C3SA

Cybersecurity Capacity Centre for Southern Africa

CYBERSECURITY CAPACITY REVIEW

Kingdom of Lesotho

C3SA 2023 Report

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers:

Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Dr Jamie Saunders, Professor Basie Von Solms, and Professor David S. Wall.

Version	***Date***	***Notes***
1	*09/09/2022*	*Sent for director's review*
2	*11/10/2022*	*Sent to the language editor*
3	*26/10/2022*	*Sent to Technical Review Board*
4	*29/11/2022*	*Sent to Lesotho (MICSTI) for comments & to the language editor*
5	*31/03/2023*	*Final version – Version 4 updated to include feedback from MICSTI and stakeholders*

Approved by: Professor Michael Goldsmith

LIST OF ABBREVIATIONS

ARINSA	Asset Recovery Inter-Agency Network Southern Africa
ARIPO	African Regional Intellectual Property Organisation
AU	African Union
CBL	Central Bank of Lesotho
CI	Critical Infrastructure
CMM	Cybersecurity Capacity Maturity Model for Nations
CSIRT	Computer Security Incident Response Team
CTO	Commonwealth Telecommunications Organisations
DDoS	Distributed Denial of Service attack
DPA	Data Protection Act of 2011
DPC	Data Protection Commission
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
IT	Information Technology
LCA	Lesotho Communications Authority
LDF	Lesotho Defence Force
LQF	Lesotho Qualification Framework
LMPS	Lesotho Mounted Police Service
MCST	Ministry of Communications, Science and Technology
MDNSE	Ministry of Defence, National Security and Environment
MICSTI	Ministry of Information, Communications, Technology and Innovation (formerly MCST)
MoET	Ministry of Education and Training
NCB	National Central Bureau
NCSC	National Cybersecurity Council
NCDC	National Curriculum Development Centre
NEWC	National Early-Warning Centre
NMDS	National Manpower Development Secretariat
NSDP	National Strategic Development Plan
NSS	National Security Service
NUL	National University of Lesotho
SADC	Southern African Development Community
SARPCCO	Southern African Regional Police Chiefs Coordination Organisation
SOC	Security Operation Center
SSL/TLS	Secure Sockets Layer/Transport Layer Security

EXECUTIVE SUMMARY

In collaboration with the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre'), the Cybersecurity Capacity Centre for Southern Africa (C3SA) undertook a review of the maturity of cybersecurity capacity in the Kingdom of Lesotho (Lesotho) at the invitation of the Ministry of Information, Communications, Technology and Innovation (MICSTI). This is the second CMM review of Lesotho and it follows one that was conducted in 2019. The objective of the review was to enable the country to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

Over the period of three days, 9 to 12 May 2022, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions, telecommunications companies, and the banking sector) and civil society organisations.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM). The CMM defines five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cybersecurity Culture and Society*
- *Building Cybersecurity Knowledge and Capabilities*
- *Legal and Regulatory Frameworks*
- *Standards and Technologies*

Each dimension contains several *factors* which describe what it means to possess cybersecurity capacity. Each factor 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. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 provides an overall representation of the cybersecurity capacity in Lesotho and illustrates the maturity estimates in each dimension. Each dimension represents one-fifth of the graphic with the five stages of maturity for each factor extending outwards from the centre of the graphic. Start-up' is closest to the centre of the graphic, and dynamic is placed at the perimeter.

[1] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition," March 2021, https://gcscc.ox.ac.uk/cmm-2021-edition

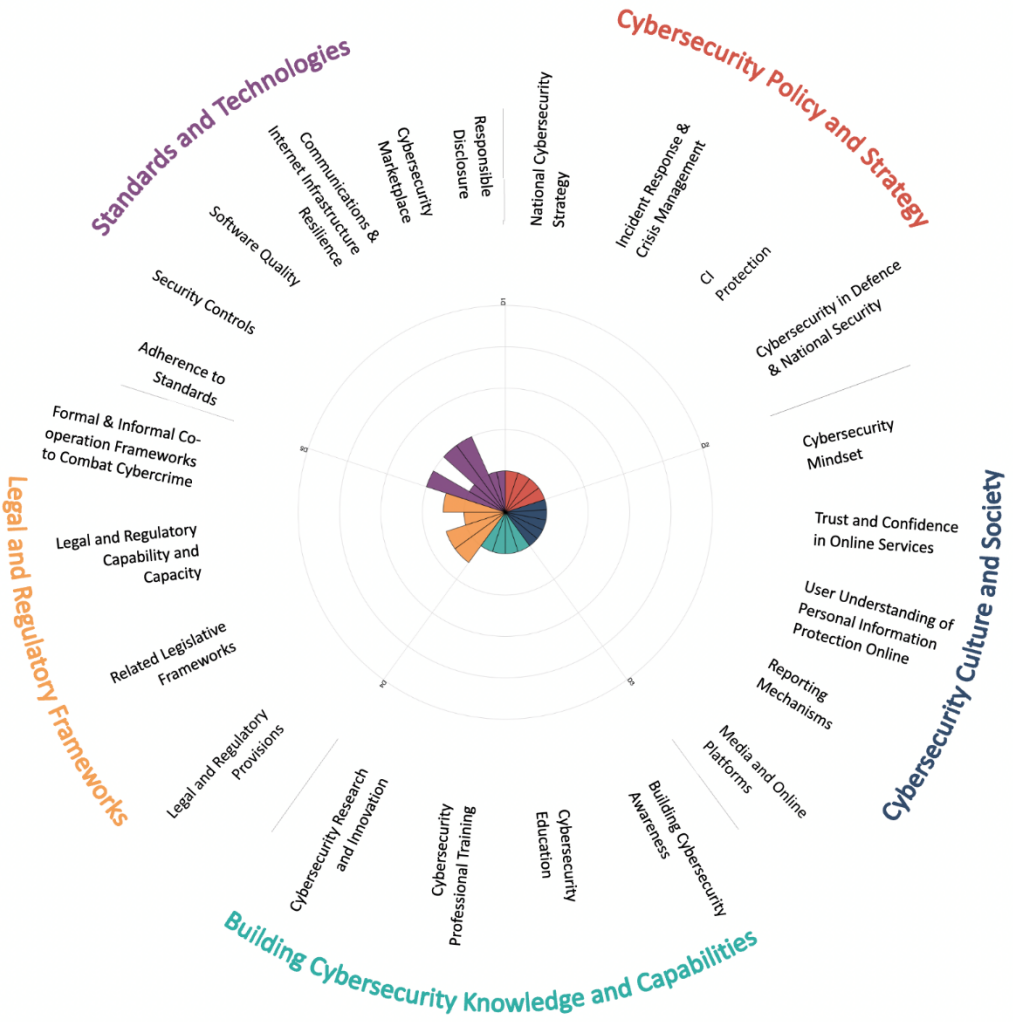

Figure 1: Overall representation of the cybersecurity capacity in the Kingdom of Lesotho

Cybersecurity Policy and Strategy

Cybersecurity policy and strategy development, implementation, and evaluation are at a start-up maturity level in Lesotho.

The Kingdom of Lesotho does not have an official National Cybersecurity strategy (NCS). It has developed a second 5-year National Strategic Development Plan 2019-2023 that barely refers to cybersecurity. The low level of reference to cybersecurity in strategic documents may suggest that cybersecurity is not yet considered a developmental strategic priority for the country. Further, the kingdom is yet to conduct a national cybersecurity risk assessment to ascertain the exposure, vulnerabilities, threats, and socio-economic risks in relation to cyberspace. Lesotho does not have an overarching national cybersecurity programme to coordinate initiatives in the country. The kingdom has yet to sign and ratify the AU convention on Cyber Security and Personal Data Protection (Malabo Convention) or enact cybersecurity legislation. There is still a substantial amount of work to be done on this front. Intensifying

collaboration with the Southern African Development Community (SADC), the African Union (AU), the International Telecommunication Union (ITU), the Commonwealth Telecommunications Organisations (CTO) and other bilateral and multilateral partners that promote the development of cybersecurity strategies will add to the momentum that is starting up for Lesotho.

Lesotho does not have a national Computer Security Incident Response Team (CSIRT) and as a result, does not have a national mechanism for identifying and categorising cybersecurity incidents. The Computer Crime and Cyber Security Bill of May 2022 has provisions for a "National Cybersecurity Advisory Council" (NCSC), and the establishment of a national CSIRT that is expected to coordinate and report to the government about cybersecurity incidents in the country. Lesotho does not have a national strategy or a policy that integrates cybersecurity into national crisis management. There is an urgent need to establish a national CSIRT and sectorial CIRST, as well as to form and operationalise the NCSC.

Lesotho does not have a list of identified national Critical Infrastructure (CI) sectors and assets. The country has yet to create a legal and regulatory framework to mandate cybersecurity standards within CI sectors. There are a few potential CI operators in industries such as the financial, telecommunication, energy, health, and public administration implementing some good cybersecurity practices; however, they were not consistent in quality within and across sectors. There is an urgent need to enact and implement a sound regulatory framework and adopt best practices for identifying and protecting CI in Lesotho. The implementation of the Computer Crime and Cyber Security Bill of May 2022 could facilitate this.

Lesotho does not have a cybersecurity strategy for the defence force. Cybersecurity discussions and initiatives, including the National Security Service (NSS) SOC or the Ministry of Defence, National Security and Environment (MDNSE) National Early-Warning Centre (NEWC), have started and are on course. However, it is not clear that these initiatives are sufficient to address the national cybersecurity risks that the kingdom is exposed to. A full national cybersecurity risk assessment incorporating national security and defence risks would help to test the adequacy of current plans and resources. This will also provide an opportunity to check that different agencies within the defence and security establishment are collaborating as they need to and that there is a clear understanding of the role of the military in supporting civil agencies.

Cybersecurity Culture and Society

Cybersecurity culture and understanding of related risks in the Kingdom of Lesotho is in its infancy, with the maturity level between start-up and formative. Cybersecurity mindset, trust and confidence in online services, user understanding of personal information protection online, reporting mechanisms of cybersecurity incident and discussions of cybersecurity in the social and mainstream media is still low. The maturity level ranges between start-up to formative.

