework,[163] and Regional Indicative Strategic Development Plan (RISDP) 2020–2030.[164] The RISDP has sections on skills development, and on the development of cybersecurity capacity. Furthermore, a recent ministerial summit ended with a call to promote cybersecurity through the establishment of national CIRTs and the development of relevant skills.[165]

D 3.1: Building Cybersecurity Awareness

Cybersecurity awareness raising initiatives have been limited in regularity, scope, and scale across the SADC region, however, there has been a little upsurge in activities since the start of the COVID-19 pandemic restrictions. The stages in cybersecurity awareness raising capacity and the levels of cybersecurity awareness in the region

[162] See SADC. (1996). *Protocol on Transport, Communications and Meteorology.* Retrieved March 6, 2022, from https://www.sadc.int/files/7613/5292/8370/Protocol_on_Transport_Communications_and_Meteorology_1996.pdf

[163] See SADC. (2010). *e-SADC Strategic Framework.* Retrieved March 15, 2022 from https://repository.uneca.org/bitstream/handle/10855/21168/32387.pdf?sequence=3&isAllowed=y

[164] See SADC. (2020). *SADC Regional Indicative Strategic Development Plan (RISDP) 2020–2030.* Retrieved February 2, 2022 from https://www.sadc.int/files/4716/1434/6113/RISDP_2020-2030_F.pdf

[165] See SADC. (July 2021). SADC Ministers of Transport, ICT, Information and Meteorology meet to discuss sectoral issues. Retrieved March 17, 2022, from https://www.sadc.int/news-events/news/sadc-ministers-transport-ict-information-and-meteorology-meet-discuss-sectoral-issues/

have remained low, and at a *Start-up* stage on the CMM scale.[166] This situation has not changed with the imposition of COVID-19 pandemic restrictions which saw more awareness raising initiatives deployed to curb internet-disseminated misinformation around the disease and growing fraudulent practices. However, with the exception of South Africa, and to a lesser extent Mauritius, no other country implemented metrics to evaluate the quality and the effectiveness of programmes on targeted populations.[167]

SADC countries are low to middle income economies and are still in the process of developing adequate digital infrastructures. The digitisation of public services is slow and concentrated in key urban centres. In 2021, at the time of the review, in most cases cybersecurity strategies, policies, legislations, and relevant regulatory institutions were less than 5 years old; this contributed to poor implementations due to a lack of experience. Despite the popularity of mobile telephony, computer literacy remains low. Key informants, and previous CMM reports indicated that the levels of awareness were perceived to be low among the general public and a notch better among the executives in the public and private sectors. The maturity level had remained the same with slight improvements from when the COVID-19 pandemic restrictions were imposed.

The private sector is more active than the public sector in terms of raising levels of awareness especially due to its exposure to international standards and best practices in its supply chain dealings. However, there are elements working against the efforts of growing cybersecurity awareness in the countries. Research shows that in other parts of the world increases in awareness raising initiatives did not result in noticeable changes in the levels of awareness.[168] Countries in the global north have a longer history with ICTs through wide and ingrained communication of ICT-related research and innovation, regulation enactment and enforcement, and socio-economic alignment with international standards and best practices. Although it is challenging to estimate the level of awareness in SADC countries, there is ground to believe that cybersecurity awareness raising initiatives alone would not suffice[169, 170] to generate a meaningful change in mindset.[171]

The content of awareness raising programs has mainly focused on the harm that would ensue if security ordinances were not followed. However, narratives about how to protect oneself, family, friends, and belonging could have a greater impact.

---

[166] See Bada, M., Von Solms, B., & Agrafiotis, I. (2018). Reviewing national cybersecurity awareness in Africa: an empirical study. *Proceedings of the Third International Conference on Cyber-Technologies and Cyber-Systems, Cyber 2018, Greece,* 78-83. https://www.thinkmind.org/index.php?view=instance&instance=CYBER+2018

[167] See campaigns advertised on http://cybersecurity.ncb.mu, which is managed by CERT-MU of Mauritius and the South African National Cybersecurity Awareness Portal at https://www.cybersecurityhub.gov.za/cyberawareness/, managed by the Department of Telecommunication and Postal Services

[168] See Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy, 9*(1), 280-306. https://doi.org/10.5325/jinfopoli.9.2019.0280

[169] See Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness for Users and Executives in Africa. *https://arxiv.org/ftp/arxiv/papers/1910/1910.01005.pdf*

[170] See Van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?. *Journal of Cybersecurity*, *6*(1), doi: 10.1093/cybsec/tyaa019

[171] See Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint.* arXiv:1901.02672.

.

D 3.2: Cybersecurity Education

The situation of cybersecurity education in the SADC is concerning, taking into account the emerging sophistication of cyberthreats and risks. Africa has become a serious target for cybercriminals, especially since the COVID-19 pandemic restrictions were imposed. The cybersecurity education in the SADC region is at a *start-up to formative* stage. There is a need for the region to address the gap with urgency due to the noted rise of cyberthreats.[172]

Cybersecurity is offered as a module or a component in computer science and related courses at higher education institutions in the SADC. At the time of writing, primary and secondary schools were still not adequately engaged with these topics. There are few qualified cybersecurity educators available and there are no local programmes for their training. Some universities, particularly in South Africa and Mauritius, and to a lesser extent in Botswana, Namibia, and Zimbabwe, have started to offer speciality cybersecurity courses and short courses, issuing certifications and qualifications. However, this is not enough for the needs of the respective countries. The need for cybersecurity education has been identified at a policy level. However, not enough is done to remedy the situation. Governments are still trying to improve digital literacy amongst the population; cybersecurity is still not an educational priority in the region. There are projects to open cybersecurity specialised schools by the private sector. However, this may take time due to the slow process in obtaining accreditation from government and education boards in host countries. Respective Ministries of education and primary and secondary education boards are yet to frame cybersecurity into curricula either as a topic, a module, or an entire course. Higher Education ministries and boards in most SADC countries have started discussions to create cybersecurity qualifications in the tertiary education.

There is also an issue of *brain circulation,* where young graduates emigrate to get employment, better earnings, and better living conditions. This makes it difficult for countries in the region to resource educational programmes. Such a lack of cybersecurity capacity in terms of skills and competences makes it challenging to implement cybersecurity strategies, leaving sub-Saharan Africans exposed when participating in the global digital commerce to connect, learn, buy, and sell.[173]

D 3.3: Cybersecurity Professional Training

The SADC is barely starting to provide professional cybersecurity training. Except for South Africa, Mauritius, Namibia, and Botswana, all the other countries offer few to no cybersecurity professional training programmes.[174] Professional training is mainly offered by higher education institutions, some national ICT regulators, affiliated private education institutions including NGOs and *for-profit* companies, technology vendors, as well as academic and other centre of excellence. Even though the public sector is present in this market, the private sector dominates it. Training is mainly available in urban agglomeration, and in areas where the internet is reliable. Online courses are

---

[172] See John, S. N., Noma-Osaghae, E., Oajide, F., & Okokpujie, K. (2020). Cybersecurity Education: The Skills Gap, Hurdle!. In *Innovations in Cybersecurity Education* (pp. 361-376). Springer, Cham.

[173] See Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter?. *Journal of Information Policy*, *9*, 280-306. https://doi.org/10.5325/jinfopoli.9.2019.0280

[174] See Lemauricien (2020, September 20). *Cybersécurité : Création d'un centre de formation régionale à Maurice*. Retrieved January 28, 2022, from https://www.lemauricien.com/actualites/cybersecurite-creation-dun-centre-de-formation-regionale-a-maurice/378283/

sought after for training. Metrics are not deployed to evaluate initiatives and to determine the magnitude of the need in skills and competences in the countries.

Most of the time, local centres and institutes only offer core IT certifications from reputed vendors such as CISCO™, IBM™, Huawei™, Amazon™ or Microsoft™, which have cybersecurity components in them. Some of them also offer governance and managerial certifications such as COBIT™ and ITIL™, which have cybersecurity policy components. Few institutions in the region offer cybersecurity certifications, for instance, ISACA certification training courses, but the demand for such courses is growing.

The shortage in cybersecurity skills and competences has been identified at country and regional levels; however, the uptake varies from one country to the next. Countries with better cybersecurity capacity levels have witness a noticeable growth in enrolment, while countries with less capacity are not managing to entice many into cybersecurity professions.

D 3.4: Cybersecurity Research and Innovation

Cybersecurity research and innovation in the SADC region is at a *start-up* stage. Except for South Africa, Mauritius, and to a lesser extent Botswana, Namibia, and Zimbabwe, there is limited research at universities. Further to this, there are a few innovation and business incubators pushing out some products and services, however, there were no national or regional research programmes on cybersecurity, making it difficult to understand local contexts, to identify and develop products and services for the cybersecurity needs of the region, and to create trust and confidence for local users as they participate in the cyberspace for social connections, work, entertainment, and commerce.

RECOMMENDATIONS

Based on the information gathered in the review of the maturity on *Building Cybersecurity Knowledge and Capabilities*, C3SA has developed the following set of recommendations for consideration by governments of member states and the SADC secretariat.

Building Cybersecurity Awareness

R3.1 The SADC secretariat should recommend to all member states to collaborate on the development of strategies and programmes for cybersecurity awareness-raising.

R3.2 Governments in SADC should collaborate with the public sector and civil society to develop and deploy targeted, relevant, and regular countrywide cybersecurity awareness-raising campaigns.

R3.3 Governments in SADC, with the involvement of the private sectors and civil society, should collaborate to develop and deploy metrics that

assess awareness-raising programs and the level of cybersecurity awareness in members states and for the region.

Cybersecurity Education

R3.4 Governments in SADC, with the involvement of the private sectors and civil society, should collaborate to develop and implement cybersecurity qualifications in secondary and tertiary education.

R3.5 The SADC secretariat should collaborate with members states to develop a model framework which would assist member states in the implementation of cybersecurity education at all levels.

Cybersecurity Professional Training

R3.6 Governments of SADC member states should collaborate with private sector and civil society to promote cybersecurity professional training

R3.7 Governments in SADC should develop and deploy metrics to assess the production and circulation of cybersecurity skills in their countries

Cybersecurity Research and Innovation

R3.8 Governments in SADC should collaborate with private sector and civil society to promote, support and even initiate cybersecurity research and innovation to enhance the understanding of local cybersecurity context, and the development of cybersecurity product and services relevant to local needs.

D.4 Cybersecurity Legal and Regulatory Frameworks in SADC

Dimension 4 examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies, and court capacities. Moreover, Dimension 4 assesses issues such as formal and informal co-operation frameworks to combat cybercrime.[175]

Figure 8 below shows the number of SADC countries a start-up, formative, and established maturity stage in each aspect within Dimension 4 in two points in time, at first, when the national CMM reviews were conducted (ten SADC countries had a CMM report during the period 2016-2020), and then, when this SADC regional report was completed (2021). Substantive cybercrime legislation, legal and regulatory requirements for cybersecurity, procedural cybercrime legislation, and human rights impact assessment are aspects under factor D4.1 legal and regulatory provisions national cybersecurity strategy. Data protection legislation, child protection online, consumer protection legislation, and intellectual property legislation are the four aspects that form factor D4.2 on related legislative frameworks. Law enforcement, prosecution, courts, and regulatory bodies are the four aspects within factor D4.3 legal and regulatory capability and capacity. Finally, law enforcement co-operation with private sector, co-operation with foreign law enforcement counterparts, and government-criminal justice sector collaboration are the three aspects that form factor D4.4 formal and informal co-operation frameworks to combat cybercrime.

To interpret Figure 8, consider for example the first aspect on substantive cybercrime legislation. The information from the ten SADC countries reviewed between 2016 and 2020 (labelled CMM 2016-20 in Figure 8) showed that only two countries had a start-up maturity stage, six countries were formative, and two were established. This regional study (labelled C3SA 2021 in Figure 8) found that, in 2021, there were four countries with an established maturity stage, while seven countries were formative and five were start-ups. This result shows progress in the region for the specific aspect on substantive cybercrime legislation. However, for other aspects in this dimension, this regional study shows that some of those ten SADC countries reviewed previously (CMM 2016-20) with maturity stages reaching established, would, in the past, not achieve this maturity stage with the requirements of the new CMM 2021 Edition. For example, while the CMM 2016-20 had two SADC countries with an established maturity stage in the legal and regulatory requirements for cybersecurity, the result of this study shows that none of the SADC countries achieved this maturity stage in 2021. Similar results were found for the cybersecurity aspects on procedural cybercrime legislation, intellectual property legislation, and law enforcement. Note likewise that although this regional study has extended the regional information on cybersecurity in the SADC, it has faced limitations to find enough evidence for all the countries in the

[175] See Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition.* https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

region. The next subsections detail the regional level of maturity in the different factors within this dimension.

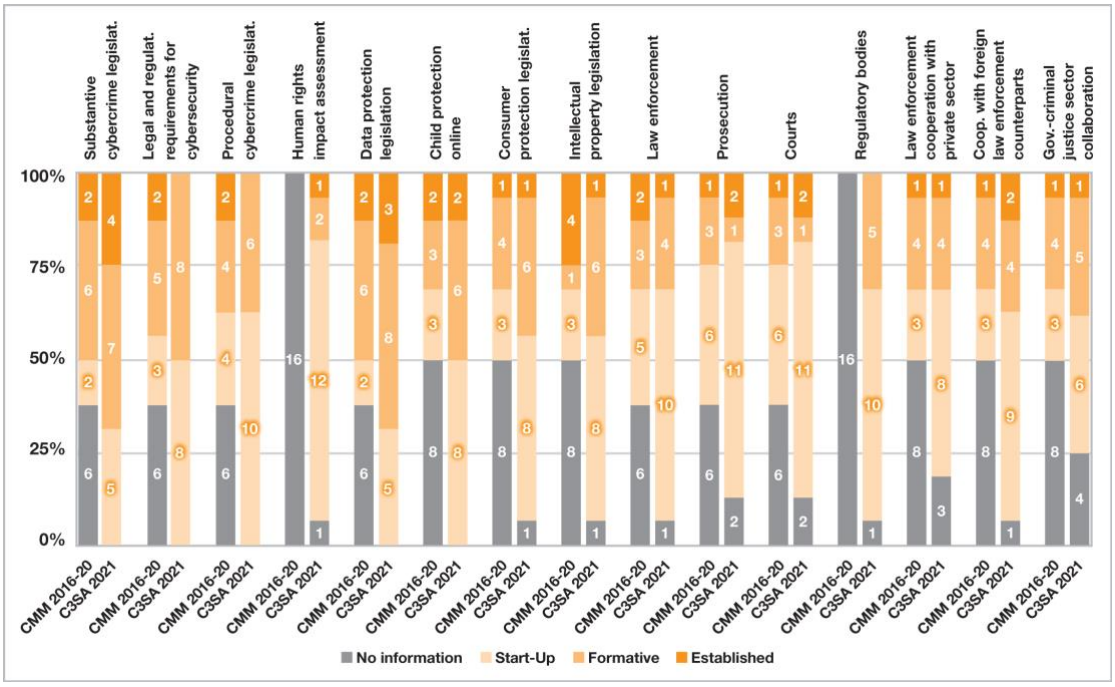

Figure 8: Number of SADC countries within each maturity stage for the CMM aspects included in dimension 4 "Legal and regulatory frameworks".
Source: C3SA (C3SA 2021) & World Bank, CTO, ITU, GCSCC (CMM 2016 – 2020)

D 4.1: Legal and Regulatory Provisions

This factor assesses the existence of legislation and regulatory provisions for cybersecurity. It also includes the assessment of legal and regulatory requirements, substantive and procedural cybercrime legislation, as well as human rights impact assessments in the development of the legislation.[176] Cybercrime legislation (i) sets out acceptable standards of behaviour for digital technology users; (ii) provides for sanctions for harmful behaviours online; and (iii) sets out rules of evidence and criminal procedure for cybercrimes.[177] Legislation should also provide for cybersecurity regulatory frameworks to enable regulatory oversight and enforcement.