There is minimal awareness of cybersecurity risks across government agencies, internet users and the private sector in the country. Although the government has recognised the importance of cybersecurity, many agencies within the public sector have not prioritised cybersecurity. This may have been attributed to a lack of legislation to guide cybersecurity initiatives in the country. Conversely, organisations in the private sector have also recognised

the need to prioritise cybersecurity and have a much better cybersecurity mindset compared to the public sector, specifically multinational companies. Safe cybersecurity practices within the public sector are mostly followed by leading government agencies and private firms. Similarly, the number of internet users that follow safe cybersecurity practices is limited due to a lack of awareness. In addition, although the majority of Internet users in the country have trust and confidence in using the internet, they do not clearly understand the risks that they are exposed to online.

The number of e-government services is growing in the country. However, there is still a limited number of e-commerce services. The uptake of these services has increased in the past years due to the outbreak of the COVID-19 Pandemic and internet growth. However, some of the online services offered by the government are not fully automated and, therefore, still require the users' physical presence. Also, most citizens have no access to e-government services due to limited internet penetration, especially in rural areas. Furthermore, digital literacy and skills among internet users remain a challenge. Therefore, most internet users are unable to critically assess information received/accessed online.

Internet service providers, the government, and civil society have developed approaches to address disinformation in the country. Some government agencies and non-government actors have made efforts to address disinformation through webinars and posts or messages on their websites to sensitise citizens. Awareness of disinformation in the media was more prevalent during the COVID-19 pandemic when misinformation about the pandemic was on the rise. However, efforts to address disinformation remain limited and are made on an ad-hoc basis.

There is general knowledge among some internet users in both the public and private sectors on how to protect personal information online. Many are aware of international data protection laws, such as the General Data Protection Regulation (GDPR). The country has also passed the Data Protection Act of 2011 to regulate the protection of personal information. However, there is no evidence regarding the level of awareness and understanding of the data protection legislation and the extent to which citizens are aware of their rights to privacy.

Formal reporting mechanisms for cybersecurity incidents such as online fraud, cyberbullying, identity theft, online child abuse and other security breaches are lacking in the country. Internet users have little knowledge of how and where to report online security incidents. As a result, most of the incidents are not reported. The absence of formal reporting mechanisms for cybersecurity incidents makes it difficult for the country to develop measures to address cybersecurity incidents. In addition, internet users rarely use social media channels to raise awareness of cybersecurity issues. As a result, discussions on cybersecurity-related matters are limited in the mainstream media.

The government should strive to create a cybersecurity culture by improving cybersecurity mindset and understanding of personal information protection through awareness-raising programmes, building trust and confidence in online services and developing reporting mechanisms for cybersecurity incidents. Furthermore, the government should coordinate with other stakeholders to develop mechanisms to address cybersecurity issues as a matter of urgency.

Building Cybersecurity Knowledge and Capabilities

Building Cybersecurity Knowledge and Capabilities (Dimension 3) in the Kingdom of Lesotho is at the start-up to formative level. The evaluation for D3.1 has stayed the same, 'start-up to formative', D3.2 has gone down from 'start-up to formative' to 'start-up', while D3.3 has improved from 'start-up' to 'start-up to formative'.

The 2019 CMM review recommended the need for the government to assign an entity to oversee the design and implementation of the national cybersecurity awareness-raising programmes. However, the recommendation has not been implemented, which has affected the progress of cybersecurity awareness in the country. Since no coordinating body exists, public, private and civil society sectors work in silos. This poses a challenge for sectors to collaborate and coordinate cybersecurity awareness initiatives. Cybersecurity awareness-raising programmes are conducted, especially in the private sector; however, they are ad hoc.

The *Education Sector Plan 2016-2026* and the revised *National Strategic Plan* acknowledges the need for the education sector to leverage ICTs for economic growth. However, they have not outlined the strategies to protect their learners from adopting ICTs, especially with the rise of cyber threats. Currently, at the primary and secondary levels, the National Curriculum Development Centre only develops computer application programmes for learners. However, cybersecurity is not incorporated into the programme. No cybersecurity-specific programmes are offered in higher learning institutions in the country. In addition, few computer science courses incorporate cybersecurity. According to the 2019 CMM review, the National University of Lesotho implemented a cybersecurity research centre to provide short cybersecurity courses and awareness programmes. However, the discussants had not encountered any activities since its opening.

The Catholic Comprehensive Community College (CCCC) has established a six-month cybersecurity certification programme for cybersecurity professional training. In addition, Lerotholi Polytechnic also offers cybersecurity certification programmes. However, the focus-group discussions still mentioned that the current landscape does not meet the country's demand for cybersecurity professional training. In addition, the government does not provide cybersecurity professional training scholarships. The only grants the National Manpower Development Secretariat offers are for the degree, master and PhD programmes.

Currently, there is no cybersecurity research and development in the country. According to the discussions, there is a lack of funding for cybersecurity research in the country. The desk research noted that recently, the Ministry of Communication, Science and Technology, in collaboration with the Organisation of Africa, Caribbean and the Pacific States, launched the Research and Innovation Policy. The policy stated the need for the government to invest and develop financing mechanisms to promote scientific research in the country. However, cybersecurity has not been mentioned in the policy as one of the areas to promote.

Legal and Regulatory Frameworks

Legal and regulatory frameworks for cybersecurity (Dimension 4) are at the start-up stage of maturity. While the review could not find published cybercrime statistics for Lesotho, there are reports of cybercrime in digital financial services, mainly in mobile money fraud and forex-trading scams. Computer-enabled harms such as cyberbullying and the non-consensual

publication of intimate images have also been reported. The Kingdom of Lesotho has enacted legislation on cybercrime through the Communications Act of 2012 and the Penal Code Act of 2012. However, these laws are limited in scope. Among other shortcomings, these laws do not address cyber-dependent crimes that compromise the confidentiality, integrity and availability of computer data and systems or violate human rights.

The National Assembly and the Senate, the two Houses of the Lesotho Parliament, approved the Computer Crime and Cyber Security Bill of 2022. However, it was yet to be passed when Parliament adjourned for elections in August 2022. The bill is a comprehensive piece of legislation on cybercrime and cybersecurity. It amends and vastly expands regulatory provisions on cybercrimes, enacted through the Communications Act of 2012 and the Penal Code Act of 2012. It also establishes the legal basis for punishing perpetrators of a broad range of cybercrimes with fines and prison sentences. As the bill has not yet been promulgated, Lesotho remains without a substantive law on computer-related and digital content-related offences.

Lesotho has some legislative frameworks related to cybersecurity that work in synergy with its legal provisions on cybersecurity and cybercrime. Lesotho has the Data Protection Act of 2011, which is modelled around the European Union's General Data Protection Regulation (EU GDPR). The financial and telecommunications sectors have some legal provisions contributing to cybersecurity, especially regarding Data Protection and Privacy. However, consumer protection for digital products and services is severely limited, and this is an area where new legislative and regulatory frameworks are needed. Lesotho does not have legislation that protects consumers from online business malpractice and fraud. In 2013, the country drafted an Electronic Transactions and Electronic Commerce law, which was based on the Southern African Development Community model law, but the law was not promulgated. Subsequently, in 2022, the government started drafting the Electronic Transactions and Communications Bill, 2022, which has also not been passed. There is no legislative protection of children online, including the protection of their rights online and the criminalisation of child abuse online.

Lesotho has limited legal and regulatory capability and capacity to combat cybercrime. Lesotho Mounted Police Service (LMPS) lacks the institutional capacity to prevent and combat cybercrime. The police do not receive adequate specialised training on cybercrime investigations. They rely on traditional crime investigation procedures as there are no legal provisions and internal standards for handling digital evidence. Furthermore, prosecutors do not receive regular training and resources to review electronic evidence or prosecute cybercrime. There is no process to equip judges to preside over cybercrime cases or cases involving electronic evidence. While the Computer Crime and Cybersecurity Bill is expected to come into operation in 2023, the country has not started training the police, the prosecutors and the judiciary on applying the new law. Sector-specific regulators have a limited understanding of the potential impact of cyber on their regulated entities, and there is no cross-sector regulatory body to supervise specific cybersecurity requirements. Lesotho should prioritise building the capacity of LMPS, the national prosecuting authority and the judiciary to effectively address cybercrimes. Regulatory bodies should review their frameworks to incorporate cybersecurity.

Co-operation between law-enforcement domestic public and private sectors on cybercrime is limited due to a lack of substantive cybercrime legislation. Co-operation between the Internet Service Providers or other technology providers and law enforcement is ad hoc and is driven

by the need for law enforcement agencies to access the digital communication records of customers during investigations. It is facilitated by laws such as the National Security Service Act of 1998, the Prevention of Corruption and Economic Offences Act of 1999 and the Communications Act of 2012, which provide for law enforcement to access personal data on networks. There is a lack of co-operation mechanisms between law enforcement agencies, Internet Service Providers and other technology providers for cybercrime prevention because of the absence of broader public-private sector collaboration arrangements, such as a national CSIRT or industry associations. Co-operation with foreign law enforcement counterparts to prevent and combat cybercrime is also at the start-up stage of maturity. The lack of substantive legislation on cybercrime impedes international co-operation to prevent and combat cybercrime in Lesotho. Lesotho's membership in international and regional law enforcement organisations such as INTERPOL, through the INTERPOL National Central Bureau (NCB) in Maseru, facilitates international co-operation on cybercrime.

To strengthen its capacity to combat cybercrime and crime facilitated by technology, Lesotho should promulgate the Computer Crime and Cybersecurity Bill and ensure that there is legislation for child-online protection, online-consumer protection, human rights online and the protection of intellectual property online. The government should also review and implement the Data Protection Act of 2011 and ratify the African Union Convention on Cyber Security and Personal Data Protection and the Budapest Convention. It should also build the intuitional capacity of the LMPS, the Directorate on Corruption and Economic Offenses (DCEO), the prosecuting authority and the judiciary to handle cybercrime cases.