Substantive cybercrime legislation in the SADC region is at a *start-up to formative* stage. Substantive cybercrime legislation defines acts and behaviours prohibited by law and enables a country to combat criminal activity involving computers and other digital modalities and specific laws are required to address digital crimes and crimes enabled by digital technology.[178] Except for a few, SADC countries have some form of legislation in place to deal with cybercrimes. Appendix 4 (*Status of substantive*

[176] See Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition.* https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[177] See UNODC. (2019, February). *Cybercrime module 3 key issues: The role of cybercrime law.* Retrieved March 6, 2022, from https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html

[178] See Cassim, F. (2010). Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study. *Potchefstroom Electronic Law Journal, 12*(4), 33-79. https://doi.org/10.17159/1727-3781/2009/v12i4a2740

and procedural cybercrime legislation SADC) provides details of the laws relevant to cybercrime in each country. Angola, Lesotho, Mozambique, Seychelles, and Zimbabwe have amended their criminal laws to include some cybercrimes. However, in some cases, the amendments to the existing criminal code are not comprehensive. For example, Lesotho has added two provisions to its *Penal Code 2012*[179] that deal with unlawful access to a computer, and the theft of data on a computer; this has left other cybercrime issues unaddressed. In 2016, Seychelles added provisions to its penal code[180] to criminalise fraud and forgery committed using digital technology.[181]

Several countries have passed legislation based on the *Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law*.[182] This model is comprehensive, and harmonised to ensure that countries in the region have compatible cybercrime legislation. It is part of a global ITU-EC-ACP (International Telecommunication, European Commission, Africa Caribbean Pacific) project aimed at assisting in the 'Harmonization of the ICT Policies in Sub-Saharan Africa' (HIPSSA) and was introduced by ITU and the European Commission (EU) and adopted by SADC in 2012.[183]

Procedural cybercrime legislation in the region is at the *start-up* stage, where most countries do not have legal provisions for investigating cybercrimes and related evidentiary requirements. The majority of SADC countries do not have specific procedural rules for cybercrimes and crimes involving digital evidence. There is a need for legislation that provides for rules on preservation orders, disclosure of preserved data, production orders, powers of access, search and seizure, real-time collection of traffic data and deletion orders.[184] In eSwatini, Lesotho, Namibia and Zimbabwe, there are on-going discussions to develop comprehensive cybercrime legislation. On the other hand, Angola, Botswana, Mauritius, South Africa, and Zambia, have more comprehensive procedural cybercrime legal frameworks and provisions for international cooperation. Procedural cybercrime legislation in the SADC, where it exists, is largely based on the harmonised legal framework, the *Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law.*[185]

---

[179] See *Penal Code 2012. Lesotho.* S.62. Retrieved February 26, 2022, from https://lesotholii.org/ls/legislation/num-act/6

[180] See *Penal Code 1955.* (Seychelles). Ss. 363A-368A. Retrieved February 26, 2022, from https://seychelleslaw.sc/p/penal-code

[181] See Athanase, P. & Uranie S. (2016, June). *Seychelles parliament passes bill to criminalize technology crimes.* Seychelles News Agency. Retrieved March 6, 2022, from http://www.seychellesnewsagency.com/articles/5307/Seychelles+parliament+passes+bill+to+criminalize+technology+crimes

[182] See ITU. (2013). *Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law.* Retrieved March 5, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

[183] See ITU. (2013). *Electronic Transactions and Electronic Commerce: Southern African Development Community (SADC) Model Law*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

[184] See UNODC. (2019, February). *Cybercrime module 3 key issues: The role of cybercrime law.* Retrieved March 6, 2022, from https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html

[185] See ITU. (2012). *Data Protection: Southern African Development Community (SADC) Model Law*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

However, Angola[186], South Africa[187] and Zambia[188] have recently passed new cybercrime laws with extensive powers to investigate, search, access and seizure.

Since cybercrime is often transnational, combatting it requires international cooperation. In addition to having regionally harmonised legislation, SADC countries need to ratify relevant international treaties. Mauritius is the only country in the SADC that has ratified the *Convention on Cybercrime of the Council of Europe* (the Budapest Convention). Mauritius has also ratified the *African Union Convention on Cyber Security and Personal Data Protection* together with Angola, Mozambique and Namibia.[189] Regional cooperation is facilitated through the SADC *Protocol on Mutual Legal Assistance in Criminal Matters*[190] and the *SADC Protocol on Extradition*.[191] Instruments for international cooperation on cybercrime rely on the existence of relevant domestic law. For this reason, the lack of comprehensive, regionally harmonised substantive cybercrime legislation in some member countries impedes the region's capacity to combat regional cybercrime.

Legal and regulatory requirements for cybersecurity in SADC is at the *start-up to formative* stage. This indicates a limited capacity for the region to protect critical infrastructure, privacy online, electronic commerce and human rights online. There is also limited evidence of cross-sector regulatory provisions in the existing laws. Some countries have passed data protection laws aligned with the General Data Protection Regulation (GDPR).[192] Others are based on the SADC model law on data protection.[193] Data protection legislation often establishes an independent and administrative body responsible for oversight on data protection.[194] Eleven of the sixteen SADC member states have enacted data protection laws with provisions for compliance oversight. The SADC secretariate, assisted by the ITU, developed the

---

[186] See Alberto Galhardo Simões. (2021). Data protection and cybersecurity laws in Angola. Retrieved March 5, 2022, from https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/angola

[187] See *Cybercrimes Act of 2020 (English/Afrikaans)* (Republic of South Africa). Retrieved March 3, 2022, from https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000

[188] See. *The Cyber Security and Cyber Crimes Act, 2021* (Republic of Zambia) Retrieved March 4, 2022, from https://www.parliament.gov.zm/node/8832

[189] See African Union. (n.d). List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection. https://au.int/sites/default/files/treaties/29560-sl AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

[190] See SADC. (2002). *SADC Protocol on Mutual Legal Assistance in Criminal Matters*. Retrieved March 6, 2022, from https://www.sadc.int/files/8413/5292/8366/Protocol_on_Mutual_Legal_Assistance_in_Criminal_Matters_2002.pdf

[191] See SADC. (2002). *SADC Protocol on Extradition.* Retrieved March 6, 2022, from https://www.sadc.int/files/3513/5292/8371/Protocol_on_Extradiction.pdf

[192] See Daigle, B. (2021). *Data protection laws in Africa: A Pan-African survey and noted trends.* Retrieved March 8,2022, from https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf

[193] See ITU. (2013). *Data Protection: Southern African Development Community (SADC) Model Law.* Retrieved March 17, 2022, from https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[194] See Daigle, B. (2021). *Data protection laws in Africa: A Pan-African survey and noted trends.* Retrieved March 8, 2022, from https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf

Electronic Transactions and Electronic Commerce: Southern African Development Community (SADC) Model Law[195] of 2013 to facilitate and regulate e-commerce. Eleven members[196] have passed a law to regulate e-commerce based on the SADC model or earlier models such as the *UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998*[197] and *UNCITRAL Model Law on Electronic Signatures (2001).*[198]

While most SADC member states have enacted laws with regulatory provisions for personal data protection, electronic commerce and digital signatures, few countries have legal and regulatory frameworks for national cybersecurity incident response, the protection of critical infrastructure assets in sectors such as energy, water, finance, and health. However, the region is starting to address these issues. For example, Zambia's *Cyber Security and Cyber Crimes Act 2021*[199] provides for the establishment of a cybersecurity regulator, the functions of which shall be the responsibility of the Zambia Information and Communication Technology Authority (ZICTA). The Act outlines the regulatory functions, obligations for critical infrastructure operators, a cybersecurity incidents response team, and the National Cyber Security Advisory Coordinating Council which is responsible for act as a cybersecurity oversight.[200] South Africa has regulatory provisions for critical infrastructure contained in the *Critical Infrastructure Protection Act 2019.*[201]

With regards to the human rights impact assessment in the development of cybercrime legislation and regulations, the region is at *start-up* stage, where there is no evidence of human rights impact assessments during the development of cybercrime legislation or cybersecurity regulations in the majority of countries. South Africa is the most advanced in this aspect; the country's cybercrime law[202] recognises the fundamental human rights on the internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association. While all countries have laws that protect human rights, due care has to be taken in the development of cybercrime legislation to ensure that the law also protects human rights online.

---

[195] See ITU. (2013). *Electronic Transactions and Electronic Commerce: Southern African Development Community (SADC) Model Law*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

[196] Angola, Botswana, Madagascar, Malawi, Mauritius, Mozambique, Seychelles, South Africa, Tanzania and Zambia

[197] See United Nations. (2002). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998.* Retrieved February 12, 2022, from https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

[198] See United Nations. (2002). *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.* Retrieved March 3, 2022, from https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf

[199] See *Cyber Security and Cyber Crimes Act of 2021.* s. 4 (Republic of Zambia). https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf

[200] See *Cyber Security and Cyber Crimes Act of 2021.* s. 5 (Republic of Zambia) https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf

[201] See *Critical Infrastructure Protection Act of 2019.* (Republic of South Africa). https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf

[202] See *Cybercrimes Act of 2020*. (Republic of South Africa). https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

D 4.2: Related Legislative Frameworks

Countries in the region increasingly recognise data protection laws, as more economic and social activities tend to take place digitally. These laws are essential in providing guidance and best practice on the use, processing, and storage of personal data. Many countries across the world have developed data protection laws; an estimate of 128 countries out of 194 countries already had put data protection and privacy in place.[203]

In Africa, regional bodies are striving to ensure the prioritisation of data protection and privacy. The AU adopted a convention on cybersecurity and personal data protection in 2014.[204] About 52% of countries in Africa have data protection and privacy legislation, while 17% have draft legislation and 24% have no data protection legislations.[205] The SADC has recognised the importance of developing data protection laws and has published a model law on data protection in 2013 to assist member countries to develop such laws.[206] The HIPSSA Data Protection Model Law is aimed at preventing misuse of data emanating from the gathering, administering, transmission, storing and use of individual data.[207] Prioritisation of data protection laws is increasingly becoming important for SADC countries with strong trade ties with the European Union (EU), where it is mandatory that countries trading with countries in the EU to comply with the EU's GDPR.

The SADC region is at the *start-up* to *formative level* of maturity with regard to the development of data protection legislation. Since the publishing of the SADC model law and GDPR, Angola, Botswana, Eswatini, Lesotho, Malawi, Mauritius, Madagascar, South Africa, and Zambia have passed data protection legislation. Namibia, Seychelles, and Zimbabwe are following suit, and are in the process of drafting their data protection legislation. However, some countries such as, Tanzania, Mozambique, Comoros, and the DRC still have no specific data protection laws. Despite this, their respective constitutions have various components that make provision for data protection in general. Tanzania, for instance, uses different pieces of legislation from various sectors to fulfill the privacy and data protection requirements.[208] Further to this, although Botswana, Seychelles, Lesotho and Madagascar have passed data protection legislation, they have not yet implemented these laws, as shown in Table 5**.**

---

[203] See UNCTAD. (2020, April 2). *Data protection and privacy legislation worldwide*. Retrieved February 10, 2022, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[204] See CIPESA. (2018, August 6). *Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa*. Retrieved January 24, 2022, from https://cipesa.org/2018/08/challenges-and-prospects-of-the-general-data-protection-regulation-gdpr-in-africa/

[205] See UNCTAD. (2021, December 14). *Data protection and privacy legislation worldwide*. Retrieved February 10, 2022, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[206] See Sylla, A., & Ford-Cox, A. (2019, October 14). *Overview of data protection laws in Africa*. Lexology. Retrieved March 10, 2022, from https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2

[207] See ITU. (2013). *Data Protection: Southern African Development Community (SADC) Model Law.* Retrieved March 5, 2022, from https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[208] See BOWMANS. (2018, December 28). *Privacy and Data Protection in Tanzania (Part 1)*. Retrieved March 6, 2022, from https://www.bowmanslaw.com/insights/intellectual-property/privacy-and-data-protection-in-tanzania-part-1/

Table 5: Status of data protection laws in SADC

Country	Legislation	Status
Angola	Law no.(s) 22/11, 23/11 and 7/17 [209, 210]	Passed
Botswana	Data Protection act of 2018[211, 212]	Passed
DRC	Law 29-2019[213]	Passed
Comoros	None (Relies on electronic communications decree)	-
Eswatini	Data Protection Bill 2020 [214]	Passed
Lesotho	Data Protection Act 2013	Passed, not enforced
Madagascar	Law No. 2014-038 (in French) [215]	Passed, not enforced
Mauritius	Data Protection Act of 2017	Passed
Mozambique	No data protection law but some protections under the Penal Code, Labour Law and Electronic Transactions Law [216, 217]	Passed
Malawi	Partial Protection via the Electronic Transactions and Cybersecurity Act No. 33 of 2016 (Has some provisions that cover personal data protection)	Passed
Namibia	None	
Seychelles	Data Protection Act 2003	Passed, not enforced
South Africa	Protection of Personal Information Act	Passed
Tanzania	Privacy recognised in the constitution and other laws, e.g. Electronic Transactions Act [218] The Electronic and Postal Communications Act, 2010 ('EPOCA') [219]	
Zambia	Electronic Transactions and Cybersecurity/Communications Act [220]	Passed
Zimbabwe	Access to Information and Protection of Privacy Act, Draft Data Protection Bill	Not yet passed

Source: C3SA 2021

[209] See https://www.huntonprivacyblog.com/2011/09/19/angola-passes-personal-data-protection-law/

[210] See https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/angola

[211] See https://www.bocra.org.bw/data-protection-act

[212] See https://www.dataguidance.com/sites/default/files/government_gazette_15th_october_2021.pdf

[213] See https://www.dataguidance.com/notes/republic-congo-data-protection-overview

[214] See http://www.gov.sz/images/ICT/The-Data-Protection-Final-1.pdf

[215] See *Sur la protection des données à caractère personnel de 2014.* (Madagascar). (Law No. 2014 038 relating to protection of personal data) (FRENCH). Retrieved March 6, 2022, from https://ictpolicyafrica.org/en/document/fes5g7flogd?page=3

[216] See DLA Piper. (2021). Global Data Protection Laws of the World – Mozambique DLA Piper Data Protection. Retrieved March 6, 2022, from https://www.dlapiperdataprotection.com/index.html?t=law&c=MZ&c2=

[217] See https://www-intic-gov-mz.translate.goog/?wpl_post_services=seguranca-cibernetica-e-proteccao-de-dados&_x_tr_sl=pt&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

[218]See Bowmans. (2019, February 2). *Privacy and Data Protection in Tanzania | Data Privacy Laws in Tanzania*. Retrieved January 27, 2022, from https://www.bowmanslaw.com/insights/intellectual-property/privacy-and-data-protection-in-tanzania-part-1/

[219] See *The Electronic and Postal Communications of 2010*. (Republic of Tanzania). Retrieved January 27, 2022, from https://www.researchictafrica.net/countries/tanzania/Electronic_and_Postal_Communications_Act_no_3_2010.pdf

[220] See https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf

The increase in connectivity and online access has provided an opportunity for online predators to exploit vulnerable people through cyberbullying, harassment, scams, and unwanted contact. Further to this, the outbreak of COVID-19 pandemic has increased the online activity of children.[221] This underscores the importance of developing online protection legislation to keep people, in particular, children, safe online. However, the Child Online Protection legislation in the region at the *start-up level* of maturity as shown in Figure 9, where most countries do not have specific child online protection legislation.

The majority of countries in the SADC region do not have specific child online protection legislation and rely on the provision made on child protection in their constitution and other laws. ITU recommends for countries to adopt comprehensive legal framework so as to ensure that legislation includes "...preventive measures; prohibition of all forms of violence against children in the digital environment; provision of effective remedies, recovery and reintegration to address violations of children's rights; the establishment of child-sensitive counselling, reporting and complaint mechanisms; and accountability mechanisms to fight impunity".[222] Specific child online protection legislation ensures laws cover these aspects adequately. In the SADC region, South Africa is considered to be one of the countries at high risk of exposure to harmful behaviour online, as per Microsoft's 2019 Digital Civility Index (DCI), with millennials and teenagers, especially girls, the most affected.[223] [224]

Angola, Eswatini,[225] Seychelles and South Africa,[226] [227] have specific legislation on child online protection. The National Childcare and Protection Policy of South Africa indicates that the Department of Communications together with the Film and Publication Board are responsible for online protection of children in the country through the provision of reliable and secure ICT infrastructure.[228] Tanzania, Namibia, Malawi, Mauritius, Madagascar, the Comoros, the DRC, Zambia and Botswana have

---

[221] ITU. (2020, April). *COVID-19 and its implications for protecting children online*. Retrieved January 20, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf

[222] See ITU. (2020). *Guidelines for policy-makers on child online protection*. p.45. Retrieved November 11, 2021, from https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[223] See Microsoft News Center. (2019, February 7). *Microsoft research reveals South Africa at high risk for harmful online behaviour.* Retrieved March 16, 2022, from https://news.microsoft.com/en-xm/2019/02/07/microsoft-research-reveals-south-africans-at-high-risk-for-harmful-online-behaviour/

224 See BizCommunity. (2019, February 8). SA is at high risk for harmful online behaviour. Retrieved March 5, 2022, from https://www.bizcommunity.com/Article/196/661/187159.html

[225] See Plessis, C. (2020, September 4). *eSwatini govt says new cybercrime bill won't limit press freedom*. Eye Witness News. Retrieved March 5, 2022, from https://ewn.co.za/2020/09/04/eswatini-govt-says-new-cybercrime-bill-won-t-limit-press-freedom

[226] See Firewater, K. (2019, December 6). *Online child protection*. Pygma Consulting. Retrieved March 6, 2022, from http://pygmaconsulting.com/online-child-protection/

[227] See Films and Publications Amendment Act of South Africa (2019, October 3). *Government Gazette*. No. 11, Retrieved March 15, 2022, from https://www.gov.za/sites/default/files/gcis_document/201910/42743gon1292.pdf

[228] See South Africa Department of Social Development. (2019). *National Child Care and Protection Policy.* Retrieved March 6, 2022, from https://www.gov.za/sites/default/files/gcis_document/202102/national-child-care-and-protection-policy.pdf

general legislation on child protection contained in their respective constitutions, but this is not specific to the online environment. In the absence of child online protection legislation, Zimbabwe developed guidelines to improve child safety online. Lesotho has no child online protection laws, while in Mozambique discussions to develop such laws are underway.