Standards and Technologies

Lesotho’s cybersecurity Standards and Technologies (Dimension 5) are at the start-up stage of maturity. Adherence to ICT standards is low. There is no nationally agreed baseline of cybersecurity-related standards and good practices. A few entities in the private and public sectors have identified and implemented information risk management standards. They have implemented the United States Department of Commerce's National Institute of Standards (NIST) framework, the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 family of information technology standards, or both. Furthermore, procurement practices in private and public sectors are not always guided by cybersecurity standards or internationally recognised best practices. Procurement policies and manuals, where they exist, do not include cybersecurity considerations. The country has no standards or best practices for securing the digital products and services developed in the country.

Software quality and assurance is at the start-up to formative level of maturity. Individual users and organisations in both the private and public sectors deploy technological security controls such as firewalls, antivirus, and good password practices to varying degrees depending on factors such as awareness levels and affordability of controls. There were several reports of government systems being compromised due to inadequate controls. Cryptographic controls for protecting data at rest and in transit are recognised and deployed by some stakeholders within the public and private sectors. Software quality and assurance approaches differ from company to company in the private sector and government parastatals. However, in the majority of government agencies, there are no established software quality and assurance standards. Furthermore, there is no catalogue of assured

software platforms and applications to inform government agencies' procurement of applications or cloud services.

Communications and internet infrastructure resilience is at the formative stage of maturity. Broadband internet services in Lesotho are widely available through the country's two mobile network operators. Fixed broadband is limited to a few urban areas. However, there are concerns about the reliability of the service. Some rural areas remain uncovered. Users complain about affordability, but Lesotho is among the countries with the most affordable internet access in Africa. Internet service providers indicated that they monitor their networks and have incident response plans. Some private sector entities and parastatals also indicated that they have incident response plans. However, there are no documented and tested incident response plans in government IT under the ICT Department of the Ministry of Communications, Science and Technology.

The cybersecurity marketplace is at the start-up stage of maturity. Cybersecurity technologies are not developed in the country and there is no evidence that Lesotho has assessed the implications of using foreign security technologies. Cybersecurity consultancy services and expertise are limited. There are a few cybersecurity consultancy service providers in the country. However, their service offerings do not meet the standards some stakeholders require. As a result, some public and private entities source services from the international market. Few cybersecurity practitioners have professional certifications. Large organisations, particularly in the banking and telecommunications sectors conduct risk assessments to determine how to mitigate the risks of outsourcing technology solutions to a third party or cloud services. However, small companies and government IT do perform comprehensive due diligence. Cyber insurance cover is available from some insurance companies based in Lesotho. However, there is no data on the uptake.

Lesotho does not have a responsible disclosure mechanism through which cybersecurity researchers can share vulnerability information. Furthermore, there is no legislation on responsible disclosure. In the few cases where cybersecurity researchers have found vulnerabilities on government websites and other websites belonging to entities based in Lesotho, they have communicated to them directly. The draft Computer Crime and Cybercrime Bill of 2022 might address the issue.

To improve its cybersecurity maturity in relation to technology and standards, Lesotho should adopt a nationally agreed baseline of cybersecurity-related standards and good practices across the public and private sectors. The Ministry of Information, Communications, Technology and Innovation (MICSTI) should adopt and implement an IT governance framework such as the Control Objectives for Information and Related Technologies (COBIT) and a cybersecurity framework such as the NIST, ISO27000 family of standards or Service Organization Control 2 (SOC 2). To improve internet reliability, LCA should closely monitor and ensure that internet services meet quality of service requirements. The government should encourage cybersecurity research by providing for responsible vulnerability disclosure and avoid criminalizing the work of cybersecurity researchers.

INTRODUCTION

At the invitation of the Ministry of Information, Communications, Technology and Innovation (MICSTI), in partnership with Lesotho Communications Authority (LCA), the Cybersecurity Capacity Centre for Southern Africa (C3SA), in collaboration with the Global Cyber Security Capacity Centre (GCSCC), conducted a review of cybersecurity capacity of the Kingdom of Lesotho. The objective of the review was to enable the country to determine areas of capacity in which the government might strategically invest in, in order to improve their national cybersecurity posture. The current CMM review is the second CMM review for the country. The first review took place in 2019.

Over the period of three days, 9 – 12 May 2022, stakeholders from the following sectors participated in a three-day consultation process:

Government ministries, agencies and legislative bodies:

- Lesotho Communications Authority (LCA)
- Ministry of Information, Communications, Technology and Innovation (MICSTI)
- Ministry of Home Affairs
- Ministry of Trade and Industry
- Ministry of Mining
- Ministry of Finance
- Ministry of Education and Training
- Ministry of Justice
- Ministry of Foreign Affairs
- Ministry of Defence, National Security and Environment
- Ministry of Energy and Meteorology
- Ministry of Health
- Lesotho Defence Force (LDF)
- Lesotho Millennium Development Agency (LMDA)
- National Security Service (NSS)
- Council on Higher Education
- Petroleum Fund

Criminal justice sector:

- Lesotho Mounted Police (LMPS)
- Lesotho Correctional Services
- Directorate for Public Prosecutions
- Magistrate Court (Maseru)
- The Directorate on Corruption and Economic Offences (DCEO)
- AGIS Chambers

Finance sector:

- Vodacom Financial Services
- Central Bank of Lesotho
- Econet Telecom Lesotho

Critical infrastructure owners and regulators:

- Econet Telecom Lesotho
- Comnet
- LEC Communications
- Zeecom
- LEO
- Vodacom Lesotho

Additional private enterprises and industry associations:

- G4S
- MTEC
- Lesotho Barcodes

Academia:

- Limkokwing University of Creative Technology (LUCT)
- Catholic Comprehensive Community College (CCCC)
- Lerotholi Polytechnic (LP)
- Lesotho Centre for Accountancy Studies (CAS)
- Institute of Development Management (IDM)

Civil society organisations:

- Media Institute of Southern Africa (MISA) Lesotho
- Internet Society Lesotho Chapter
- She-Hive Association

International community:

- none were represented.

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM)[2] which is composed of five distinct *dimensions* of cybersecurity capacity.

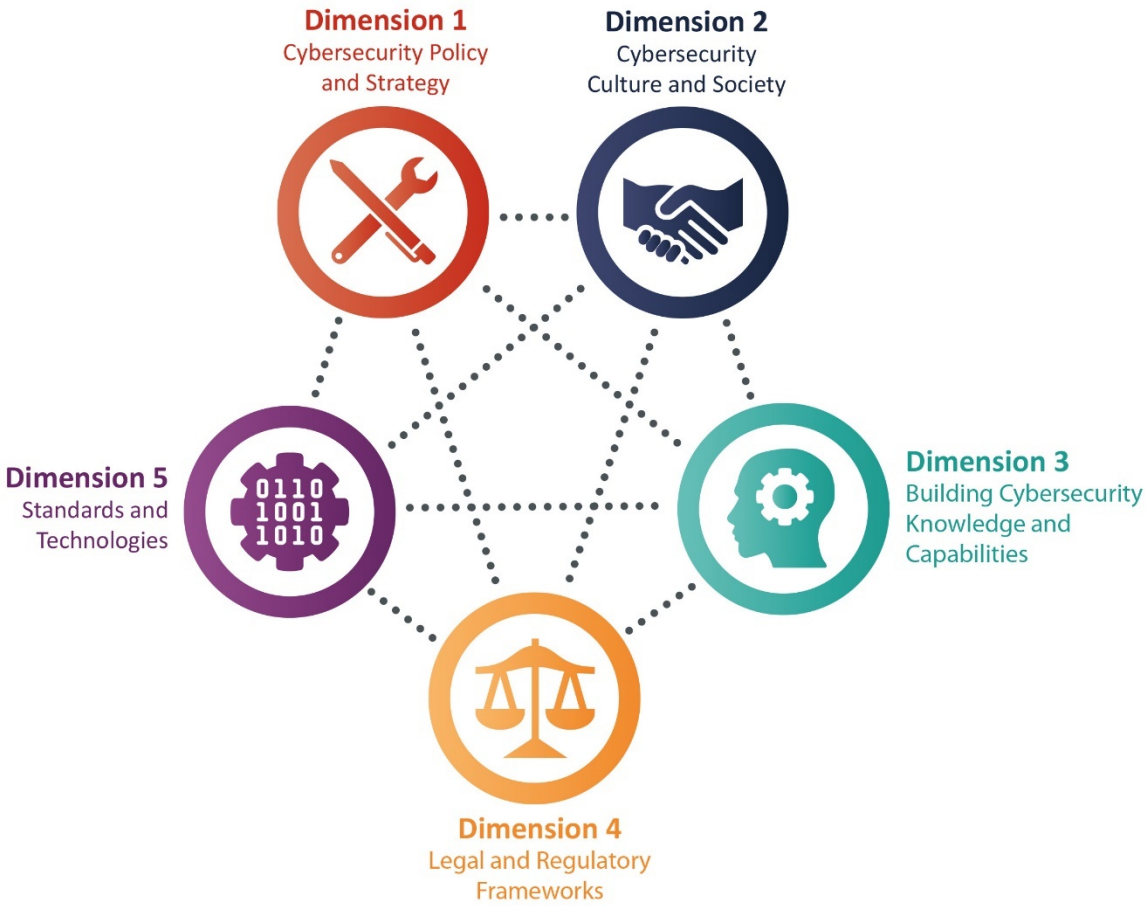

Figure 2: CMM 5 dimensions of cybersecurity capacity

[2] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 Edition," March 2021, https://gcscc.ox.ac.uk/the-cmm#/.

Each CMM dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. Table 1 below summarises the five dimensions together with the factors, which each presents:

DIMENSIONS	FACTORS
Dimension 1 Cybersecurity Policy and Strategy	D1.1 Strategy Development 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 Mindset 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 Co-operation 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

Table 1: Dimensions and factors of the CMM

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension contains a number of *factors* which describe 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. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, 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:

- **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, but no concrete actions have been taken. There may be an absence of observable evidence at this Stage;
- **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;
- **established:** the Indicators of the Aspect are in place, and evidence shows that they are working. There is not, however, 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. But the Aspect is functional and defined;
- **strategic:** choices have been made about which parts of the Aspect are important, and which are less important for the particular organisation or nation. The strategic Stage reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances; and
- **dynamic:** at this Stage, there are clear mechanisms in place to alter national strategy depending on the prevailing circumstances, such as the technology 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. Key sectors, at least, have devised methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this Stage.

The assignment of maturity stages is based upon the evidence collected, including the general or consensus view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Lesotho and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN THE KINGDOM OF LESOTHO

Economic Outlook

Lesotho is a landlocked country encircled by the territory of South Africa, covering a land mass of 30,355 square kilometres with a population of about 2.2 million.[3][4] The country gained independence from the United Kingdom in 1966; it remains part of the Commonwealth.[5] It is a parliamentary constitutional monarchy. The head of state is the King, and the head of government is the Prime Minister.

The country is divided into ten administrative districts. Lesotho has been on the United Nations (UN) list of least developed countries since 1971 when the list was first established.[6] The United Nations Development Programme (UNDP) 2020 Human Development Index (HDI), which represents human development in terms of health, education attainment, and the standard of living in a country[7], ranked Lesotho 165 out of 189 countries, an indicator of low human development.[8] The World Bank classifies Lesotho as a lower-middle-income country with a GDP per capita of US$ 1,166.5 in 2021.[9] The economy has been in decline since 2017[10]

---

[3] World Bank. (2022). https://www.worldbank.org/en/country/lesotho/overview

[4] The Information Architects of Encyclopaedia Britannica. (2022). *Lesotho.* Britannica. https://www.britannica.com/facts/Lesotho

[5] Commonwealth Secretariat. (2023). *Lesotho.* https://thecommonwealth.org/our-member-countries/lesotho

[6] United Nations – Committee for Development Policy. (2021). L*ist of Least Developed Countries (as of 24 November 2021).* https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/ldc_list.pdf

[7] UNDP. (2022). *Human Development Index (HDI)*. https://hdr.undp.org/data-center/human-development-index#/indicies/HDI

[8] UNDP (United Nations Development Programme). (2020). *Human Development Report 2020: The Next Frontier: Human Development and the Anthropocene*. New York. https://www.undp.org/belarus/publications/next-frontier-human-development-and-anthropocene

[9] World Bank. (2021). *GDP per capita (current US$) - Lesotho*. https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=LS

[10] Acadia Economics. (2021). *Lesotho Financial Inclusion Refresh.* https://uncdf-cdn.azureedge.net/media-manager/documents/126306?sv=2018-03-28&sr=b&sig=61zAU%2FrpNEQItihURMlDrFKj0zxVUFftmt9p49nwTnU%3D&se=2022-07-

and it has been adversely affected by the COVID-19 pandemic, declining revenues from Southern African Customs Union (SACU).[11, 12]

The Lesotho economy is centred around textile manufacturing, agriculture, and remittances from migratory work in neighbouring South Africa.[13] Main exports are clothing, diamonds, water, wool, and mohair.[14] The Lesotho economy is closely linked to the South African economy, on which it relies for imports of various goods and services. The country relies on South Africa for 80% of its food supplies.[15] Lesotho is also linked to the regional economy as part of the five-member Southern African Customs Union (SACU) together with Botswana, Eswatini, Namibia and South Africa. SACU is a significant source of Lesotho's revenue though it has been declining over the years.[16] Lesotho is also a member of the Common Monetary Area (CMA) along with eSwatini, Namibia and South Africa, a currency exchange area whereby the currencies are all pegged to the South African Rand. The South African Rand is accepted as legal tender in Lesotho. Lesotho is also a member of the Southern African Development Community (SADC), a treaty-based organisation whose objective is to provide a framework for members to cooperate on economic development and regional integration.[17]

Socio-cultural outlook

The culture in Lesotho is a mix of traditional and western. The country is governed through a bi-cameral parliamentary system, with a proportional representation component.[18] Since 2012, government administration has been formed by a coalition of parties. The coalitions have been unstable and could not complete their five-year tenure. This resulted in policy instability. At the local level, in the villages, the governance is a combination of the chieftainship system and community councils.

08T09%3A19%3A43Z&sp=r&rscd=attachment%3Bfilename%3D2021-11-03_Lesotho%20financial%20inclusion%20refresh%202021_final.pdf

[11] International Monetary Fund. (2022). Kingdom of Lesotho: 2022 article IV consultation press release; staff report; and statement by the executive director for the kingdom of Lesotho. [Press release]. https://www.imf.org/-/media/Files/Publications/CR/2022/English/1LSOEA2022002.ashx

[12] 'Nyane, H. (2022, July 4). Lesotho due to hold elections despite lack of progress on key political reforms. *The Conversation*. https://theconversation.com/lesotho-due-to-hold-elections-despite-lack-of-progress-on-key-political-reforms-185542

[13] Central Intelligence Agency. (2022). *The world fact book.* https://www.cia.gov/the-world-factbook/countries/lesotho/

[14] International Trade Administration. (2021, October 16). *Lesotho - country commercial guide*. https://www.trade.gov/country-commercial-guides/lesotho-market-overview

[15] African Development Bank. 2020). *African economic outlook 2021*. https://www.afdb.org/en/documents/african-economic-outlook-2021

[16] Khoabane, S. (2020, June 17). *The Scope of Government Revenue Mobilization in Lesotho.* Central Bank of Lesotho. https://www.centralbank.org.ls/index.php/component/k2/item/7-the-scope-of-government-revenue-mobilization-in-lesotho

[17] SADC. (1993). *Declaration and Treaty*. https://www.sadc.int/files/8613/5292/8378/Declaration__Treaty_of_SADC.pdf

[18] 'Nyane, H. (2019). *Bicameralism in Lesotho: A review of the powers and composition of the second chamber*. http://dx.doi.org/10.17159/2077-4907/2019/ldd.v23a2

English and Sesotho are the official languages provided for in the 1993 constitution.[19] English is the predominant language of business and one in which most government documents are written. Around 90% of the population is fluent in spoken and written Sesotho. Much fewer people are fluent in English. Other spoken languages are Zulu, Phuthi, Xhosa and Swati.[20] The has been a push for the declaration of minority languages Xhosa, Phuthi, and Sign Language in the Constitution as official languages.[21]

Lesotho has a high literacy rate. The literacy rate of people aged 15 and above is 77%[22] but higher, at 92% among the 15 to 24 age group.[23] The high literacy rate is attributed to a compulsory[24] and free primary school education where the completion is 86%.[25] However, about 32%[26] complete upper secondary and 4.2%[27] complete post-secondary education, as most families cannot afford the cost of tuition and amenities.

Over 70% of the population lives in rural areas. The main occupation is subsistence agriculture. According to the national statistics office's 2019 Labour Force Survey, the unemployment rate, using the expanded definition of unemployment, which includes discouraged jobseekers, is 38.3%.[28] Due to few job opportunities in the country, particularly in rural areas, a large number of Lesotho citizens are migrant workers in South Africa and far-afield. In 2020, international remittances contributed 20% to Lesotho's GDP.[29]

---

[19]The Comparative Constitutions Project. (2022). *Lesotho's Constitution of 1993 with Amendments through 2018.* https://www.constituteproject.org/constitution/Lesotho_2018.pdf?lang=en

[20] Cobbe, J. Hamilton, Legum, Colin and Guy, J.J. (2022, October 28). Lesotho. Encyclopedia Britannica. https://www.britannica.com/place/Lesotho

[21] National Dialogue Planning Committee. (2019). *Multi-stakeholder National Dialogue Plenary II Report*. Retrieved 12 July 2022 from http://www.lcn.org.ls/Resource/MSND%20Plenary%20II%20Report.pdf

[22] World Bank. (2022). *Literacy rate, adult total (% of people ages 15 and above) - Lesotho*. https://data.worldbank.org/indicator/SE.ADT.LITR.ZS?locations=LS

[23] Leenknecht, F., Lerotholi, L. & Petersen, T. (2021). *2021 MICS-EAGLE Lesotho Education Fact Sheets*. https://data.unicef.org/wp-content/uploads/2021/09/Lesotho_MICS_EAGLE_Fact-Sheets.pdf

[24] UNICEF. (2010, May 11). Free education becomes legally compulsory in Lesotho. ReliefWeb. [Press Release]. https://reliefweb.int/report/lesotho/free-education-becomes-legally-compulsory-lesotho#:~:text=The%20entering%20into%20force%20of,the%20country%20as%20a%20whole

[25] World Bank. (2022). Primary completion rate, total (% of relevant age group) - Lesotho (UNESCO Institute for Statistics (uis.unesco.org)). https://data.worldbank.org/indicator/SE.PRM.CMPT.ZS?locations=LS

[26] UNICEF. (2021). Lesotho education fact sheets 2021, analyses for learning and equity using MICS data. https://data.unicef.org/wp-content/uploads/2021/09/Lesotho_MICS_EAGLE_Fact-Sheets.pdf

[27] Knoema. (2022). *Lesotho - Gross graduation ratio for tertiary education.* https://knoema.com/atlas/Lesotho/topics/Education/Tertiary-Education/Gross-graduation-ratio-for-tertiary-education

[28] Bureau of Statistics. (2021). *2019 Labour Force Survey (LFS) Report*. Statistical Report No.5 of 2021. https://www.bos.gov.ls/New%20Folder/Copy%20of%20Demography/2019_Lesotho_LFS_Report.pdf

[29] World Bank. (2022). *Personal remittances received (% of GDP)* - Lesotho. https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=LS

ICT outlook

In recent decades Lesotho has experienced significant growth in digitalization and adoption of ICT technology amongst its population. This has led to the emergence of a digital economy based primarily on mobile networks. Mobile network access is widespread: 98% of the inhabited areas are covered with a 3G network, while 4G coverage is at 67%.[30] However, access to fixed broadband is severely limited to a few urban areas, translating into a penetration rate of 0.24% compared to a global average of 15.9%.[31] Fixed broadband access in Lesotho is commonly provided through fibre-to-the-x (FTTx) technologies. An entry-level package, which provides 10GB monthly and advertised speeds of up to 150 Mbps, costs just under US$6 per month on a prepaid contract.[32] Over 90% of households have a mobile phone or a computer.[33] However, based on the latest available (2020) data, 43% of the population was using the internet in Lesotho, compared to the world average of 59%.[34] In addition to affordability, factors inhibiting meaningful access and use of the internet are the lack of access to electricity and digital skills. In 2020, 47.4% of the population had access to electricity.[35] According to the ITU, digital skills among the population stood at 12% for females and 15% for males.[36] Due to these factors, Lesotho's digital economy is underutilized.[37]