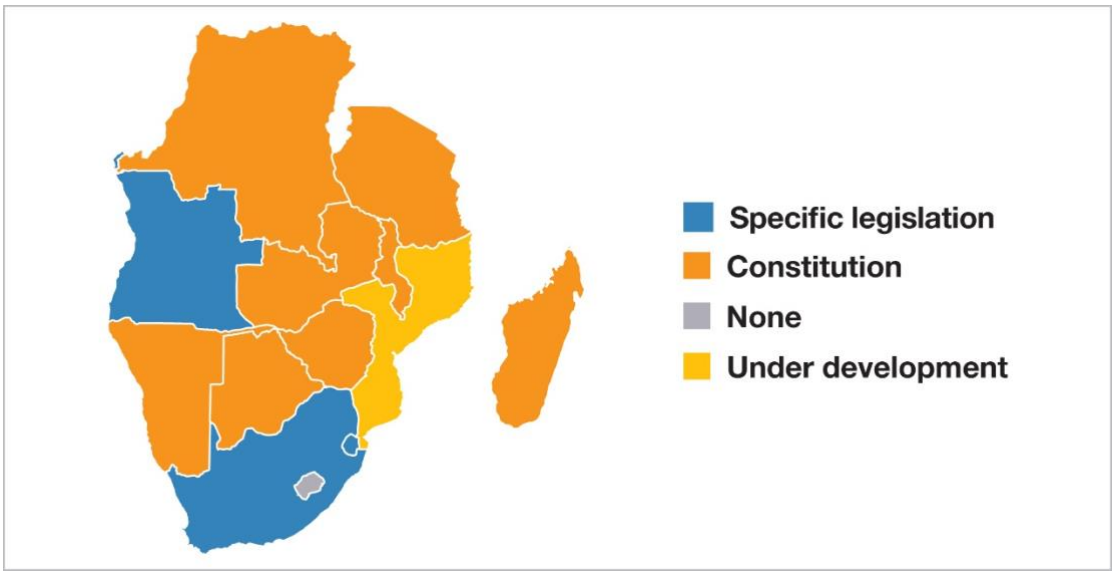

Figure 9: Illustrative map of the status of child online protection legislation in the SADC

Source: C3SA

Consumer protection legislation promotes and protects the interest of the consumers and ensures a fair marketplace for consumer services.[229] These services can also be provided online. There is a need, therefore, for tailored legislation for the online environment. However, the region is still at the *start-up level* of maturity on this aspect. Most SADC countries do not have consumer protection legislation specific to online services. Instead, governments in Malawi, Zambia, and Mozambique have made provisions through the Electronic Transaction Act, and others, for instance, Namibia and Comoros have made online consumer protection provisions through the Communications Act. However, these laws do not fully address consumer protection legislation aspects.[230, 231] Mauritius and Botswana have general laws to handle consumer protection. However, the scope of these general laws is limited, and does not address the online aspect.

Intellectual property legislation is the *start-up* level of maturity in the region. As shown in Figure 8, only one country is at the established stage of maturity, while the majority are at the start-up stage. A smaller number is at the *formative* level. Most of the countries in the region are members of the African Regional Intellectual Property

[229] See Lombard, M. (2021). Parol evidence and the Consumer Protection Act 68 of 2008. *Potchefstroom Electronic Law Journal*, *24*, 1–27. https://doi.org/10.17159/1727-3781/2021/v24i0a9486

[230] See Mwasomola U.L., Ojwang E., Pastory D., (2020). Examining The Consumer Protection And Comprehensive in E-Commerce in Tanzania. *Business Education Journal, 4*(1). http://www.cbe.ac.tz/bej

[231] See Mwakatumbula, H. J., Moshi, G. C., & Mitomo, H. (2019). Consumer protection in the telecommunication sector: A comparative institutional analysis of five African countries. *Telecommunications Policy*, *43*(7), 101808. https://doi.org/10.1016/j.telpol.2019.02.002

Organisations (ARIPO), World Trade Organisations (WTO), and World Intellectual Property Organisations (WIPO). There are legislations dealing with intellectual property in South Africa, Seychelles, the DRC, and Madagascar. However, they do not address the online environment. Some other countries, for example, Botswana, are in the process of amending the existing intellectual property legislation to incorporate the online component. Some countries, such as Namibia and Malawi, use the Copyright Act to address intellectual property. Despite having IP legislation in place, piracy[232] is still a growing concern in many of the SADC countries, due to a lack of enforcement.[233] Table 6 shows the status of intellectual property laws in the SADC region.

D 4.3. Legal and Regulatory Capability and Capacity

This factor assesses the capacity of law enforcement to investigate cybercrimes. It also assesses the capacity of the prosecuting authorities to prosecute cybercrime and electronic evidence cases, the capacity of courts to preside over cybercrime cases and cases involving electronic evidence, as well as the existence of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations.[234]

This review found that the law enforcement agencies in the SADC region are in the *start-up* stage, implying that that the agencies do not have sufficient institutional and human capacity to investigate and manage cybercrime cases, and cases involving electronic evidence.[235] In particular, law enforcement agencies in ten countries have limited capacity to prevent and combat cybercrime. In another five countries, the capacity of law enforcement agencies is higher; these countries have developed some skills and acquired tools to investigate cybercrime cases and crimes involving digital evidence. Mauritius is the most advanced in this aspect. The Mauritius police force has institutional structures for dealing with cybercrimes, namely the Cybercrime Unit and the Police Information Technology Unit with the national CSCIRT (CERT-MU) providing technical support.[236] Further, the Mauritian police force has benefited from training from the US government.[237] It also has a digital forensics laboratory to facilitate the investigation of cybercrime and crimes involving digital evidence.[238] It is evident that law enforcement in Mauritius has comprehensive institutional capacity with sufficient human, procedural, and technological resources to investigate cybercrime

[232] See The Software Alliance. (2018). *Software Management: Security Imperative, Business Opportunity.* Global Software Survey, 24. Retrieved March 14, 2022, from https://www.bsa.org/news-events/news/bsas-2018-global-software-survey-shows-better-software-management-can-improve-security-and-boost-bottom-line

[233] See Ncube, C. B., Schonwetter, T., Oguamanam, C., & de Beer, J. (2017). Intellectual Property Rights and Innovation: Assessing Regional Integration in Africa (Aria VIII). *SSRN Electronic Journal*, *May*. https://doi.org/10.2139/ssrn.3078997

[234] See GCSCC. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Retrieved February 11, 2022, from https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[235] See GCSCC. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition.* Retrieved February 11, 2022, from https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[236] See Republic of Mauritius. (2020). *Cyber Security*. Retrieved March 10, 2022, from https://govmu.org/EN/infoservices/comm/Pages/security.aspx

[237] See Overseas Security Advisory Council. (2019). *Mauritius 2019 Crime & Safety Report*. Retrieved February 9, 2022, from https://www.osac.gov/Country/Mauritius/Content/Detail/Report/e248beb4-219e-4708-a774-15f4aed12f9e

[238] See Mauritius Police Force. (2021). *Police IT Unit*. Retrieved March 5, 2022, from https://police.govmu.org/police/?page_id=5779

cases. Mauritius' established structures for dealing with cybercrime is lacking in other SADC countries, which remain at the start-up level.

The capacity of prosecution authorities in the SADC to handle cybercrime cases and cases involving digital evidence is in the *start-up* stage. Eleven countries lack basic human and technical resources to review electronic evidence and prosecute cybercrimes and crimes involving electronic evidence. Two countries, viz; Botswana and South Africa have prosecuting authorities with some capacity to conduct cybercrime cases, as well as to handle digital evidence, even though the capacity is not institutionalised in the sense that cybercrime prosecution capabilities have not been mainstreamed, so that they are generally available among all prosecutors. The prosecutors received training, though it is ad hoc. Prosecuting authorities in Mauritius and South Africa are better prepared capacitated in terms of technology and human resources to review cybercrime cases. Prosecutors in Mauritius have participated in cybercrime training for several years with the support of the Council of Europe and the Mauritian Government.[239] Mauritius has a prosecuting authority with sufficient institutional capacity to handle cybercrime cases as well as cases involving digital evidence. In terms of capacity building, prosecutors in Mauritius have benefited from continuous training since 2014. South Africa has examples of successful prosecution of cybercrimes and crimes involving digital evidence.[240]

The assessment found that the region is at the *start-up stage* with respect to the capacity of courts to ensure effective prosecution of cybercrimes and crimes involving electronic evidence. With a few exceptions (Mauritius and South Africa) the capacity of courts in the SADC to preside over such cases is low. Courts in Mauritius and South Africa are the most advanced, both being at an *established* stage. They have sufficient human and technological resource for effective and efficient legal proceedings relating to cybercrime and cases involving electronic evidence. Judicial officers, together with law enforcement officers and prosecutors in Mauritius, have been capacitated over the years. A group of Mauritian law enforcement and judicial officers were enrolled in a train-the-trainer course offered by the Council of Europe to ensure a sustainable source of trainers.[241] Subsequent to that, the judiciary in Mauritius received judicial training on cybercrime in 2014[242] and 2015, and the courts have been adjudicating cybercrime cases.[243] South African courts have extensive experience adjudicating cases involving digital evidence, as illustrated through several cases that have been

---

[239] See Global Prosecutors E-Crime Network. (n.d.). *Global prosecutors e- crime network. History of the Global Prosecutors E-Crime Network.* International Association of Prosecutors. Retrieved February 23, 2022, from https://www.iap-association.org/GPEN/About-GPEN/History

[240] See Nortjé, J.G.J., & Myburgh, D.C. (2019). The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa. *Potchefstroom Electronic Law Journal, 22*(22), 1-42. http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886

[241] See Council of Europe. (n.d.) *Judicial training skills and introductory cybercrime and electronic evidence course.* Retrieved February 10, 2022, from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803036db

[242] See Council of Europe (2014, August 11). *GLACY cybercrime capacity building in Mauritius*. Retrieved February 10, 2022, from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803028a5

[243] See Council of Europe. (2019) (n.d.). *Mauritius*. Octopus Cybercrime Community. Retrieved March 16, 2022, from https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/mauritius?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/

adjudicated over the years.[244] While Namibia's courts are not as developed as those of Mauritius and South Africa, they have developed come capacity to handle cybercrime cases.

Communication regulatory bodies in SADC are starting to establish their cybersecurity roles but region's capacity is at the *start-up* stage of maturity. This is in line with the finding in *D 4.1: Legal and Regulatory Provisions* that most SADC countries have not yet established legal and regulatory requirements for cybersecurity. Regulators in the telecommunications and financial sector have started including cybersecurity requirements in their regulations or guidelines. For example, the Central Bank of Seychelles and the Reserve Bank of Malawi have issued guidelines on cybersecurity for deposit-taking financial institutions.[245, 246] Similarly, the Reserve Bank of Zimbabwe has issued a directive and guidelines, which set out the responsibilities and obligations of regulated entities in respect of cybersecurity.[247, 248] The Bank of Mauritius has issued regulations the minimum standards for internet banking.[249]

In the telecommunications sector, policy makers and regulators are starting to understand their cybersecurity roles, for example, by reviewing their regulations and establishing sectoral CSIRTs. Examples of countries that have established their CSIRT are Botswana, Malawi and Zambia. In South Africa, the ECTA (Electronic Communications and Transactions Act) provides for various regulatory roles even though some have not been implemented.[250] Where the CIRTs have been established, they lack resources to be effective as observed in the cases of Zambia and Malawi. Sector-specific regulators, such as the regulators in the banking sector, have started to establish cybersecurity roles.

Some ICT sector regulators in the region have oversight roles over cybersecurity established in law but for most of them, there is no record on implementation in areas such as e-commerce (e.g., digital signatures, consumer protection, domain name administration). For example, in South Africa, cyber inspectors envisaged in the ECT Act have not been established, and fewer CSIRTs than anticipated have been

---

[244] See Swales, L. (2018). An analysis of the regulatory environment governing hearsay electronic evidence in South Africa: suggestions for reform–part two. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, 21*(1). http://www.saflii.org/cgi-bin/disp.pl?file=za/journals/PER/2018/47.html&query=cybercrime

[245] See Central Bank of Seychelles. (2021). *Central Bank of Seychelles cyber security guidelines 2019.* Retrieved March 5, 2022, from https://cbs.sc/Downloads/legislations/Cyber%20Security%20Guidelines%20April%202019.pdf

[246] See Registrar of Financial Institutions - Reserve Bank of Malawi. (2019). *Guidelines on information and cybersecurity risk management for banks.* Retrieved March 6, 2022, from https://www.rbm.mw/Home/GetContentFile/?ContentID=35422

[247] See Reserve Bank of Zimbabwe. (2021). *CIRCULAR NO. NPS/02 /2021*. Retrieved February 21, 2022, from https://www.rbz.co.zw/documents/nps/2021/NPS-CIRCULAR-ON-THE-ISSUANCE-OF-CYBER-SECURITY-FRAMEWORK.pdf

[248] See Reserve Bank of Zimbabwe. (2021). *National payment systems risk based guideline on cybersecurity.* Retrieved February 21, 2022, from https://www.rbz.co.zw/documents/nps/2021/NPS-CYBER-SECURITY-FRAMEWORK-20210427.pdf

[249] See Bank of Mauritius. (2001). *Guideline on internet banking*. Retrieved March 5, 2022, from https://www.bom.mu/sites/default/files/Guideline_on_internet_banking.pdf

[250] See *Electronic Communications and Transactions Act 25 of 2002. ZA*. Ss. 80-84. Retrieved March 6, 2022, from https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf

established.[251] There is no evidence of sector-specific cybersecurity requirements in sectors such as energy, water, health, and transport.

Cross-sector regulators, such as those responsible for data protection, electronic commerce and critical infrastructure, are just starting up in the region, even though laws that establish them have existed for some time. Angola, Mauritius, Mozambique and South Africa are the only SADC countries that have established data protection regulators. For critical infrastructure, and electronic commerce the oversight function is vested in either existing ICT regulators, as in the cases of Zambia, or newly established regulators, such as in the case of the Mozambique's National Institute of Information and Communication Technologies (INTIC).[252]

D 4.4: Formal and Informal Co-operation Frameworks to Combat Cybercrime

Cybersecurity risks are increasingly spanning national borders and cannot be the mandate of a few stakeholders and/or countries. Collaboration is crucial in tackling in dealing with the scourge, and for this reason, national, regional, and international cooperation is necessary.[253] The formal and informal co-operation frameworks factor of the CMM addresses the existence of mechanisms that enable co-operation of domestic and international actors to deter and combat cybercrime.[254] Beyond collaborating with other countries, public-private partnerships ensure the exchange of information, sharing of good practice and communication needs and priorities. This review showed that there is limited collaboration to combat cybercrime between the public and private sectors in most countries in SADC. On all aspects of formal and informal co-operation frameworks, in order to combat cybercrime, the region is at the *start-up* level of maturity.

There is generally minimal formal or informal cooperation frameworks on cybercrime. Most SADC countries were at start-up to formative level on all three factors, viz.: law enforcement cooperation with the private sector; cooperation with foreign law enforcement; and government-criminal justice sector collaboration. Few countries have some frameworks in place to allow for collaboration among stakeholders on combating cybercrime. For example, Mauritius and Namibia having ratified and signed the AU convention have better collaboration mechanisms and channels in terms of international cooperation. Some of the structures in the convention include a 24/7 point of contact network to facilitate mutual legal assistance for computer systems criminal offences,[255, 256] and investigations involving electronic evidence. Among the few

[251] See Malatji, M.; Marnewick, A.L.; von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability, 13*(1), 291. https://doi.org/10.3390/su13010291

[252] See INTIC. (2021). Presentation. Retrieved February 15, 2022, from https://www-intic-gov-mz.translate.goog/?page_id=565&_x_tr_sl=pt&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

[253] See Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition.* Retrieved February 11, 2022, from https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[254] See Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition*. Retrieved February 11, 2022, from https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[255] See Council of Europe (2022). *The Budapest Convention 24/7 point of contact network*. Retrieved March 5, 2022, from https://rm.coe.int/3148-afc2018-ws8-24-7bc-ml/16808e6884

[256] See The G8 24/7 Network of Contact Points. (n.d.). *Protocol statement*. Retrieved March 10, 2022, from http://www.oas.org/juridico/english/cyb_pry_g8_network.pdf

African countries in SADC that are members of the G8 24/7 network are South Africa and Namibia.

While ratification of multinational agreements may still be lacking, the region has some organised institutions that could be leveraged for cybersecurity. The Southern African Regional Police Chiefs Co-operation Organisation (SARPCCO) was established in 2006[257] as the primary body for the prevention and fighting of cross-border crime in Southern Africa. There is, however, no evidence on how SADC member states may be taking advantage of such structures to combat cybercrime.

RECOMMENDATIONS

Following the information presented during the study of the maturity of *Cybersecurity Legal and Regulatory Frameworks*, C3SA has developed the following set of recommendations for consideration by governments of member states and the secretariat of the SADC.

Legal and Regulatory Provisions

R4.1 SADC countries ought to develop comprehensive cybercrime legislation to effectively combat digital related criminal activities.

R4.2 SADC countries ought to ratify regional and international treaties such as the African Union Convention on Cyber Security and Personal Data Protection and the Convention on Cybercrime of the Council of Europe to combat cybercrime.

Related Legislative Frameworks

R4.3 SADC countries that have not yet formulated data protection legislation should develop data protection legislation. The model law can be used as a framework to develop data protection legislation in these countries. SADC countries that are in the process of drafting data protection legislation ought to allocate adequate resources and collaborate with relevant stakeholders to finalised data protection legislation.

R4.4 Governments in the SADC region should develop specific Child Online Protection legislation in line with the provision made in their constitution.

R4.5 Countries in the SADC region that do not have consumer protection legislation need to develop the legislation. Furthermore, there is a need to amend current provisions to include online environment.

[257] See SADC (2012). *Southern African Regional Police Chiefs Co-operation Organisation*. Retrieved February 17, 2022, from https://www.sadc.int/themes/politics-defence-security/police-sarpcco/

R4.6 SADC countries ought to amend existing intellectual property legislation to include online services. The countries that are currently developing the legislation, need to take into account guidelines that are best suited for online environment.

Legal and Regulatory Capability and Capacity

R4.7 SADC should develop a regional strategy for building human and technological capacity for law enforcement, prosecutors, judges on the handling of cybercrime cases and digital evidence.