The ICT sector in Lesotho is underdeveloped. Few businesses, government ministries, and agencies have transformed from paper-based processes to digital by default. Lesotho is ranked 127 out of 131 countries on the Portulans Institute's 2022 Network Readiness Index, an index that measures the application and impact of information and communication technology (ICT) in economies around the world, based on four pillars, namely, technology, people, governance, and impact.[38] Lesotho's ranking has declined, as it was ranked 123 out of

---

[30] ITU DataHub. (2022). Lesotho: Population coverage, by mobile network technology. https://datahub.itu.int/data/?e=LSO&c=701&i=100095

[31] ITU DataHub. (2022). Fixed broadband subscriptions. https://datahub.itu.int/data/?e=LSO&c=701&i=19303

[32] The World Bank Group. (2020). *Lesotho Digital Economy Diagnostic.* Retrieved May 7, 2022, from https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y

[33] Krönke, M. (202). Africa's digital divide and the promise of e-learning. AfroBarometer Policy Paper no. 66. Retrieved 13 July 2022 from https://afrobarometer.org/sites/default/files/publications/Policy%20papers/pp66-africas_digital_divide_and_the_promise_of_e-learning-afrobarometer_policy_paper-14june20.pdf

[34] ITU DataHub. (2022). Lesotho: Individuals using the Internet. https://datahub.itu.int/data/?e=LSO&c=701&i=11624

[35] World Bank. (2022). Access to electricity (% of population) - Lesotho, Samoa. World Bank Global Electrification Database. https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?locations=LS-WS

[36] International Telecommunication Union. (2021). Connectivity in the least developed countries: status report 2021. https://www.itu.int/en/myitu/Publications/2021/09/17/11/46/Connectivity-in-the-Least-Developed-Countries-Status-report-2021

[37] The World Bank Group. (2020). *Lesotho Digital Economy Diagnostic.* https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y

[38] Portulans Institute. (2022). *The Network readiness index 2022*. Retrieved 28 November 2022 from https://networkreadinessindex.org/wp-content/uploads/reports/countries/lesotho.pdf

130 countries in the 2021 index.[39] ICT indicators that the index found Lesotho weakest in are: ICT services exports, domestic ICT market size, international internet bandwidth, government promotion of investment in emerging technologies, mobile broadband internet traffic within the country and the Patent Cooperation Treaty (PCT) patent applications.[40] The weakness ICT service exports and the low PCT patent applications indicate a lack of innovation in the country. The digital communications market is dominated by two vertically integrated communications providers that also provide digital financial services, Econet and Vodacom Lesotho.[41] Several small to medium enterprises deal in the supply of imported hardware, systems integration, and software development.[42]

The public sector is leading the way in the digitization of government services to improve service delivery and national competitiveness under the e-Government[43] project and the Private Sector Competitiveness and Economic Diversification Project.[44] The government has digitised the management of civil registrations (births, deaths and marriages)[45] , immigration services, land administration services, public service human resource management and financial management, among others.[46] Registration of companies and the issuance of traders' licences and residents' permits have also moved online. The Revenue Services Lesotho (formerly Lesotho Revenue Authority) has also moved customs clearing, tax-clearing and filing online.[47] These digitization efforts by the government have seen Lesotho's E-Government Development Index (EGDI) ranking improve from 165 in 2018[48] to 135 in 2020.[49]

---

[39] Portulans Institute. (2021). The Network readiness index 2021. Retrieved 14 July 2022 from https://networkreadinessindex.org/#

[40] Portulans Institute. (2022). The Network readiness index 2022. Retrieved 28 November 2022 from https://networkreadinessindex.org/wp-content/uploads/reports/countries/lesotho.pdf

[41] World Bank. (2020). *Lesotho Digital Economy Diagnostic*. https://openknowledge.worldbank.org/handle/10986/33881

[42] Examples:

https://www.enigma.co.ls/;

https://www.cbs.co.ls/software/

[43] African Development Bank. (2022). *Lesotho - eGovernment Infrastructure - Project Completion Report.* https://www.afdb.org/en/documents/lesotho-egovernment-infrastructure-project-completion-report

[44] Private Sector Competitiveness and Economic Diversification Project (PSCEDP). (2019). *About PSCEDP.* https://www.psc.org.ls/

[45] Ort, R. & Raboletse, T. (2021). *National ID in Lesotho is putting citizens at the center*. https://blogs.worldbank.org/governance/national-id-lesotho-putting-citizens-center

[46] World Bank Group. (2019). *Lesotho Digital Economy Diagnostic.*

https://openknowledge.worldbank.org/handle/10986/33881

[47] Revenue Services Lesotho. (2022). https://www.rsl.org.ls/

[48] United Nations. (2018). *UN E-Government Survey 2018.* https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

[49] United Nations. (2020). *UN E-Government Survey 2020.* https://desapublications.un.org/file/781/download

Despite the digitization trends in both the public and private sectors, basic digital skills are limited among the general population. According to the ITU 2019 data[50], only 3% of the general population had advanced ICT skills, 5% had standard skills and 11% had basic skills.[51]This is because the provision of digital skills education is limited in both the basic and tertiary education systems. Most schools in Lesotho lack basic infrastructure such as electricity and computers and teachers with ICT skills. To improve science, technology, engineering and math education and, in turn, to boost ICT skills development, the government, with the assistance of development partners, is implementing online training for secondary school maths and science teachers.[52] Outside the school system, the provision of digital skills training is available through professional training centres, though they are only found in large urban centres. However, enrolment in professional ICT courses is also limited.

The government recognises the importance of ICT and in its key economic planning document is the National Strategic Development Plan II (2018-19 – 2022-23), the government commits itself to a) improve ICT access and use, b) improve regulation in ICT sector, c) enhance e-Government services, d) improve digital economy uptake and e) improve governance of ICT sector.[53] However, the ICT policy development in Lesotho has not kept pace with technological developments. The current ICT policy was approved in 2005 but faced implementation challenges until 2020, when MICSTI, assisted by United Nations Development Programme (Lesotho), started developing a new ICT policy.[54] However, Cabinet had not approved the draft policy during this CMM review. In 2021, Prime Minister's Delivery Unit engaged experts to produce a National Digital Transformation Strategy for the country.[55] However, there is no evidence that the government adopted the strategy. The National ICT in Education Policy which was expected to provide strategic direction for ICT skills development was drafted in 2019.[56] A 2020 study by Turugare and Rhudumbu found that the level of technology integration in institutions of higher education was low.[57]

---

[50] For definitions of basic, standard and advanced ICT skills, see The ITU ICT SDG indicators. https://www.itu.int/en/ITU-D/Statistics/Pages/SDGs-ITU-ICT-indicators.aspx

[51] International Telecommunication Union. (2022). *Digital Development Dashboard: An overview of digital development around the works based on ITU data.* https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_LSO.pdf

[52] The World Bank. (2022). *Lesotho: World Bank to help strengthen basic education and keep children in school.* [Press Release]. https://www.worldbank.org/en/news/press-release/2022/04/20/lesotho-world-bank-to-help-strengthen-basic-education-and-keep-children-in-school

[53] The Government of Lesotho. (2018). *National Strategic Development Plan II*. P.133. https://www.gov.ls/wp-content/uploads/2021/06/National-Strategic-Development-Plan-II-2018-19-2022-23.pdf

[54] United Nations Development Programme. (2020, July 1). *Review and development of the Lesotho ICT policy (2005)*. [Procurement Notices] https://procurement-notices.undp.org/view_notice.cfm?notice_id=67434

[55] Genesis Analytics. (2021). *Formulating Lesotho's National Digital Transformation Strategy.* https://www.genesis-analytics.com/projects/strategy-for-digital-transformation-across-all-of-lesotho-government

[56] The World Bank Group. (2020). *Lesotho Digital Economy Diagnostic.* http://hdl.handle.net/10986/33881

[57] Turugare, M., & Rudhumbu, N. (2020). Integrating technology in teaching and learning in universities in Lesotho: opportunities and challenges. *Education and Information Technologies*. Volume 25. Issue 5 Sep 2020 pp 3593–3612https://doi.org/10.1007/s10639-019-10093-3

Lesotho maintains membership in multiple international organizations relevant to ICT administration and cybersecurity. The most important are the International Telecommunication Union (ITU), the Commonwealth Telecommunications Organisation (CTO) and the SADC. The ITU's global cybersecurity index for 2020 ranks Lesotho as number 164 out of 194. The regional rank for the country stands at 38 out of 43. A meaningful part of the explanation for Lesotho's low global ranking and relatively low regional position lies in weak scores on the indicators for technical and organizational measures.[58] Lesotho had a CMM review in 2019. However, there is no evidence that the recommendations were implemented.

[58] ITU. *Global Cybersecurity Index 2020.* https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

REVIEW REPORT

OVERVIEW

This section provides an overall representation of the cybersecurity capacity in Lesotho. Figure 2 below presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' at the perimeter.

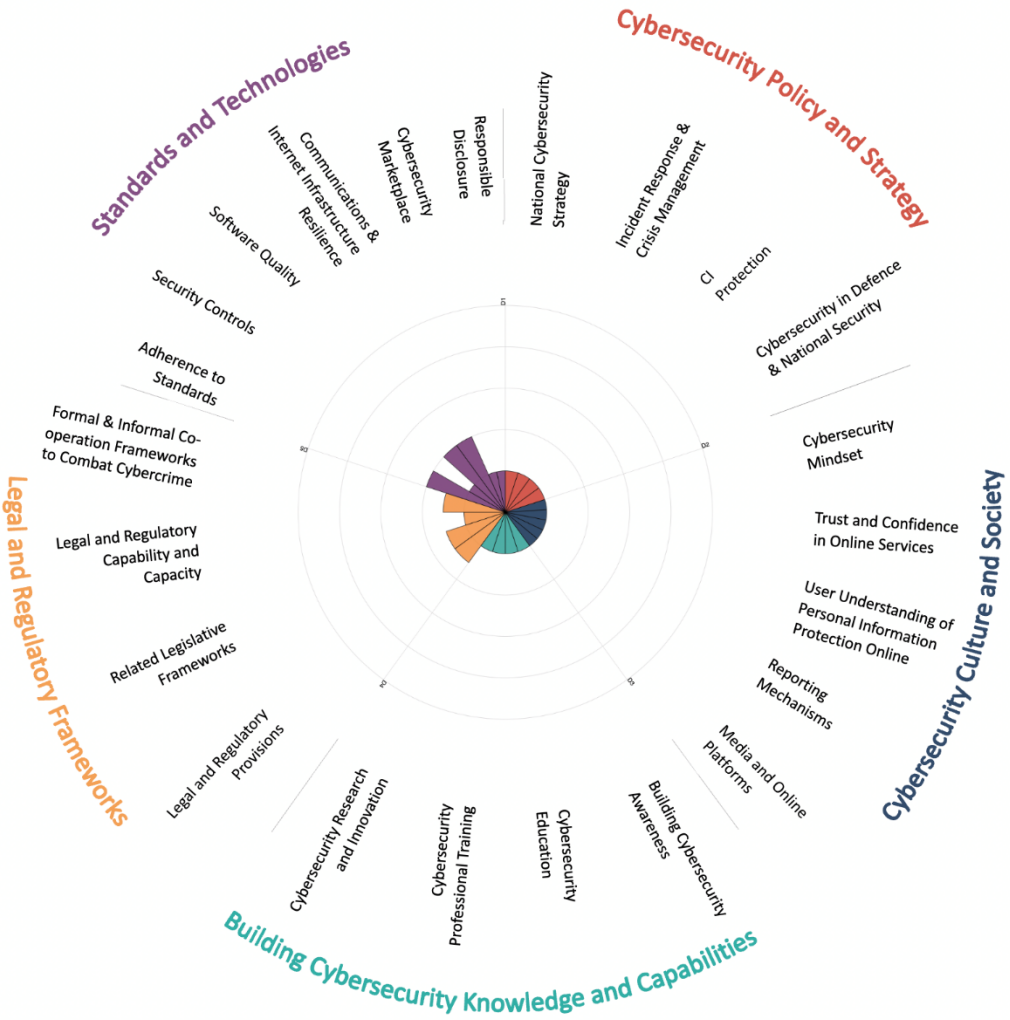

Figure 3: Overall representation of the cybersecurity capacity of the Kingdom of Lesotho

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

This Dimension explores the capacity of Lesotho 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. (See Figure 4 below)

Figure 4: Factors and aspects of the Dimension 1 of the CMM

Overview of results

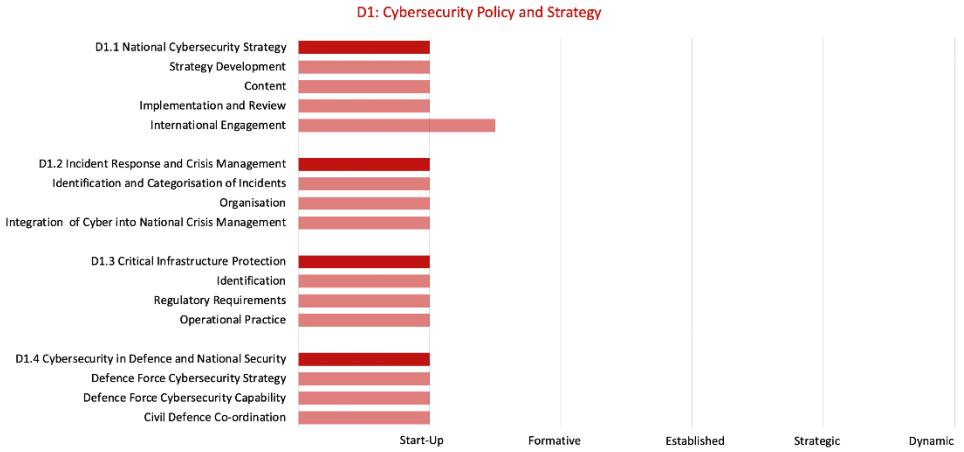

Figure 5: Result of the assessment of the cybersecurity policy and strategy of the Kingdom of Lesotho

D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.

Stage: [Start-up]

Strategy Development (Start-up)

The Kingdom of Lesotho does not have an official National Cybersecurity Strategy (NCS). The country acknowledges its vulnerability to cybercrime, and to cyber threats and risks,[59] and has been putting efforts into turning the situation around. However, the country is yet to conduct a national cybersecurity risk assessment to ascertain its exposure, vulnerabilities, threats, and socio-economic risks in relation to the cyberspace. The Kingdom of Lesotho has developed a second 5-year National Strategic Development Plan 2019-2023[60] that has digital transformation components. However, the plan barely refers to cybersecurity under the section on *Technology and Innovation*. Focus-group discussion participants noted that no process has been agreed on for consulting key stakeholder groups about the cybersecurity

[59] Government of Lesotho. (2020). *Cyber Crime - A risk to Lesotho*. https://www.gov.ls/cyber-crime-a-risk-to-lesotho/

[60] Government of Lesotho (2018). *National strategic development plan II* – 2018/2019 - 2022/2023. https://www.gov.ls/documents/national-strategic-development-plan-ii-2018-19-2022-23/

strategy, be they private sector, civil society, or international partners. The country received recommendations to develop an NCS in the 2019 CMM review conducted by the GCSCC, with the support of the World Bank. The country has also sought advice and guidance from the ITU for the development of the NCS for the Kingdom.

Content (Start-up)

Lesotho is yet to develop a National Cybersecurity Strategy (NCS). It is expected that the content of the NCS document will draw from existing national ICT, security, defence, communication, and trade-related policies and regulatory frameworks, in accordance with national priorities, and local and international commitments. However, the Lesotho 2020 Vision[61] and the Lesotho Reforms Framework and Road Map of 2017[62] do not refer to digital transformation or cybersecurity. The MCST strategic plan 2020-2023 includes some elements related to the cybersecurity of government data centres and to the computer crimes and cybersecurity bill.[63] The NSDP II[64] also makes some references to cybersecurity. Focus-group discussion participants indicated that the National Security Service (NSS) has an internal cybersecurity strategy whose content could inspire some aspects of the national cybersecurity strategy. The low level of reference to cybersecurity in strategic documents may suggest that cybersecurity is not yet considered a developmental strategic priority for the country.

Implementation and review (Start-up)

The Kingdom of Lesotho does not have an overarching national cybersecurity programme to coordinate initiatives in the country. However, the country has a digital transformation vision containing cybersecurity aspects suggested in the national ICT Policy.[65] The Computer Crime and Cyber Security Bill of 2022 sets a framework that is meant to be used to initiate coordinating cybersecurity programs in the country.[66] However, focus-group discussion participants indicated that the Lesotho Communication Authority (LCA) under the Ministry of Information, Communications, Technology and Innovation (MICSTI) has been informally acting as national coordinator for cybersecurity matters. Focus-group discussion participants pointed at energy availability, lack of skills, lack of financial and other resources, and lack of political will and leadership championing the cybersecurity agenda in the public sector amongst the challenges to the implementation of cybersecurity policy initiatives.

---

[61] Government of Lesotho (2020). *Lesotho Vision 2020*. https://www.gov.ls/download/lesotho-vision-2020/

[62] Government of Lesotho (2017). *Lesotho Reforms Framework & Road Map*. https://www.gov.ls/download/lesotho-reforms-framework-road-map-2/

[63] Computer crime and Cyber Security Bill 2022 (Lesotho)). https://senate.parliament.ls/2022/05/19/computer-crime-and-cyber-security-bill-2022/

[64] Government of Lesotho (2018). *National strategic development plan II – 2018/2019 - 2022/2023.* https://www.gov.ls/documents/national-strategic-development-plan-ii-2018-19-2022-23/

[65] Government of Lesotho (2005). *ICT Policy for Lesotho*. http://www.communications.gov.ls/document/Lesotho_ICT_Policy_Final.pdf

[66] Government of Lesotho (2018). *National strategic development plan II – 2018/2019 - 2022/2023.* https://www.gov.ls/documents/national-strategic-development-plan-ii-2018-19-2022-23/

International Engagement (Start-up to formative)

The Kingdom of Lesotho is a member of SADC, the African Union (AU), the United Nations (UN), ITU, the Commonwealth of Nations, and the Commonwealth Telecommunications Organisation (CTO) which all promote the development of cybersecurity strategies. The MICSTI has been collaborating with these entities to improve cybersecurity capacity in the country. The Internet Society Lesotho Chapter (ISOC Lesotho) established the Lesotho Internet Governance Forum (LesIGF) in 2021 to contribute to internet governance debates, including cybersecurity topics.[67] However, the country is yet to sign and ratify the AU convention on Cyber Security and Personal Data Protection (Malabo Convention) or enact cybersecurity legislation at least guided by the HIPSSA (Harmonization of ICT Policies in Sub-Saharan Africa) SADC Cybersecurity model law.

D 1.2 INCIDENT RESPONSE AND CRISIS MANAGEMENT

This Factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, co-ordinate, and operationalise incident response, and whether cybersecurity has been integrated into the national crisis management framework.

Stage: [Star-up]

Identification and categorisation of incidents (Start-up)

Lesotho does not have a national Computer Security Incident Response Team (CSIRT). As a result, the country does not have a national mechanism for identifying and categorising cybersecurity incidents. That situation has not changed despite the recommendations of the 2019 CMM review to develop such mechanism. Focus-group discussion participants noted that the National Security Service (NSS) had some capability within its Security Operation Centre (SOC) enabling it to identify and categorise incidents. However, a myriad of challenges hinders other public entities, the private sector, and the civil society from benefiting from the facility. Further, many organisations in the private sector assess, monitor, and keep track of events in the cybersecurity threat and risk landscape of their industries. There is an urgent need to establish a national CSIRT.