R4.8 Governments in the SADC ought to mainstream capacity for the investigation, prosecution and adjudication of cybersecurity cases.

R4.9 Governments in the SADC should review their policy and regulatory frameworks to include cybersecurity roles for regulators for CI sectors such as ICT, finance/banking, health, energy, water, government services and transportation to ensure CI protection.

Formal and Informal Co-operation Frameworks to Combat Cybercrime

R4.10 Establish channels and mechanisms for information exchange on cybercrime between public and private sectors including cooperation with ISPs.

R4.11 Countries that have not yet signed and/or ratified the Malabo and Budapest conventions should prioritise this, and use such existing legal frameworks to establish formal international cooperation mechanism. SADC member states should also collaborate by building on the substantive laws that exist at a national level to establish harmonised cybercrime laws to combat and criminalise cybercrime in the region, as well as setting rules of evidence and criminal procedure. This will help member states that are lagging behind to have a safe cyberspace while they focus on developing the national legal environment.

R4.12 Allocate resources and determine legislative requirements to support information sharing between the public and private sectors at the national level.

R4.13 Equip and build cybersecurity capacity within the Southern African Regional Police Chiefs Co-operation Organisation (SARPCCO) to drive and enforce regional cybercrime legislation.

D.5 Cybersecurity Standards and Technologies in SADC

Dimension 5 addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.[258]

Figure 10 below shows the number of SADC countries a start-up, formative, and established maturity stage in each aspect within Dimension 5 in two points in time, when the national CMM reviews were conducted (ten SADC countries had a CMM report during the period 2016-2020) and when this SADC regional report was completed (2021). ICT security standards, standards in procurement, and standards for provision of products and services are the three aspects under factor D5.1 adherence to standards. Technological security controls and cryptographic controls are the two aspects that form factor D5.2 security controls. Software quality and assurance is the only aspect within factor D5.3 software quality. Internet infrastructure reliability, and monitoring and response are the two aspects that form factor D5.4 communications and internet infrastructure resilience. Cybersecurity technologies, cybersecurity services and expertise, security implications of outsourcing, and cyber insurance are the four aspects included in factor D5.5 cybersecurity marketplace. Finally, sharing vulnerability information and policies, processes, and legislation for responsible disclosure of security flaws are the two aspects that form factor D5.6 responsible disclosure.

To interpret Figure 10, consider, for example, the first aspect on ICT security standards. The information from the ten SADC countries reviewed between 2016 and 2020 (labelled CMM 2016-20 in Figure 10) shows that six countries out of ten had a start-up maturity stage, while the remaining four countries were formative. This regional study (labelled C3SA 2021 in Figure 10) found that, in 2021, the proportion of SADC countries with a start-up maturity stage was 75%, and the rest (25% or four countries) were at formative maturity stage. This regional analysis found limited evidence on all the aspects in Dimension 5 for all the SADC countries, although it has extended the available information on cybersecurity capacity in the SADC. The analysis shows that, in 2021, the region had a low proportion of countries with start-up maturity stages, especially in cybersecurity aspects related to security controls and internet infrastructure reliability. Moreover, while those ten SADC countries reviewed previously (CMM 2016-20) had had formative or start-up maturity stages in the past, the results of this regional study show that, in 2021, the SADC region had more mature countries in all aspects, including in Dimension 5; except those aspects related to the adherence to standards, software quality and assurance, and some aspects related to the cybersecurity marketplace. In particular, some countries reviewed previously (CMM 2016-20) with an established maturity stage in cybersecurity technologies would not achieve that maturity stage with the new CMM 2021 Edition. The lower maturity level was due mainly to the latest edition having more aspects, thus demanding higher

[258] See GCSCC, (2021). C*ybersecurity Capacity Maturity Model for Nations (CMM)*. Retrieved February 11, 2022, from https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

performance. The next subsections describe in detail the regional level of maturity in the different factors within Dimension 5.

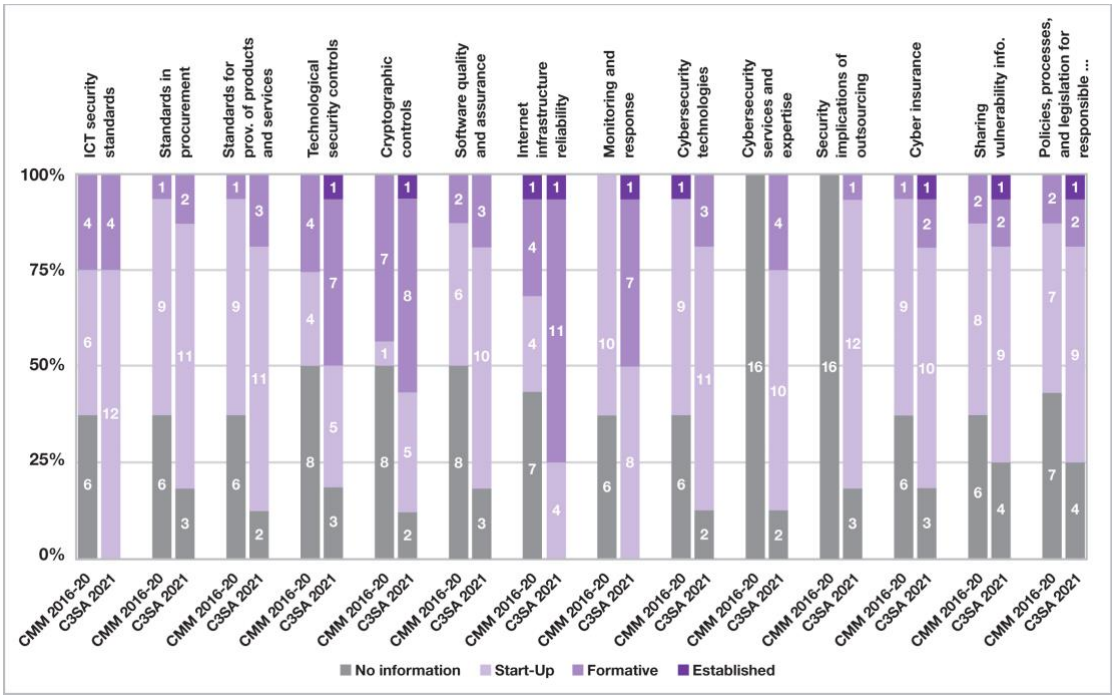

Figure 10: Number of SADC countries within each maturity stage for the CMM aspects included in dimension 5 "Standards and technologies"

Source: C3SA (C3SA 2021) & GCSCC (CMM 2016 – 2020)

D 5.1 Adherence to Standards

Compliance with cybersecurity standards and best practices is necessary towards in ensuring a cyber hygiene environment and the effort towards fighting cybercrime. In an effort to ensure compliance to cybersecurity standards and best practices, the SADC region has implemented model laws to assist member states to develop cybersecurity frameworks.[259]

CMM reviews conducted in SADC countries showed that the adoption of ICT security standards is still minimal. The maturity level of most SADC countries ranges from *start-up to formative*. According to the CMMs conducted between 2016 and 2020, most SADC countries did not have information on the adherence to ICT security standards. However, SADC countries are acknowledging the importance of ICT Security Standards and some countries have already adopted ICT security standards.[260] The adoption of international ICT security standards, such as ISO 27000 in the SADC region is more prevalent in the private sector organisations, such as banking institutions and telecommunication companies, which are subsidiaries of international organisations. ICT security standards are also adopted across governments in some SADC countries. Zimbabwe, Zambia, Namibia, Botswana, Lesotho, Malawi, and

[259] See Orji, U. J. (2015, May). Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation? In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, (pp. 105-118). IEEE. https://ieeexplore.ieee.org/stamp.jsp?tp=&arnumber=7158472

[260] See SADC. (2012). *Southern African Development Community: ICT & Telecommunications*. Retrieved March 6, 2022, from https://www.sadc.int/themes/infrastructure/ict-telecommunications/

Tanzania have adopted and implemented ICT security standards. While Seychelles, Mozambique, Mauritius, Comoros, DRC, Madagascar, and Angola have either no official approved ICT security standards or identified such standards.

Many SADC countries are yet to be actively involved in the development of ICT security standards, since most SADC countries are still at *start-up* stage. In Zambia, for instance, the public sector lacks appropriate standards to guide the formulation and use of software to prevent cyber threats.[261] South Africa identified information risk management standards, while Eswatini has adopted ISO standards.

Many SADC countries have general procurement processes to promote transparency and accountability. However, these countries lack specific cybersecurity standards and best practices to guide the procurement process.

The maturity level for the adoption of cybersecurity standards for procurement in the SADC region is from *start-up to formative* stage. Many SADC countries are yet to fully adopt these standards. Governments in the SADC region have established institutions to oversee and reform public procurement. In Zimbabwe, the government is preparing for e-government procurement,[262] while Zambia has already adopted e-procurement,[263] but it is not yet in operation. In Tanzania, South Africa, Namibia, Mozambique, Botswana, Lesotho, Eswatini, the Comoros, Angola, and Mauritius, there are no specific cybersecurity standards for procurement; the DRC and Botswana have adopted industry specific standards and cybersecurity standards in the private sector; and the Seychelles, Madagascar and Malawi have legislation that makes reference and provision for cybersecurity procurement.

The SADC region lacks standards for the provision of products and services. The maturity level is at *start-up* stage. The DRC, Comoros, Eswatini, Mauritius, Namibia, South Africa, and Zambia have no standards for the provision of products and services. Also, there is no evidence of the existence of standards for the provision of products and services in Angola, Botswana, and the Seychelles. Tanzania has implemented standards for the provision of products and services, while Lesotho has mechanism in place to secure customer data, although there are differences their application. While Malawi uses the provision in its Public Sector ICT standards of 2014, in Mozambique, there is a slow adoption of software development standards in both the public and private sector, while Zimbabwe is in the process of identifying such standards. Additionally, in a country such as Madagascar, the standards for the provision of products and services are mostly applied by national operators that have multinational parent companies.

Overall, adherence to standards in the SADC region remains embryonic as most SADC countries lack ICT standards and good practices. Additionally, some countries have either implemented these standards partially or on ad-hoc basis, or are using general provisions set out in other legislation.

---

[261] See Ministry of Transport and Communications. (2021). *National Cybersecurity Policy 2021*. Retrieved January 5, 2022, from https://www.mtc.gov.zm/wp-content/uploads/2021/06/National-Cybersecurity-Policy2_compressed.pdf

[262] See Procurement Regulatory Authority of Zimbabwe. (2021). *Highlights of Procurement Reforms*. PRAZ. http://www.praz.org.zw/?page_id=90

[263] See Zambia Public Procurement Authority. (2015). *e-Procurement system*. ZPPA. Retrieved January 5, 2022, from https://www.zppa.org.zm/e-procurement-system

D 5.2 Security Controls

A little more than half of SADC countries (nine out of 16 countries) have achieved a formative to established level of deployment of technological security and cryptographic controls in the private and the public sectors. The remainder are still starting-up, with limited and ad-hoc deployment of security controls.

Technological security controls are deployed inconsistently in the portion of SADC countries achieving formative to established stages of maturity. The public and private sectors in these countries have recognised the need to develop policies for the governance and management of technological security controls. Items such as software and hardware updates, anti-malware software, firewall systems, access control, intrusion detection systems, and security audits are deployed at varying degrees in private and public institutions; most of the time without clear guiding policies, procedures, or guidelines. The private sector displays a greater regularity than the public sector in deploying these items. Little is known about how individual general members of the public access and use technological security controls. Some reports suggest that there is an *ad hoc* and inconsistent use of anti-malware software, firewalls, and password managers amongst the public, due to a lack of awareness about their existence or the lack of *know-how* in how to operate them. Mauritius and South Africa are the best performers for this aspect, but they need to improve on the coordination with stakeholders, their review of initiatives, and a better inclusion of rural areas in the programmes.

The other portion of SADC countries is at a start-up level for this aspect. Key informants indicated that there was a limited and *ad-hoc* use of cybersecurity controls in public and private sectors. There is inconsistency and scarce deployment of software updates, firewall rule setting, access control, and basic intrusion detection systems in the private and public sectors. Multinational representatives were reported to be more likely to deploy these security controls in complying with headquarters directives or policies or simply industry related cybersecurity technological control standards.

Nine SADC countries are leading in the use of cryptographic and have achieved formative to established maturity stages. These countries are Botswana, eSwatini, Lesotho, Malawi, Mauritius, Namibia, South Africa, Zambia and Zimbabwe. The review notes the need for cryptographic controls such as Public Key Infrastructures (PKI) (includes authentication, non-repudiation, digital signatures, digital certificates, and summaries), systematic use of SSL (Secure Socket Layer) and TLS protocols for the encryption of data at rest or on transit, and the use of VPNs (Virtual Private Networks) in both private and public sectors. These tools are used in an ad-hoc manner depending on the need and the sensitivity of the information and communication being protected. This group of nine countries do not yet have standards and policies in place which coordinates the use of cryptographic controls in the public and private sectors.

The second group of SADC countries recognises the value of cryptographic controls, but have not taken steps towards their wide usage and standardisation in public and private sectors. In these countries, the use of cryptographic controls is limited. Sometimes, the countries have passed regulation fostering the use of cryptography, but these regulations have yet to be applied.

D 5.3 Software Quality

Regarding software quality, much of the SADC is at a start-up level. The exceptions to this are Lesotho, Mauritius, and Zimbabwe, which are at a formative level. In Zimbabwe, software quality and functional requirements in public and private sectors are recognised and identified, albeit not in a strategic manner. In Mauritius, Government promotes secure software development, the implementation of information security standards in the civil service and the adoption of guidelines for procurement of ICT products. Software quality and functional requirements in public and private sectors are recognised and identified, but not necessarily in a strategic manner. Finally, in Lesotho, the 2019 CMM found that "neither the government nor private-sector entities maintain lists of approved software, nor do they appear to monitor the use of software."

Regardless of the shortcomings shown in the maturity levels of software quality in SADC, the SADC secretariate offers guidelines that “provide guidance on the policies and procedures that govern the procurement of goods, works, and services as well as the contracting of grants to all the staff members involved in the various stages of the procurement activities conducted by the SADC Secretariat”.[264] Such guidelines[265] may be applied by individual countries in the region to the policies and processes for software quality and assurance.

D 5.4 Communications and Internet Infrastructure Resilience

The study assessed the extent to which the respective SADC member states had reliable internet services and infrastructure, and the existence of rigorous security processes across private and public sectors. It also assessed the control that the government in each country has over its internet infrastructure, and the extent to which networks and systems are outsourced. This is achieved by examining access and reliability and the level of national oversight on the infrastructure.

In terms of internet infrastructure resilience, the SADC region is at the *formative* stage of maturity. Globally, the need for reliable internet connectivity has risen sharply as a result of the need for social-distancing due to the COVID-19 pandemic.[266] However, while the situation in each country is unique, most countries in SADC are faced to varying degrees with unreliable internet access. For example, the Comoros, the DRC, Madagascar and Malawi lack reliable and affordable internet access. Even though Madagascar's internet infrastructure is fairly developed and is continuously expanding, internet downtime and interruptions, often caused by power outages, are frequent.[267]

---

[264] See Southern African Development Community Secretariat. (2017). *SADC Guidelines for Procurement and Grants of 1st January 2017. As amended on 20th November.* SADC Secretariat. https://www.sadc.int/files/6816/0620/8029/SADC_Procurement_and_Grants_Guidelines_20_November_2020.pdf

[265] See SADC. (2012). *Provision of Microsoft Enterprise Agreement for Southern African Development Community*. Retrieved March 13, 2022, from https://www.sadc.int/opportunities/procurement/closed-opportuniti/provision-microsoft-enterprise-agreement-southern-african-development-community-sadc/

[266] See Organisation for Economic Co-operation and Development. (2020). *OECD Policy Responses to Coronavirus (COVID-19): Keeping the Internet up and running in times of crisis*. Retrieved January 14, 2022, from https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/

[267] See Finmark Trust, Cenfri & UNCDF. (2017). Madagascar: Catalysing and supporting the financial services sector to enhance inclusiveness in Madagascar: Financial Inclusion Roadmap. Retrieved

Internet infrastructure in Angola, Botswana,[268] the Comoros, eSwatini, Lesotho, Mozambique, Namibia, the Seychelles, Tanzania, Zambia and Zimbabwe have not yet attained the capacity to withstand disasters with minimal disruption; network reliability is a common concern. In these countries, acceptable internet services and their infrastructure are in place, however, their resilience can hardly be guaranteed. The reliability of the internet infrastructure in Mauritius and South Africa was estimated at the established level of maturity.

Monitoring and response are critical for a resilient internet infrastructure. The practice is most established in South Africa compared to the rest of countries. Technology and processes deployed for internet infrastructure meet international IT guidelines, standards, and good practices and national infrastructure is formally managed, with documented processes, roles and responsibilities and limited redundancy. For the other countries, networks are monitored for vulnerabilities, but there is no evidence of incident response planning.

D 5.5 Cybersecurity Marketplace

More than half of the countries in the SADC region are at *start-up* level in the cybersecurity marketplace. Many countries are still not aware of the risks involved in outsourced IT products despite the increase of cybercrimes in the region.[269] Few institutions within the respective countries, especially the financial sector, have some level of awareness on the impact of these outsourced cybersecurity solutions, such that the organisations have implemented their contingency plans in case of any cyber incidents. However, this does not apply to many institutions in the respective countries. Many countries in the SADC region do not produce local cybersecurity technologies. For instance, Botswana and South Africa offer a limited range of cybersecurity technologies. Most countries adopt foreign cybersecurity technologies, and the majority of the countries in the region have not considered the implication of these outsourced IT services. Many countries do not conduct risk assessments on outsourced IT products. This is primarily due to the lack of awareness of the risks associated with the outsourced IT products.