[67] ISOC Lesotho (2021). *School of Internet Governance and Internet Governance Forum page* – https://isoc.org.ls/school-of-internet-governance-and-internet-governance-forum-page/

Organisation (Start-up)

Since the country does not have a national CSIRT, LCA and MICSTI have been trying to occupy the space of coordinating entities for cybersecurity in the country. Focus-group discussion participants indicated that the National Security Service (NSS) has constituted a Security Operation Centre (SOC) as part of its defence portfolio and sometimes assists civil public organisations when investigating cybercrimes. The Computer Crime and Cyber Security Bill of May 2022 has provisions for a "National Cybersecurity Advisory Council" (NCSC) that is expected to coordinate and report to the government about cybersecurity incidents in the country.[68]

Integration of cybersecurity into national crisis management (Start-up)

The Kingdom of Lesotho does not have a national strategy or a policy that integrates cybersecurity into national crisis management. The country passed the National Disaster Management Act No2 of 1997[69], providing for the functioning of Lesotho's disaster management plan, disaster reconstruction, rehabilitation and recovery plan, and the establishment of the disaster management authority, national disaster relief task force, and district and village disaster management teams. The Disaster Management Authority (DMA) of Lesotho has been involved in government interventions against droughts, famine, and other natural disaster areas. The DMA participates in the Global Facility for Disaster Reduction and Recovery (GFDRR) led by ACP-EU Natural Disaster Risk Reduction Program that performs climate risk analysis and establishes an Early Warning System (EWS) supported by EWS Information Management Systems[70] It is not clear to what extent the DMA mandate or interventions take cybersecurity into account. Focus-group discussion participants indicated that there were collaboration challenges between cybersecurity stakeholders preventing the establishment of a crisis management framework integrating cybersecurity. The NCSC is expected to fill that gap by serving as a cybersecurity nexus once it is formed and operational.

[68] Computer Crime and Cybersecurity Bill 2022. (Lesotho) https://senate.parliament.ls/2022/05/19/computer-crime-and-cyber-security-bill-2022/

[69] Disaster Management Act Kingdom of Lesotho (1997). https://leap.unep.org/countries/ls/national-legislation/disaster-management-act-1997-act-no-2-1997

[70] Global Facility for Disaster Reduction and Recovery (2016). *Lesotho: Climate Risk Analysis & EWS Information Management Systems*. https://www.gfdrr.org/en/lesotho-climate-risk-analysis-ews-information-management-systems

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This Factor studies the government's capacity to identify CI assets, the regulatory requirements specific to the cybersecurity of CI, and the implementation of good cybersecurity practice by CI operators.

Stage: [Start-up]

Identification (Start-up)

Lesotho does not have a list of identified national critical Infrastructure (CI) sectors and assets. In addition, it does not have relevant legal and regulatory frameworks that mandate the operationalisation of their cybersecurity protection. The Computer Crime and Cyber Security Bill of 2022 makes provision for the identification and the "Protection of Critical Information Infrastructure";[71] but the regulation is yet to be enacted and the entities that it is supposed to spawn are yet to be created.

Regulatory Requirements (Start-up)

The Kingdom of Lesotho is yet to pass into law the cybersecurity bills relevant to Critical Infrastructure (CI) sectors and assets. Especially, the Computer Crime and Cyber Security Bill of 2022 which has provisions for CI protection, is still in the works of the legislature. As a result, there are no existing regulatory requirements specific to the cybersecurity of CI in the country.

Operational practice (Start-up)

Focus-group discussion participants indicated that a few potential CI operators in sectors such as the financial, telecommunication, energy, health, and public administration implement some good cybersecurity practices. However, they were not consistent in quality within and across sectors. The 2019 CMM review of the Kingdom indicated that threat and vulnerability disclosure among CI operators, usually in the private sector and the government, is informal and ad-hoc. There are no information-sharing and incident-reporting obligations at the moment. There is a need for specific regulations or guidelines to oblige Critical Information Infrastructure operators to report cyber incidents.

[71] Computer Crime and Cyber Security Bill 2022. (Lesotho). https://senate.parliament.ls/2022/05/19/computer-crime-and-cyber-security-bill-2022/

D 1.4 CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

This Factor explores whether the government has the capacity to design and implement a strategy for cybersecurity within national security and defence. 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.

Stage: [Start-up]

Defence Force Cybersecurity Strategy (Start-up)

Lesotho does not have a defence force cybersecurity strategy and neither has there been a formal assessment of the cyber risks that the defence forces might be exposed to. Security forces in the country are constituted of the Lesotho Defence Force (LDF),[72] the Lesotho Mounted Police Service (LMPS), and the National Security Service (NSS). The regulations mandating their operation do not have provisions for cybersecurity. The 2019 CMM review pointed out that the National Security Service Act of 1998 and the Lesotho Defence Act of 1996 did not have cyber-defence-related provisions. However, according to focus-group discussion participants, cybersecurity discussions and some initiatives, including the NSS SOC, have started and are on course.

Defence Force Cybersecurity Capability (Start-up)

Specialist cybersecurity capability within the country's national defence and security establishment is limited. Focus-group discussion participants of the defence and security community indicated that the NSS has a cybersecurity defensive capability through its SOC. Further, the 2019 CMM review indicated that the Ministry of Defence, National Security and Environment (MDNSE) had created a National Early-Warning Centre (NEWC) that monitors cyber activities aimed against the country.

Focus-group discussions participants also mentioned that the NSS has collaborated with the LMPF on cybersecurity analysis and forensics. However, the collaboration between defence and security agencies was limited; and the collaboration between defence and security agencies, and civil entities was scarce. Issues of leadership commitment to such collaboration, clash of mandates amongst public entities, lack of human resources and poor digitization, were also raised to explain the *status quo*.

Civil Defence Co-ordination (Start-up)

Collaboration on cybersecurity between civil and defence entities is limited. The LDF has active troops and no reserves.[73] The country does not have a cyber-defence reserve force. A civilDefence Coordination entity could be formed by recruiting and training graduates in

[72] Lesotho Defence Force. (n.d.). http://www.ldf.gov.ls/index.html

[73] Guy., J. Legum,. Colin. Hamilton, & James (2022). *Lesotho. Encyclopedia Britannica*. https://www.britannica.com/place/Lesotho

national cyber-defence practices. As a reserve force they would be in civilian roles until such a time that they are called upon to support their country's defence with their skills.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of Lesotho. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 MICSTI through LCA should conduct a national cybersecurity risk assessment to ascertain the countries exposure, vulnerabilities, threats, and socio-economic risks in relation to the cyberspace.

R1.2 MICSTI through LCA should develop a national cybersecurity strategy in consultation with all cybersecurity stakeholders (e.g., Civil society, international partners, Public and private sectors) in Lesotho.

R1.3 The government through the MICSTI should speed up the creation of the National Cybersecurity Advisory Council to oversee cybersecurity activities in the country and advise government accordingly.

INCIDENT RESPONSE AND CRISIS MANAGEMENT

R1.4 The Government, through MICSTI should prepare for the establishment of the NCAC and a national CSIRT and establish these entities without delay following the promulgation of the Computer Crime and Cybersecurity legislation.

R1.5 MICSTI through LCA should collaborate with public, private, and civil society sectors to develop sectorial CSIRT in economic and social and cultural spaces.

R1.6 MICSTI should develop in collaboration with the DMA, civil society, public and private sectors organisation, a national cyber crisis management and business continuity plans.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.7 MICSTI should, in collaboration with cybersecurity stakeholders from the civil society, develop public and private organisations, a list of Critical Infrastructure (CI) sector, entities, and assets.

R1.8 The government, through MICSTI, should establish a legal and regulatory framework necessary to ensure that adequate cybersecurity measures are taken by the relevant CI operators.

R1.9 MICSTI should develop in consultation with civil society, public and private sectors, cybersecurity operational standards and best practices for CI operators.

CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

R1.10 The Ministry of Defence, National Security and Environment (MDNSE), in collaboration with the Ministry of Police and Public Safety, and the Ministry of Justice and the MICSTI should develop a national cybersecurity strategy and policy framework in defence and national security in response to the findings of the national risk assessment.

R1.11 The government of Lesotho should amend the National Security Service Act of 1998 and the Lesotho Defence Act of 1996 to include adequate provisions for cybersecurity in defence and national security.

R1.12 The LDF, the LMPS, LCS and the NSS should consider what capabilities and resources are required to implement the strategy and to take steps to establish the necessary structures.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

This dimension 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. Moreover, this Dimension 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 (See figure 6 below). The results of the evaluation are summarised in Figure 7 and further elaborated in paragraphs afterwards.

Figure 6: Factors and aspects of the Dimension 2 of the CMM

Overview of results

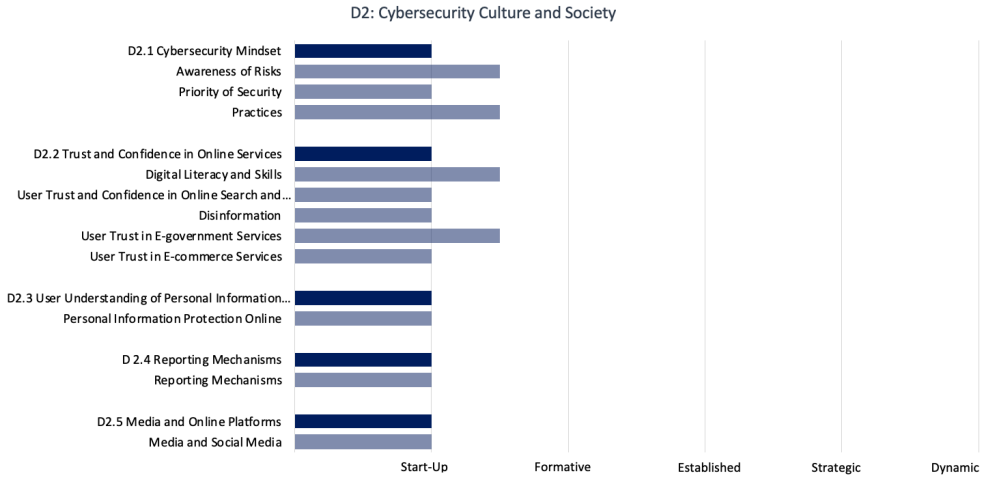

Figure 7: Result of the assessment of the cybersecurity culture and society of the Kingdom of Lesotho

D 2.1 CYBERSECURITY MINDSET

This Factor 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. A cybersecurity mindset consists of values, attitudes and practices–including habits of individual users, experts, and other actors–in the cybersecurity ecosystem that increase the capacity of users to protect themselves online.