Cybersecurity consultancy services and expertise in the region are limited. A few consultancies are local, where many outsource these services to either local or international consultants. The main contributing factor is a shortage of cybersecurity

January 10, 2022, from https://finmark.org.za/system/documents/files/000/000/228/original/Madagascar-Roadmap.pdf?1601992328

[268] See Mokeresete, M., & Esiefarienrhe, B. M. (2020, November). Users' perspective on the assessment of Botswana Fibre Backbone Network Infrastructure. In *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 1-8). IEEE. https://doi.org/10.1109/IMITEC50163.2020.9334128

[269] See Richards, N. U., & Eboibi, F. E. (2021). African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law? *International Review of Law, Computers & Technology, 35*(2), 131-161. https://doi.org/10.1080/13600869.2021.1885105

manpower in the region.[270, 271] Mauritius and Malawi have a growing number of consultancies that offer services in the country.

Cybercrimes cost African countries millions of dollars every year.[272] However, many countries in the region have not recognised the need for cybersecurity insurance. Mauritius has limited companies offering cybersecurity insurance.

D 5.6 Responsible Disclosure

Most countries in the SADC region are at a start-up stage for sharing vulnerability information. The exceptions to this are Mauritius, Namibia, and South Africa, whose maturity stages are formative, and formative-to-established, respectively. For policies, processes and legislation for responsible disclosure of security flaws, Mauritius, Mozambique and South Africa have the maturity stages, formative, formative-to-established, and established, respectively. The rest of the SADC region has the maturity stage of start-up.

Mauritius is at a formative maturity stage of responsible disclosure, where there is required and ad hoc sharing of vulnerability information amongst professionals and the Computer Emergency Response Team of Mauritius (CERT-MU). The "Data Protection Act 2017" of Mauritius establishes a standard for the handling of personal data by any entity operating in the country. Within the banking sector, and particularly amongst the large financial institutions, the central bank imposes disclosure requirements for major incidents.

South Africa has an established maturity stage, where the country has a vulnerability disclosure framework in place. The framework includes a disclosure deadline, scheduled resolution, and an acknowledgement report. With the framework, organisations in South Africa have established processes to receive and disseminate vulnerability information.

RECOMMENDATIONS

Following the information presented during the study of the maturity of *Cybersecurity Standards and Technologies*, C3SA has developed the following set of recommendations for consideration by governments of member states and the secretariat of the SADC.

[270] See Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

[271] See Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018). Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index. *SSRN Electronic Journal,* 1–21. https://doi.org/10.2139/ssrn.3142296

[272] See Serianu. (2020). Africa *Cyber Security Report - Kenya 2019/2020. Local Perspective on Data Protection and Privacy Laws: Insights from African SMEs*. https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

Adherence to Standards

R5.1 SADC countries should improve the level of compliance to cybersecurity standards and best practices by devising measures to monitor compliance across the public and private sectors. In addition, measures should be coordinated across SADC countries to enhance collective cybersecurity in both the private and public sectors.

R5.2 Governments, in collaboration with the private sectors in the SADC region, should promote the adoption of cybersecurity standards and best practice shared from neighbouring countries.

R5.3 Governments across the SADC region should adopt standards for ensuring that public procurement processes include cybersecurity as a factor in all procurement of goods and services.

Security Controls

R5.4 Cybersecurity regulators in SADC countries should adopt national standards and policies on the deployment of technological security controls for public and private sectors.

R5.5 Governments in SADC countries, in collaboration with relevant cybersecurity stakeholders, should mandate appropriate local regulators, set standards and develop policies to coordinate the use of cryptographic controls in the public and private sectors. The know-how on how to operate security controls can be shared from best practice performers in the region and coordinated across borders in order to improve regulation and utilise security controls in a consistent manner.

R5.6 The SADC secretariat should adopt, in collaboration with members states, a regional framework for the promotion and coordination of the use of cryptographic controls in the public and private sectors.

Software Quality

R5.7 Governments in the SADC should follow guidelines that the SADC Secretariate has set forth for itself in SADC Guidelines for Procurement and Grants. These Guidelines are intended to provide guidance on the

policies and procedures that govern the procurement of goods, works, and services.

Communications and Internet

R5.8 SADC countries should invest in internet infrastructure to ensure wider internet access and affordability.

R5.9 Governments in SADC countries should adopt mechanisms to ensure internet infrastructure resilience to avoid major disruption during disasters.

Cybersecurity Marketplace

R5.10 Governments in the SADC region should prioritise raising awareness of the risks associated with third party services. Regional Summits could be utilised by SADC countries as a platform to reach relevant stakeholders in the region.

R5.11 Governments should promote awareness among citizens of the importance of assessing the security of digital products before acquiring them.

R5.12 SADC countries should encourage the establishment of cybersecurity insurance market across the region.

Responsible Disclosure

R5.13 The SADC Secretariate should encourage nations within the SADC region to develop policies that allow for responsible disclosure between stakeholders within these nations so that cybersecurity vulnerabilities are addressed in both formal and informal settings.

R5.14 Governments in the SADC should guarantee the legal protection of cybersecurity researchers by the work of cybersecurity researchers ensuring that the creation, possession, or distribution of tools designed to test or compromise the security of a system, service is not unduly criminalised or punished in other ways.

Discussion and Conclusions

Since its first deployment in 2015, the CMM has been used to assess the cybersecurity capacity of more than 80 nations. This allows cross-national comparisons of the level of maturity over the different dimensions of cybersecurity included in the framework. The present regional study not only updates the information on the cybersecurity capacity of the SADC countries, considering new cybersecurity areas and actions included in the new CMM 2021 edition,[273] but also expands the information on cybersecurity beyond the sample of countries reviewed through the CMM. This valuable new information allows for a better regional understanding of the cybersecurity capacity within SADC and to situate this region in the international picture by comparing it with the rest of countries reviewed under the CMM. In particular, when this study was done, there was data on 83 countries that can be split into three different regions: SADC (16 SADC countries reviewed in this study), rest of Africa (14 countries reviewed between 2016 and 2020), and rest of the world (59 countries reviewed between 2015 and 2020).[274] As the SADC countries assessed in this study were the only ones considering all the aspects and factors in the new 2021 CMM edition, the cross-country comparison in this section uses the revised CMM 2016.[275]

Figure 11 displays the average maturity stage of the five dimensions of the CMM for the three regional groups.[276] In the three regions the average maturity stages were between start-up and formative. While the SADC region had a balanced maturity stage across the five dimensions, on average, the countries in the rest of Africa and the rest of the world were more mature in cybersecurity legal and regulatory frameworks than were the other cybersecurity dimensions, achieving the formative maturity stage in Dimension 4. Moreover, the SADC region and the rest of Africa region had, on average, maturity stages below the rest of the world across all the dimensions. While the SADC region was slightly more mature than the rest of Africa in Dimension 5 (standards and technologies), the rest of Africa was slightly more mature than the SADC region in Dimensions 3 (building cybersecurity knowledge and capabilities) and 4 (legal and regulatory frameworks). On average, these two regions show similar maturity levels in Dimensions 1 (cybersecurity policy and strategy) and 2 (cybersecurity culture and society).

[273] See GCSCC. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Retrieved February 11, 2022, from https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[274] The regional group “rest of the world” includes three countries in South Asia, 32 countries in Latin America and the Caribbean, 14 countries in Europe and Central Asia, and 10 countries in East Asia and Pacific. For more information see https://gcscc.ox.ac.uk/cmm-reviews#/.

[275] Since its launch in 2014, the CMM has been edited twice to incorporate new cybersecurity topics in the framework, viz. the 2016 edition of the CMM (Global Cyber Security Capacity Centre, 2016) and the newest 2021 (Global Cyber Security Capacity Centre, 2021).

[276] The average maturity stage of each dimension was calculated with data of the maturity stages of the aspects following the dimension/factor/aspect hierarchy. First, the average maturity stage of factors was calculated with the maturity stage of aspects within each factor, following which, the average maturity stage of dimensions was calculated, using the average maturity stage of factors within each dimension.

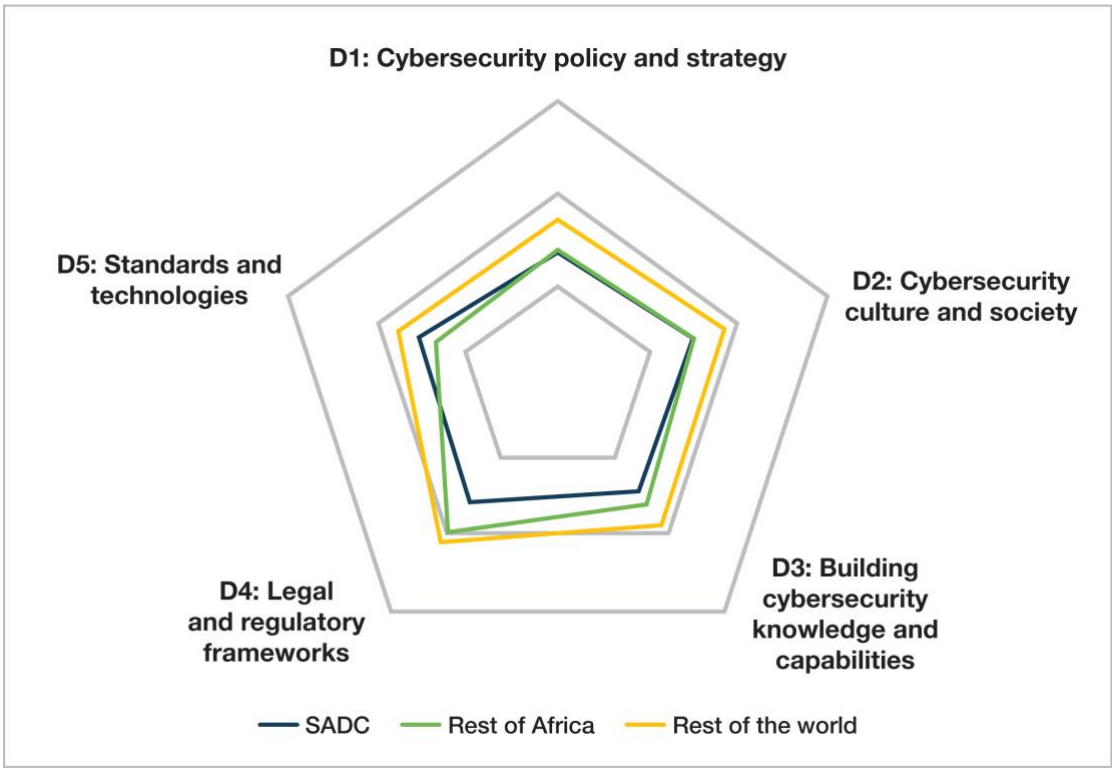

Figure 11: Average maturity stage of each CMM dimension per region.

The interior grey ring corresponds to the start-up maturity stage, the middle grey ring to the formative, and the exterior grey ring to the established.

When looking at the distribution of the average maturity stage in each dimension, there was variability observed within regions. In particular, the region referred to as 'rest of the world' contains very different countries, resulting in a high variance of the average maturity stages in all the dimensions. This region and the SADC region had some relatively extreme observations in the top distribution of some dimensions, with some countries achieving maturity stages above the established one. However, the SADC region had a higher proportion of countries with start-up maturity stages than the other two regions, resulting in a lower average maturity stage. This observation is repeated for all the CMM dimensions, except for Dimension 5 (standards and technologies) where, on average, the SADC region was more mature than the sample countries in the rest of Africa.

Regarding **Dimension 1** on the cybersecurity policy and strategy, for all the three regions national cybersecurity strategy and incident response were the two most mature factors on average. Although some countries in the SADC region increased the maturity in identification of incidents, the gap between the SADC region and the rest of the world was particularly large in the national incident response. Crisis management and cyber defence appeared to be less mature across the three regions, although the SADC region showed more maturity than the rest of Africa in crisis management.

On average, for all the three regions, media and social media were one of the most mature factors under **Dimension 2** on cybersecurity culture and society. Reporting mechanisms also stood out, particularly for SADC and the rest of Africa, while in the rest of world, maturity in trust and confidence on the internet and online services was more prominent. In contrast, the trust and confidence on the internet and online services was, on average, the least mature factor in the SADC region. The less mature

factor for the rest of Africa and the rest of world was the users' understanding of personal information protection online, which was not mature in the SADC region either.

In **Dimension 3** on the cybersecurity knowledge and capabilities, awareness raising was one of the most mature factors for the three regions. For some SADC countries previously assessed under the CMM, there was an increase in maturity in raising cybersecurity awareness, although more effort would be needed to eliminate the maturity gap between the SADC region and the other two regions. The framework for education and for professional training had a similar maturity level in the SADC region as it did in the rest of Africa. In the rest of the world region, the average value was closer to formative stage in the three factors, and the major maturity gap between this region and both the SADC and the rest of Africa regions was in the framework for professional training in cybersecurity.

As mentioned above, **Dimension 4** on cybersecurity legal and regulatory frameworks was the most mature dimension, where, on average, for the rest of Africa and the rest of the world. While the SADC region was showing progress in building capacity towards the formative stage, especially in those aspects related to the legal frameworks, the rest of Africa, on average, already achieved the formative maturity stage for the legal frameworks and the formal and informal cooperation frameworks to combat cybercrime. On average, the formal and informal cooperation framework was more mature in the rest of Africa region than it was in the rest of the world.

In **Dimension 5,** the internet infrastructure resilience and the cryptographic controls were two of the most mature factors for the three regions. Some SADC countries previously reviewed by the CMM showed improvements, particularly in the technical security controls and the cybersecurity marketplace. However, the cybersecurity marketplace is one of the less mature aspects for the three regions. Moreover, the SADC and the rest of Africa regions had a low maturity level in software quality and adherence to standards.

In summation, the CMM and C3SA data showed that the sample nations across the world were, on average, still in the initial phase of building cybersecurity capacity. While the SADC built capacity in a proportional way across the different dimensions, the rest of Africa and the world, on average, built cybersecurity at a faster pace, and with a stronger focus on the legal and regulatory frameworks of cybersecurity. As a consequence, certain gaps arose. The major differences in maturity between the SADC region and the rest of world, being the SADC region the less mature region, were in the trust and confidence on the internet (Dimension 2), the national incident response (Dimension 1), and the legal frameworks of cybersecurity (Dimension 4). The differences in maturity between the SADC region and the rest of Africa were less pronounced, although the largest ones were in formal and informal cooperation frameworks to combat cybercrime (Dimension 4), due to the fact that the SADC region less mature than the rest of Africa, and with regards to internet infrastructure resilience (Dimension 5), is more mature than the rest of Africa. Most countries in the sample revealed cybersecurity marketplace and software quality as low mature factors, raising concerns about the potential national dependence on foreign cybersecurity technology.

It is important to highlight that the different dimensions, factors, and aspects of cybersecurity are highly interconnected. For this reason, building capacity in a dimension is likely to improve the capacity of another dimension. For example, if the SADC region invests in raising awareness on cybersecurity, this may increase the user understanding of personal information protection online and, thus, the trust and confidence on the internet. Similarly, overlooking one of the cybersecurity dimensions

can hamper the potential benefits from investing efforts in the rest of cybersecurity dimensions. This regional study can help policy makers and stakeholders to identify key areas of prioritisation to build cybersecurity capacity that will make the most impact of their investments in the SADC countries, especially in times when cybersecurity competes with other urgent areas of investment, such as in the case of palliative measures against the COVID-19 pandemic.

Finally, the research team involved in this regional report faced some challenges when gathering evidence on the cybersecurity capacity of SADC countries. First, some internet connection problems were experienced during the interviews with cybersecurity expert and key informants. Second, notwithstanding the fact that diversity of languages in the region constitutes a source of cultural wealth, the lack of documents in English can be a barrier for international studies. This report came up against little or lack of evidence in English for some SADC countries that do not use English as an official language. That led the research team to search for documents in French and Portuguese in addition to English to minimise the risk of overlooking what may be relevant. Finally, the researchers were challenged by the lack of available information about SADC countries on the different topics and dimensions of cybersecurity of the CMM such as cybersecurity metrics, cybersecurity marketplace, and cyber defence. The difficulty of finding information on certain cybersecurity indicators was particularly important for countries that have not had a CMM review yet, as this has led to information gaps for some CMM aspects for those countries. As shown in Table 1, countries that have not yet had a full CMM review are Angola, the Comoros, the DRC, Seychelles, Zimbabwe and South Africa.

Appendices

Appendix 1: Cybersecurity Capacity Maturity Model – 2021 Edition

Dimensions of Cybersecurity Capacity

The Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, in consultation with over 200 international experts, developed the Cybersecurity Capacity Maturity Model for Nations (CMM). The model aims to provide a means for assessing a country's cybersecurity capabilities across and within multiple dimensions, providing a theoretical framework that allows to compare cybersecurity capacity across different nations. Concretely, the CMM considers five *dimensions* of cybersecurity capacity that encloses from developing policies to encouraging responsible cybersecurity culture within society, building cybersecurity knowledge, creating an effective legal framework, and controlling risks through standards and technologies. Each dimension consists of a set of *factors*, which describe and define what it means to possess cybersecurity capacity. Each factor in the CMM dimensions presents a number of *aspects* grouping together related *indicators*, which describe steps and actions that, once observed, define the stage of maturity of that aspect. Concretely, the CMM framework has 62 aspects and over 700 indicators (Global Cyber Security Capacity Centre, 2021). Table 6 shows the five dimensions together with the factors which constitute each one.

Table 6: CMM dimensions and corresponding factors

DIMENSIONS	FACTORS
Dimension 1 Cybersecurity Policy and Strategy	D1.1 National Cybersecurity Strategy D1.2 Incident Response and Crisis Management D1.3 Critical Infrastructure (CI) Protection D1.4 Cybersecurity in Defence and National Security
Dimension 2 Cybersecurity Culture and Society	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence in Online Services D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Online Platforms
Dimension 3 Building Cybersecurity Knowledge and Capabilities	D3.1 Building Cybersecurity Awareness D3.2 Cybersecurity Education D3.3 Cybersecurity Professional Training D3.4 Cybersecurity Research and Innovation
Dimension 4 Legal and Regulatory Frameworks	D4.1 Legal and Regulatory Provisions D4.2 Related Legislative Frameworks

	D4.3 Legal and Regulatory Capability and Capacity D4.4 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 Standards and Technologies	D5.1 Adherence to Standards D5.2 Security Controls D5.3 Software Quality D5.4 Communications and Internet Infrastructure Resilience D5.5 Cybersecurity Marketplace D5.6 Responsible Disclosure

Stages of Cybersecurity Capacity

There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage, and each aspect has its own indicators across the maturity stages. However, the maturity stages have been defined across aspects with the aim of being comparable. The start-up stage implies no existence of capacity or embryonic in nature, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

1) **Start-up:** at this stage either no cybersecurity maturity exists, or it is embryonic in nature. There might be initial discussions about cybersecurity capacity building; however, no concrete actions have been taken. There may be an absence of observable evidence of cybersecurity capacity at this stage.

2) **Formative:** some features of the aspect have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated.

3) **Established:** the indicators of the aspect are in place, and functioning. However, there is no well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the aspect. However, the aspect is functional and defined.

4) **Strategic:** at this stage, choices have been made about which parts of the aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the particular circumstances of the state or organisation.

5) **Dynamic:** there are clear mechanisms in place to alter strategy depending on the prevailing circumstances, such as the technological sophistication of the threat environment, global conflict, or a significant change in one area of concern (e.g., cybercrime or privacy). There is also evidence of global

leadership on cybersecurity issues. Dynamic organisations and key sectors, at least, have developed methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

National CMM Reports

Due to the limitations explained in Appendix 2, this regional study uses the CMM only as a framework to analyse the cybersecurity capacity landscape in the SADC region. However, the CMM is designed to be implemented at the national level, its deployment has its own methodology, and its output is a national evidence-based CMM report. This section briefly describes the national deployment of the CMM after a country has been identified to be reviewed or has requested a CMM review.

First, a team of researchers from the GCSCC (or implementation partner)[277] establishes a working relationship with a local host, sharing relevant logistical information in preparation for the review. The team of researchers conducts contextualising desk-research and travels to the country to conduct a three-day consultation process with representatives of national stakeholders from ten different clusters: (1) academia, civil society groups, and internet governance representatives; (2) criminal justice and law enforcement; (3) defence and intelligence community; (4) government ministries; (5) legislators and policy owners; (6) CSIRT and IT leaders from the government and the private sector; (7) critical national infrastructure; (8) private sector and business; (9) cyber task force responsible for developing cybersecurity strategy; and (10) international cooperation such as international organisations and relevant embassy partners. The representatives of these stakeholder clusters are previously identified and invited to participate in open discussions related to one or two dimensions of the CMM. Usually there are ten discussion sessions and participants are clustered into sessions based on their expertise in each dimension of the CMM. Sessions are organised in such a way that a dimension is discussed at least in two different sessions, and the data collected during the sessions needs to be evidenced.

After the in-country review, the team of researchers produces an evidence-based report and assigns maturity stages for each aspect in the CMM to benchmark the maturity of a country's cybersecurity capacity. This national report describes the in-country cybersecurity context, summarises the findings for each CMM factor and aspect, identifies priorities for investment, and provides recommendations that enable the country to enhance its cybersecurity capacity. If there were any gaps, these would be covered with subsequent desk research or remote follow-up sessions with stakeholders. During the process of drafting the report, the government provides feedback and additional evidence if needed. The final report is submitted to the government, and it is at its discretion to publish it or not.

Overall, the CMM process to review a nation typically lasts five months, from the initial agreement for reviewing a country to the completion of the national CMM report. Given

[277] The strategic and implementation partners of the GCSCC are the World Bank, Organization of American States, Oceania Cyber Security Centre, the International Telecommunication Union, Commonwealth Telecommunications Organisation, and Cybersecurity Capacity Centre for Southern Africa (C3SA).

the ambition of assessing the cybersecurity capacity of the SADC region under the CMM in a short period of time, this regional study used a different methodology which is described in Appendix 2.

Appendix 2: Study Methodology

The aims of this study are to ascertain the maturity of the cybersecurity capacity in the SADC region and to outline a possible path to improvement through key recommendations. The C3SA and its partners elected to follow a deductive mixed methods approach. Data was collected using an extensive document review (a desktop study) and in-depth interviews of key cybersecurity experts to fill the gaps in the desktop study. Data was analysed using thematic analysis and descriptive statistics for a time comparison regional analysis.

A Deductive Mixed Methods Approach

This cybersecurity capacity review of the SADC region is mainly a desktop study supported by key informant in-depth interviews. The aim is to get an estimate of the cybersecurity maturity of the SADC region. The study combines in a complementary manner, qualitative and quantitative data from various reports and publications with the views of subject matter experts. The study applies a deductive reasoning by using the 2021 edition of the CMM as a sensitising device and a lens in collecting and analysing data.

Data collection

The data for the study was collected in 2 phases. The first phase was a broad document review classifying documents as per aspects and factors of the CMM. The second phase consisted in conducting key informants' in-depth interviews.

Documents were collected and reviewed between March and June 2021. The starting point of the review was published and unpublished CMM review reports of countries in the region. When a national CMM report was available from a SADC country (Botswana, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, United Republic of Tanzania, and Zambia), this was reviewed as part of this regional study.[278] Given that CMM reviews of some SADC countries were conducted in 2016 (Table 1) and the cybersecurity landscape has changed, the data pool was broadened by adding other sources including official laws, policies, strategies, regulations, academic literature, reports from reputed international institutions and Non-Governmental Organisations (NGOs), and grey literature such as online media outlets. Documents were thoroughly read and examined according to the CMM. For every relevant document, a search for the words making a CMM aspect was executed looking for specific statements and explanations. The review covered over 200 documents.

The second phase of data collection consisted in key informant interviews. The aim of using key informant interviews was to assist in mending information discrepancies from the document review.[279] The key informants were selected purposefully and on recommendation because of their broad knowledge of the cybersecurity situation in their country and within the SADC; some key informants had already attended a CMM

[278] See Global Cyber Security Capacity Centre. (2021). *CMM Reviews around the World.* Retrieved March 28, 2022, from https://gcscc.ox.ac.uk/cmm-reviews

[279] See Marshall, M. N. (1996). The key informant technique. *Family practice*, *13*, 92-97.

review focus group in the past. Five in-depth interviews of cybersecurity experts were conducted respectively with representatives of ISOC Zimbabwe, MACRA CSIRT Malawi, the Ministry of PT&ICT in DRC, Wolfpack Risk Ltd in South Africa, and the INTIC + INCM Mozambique respectively assigned descriptors expert 1 to expert 5 (see Appendix 3). Data saturation was attained within this sample and no further exchanges were needed. All the interviews took place online on Microsoft Teams™ and Zoom™ platforms depending on the interviewee preference.[280, 281] For every encounter, consent was orally obtained, exchanges were recorded using an external audio-taping device to avoid any potential leak afforded by the digital data ease of copy, and the recording of 60 to 90 minutes was then transcribed.

The data from the document review and from the key informant interviews thereof was recorded into a detailed spreadsheet broken down into the various aspects of the CMM analytical framework.

Data analysis

The document review allowed to group findings per country and per usage as media article, report, strategy, policy, procedures and guidelines, regulations, and academic publications. From there, a deductive thematic analysis was conducted using the constructs of the CMM as search keywords. That process allowed us to ascertain evidence of relevant events, mechanism, infrastructure, resources and stakeholders. The evidence was collated for all countries in the SADC on an MS Excel spreadsheet to make it easy to ascertain differences and their scales.

Interviews were transcribed verbatim, and responses anonymised. Transcripts were analysed separately also using deductive thematic analysis, structuring the data into categories and then themes representing aspects and factors of the CMM. Transcripts were first read as a whole a few times so that researchers could immerse themselves in the data. Phrases were then selected and assigned to an adequate CMM aspect serving as code. Categories were identified from the codes as relationships and links were appreciated. This approach permitted a better understanding of key informants' perceptions and experiences regarding cybersecurity in the SADC. The result of this process was used to complement the lack of information in the spreadsheet.

For every SADC country, a national maturity stage was estimated for every aspect of capacity according to the five stages of maturity suggested in the CMM. To determine the level of maturity for the region, we counted the number of countries within each maturity stage of a given CMM aspect. That approach allowed us to have a grounded view of the cybersecurity capacity maturity of the SADC. Moreover, to allow for a regional time comparison, similar regional indicators were constructed with data at the aspect level from those ten SADC countries previously reviewed under the CMM (see Table 1). This data was facilitated by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. Those ten CMM reports were conducted between 2016 and 2020, and not all the reports considered the new aspects incorporated in the CMM over time. This generated missing information in some cases. Moreover, for

[280] The interviews took place online due to the COVID-19 restrictions prohibiting travel and promoting social distancing.

[281] See Innes, K., Jackson, D., Plummer, V., & Elliott, D. (2017). Emergency department waiting room nurse role: A key informant perspective. *Australasian Emergency Nursing Journal*, *20*(1), 6-11.

three countries, the data on the maturity stage of each aspect was not available, only the maturity stages at the factor level. To avoid losing more information, the maturity stage of aspects was extrapolated from the maturity stage of the corresponding factors. The resulting data at the aspect level is displayed in graphics, one per each dimension. The report anonymises the countries and does not discuss maturity at a national level. This was necessary because most national CMM reports in SADC are yet to be in the public domain. On request, data at a country level can be provided for consideration to all SADC countries.

Developing recommendations

For each dimension, the review recommends the next steps to be taken by countries individually and by the region to enhance their cybersecurity capacity. Some of the recommendations arose from discussions with and between stakeholders. If the capacity of a country for a certain aspect is at a formative stage of maturity, the country may look at the CMM indicators for the next stage and decide what to target. The recommendations provide advice and steps aimed at improving existing cybersecurity capacity as per the considerations of the CMM. The recommendations are provided specifically for each factor.

Limitations of the Study

The main limitations to the study include the limited time frame of 6 months to try to cover 16 countries in addition to their regional governance initiatives, the limited resources available to the study, and privacy and confidentiality requirements either limiting access to data or preventing its disclosure as evidence in the work.

Appendix 3: List of keynote interviewees

Descriptor	Position or specialty
Expert1	Technical – ISOC Zimbabwe
Expert2	MACRA - CSIRT-MW + Malawi
Expert3	Advisor to Minister of PT&ICT + Democratic Republic of the Congo
Expert4	Wolfpack Information Risk Ltd + https://wolfpackrisk.com + RSA
Expert5	INTIC + INCM Mozambique

Appendix 4: Status of substantive and procedural cybercrime legislation SADC

Country	Legislation
Angola	→ Criminal Code (Law 38/20) & Code of Criminal Procedure (Law 39/20)[282]
Botswana	→ Cybercrime and Computer Related Crimes Act 2018[283] → Communications Regulatory Authority Act 2012[284] → Electronic Communications and Transactions Act 2014[285] → Electronic Records (Evidence) Act 2014[286] → Data Protection Act 2018[287]
DRC	None
Comoros	None
Eswatini	→ Computer Crime and Cybercrime Bill, 2017 → Electronic Records (Evidence)
Lesotho	→ Lesotho is the Data Protection Act 2011[288] → Penal Code Act, 2012 (s 62 & 63).[289] → Computer Crime and Cybercrime Bill[290]
Madagascar	→ Law No. 2014-006 on the Fight Against Cybercrime (Loi n°2014-006 sur la lutte contre la cybercriminalité), → Law No. 2014-024 on Electronic Transactions (Loi n°2014-024 sur les transactions électroniques), → Law No. 2014-025 on Electronic Signature (Loi n°2014-025 sur la signature électronique), → Law No. 2014-026 Establishing the General Principles Relating to the Dematerialisation of Administrative Procedures (Loi n°2014-026 fixant les principes généraux relatifs à la dématérialisation des procédures administratives),

[282] See VDA Legal Partners. (2020). Angola Criminal Law in Line with International Standards. VDA Legal Partners. Retrieved December 14, 2021, from https://www.vda.pt/xms/files/05_Publicacoes/2020/Flashes_Newsletters/Flash_Vda_Legal_Partners_-_Angola_-_Criminal_Law_overhaul_in_line_with_International_Standards.pdf

[283] See https://www.bocra.org.bw/cybercrime-and-computer-related-crimes-act-2018

[284] See https://www.bocra.org.bw/communications-regulatory-authority-act-2012

[285] See https://www.bocra.org.bw/sites/default/files/Electronic-Communications-and-Transactions-Act-2014.pdf

[286] See https://www.bocra.org.bw/sites/default/files/Electronic%20Records%20and%20Evidence%20Act%202014.pdf

[287] See https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf

[288] See *Data Protection Act 2011.* (LSO). http://www.nic.ls/lsnic/community/policies/Data_Protection_Act_2011_Lesotho.pdf

[289] See https://lesotholii.org/ls/legislation/num-act/6

[290] See https://ictpolicyafrica.org/en/document/7hwpifnqr6l

	→ Law No. 2014-038 on the Protection of Personal Data (Loi n° 2014-038 sur la protection des données à caractère personnel).
Mauritius	→ Misuse and Cyber-Crime Act of 2003 (CMCA)[291] → The Data Protection Act of 2017[292] → The Electronic Transaction Act of 2000[293] → Child Protection Act of 1995[294] → Copyright Act of 2014[295] → National Payment Systems Act of 2018[296]
Mozambique	→ Penal Code, recently revised (Law n.º 24/2019)[297] → Electronic Transactions Act n.º 3/2017, → Telecommunications Traffic Control Decree, Decree n.º 75/2014 → Telecommunications Act, n.º 4/2016
Malawi	→ Electronic Transactions and Cyber Security Act (2016)[298] → Communications Act (2016)[299] → Data Protection Bill 2021[300]
Namibia	→ Electronic Transactions Act 4 of 2019[301] → Communications Act (2008)[302] → Cybercrime Law by 2016 (Draft)[303]
Seychelles	→ Computer Misuse Act 1998[304] → Penal Code[305]
South Africa	→ Films and Publications Amendment Act 11 of 2019[306]

[291] See https://www.icta.mu/docs/laws/cyber.pdf

[292] See https://mauritiusassembly.govmu.org/Documents/Acts/2017/act2017.pdf

[293] See https://www.icta.mu/docs/laws/eta.pdf

[294] See https://www.icta.mu/docs/laws/child_protection.pdf

[295] See https://www.icta.mu/docs/laws/copyright2014.pdf

[296] See https://www.bom.mu/sites/default/files/the_national_payment_systems_act_2018_amended_12.08.21_plain.pdf

[297] See https://reformar.co.mz/documentos-diversos/lei-24-2019-lei-de-revisao-do-codigo-penal.pdf

[298] See https://malawilii.org/mw/legislation/act/2016/33

[299] See https://malawilii.org/mw/legislation/act/2016/33

[300] See https://cipesa.org/2021/06/data-protection-law-on-the-horizon-in-malawi/

[301] See http://www.lac.org.na/laws/2019/7068.pdf

[302] See https://www.lac.org.na/laws/annoSTAT/Communications%20Act%208%20of%202009.pdf

[303] See https://www.coe.int/en/web/octopus/-/namibia?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3Zl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2

[304] See https://www.seychelleslaw.sc/c/computer-misuse-act-1998

[305] See https://greybook.seylii.org/w/se/CAP158#!fragment/zoupio-_Toc47936089/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgBYB2ATgGYAbAAYAHDwCUAGmTZShCAEVEhXAE9oAcg2SIhMLgRKV6rTr0GQAZTykAQuoBKAUQAyTgGoBBAHIBhJ5KkYABG0KTs4uJAA

[306] See https://www.gov.za/documents/films-and-publications-amendment-act-11-2019-3-oct-2019-0000

	→ Electronic Communications and Transactions Act 25 of 2002[307] → Protection of Personal Information Act, No 4 of 2013[308] → Cybercrimes Act 19 of 2020[309]
Tanzania	→ Cybercrime Act of 2015[310] → Electronic Transactions Act 2015[311]
Zambia	→ Cyber Security and Cyber Crimes Act No. 2 of 2021[312] → Electronic Communications and Transactions Act No. 4 of 2021[313] → Data Protection Act No. 3 of 2021[314] → Information and Communications Technologies Act No. 15 of 2009[315]
Zimbabwe	→ The Interception of Communications Act of 2007[124] → Postal and Telecommunications Act of 2000, as amended[316] → Criminal Law Code has been revised to include cyber-crimes (Section 162 - 168)[125] → Cybersecurity and Data Protection Bill 2019[317]

Source: C3SA 2021

[307] See https://www.gov.za/documents/electronic-communications-and-transactions-act

[308] See https://www.gov.za/documents/protection-personal-information-act

[309] See https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000

[310] See http://www.parliament.go.tz/polis/uploads/bills/acts/1452061463-ActNo-14-2015-Book-11-20.pdf

[311] See https://tanzlii.org/tz/legislation/act/2015/13-0

[312] See https://www.dataguidance.com/sites/default/files/act_no._2_of_2021the_cyber_security_and_cyber_crimes.pdf

[313] See https://www.dataguidance.com/sites/default/files/act_no._4_of_2021_the_electronic_communications_and_transactions_0.pdf

[314] See https://www.dataguidance.com/sites/default/files/act_no._3_the_data_protection_act_2021_0.pdf

[315] See https://www.parliament.gov.zm/sites/default/files/documents/acts/Information%20and%20Communication%20Technologies%20Act,%202009.pdf

[316] See http://www.potraz.gov.zw/?ddownload=896

[317] See https://www.dataguidance.com/notes/zimbabwe-data-protection-overview

Bibliography

Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018). Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index. *SSRN Electronic Journal,* 1–21. https://doi.org/10.2139/ssrn.3142296

Africa Center for Strategic Studies. (2021). *Africa's Evolving Cyber Threats.* https://africacenter.org/spotlight/africa-evolving-cyber-threats/

AfricaCERT. (n.d.). *African CSIRTs*. Retrieved March 5, 2022, from https://www.africacert.org/african-csirts/

African Union (2014, June 27). *African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

African Union. (n.d). List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection. https://au.int/sites/default/files/treaties/29560-sl AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

Alberto Galhardo Simões. (2021). Data protection and cybersecurity laws in Angola. Retrieved March 5, 2022, from https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/angola

Athanase, P. & Uranie S. (2016, June). *Seychelles parliament passes bill to criminalize technology crimes.* Seychelles News Agency. Retrieved March 6, 2022, from http://www.seychellesnewsagency.com/articles/5307/Seychelles+parliament+passes+bill+to+criminalize+technology+crimes

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf*

Bada, M., Von Solms, B., & Agrafiotis, I. (2018). Reviewing national cybersecurity awareness in Africa: an empirical study. *Proceedings of the Third International Conference on Cyber-Technologies and Cyber-Systems, Cyber 2018, Greece,* 78-83. https://www.thinkmind.org/index.php?view=instance&instance=CYBER+2018

Bada, M., Von Solms, B., & Agrafiotis, I. (2019, October 2). Reviewing national cybersecurity awareness for users and executives in Africa. *International Journal on Advances in Security 12*(1&2), 108-118. https://arxiv.org/abs/1910.01005

Bank of Mauritius. (2001). *Guideline on internet banking*. Retrieved March 5, 2022, from https://www.bom.mu/sites/default/files/Guideline_on_internet_banking.pdf

BizCommunity. (2019, February 8). SA is at high risk for harmful online behaviour. Retrieved March 5, 2022, from https://www.bizcommunity.com/Article/196/661/187159.html

Bowmans. (2018, December 28). *Privacy and Data Protection in Tanzania (Part 1)*. Retrieved March 6, 2022, from https://www.bowmanslaw.com/insights/intellectual-property/privacy-and-data-protection-in-tanzania-part-1/

Bowmans. (2019, February 2). *Privacy and Data Protection in Tanzania | Data Privacy Laws in Tanzania*. Retrieved January 27, 2022, from https://www.bowmanslaw.com/insights/intellectual-property/privacy-and-data-protection-in-tanzania-part-1/

Calandro, E., & Berglund, N. (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC case. *In GIGAnet annual symposium. Berlin.* https://researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf

Caralli, R., Knight, M. & Montgomery, A. (2012). *Maturity Models 101: A primer for applying maturity models to smart grid security, resilience, and interoperability*. (p.3). Retrieved November 11, 2021, from https://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf

Cassim, F. (2010). Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study. *Potchefstroom Electronic Law Journal, 12*(4), 33-79. https://doi.org/10.17159/1727-3781/2009/v12i4a2740

Central Bank of Seychelles. (2021). *Central Bank of Seychelles cyber security guidelines 2019.* Retrieved March 5, 2022, from https://cbs.sc/Downloads/legislations/Cyber%20Security%20Guidelines%20April%202019.pdf

Centre for Strategic and International Studies. (2017, June 30). *Concept and Definition of Civil Society Sustainability*. Retrieved March 17, 2022, from https://www.csis.org/analysis/concept-and-definition-civil-society-sustainability

Choo, K.K.R. 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Churu, J. (2021, October 6). *Network of Young Cybersmart Champions launched in Botswana*. https://www.biztechafrica.com/article/network-young-cybersmart-champions-launched-botswa/16811/

CIPESA. (2018, August 6). *Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa*. Retrieved January 24, 2022, from https://cipesa.org/2018/08/challenges-and-prospects-of-the-general-data-protection-regulation-gdpr-in-africa/

Cisco Systems. (2022). *What is Cybersecurity?* Retrieved March 15, 2022, from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Connecting Africa. (2020, September 30). *Strong mobile growth predicted for sub-Saharan Africa - GSMA*. Retrieved February 22, 2022, from https://www.connectingafrica.com/author.asp?section_id=761&doc_id=764310

Council of Europe (2014, August 11). *GLACY cybercrime capacity building in Mauritius*. Retrieved February 10, 2022, from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803028a5

Council of Europe (2022). *The Budapest Convention 24/7 point of contact network*. Retrieved March 5, 2022, from https://rm.coe.int/3148-afc2018-ws8-24-7bc-ml/16808e6884

Council of Europe. (2019) (n.d.). *Mauritius*. Octopus Cybercrime Community. Retrieved March 16, 2022, from https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/mauritius?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/

Council of Europe. (n.d.) *Judicial training skills and introductory cybercrime and electronic evidence course.* Retrieved February 10, 2022, from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803036db

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. *Personal and Ubiquitous Computing*, 1-15.

Critical Infrastructure Protection Act of 2019. (Republic of South Africa). https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf

Cyber Security and Cyber Crimes Act of 2021. s. 4 (Republic of Zambia). https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf

Cyber Security and Cyber Crimes Act of 2021. s. 5 (Republic of Zambia) https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf

Cyber4Dev. (2020, November 18). *Young people of Botswana find creative ways to promote Cyber Resilience.* Retrieved February 16, 2022, from https://cyber4dev.eu/2020/11/18/young-people-of-botswana-find-creative-ways-to-promote-cyber-resilience/

Cybercrimes Act of 2020. (Republic of South Africa). https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

Cybersecurity Observatory. (2020). *Cybersecurity Risks, Progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Cybersecurity Tech Accord. (2020). *Cybersecurity Awareness in the Commonwealth of Nations*. https://cybertechaccord.org/uploads/prod/2020/03/TechAccord-awareness-06.pdf

Daigle, B. (2021). *Data protection laws in Africa: A Pan-African survey and noted trends.* Retrieved March 8,2022, from https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf

Data Protect. (2019). *La cybersécurité dans le secteur financier Africain*. https://www.sciencetech.com/fr/wp-content/uploads/2021/01/Afrique_Faits-saillants_12sep19.pdf

Data Protection Act 2011. (LSO). http://www.nic.ls/lsnic/community/policies/Data_Protection_Act_2011_Lesotho.pdf

De Wet, P. & Benjamin, C. (2015, January 22). National key points: The list you weren't meant to see. *Mail & Guardian*. Retrieved March 4, 2022, from https://mg.co.za/article/2015-01-22-national-key-points-the-list-you-werent-meant-to-see

DLA Piper. (2021, December 7). *Global Data Protection Laws of the World – Namibia*. DLA Piper Global Data Protection Laws of the World. Retrieved March 6, 2022, from https://www.dlapiperdataprotection.com/index.html?t=law&c=NA&c2=

DLA Piper. (2021). *Global Data Protection Laws of the World – Mozambique*. DLA Piper Data Protection. Retrieved March 6, 2022, from https://www.dlapiperdataprotection.com/index.html?t=law&c=MZ&c2=

Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of cybersecurity: a South African context. *Acta Criminologica: African Journal of Criminology & Victimology, 31*(3), 111-131 https://sahs.ukzn.ac.za/wp-content/uploads/2019/07/PUBLIC-PERCEPTIONS-OF-CYBERSECURITY-A-SOUTH-AFRICAN-CONTEXT.pdf

Dutton, W. H. (2017). Fostering a cyber security mindset. *Internet Policy Review, 6*(1). https://doi.org/10.14763/2017.1.443

Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology. *Information, Communication & Society*, *9*(4), 433-451.

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy, 9*(1), 280-306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Electronic Communications and Transactions Act 25 of 2002. ZA. Ss. 80-84. Retrieved March 6, 2022, from https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf

Films and Publications Amendment Act of 2019. (South Africa). Retrieved March 15, 2022, from https://www.gov.za/sites/default/files/gcis_document/201910/42743gon1292.pdf

Finmark Trust, Cenfri & UNCDF. (2017). Madagascar: Catalysing and supporting the financial services sector to enhance inclusiveness in Madagascar: Financial Inclusion Roadmap. Retrieved January 10, 2022, from https://finmark.org.za/system/documents/files/000/000/228/original/Madagascar-Roadmap.pdf?1601992328

Firewater, K. (2019, December 6). *Online child protection*. Pygma Consulting. Retrieved March 6, 2022, from http://pygmaconsulting.com/online-child-protection/

Gallagher, R. & Burkhardt, P. (2021, July 29). '*Death Kitty' Ransomware Linked to South African Port Attack*. Bloomberg. Retrieved March 5, 2022, from https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports

Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition*. Retrieved February 11, 2022, from https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

Global Cyber Security Capacity Centre. (2022). *CMM Reviews around the World*. https://gcscc.ox.ac.uk/cmm-reviews#/

Global Prosecutors E-Crime Network. (n.d.). *Global prosecutors e- crime network. History of the Global Prosecutors E-Crime Network.* International Association of Prosecutors. Retrieved February 23, 2022, from https://www.iap-association.org/GPEN/About-GPEN/History

Government of Malawi. (2019). *Malawi National Cybersecurity Strategy (2019-2024)*. https://api.pppc.mw/storage/160/National-Cybers-col.pdf

Government of Mozambique. (2017). *Estratégia Nacional de Segurança Cibernética de Moçambique - (Proposta) (2017-2021) Versão*. https://www.oam.org.mz/wp-content/uploads/2017/06/Draft_National_Cyber_Security_Strategy_Mozambique_PT_GT_24052017FINAL.pdf

GSM Association. (2019). *The Mobile Economy Sub-Saharan Africa 2019*. Retrieved February 20, 2022, from https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=45121567&file=2794-160719-ME-SSA.pdf

GSM Association. (2021). *The Mobile Economy Sub-Saharan Africa 2021*. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf

GSM Association. (2021). *The Mobile Economy Sub-Saharan Africa 2021*. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf

IBM Global Technology Services. (2014). *IBM Security Services 2014 Cyber Security Intelligence Index.* https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

IFC. (2020). *e-Conomy Africa 2020 - Africa's $180 Billion Internet Economy Future.* https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/google-e-conomy

Ilori, T. (n.d.). Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions. 1–18.

IMF Blog. (2020). *Fintech in Sub-Saharan Africa: A Potential Game Changer*. https://blogs.imf.org/2019/02/14/fintech-in-sub-saharan-africa-a-potential-game-changer/

Innes, K., Jackson, D., Plummer, V., & Elliott, D. (2017). Emergency department waiting room nurse role: A key informant perspective. *Australasian Emergency Nursing Journal*, *20*(1), 6-11.

International Finance Corporation. (2020). *e-Conomy Africa 2020 - Africa's $180 Billion Internet Economy Future*. Retrieved March 6, 2022, from https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/google-e-conomy

International Monetary Fund (IMF). (2019). *Fintech in Sub-Saharan Africa: A Potential Game Changer.* https://blogs.imf.org/2019/02/14/fintech-in-sub-saharan-africa-a-potential-game-changer/

INTERPOL. (2021). *African cyberthreat assessment report*. Retrieved March 4, 2022, from https://www.interpol.int/en/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

ITU. (2012). *Data Protection: Southern African Development Community (SADC) Model Law*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

ITU. *(2012). Draft Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce.* Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA). https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/electronic%20transaction.pdf

ITU. (2012). Draft Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce. *Support for Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA)*. https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/electronic%20transaction.pdf

ITU. (2013). *Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law.* Retrieved March 5, 2022 from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

ITU. (2013). *Data Protection: Southern African Development Community (SADC) Model Law.* Retrieved March 5, 2022, from https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

ITU. (2013). *Electronic Transactions and Electronic Commerce: Southern African Development Community (SADC) Model Law*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

ITU. (2013). *Electronic Transactions and Electronic Commerce: Southern African Development Community (SADC) Model Law*. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

ITU. (2020, April). *COVID-19 and its implications for protecting children online*. Retrieved January 20, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf

ITU. (2020). *Global Security Index*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU. (2020). *Guidelines for policy-makers on child online protection*. p.45. Retrieved November 11, 2021, from https://8a8e3fff-ace4-4a3a-a495-

4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

ITU. (2021). Digital Trends in Africa 2021. Information and communication technology trends and developments in the Africa region 2017-2020

Jenalda, M., & Kurebwa, J. (2020). Multilateral Responses to Cybercrimes in the SADC Region: *The Case of Zimbabwe and South Africa*. https://doi.org/10.3968/11946

John, S. N., Noma-Osaghae, E., Oajide, F., & Okokpujie, K. (2020). Cybersecurity Education: The Skills Gap, Hurdle!. In *Innovations in Cybersecurity Education* (pp. 361-376). Springer, Cham.

Kainja, J. (2021, June 22). *Data Protection Law on the Horizon in Malawi*. CIPESA. Retrieved March 16, 2022, from https://cipesa.org/2021/06/data-protection-law-on-the-horizon-in-malawi/

Kathuria, Vinish & Oh, Keun Yeob. (2018). ICT access: Testing for convergence across countries. *The Information Society, 34*(3), 166–182. https://doi.org/10.1080/01972243.2018.1438549

Kingdom of eSwatini. (2020). *Eswatini National Cybersecurity Strategy 2025*. http://www.gov.sz/images/ICT/Eswatini-National-Cybersecurity-Strategy-NCS-2025.pdf

KnowBe4 Africa. (2020). *2020 African Cybersecurity Research Report*. https://www.knowbe4.com/hubfs/2020%20African%20Cybersecurity%20Research%20Report.pdf?hsCtaTracking=9de8b71e-3443-4b75-a7df-ccdc81607b89%7C3ac45c4f-3fac-404d-8b48-59c0c204d07f

Koyabe, M. (2019). *Critical Information Infrastructure Protection: Commonwealth Perspective.* https://www.torchlightgroup.com/media/CTO-FCO-Critical_National_Information_Infrastructure_Protection.pdf

Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity, 2012*, 1.

Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity, 2012*, 1.

Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity, 2012*, 1.

Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313-338.

Kshetri, N. (2016). Cybersecurity and development. *Markets, Globalization & Development Review, 1*(2). https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1012&context=mgdr

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77-81. https://doi.org/10.1080/1097198x.2019.1603527

Kubatana. (2020, October 2). *An analysis of Social Media use in the SADC region 2014 – 2020*. Retrieved February 10, 2022, from https://kubatana.net/2020/10/02/an-analysis-of-social-media-use-in-the-sadc-region-2014-2020/

Kwaramba, M. (2020, October 14). *Zimbabwe's restrictions on mobile money punish the users, not the offenders*. Retrieved March 10, 2022, from https://www.theafricareport.com/45825/zimbabwes-restrictions-on-mobile-money-transfers-punish-the-users/

Lemauricien (2020, September 20). *Cybersécurité : Création d'un centre de formation régionale à Maurice*. Retrieved January 28, 2022, from https://www.lemauricien.com/actualites/cybersecurite-creation-dun-centre-de-formation-regionale-a-maurice/378283/

Lombard, M. (2021). Parol evidence and the Consumer Protection Act 68 of 2008. *Potchefstroom Electronic Law Journal*, *24*, 1–27. https://doi.org/10.17159/1727-3781/2021/v24i0a9486

Mahler, D., Montes, J., & Newhouse, D. (2019). *Internet Access in Sub-Saharan Africa. World Bank Group. Poverty & Equity Notes*. Retrieved March 5, 2022, from https://documents1.worldbank.org/curated/en/518261552658319590/pdf/Internet-Access-in-Sub-Saharan-Africa.pdf

Malatji, M.; Marnewick, A.L.; von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability, 13*(1), 291. https://doi.org/10.3390/su13010291

Mannion, C. (2020). Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets. *Vanderbilt Law Review, 53,* 685.

Markowitz, C. (2019). Harnessing the 4IR in SADC: Roles for Policymakers Occasional Paper 303. *South African Institute of International Affairs*, *October*, 1–47. https://media.africaportal.org/documents/Occasional-Paper-303-markowitz.pdf

Marler, W. (2018). Mobile phones and inequality: Findings, trends, and future directions. *New Media & Society, 20*(9), 3498-3520.

Marshall, M. N. (1996). The key informant technique. *Family practice*, *13*, 92-97.

Mauritius Police Force. (2021). *Police IT Unit*. Retrieved March 5, 2022, from https://police.govmu.org/police/?page_id=5779

Mawarire, T. (2020). "Things will never be the same again". *Covid-19 effects on freedom of expression in Southern Africa.* https://internews.org/wp-content/uploads/2021/02/Internews_Effects_COVID-19_Freedom_of_Expression_Southern_Africa_2020-12.pdf

McKinsey & Company. (2020). *How the COVID-19 crisis can catalyze change across the continent*. https://www.mckinsey.com/featured-insights/middle-east-and-africa/reopening-and-reimagining-africa

Microsoft News Center. (2019, February 7). *Microsoft research reveals South Africa at high risk for harmful online behaviour.* Retrieved March 16, 2022, from https://news.microsoft.com/en-xm/2019/02/07/microsoft-research-reveals-south-africans-at-high-risk-for-harmful-online-behaviour/

Mokeresete, M., & Esiefarienrhe, B. M. (2020, November). Users' perspective on the assessment of Botswana Fibre Backbone Network Infrastructure. In *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 1-8). IEEE. https://doi.org/10.1109/IMITEC50163.2020.9334128

Mudavanhu, E. (2021, April). *Lesotho - Data Protection Overview*. Retrieved February 10, 2022, from https://www.dataguidance.com/notes/lesotho-data-protection-overview

Munyoka, W., & Maharaj, M. (2017, May). Understanding eGovernment utilisation within the SADC. In *2017 IST-Africa Week Conference (IST-Africa)* (pp. 1-10). IEEE.

Munyoka, W., & Maharaj, M. S. (2019). Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries. *SA Journal of Information Management*, *21*(1), 1–9. https://doi.org/10.4102/sajim.v21i1.983

Mutsaka, F. (2020, December 7). Zimbabwe arrests 2 men for selling fake COVID-19 results. Retrieved March 5, 2022, from https://apnews.com/article/arrests-zambia-zimbabwe-coronavirus-pandemic-6d8fc1964f5a152c5a0d1b71d4f5f9b0

Mwakatumbula, H. J., Moshi, G. C., & Mitomo, H. (2019). Consumer protection in the telecommunication sector: A comparative institutional analysis of five African countries. *Telecommunications Policy*, *43*(7), 101808. https://doi.org/10.1016/j.telpol.2019.02.002

Mwasomola U.L., Ojwang E., Pastory D., (2020). Examining The Consumer Protection And Comprehensive in E-Commerce in Tanzania. *Business Education Journal, 4*(1). http://www.cbe.ac.tz/bej

National Key Points Act of 1980. (Republic of South Africa). https://www.gov.za/sites/default/files/gcis_document/201503/act-102-1980.pdf

Ncube, C. B., Schonwetter, T., Oguamanam, C., & de Beer, J. (2017). Intellectual Property Rights and Innovation: Assessing Regional Integration in Africa (Aria VIII). *SSRN Electronic Journal*, *May*. https://doi.org/10.2139/ssrn.3078997

Nganje, F. (2021). *Building Anticipatory Governance in SADC: Post-COVID-19 Governance Outlook.* https://media.africaportal.org/documents/Occasional-Paper-324-nganje.pdf

Nortjé, J.G.J., & Myburgh, D.C. (2019). The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa. *Potchefstroom Electronic Law Journal, 22*(22), 1-42. http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886

Nyimbiri, B. A. (2021). The Impact of the Mobile Money on People's Use of Financial Services in Sub-Sahara Africa. *Management Dynamics in the Knowledge Economy*, *9*(1), 137-146.

Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on Facebook social media: Facebook. *South African Journal of Sciences*, *114*(5), 1–5. http://www.sajs.co.za

Oozeer, A. (2021, April). *Mauritius - Data Protection Overview*. Retrieved February 10, 2022, from https://www.dataguidance.com/notes/mauritius-data-protection-overview

Organisation for Economic Co-operation and Development. (2020). *OECD Policy Responses to Coronavirus (COVID-19): Keeping the Internet up and running in times of crisis*. Retrieved January 14, 2022, from https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/

Orji, U. J. (2015, May). Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation? In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, (pp. 105-118). IEEE. https://ieeexplore.ieee.org/stamp.jsp?tp=&arnumber=7158472

Overseas Security Advisory Council. (2019). *Mauritius 2019 Crime & Safety Report*. Retrieved February 9, 2022, from https://www.osac.gov/Country/Mauritius/Content/Detail/Report/e248beb4-219e-4708-a774-15f4aed12f9e

Penal Code 1955. (Seychelles). Ss. 363A-368A. Retrieved February 26, 2022, from https://seychelleslaw.sc/p/penal-code

Penal Code 2012. s.62. (Lesotho) Retrieved February 26, 2022, from https://lesotholii.org/ls/legislation/num-act/6

Plessis, C. (2020, September 4). *eSwatini govt says new cybercrime bill won't limit press freedom*. Ewn. Retrieved March 5, 2022, from https://ewn.co.za/2020/09/04/eswatini-govt-says-new-cybercrime-bill-won-t-limit-press-freedom

Procurement Regulatory Authority of Zimbabwe. (2021). *Highlights of Procurement Reforms*. PRAZ. http://www.praz.org.zw/?page_id=90

Raytheon. (2015). *2015 industry drill-down report financial services*. Retrieved March 6, 2022, from http://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf

Registrar of Financial Institutions - Reserve Bank of Malawi. (2019). *Guidelines on information and cybersecurity risk management for banks.* Retrieved March 6, 2022, from https://www.rbm.mw/Home/GetContentFile/?ContentID=35422

Republic of Botswana. (n.d). *National Cybersecurity Strategy*. Retrieved March 3, 2022, from https://www.bocra.org.bw/sites/default/files/documents/approved%20botswana-national-cybersecurity-strategy.pdf

Republic of Mauritius. (2014). *National Cybersecurity Strategy 2014 – 2019.* https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Mauritius_2014_National%20Cyber%20Security%20Strategy%20-%202014%20-%20EN.pdf

Republic of Mauritius. (2020). *Cyber Security*. Retrieved March 10, 2022, from https://govmu.org/EN/infoservices/comm/Pages/security.aspx

Republic of Zambia. (2021). *National Cybersecurity Policy 2021*. Retrieved January 5, 2022, from https://www.mtc.gov.zm/wp-content/uploads/2021/06/National-Cybersecurity-Policy2_compressed.pdf

Republic of Zambia. (2021). *National Cybersecurity Policy Implementation Plan 2021-2025*. Retrieved March 4, 2022. https://www.mtc.gov.zm/wp-content/uploads/2021/06/National-Cybersecurity-Policy-Implementation-Plan-2021-2025.pdf

Research ICT Africa. (2018). *After Access*. Retrieved February 17, 2022, from https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Reserve Bank of Zimbabwe. (2021). *CIRCULAR NO. NPS/02 /2021*. Retrieved February 21, 2022, from https://www.rbz.co.zw/documents/nps/2021/NPS-CIRCULAR-ON-THE-ISSUANCE-OF-CYBER-SECURITY-FRAMEWORK.pdf

Reserve Bank of Zimbabwe. (2021). *National payment systems risk based guideline on cybersecurity.* Retrieved February 21, 2022, from https://www.rbz.co.zw/documents/nps/2021/NPS-CYBER-SECURITY-FRAMEWORK-20210427.pdf

Richards, N. U., & Eboibi, F. E. (2021). African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law? *International Review of Law, Computers & Technology, 35*(2), 131-161. https://doi.org/10.1080/13600869.2021.1885105

SADC (2012). *Southern African Regional Police Chiefs Co-operation Organisation*. Retrieved February 17, 2022, from https://www.sadc.int/themes/politics-defence-security/police-sarpcco/

SADC. (1996). *Protocol on Transport, Communications and Meteorology.* Retrieved March 6, 2022, from https://www.sadc.int/files/7613/5292/8370/Protocol_on_Transport_Communications_and_Meteorology_1996.pdf

SADC. (2002). *SADC Protocol on Extradition.* Retrieved March 6, 2022, from https://www.sadc.int/files/3513/5292/8371/Protocol_on_Extradiction.pdf

SADC. (2002). *SADC Protocol on Mutual Legal Assistance in Criminal Matters*. Retrieved March 6, 2022, from https://www.sadc.int/files/8413/5292/8366/Protocol_on_Mutual_Legal_Assistance_in_Criminal_Matters_2002.pdf

SADC. (2010). *e-SADC Strategic Framework.* Retrieved March 15, 2022. https://repository.uneca.org/bitstream/handle/10855/21168/32387.pdf?sequence=3&isAllowed=y

SADC. (2012). *Provision of Microsoft Enterprise Agreement for Southern African Development Community*. Retrieved March 13, 2022, from https://www.sadc.int/opportunities/procurement/closed-opportuniti/provision-microsoft-enterprise-agreement-southern-african-development-community-sadc/

SADC. (2012). *SADC overview*. Retrieved March 6, 2022, from https://www.sadc.int/about-sadc/overview

SADC. (2012). *Southern African Development Community: ICT & Telecommunications*. Retrieved March 6, 2022, from https://www.sadc.int/themes/infrastructure/ict-telecommunications/

SADC. (2020, October). *SADC Regional Indicative Strategic Plan (RISPD) 2020-2030*. Retrieved February 2, 2022, from https://www.sadc.int/files/4716/1434/6113/RISDP_2020-2030_F.pdf

SADC. (2022). Consultancy for revision and modernisation of the SADC data protection model law. Retrieved March 7, 2022, from https://www.sadc.int/files/8216/4400/4803/CONSULTANCY_FOR_THE_SADC_DATA_PROTECTION_MODEL_LAW_04022022.pdf

SADC. (2022). *Southern African Development Community Vision 2050*. Retrieved February 20, 2022, from https://www.sadc.int/files/9316/1470/6253/SADC_Vision_2050.pdf

SADC. (July 2021). SADC Ministers of Transport, ICT, Information and Meteorology meet to discuss sectoral issues. Retrieved March 17, 2022, from https://www.sadc.int/news-events/news/sadc-ministers-transport-ict-information-and-meteorology-meet-discuss-sectoral-issues/

Schia, N. N., & Gjesvik, L. (2018). *Managing a Digital Revolution - Cyber Security Capacity Building in Myanmar*. NUPI Report. http://hdl.handle.net/11250/2563201

Serianu. (2016). *Africa Cyber Security Report*. Retrieved December 11, 2021, from http://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

Serianu. (2016). *Africa Cybersecurity Report*. https://www.cybersecurityhub.gov.za/cyberawareness/images/pdfs/AfricaCyberSecurityReport20161.pdf

Serianu. (2018). Cyber security Report-Lesotho. *Cyber security skills gap.* https://www.serianu.com/downloads/LesothoCyberSecurityReport2018.pdf

Serianu. (2019). *Africa Cyber Security Report. Local Perspective on Data Protection and Privacy Laws: Insights from African SMEs*. Retrieved March 10, 2022, from https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

South Africa Department of Social Development. (2019). *National Child Care and Protection Policy.* Retrieved March 6, 2022, from https://www.gov.za/sites/default/files/gcis_document/202102/national-child-care-and-protection-policy.pdf

South African Banking Risk Information Centre. (2020). Annual Report 2020. Retrieved March 3, 2022, from https://www.sabric.co.za/media/lejmweri/sabric_annual-report_2020.pdf

South African Government. (n.d.). Fake news-Coronavirus COVID-19. Retrieved March 6, 2022, from https://www.gov.za/covid-19/resources/fake-news-coronavirus-covid-19

SADC. (n.d.). *About SADC*. Retrieved March 1, 2022, from https://www.sadc.int/about-sadc/

SADC (2017). *SADC Guidelines for Procurement and Grants of 1st January 2017. As amended on 20th November.* SADC Secretariat https://www.sadc.int/files/6816/0620/8029/SADC_Procurement_and_Grants_Guidelines_20_November_2020.pdf

Sur la protection des données à caractère personnel de 2014. (Madagascar). (Law No. 2014 038 relating to protection of personal data) (FRENCH). Retrieved March 6, 2022, from https://ictpolicyafrica.org/en/document/fes5q7floqd?page=3

Swales, L. (2018). An analysis of the regulatory environment governing hearsay electronic evidence in South Africa: suggestions for reform–part two. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, 21*(1). http://www.saflii.org/cgi-bin/disp.pl?file=za/journals/PER/2018/47.html&query=cybercrime

Sylla, A., & Ford-Cox, A. (2019, October 14). *Overview of data protection laws in Africa*. Lexology. Retrieved March 10, 2022, from https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2

The Cyber Security and Cyber Crimes Act, 2021 (Republic of Zambia) Retrieved March 4, 2022, from https://www.parliament.gov.zm/node/8832

The Electronic and Postal Communications of 2010. (Republic of Tanzania). Retrieved January 27, 2022 from https://www.researchictafrica.net/countries/tanzania/Electronic_and_Postal_Communications_Act_no_3_2010.pdf

The European Union Agency for Cybersecurity. (2017). *Cyber Security Culture in Organisations*. Retrieved March 7, 2022, from https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

The G8 24/7 Network of Contact Points. (n.d.). *Protocol statement*. Retrieved March 10, 2022, from http://www.oas.org/juridico/english/cyb_pry_g8_network.pdf

The National Institute of Information and Communication Technologies (INTIC). (2021). Government approves national cybersecurity policy and strategy. Retrieved March 25, 2022, from https://www-intic-gov-mz.translate.goog/?p=979&_x_tr_sl=pt&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

The Software Alliance. (2018). *Software Management: Security Imperative, Business Opportunity.* Global Software Survey, 24. Retrieved March 14, 2022, from https://www.bsa.org/news-events/news/bsas-2018-global-software-survey-shows-better-software-management-can-improve-security-and-boost-bottom-line

The World Bank. (2022). *Individuals using the Internet (% of population) - Sub-Saharan Africa | Data*. Retrieved March 6, 2022, from https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZG

The World Bank. (2022). *Individuals using the internet (% of population)*. Retrieved March 5, 2022, from https://data.worldbank.org/indicator/IT.NET.USER.ZS

UNCTAD. (2020, April 2). *Data protection and privacy legislation worldwide*. Retrieved February 10, 2022, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

UNCTAD. (2021, December 14). *Data protection and privacy legislation worldwide*. Retrieved February 10, 2022, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

United Nation Development Programme. (2006). *Country evaluation: Assessment of development results: Honduras.* Retrieved February 12, 2022, from http://web.undp.org/evaluation/documents/ADR/ADR_Reports/ADR_Honduras.pdf

United Nations Conference on Trade and Development. (2020). *The UNCTAD B2C e-commerce index 2020 Spotlight on Latin America and the Caribbean*. Retrieved from https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf

United Nations. (2002). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998.* Retrieved February 12, 2022, from https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

United Nations. (2002). *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.* Retrieved March 3, 2022, from https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf

United Nations. (2020). *E-Government Survey 2020: Digital Government in Decade of Action for Sustainable Development.* Retrieved February 11, 2022, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

United Nations. (n.d.). *Capacity-Building*. Retrieved November 11, 2021, from https://www.un.org/en/academic-impact/capacity-building

UNODC. (2019, February). *Cybercrime module 3 key issues: The role of cybercrime law.* Retrieved March 6, 2022, from https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html

Van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?. *Journal of Cybersecurity*, *6*(1), doi: 10.1093/cybsec/tyaa019

VDA Legal Partners. (2020). Angola Criminal Law in Line with International Standards. VDA Legal Partners. Retrieved December 14, 2021, from https://www.vda.pt/xms/files/05_Publicacoes/2020/Flashes_Newsletters/Flash_Vda_Legal_Partners_-_Angola_-_Criminal_Law_overhaul_in_line_with_International_Standards.pdf

Verkijika, S. F., & De Wet, L. (2018). A usability assessment of e-government websites in Sub-Saharan Africa. *International Journal of Information Management*, *39* (September 2017), 20–29. https://doi.org/10.1016/j.ijinfomgt.2017.11.003

Zambia Public Procurement Authority. (2015). *e-Procurement system*. ZPPA. Retrieved January 5, 2022, from https://www.zppa.org.zm/e-procurement-system

Zambian Cyber Security Initiative Foundation. (2021, December 8). *Home* [Facebook page]. Facebook. Retrieved March 25, 2022, from https:////www.facebook.com/ZCSIF/

Zucule de Barros, M. J., & Lazarek, H. (2018). Comparative study of cybersecurity policy among South Africa and Mozambique. *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*, *2018-March*, 521–529.






C3SA Researchers:

Professor Wallace Chigona, Dr Enrico Calandro, Dr Laban Bagui, Dr Shallen Lusinga, Dr Karen Sowon, Ms Chimwemwe Queen Mtegha, Ms Nthabiseng Pule, and Mr Teofelus Tuyeni.

Cybersecurity Capacity Centre for Southern Africa (C3SA)
School of IT, Department of Information System, University of Cape Town.
Leslie Commerce Building, Upper Campus.
Rondebosch, Cape Town, Western Cape 7701
South Africa
Tel: +27 (0)21 650 4345
Email: c3sa@uct.ac.za
Web: http://www.c3sa.uct.ac.za/

NUPI Researchers:

Claudia E. Aanonsen and Erik Kursetgjerde

Norwegian Institute of International Affairs
NUPI's Centre for Digitalization and Cyber Security Studies
C.J. Hambros plass 2D
PB 7024 St. Olavs Plass
0130 Oslo
Norway
Tel: +47 22 99 40 00
Email: post@nupi.no
Web: https://www.nupi.no/nupi_eng/

GCSCC Researchers:

Professor William Dutton, Professor Michael Goldsmith, Dr Patricia Esteve-González, Professor Basie Von Solms, Dr Eva Nagyfejeo, and Carolin Weisser Harris.

Global Cyber Security Capacity Centre
Department of Computer Science, University of Oxford
Wolfson Building, Parks Road
Oxford OX1 3QD
United Kingdom
Email: cybercapacity@cs.ox.ac.uk
Web: https://gcscc.ox.ac.uk/

978-1-991228-00-0 (PRINT)

978-1-991228-01-7 (PDF)

C3SA