Stage: [Start-up to Formative]

Awareness of risks (Start-up to Formative)

The level of awareness of cybersecurity risks within the government, private sector and among users is minimal. The 2019 CMM review found that although there has been a slight improvement in the level of awareness in the country, it remains low. Some private sector organisations e.g., financial institutions and mobile telephony companies, conduct awareness campaigns for their employees and clients. Cybersecurity awareness is mostly conducted during special events such as the Internet Day, cybersecurity awareness month in October and

the Girls in ICT Day.[74] The focus-group discussion participants indicated that the public lack awareness of cybersecurity risks, especially at the grassroots level. They further indicated that awareness raising is mostly conducted within the private sector organisations and differs across these organisations. Another issue the focus-group discussion participants highlighted is the cybersecurity language; they believe the language needs to be simplified for people to understand. Also, the absence of cybersecurity policies and strategies has contributed to a lack of awareness of cybersecurity risks in the country.

Priority of security (Start-up)

The government of the Kingdom of Lesotho has recognised the importance of prioritising cybersecurity. The passing of the cybercrime and cybersecurity bill demonstrates effort to address cybersecurity issues in the country. In addition, various cybersecurity symposiums are held in the country on an annual basis.[75] However, there is no sense of urgency by the government to enhance cybersecurity in the country. Therefore, prioritisation of cybersecurity within the public remains a big concern.

Participating private organisations recognised the need to prioritise cybersecurity in the country. Focus-group discussion participants stated that prioritisation of cybersecurity differs between local and multinational companies. Multinational companies tend to prioritise cybersecurity more than local companies. According to the focus-group discussion participants, private organisations have been more successful in developing cybersecurity policies to improve cybersecurity awareness.

Focus-group discussions suggest that some internet users recognise the importance of prioritising cybersecurity. However, the majority only prioritise cybersecurity after falling victim to cyberattacks. Understanding of cybersecurity risks among the general public is still a challenge. There are no metrics available to assess the level of knowledge on cybersecurity in the country. Therefore, the level of knowledge on cybersecurity in Lesotho is not known.

Practices (Start-up to Formative)

Most government agencies in the country do not adhere to safe cybersecurity practices. The 2019 CMM review indicated that there are no policies and guidelines across government agencies for the implementation of safe cybersecurity practices. According to the focus-group discussion participants, policies and guidelines on safe cybersecurity practices can only be developed once the cybercrime and cybersecurity bill has been enacted.

Most private sector organisations adhere to safe cybersecurity practices. Private sector organisations are affiliated with international organisations and therefore, adopt international standards and best practices on cybersecurity. According to the participants, the private sector follows cybersecurity best practices. These are adopted from international standards such as International Organisations for Standards (ISO) and International Electrotechnical Commission (IEC).

---

[74] Vodacom Lesotho. (2022). Cyber security awareness message. https://www.vodacom.co.ls/?p=6175

[75] LENA. (2020, February 28). Cybercrime a risk to Lesotho. https://www.gov.ls/cyber-crime-a-risk-to-lesotho/

A limited proportion of internet users in the country follow safe cybersecurity practices. In addition, awareness of appropriate online behaviours is minimal. This may be attributed to a lack of awareness of cybersecurity risks. Focus-group discussion participants pointed to the need to sensitise the public to cyber threats and how they can protect themselves online.

Online forums such as "ICT forum" which are mostly used by ICT specialists in the country are helpful to both the government, the private sector and individuals as they provide useful information on cybersecurity issues.

D 2.2 TRUST AND CONFIDENCE IN ONLINE SERVICES

This Factor reviews critical skills, the management of disinformation, the level of users' trust and confidence in the use of online services in general, and of e-government and e-commerce services in particular.

Stage: [Start-up]

Digital literacy and Skills (Start-up to Formative)

Few internet users in the country critically assess what they see or receive online. However, as in many other developing countries, most of the citizens in the Kingdom of Lesotho, especially in the rural areas, are unable to participate in the digital space due to a lack of digital literacy skills.[76] Focus-group discussion participants stated that only a limited proportion of internet users can identify cybersecurity risks and are confident that they can protect themselves online. Nevertheless, they indicated that despite the lack of trust and confidence, users have no choice but to use the internet. However, there are no metrics in the country to evaluate internet users' trust and confidence online.

A non-governmental organisation, Help Lesotho, established an initiative in 2013 to enhance computer literacy in the country. The programme has thus far benefited 2000 individuals from both the government and the private sector.[77] ICT skills among the youth aged 15 to 24 was estimated to be 14% according to the Lesotho Education Facts Sheets 2021. Youth aged 15 to 24 in the Urban areas were more engaged in ICT activity compared to rural areas.[78] In 2018, LCA sent out a Request For Proposals (RFP) for digital literacy training for the teachers as part

[76] Mochone, T. (2020, September 22). *Preserving an open Internet in Lesotho through a multistakeholder dialogue*. https://openinternet.global/news/preserving-open-internet-lesotho-through-multi-stakeholder-dialogue#:~:text=An%20astonishing%2083%25%20of%20Lesotho%27s,digital%20divide%20in%20the%20country

[77] Sello.R. (2022, January 12). *Computer literacy scheme a success in Lesotho*. https://www.cajnewsafrica.com/2022/01/12/computer-literacy-scheme-a-success-in-lesotho/

[78] UNICEF. (2021*). Lesotho education fact sheets 2021, analyses for learning and equity using MICS data*. https://data.unicef.org/wp-content/uploads/2021/09/Lesotho_MICS_EAGLE_Fact-Sheets.pdf

of an agreement signed in 2016 with the Ministry of Education and Training (MoET). The training aimed to address the digital literacy skills gaps in the country's schools.[79]

User Trust and Confidence in Online Search and Information (Start-up)

A limited number of internet users have sufficient trust and feel confident in using the internet. Although there are no metrics to evaluate users' trust and confidence online, the focus-group discussion participants indicated that there is too much of a blind trust in websites and information received online. They further indicated that internet users have a limited ability to differentiate between legitimate websites and those that are not safe. However, the country's secure internet servers (per 1 million people) increased from 138 in 2019 to 150 in 2020.[80]

Disinformation (Start-up)

Internet service providers (ISPs) in the country are doing little to address the problem of disinformation. Focus-group discussions pointed out that ISPs have no approaches in place to adequately address issues of disinformation.

The country's Internet Society chapter held a webinar in November 2020 to discuss the implications of fake news, misinformation and disinformation, and how they can be addressed.[81] LCA uses its website to sensitise the public about the danger of misinformation.[82] The paucity of media outlets such as newspapers, radio and television stations has led citizens in the country to rely more on social media for news. Some social media pages are valuable sources, but some outlets often reproduce and spread information that misinforms the public. This further undermines trust and confidence online.

User trust in E-government Services (Start-up to Formative)

There are e-government services in the country, such as online business registration, tax registration and clearance.[83] Focus-group discussion participants indicated that the uptake of e-services has increased, partly since the outbreak of the COVID-19 pandemic. However, some online services are not fully automated. Participants stated that their experience to-date with online services has been good.

---

[79] Lesotho Communication Authority. (2018, October 29). *Request for proposals | Digital literacy training for teachers.* https://lca.org.ls/general-documents/

[80] The World Bank. (2022). *Secure Internet servers-Lesotho*. https://data.worldbank.org/indicator/IT.NET.SECR?locations=LS

[81] Internet Society Lesotho Chapter. (2020, November 24). *Fake news, misinformation & disinformation.* https://isoc.org.ls/event/fake-news-misinformation-disinformation/

[82] Lesotho Communication Authority. (2020, April 2). *Warning on distribution of false and fake information using communications platforms*. https://www.lca.org.ls/2020/04/

[83] The Government of Lesotho. (n.d.). *E-services.* https://www.gov.ls/services/

A growing number of Internet users are using e-government services in the country. However, according to the focus-group discussion participants, majority of the users utilise these services because they do not have other alternatives and not necessarily because they believe that they are secure.

Government entities do not have metrics to assess internet users' trust and satisfaction with e-government services. Thus, statistics on internet users' trust in e-government services that could help improve these services are not available.

There is a lack of information on e-government security and security breaches in the country. From the observed websites in the country, there is no published information to sensitise users about their privacy and security breaches.

User Trust in E-commerce services (Start-up)

E-commerce is not widely used in the Kingdom of Lesotho. The country's e-commerce industry remains underdeveloped.[84] However, there is a growth in the promotion of online shopping and cashless transactions. Large organisations and institutions are migrating to the digital environment for operation efficiency and because of the COVID-19 restrictions. One of the country's commercial banks, First National Bank (FNB), recently launched an e-commerce platform to enable clients to buy and sell goods and services.[85] The country's National Commission for UNESCO also launched an e-commerce platform aimed at promoting the cultural sector.[86] Focus-group discussion participants indicated that e-commerce services are not popular in the country. This may have been attributed to the low digital literacy and skills. They further mentioned that internet users in the country tend to trust e-commerce services provided by reputable organisations as they believed that they are secure. Since international companies provide most of the e-commerce services, they comply with international standards and best practices, especially on security measures and features.

There are no measures in place to assess users' trust in e-commerce services. Focus-group discussion participants indicated that some organisations have metrics to evaluate customer satisfaction but not on trust.

[84] United States Department of Commerce. (2016, January 11). *Lesotho-eCommerce. International Trade Administration*. https://legacy.export.gov/article?id=Lesotho-ecommerce

[85] Africa Press. (n.d.). *FNB introduces local E-commerce platform*. https://www.africa-press.net/lesotho/all-news/fnb-introduces-local-e-commerce-platform

[86] The Government of Lesotho. (n.d.). *UNESCO launches e-Commerce.* https://www.gov.ls/unesco-launches-e-commerce/

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This Factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protecting personal information online, and whether they are sensitive of their privacy rights.

Stage: [Start-up to Formative]

Personal Information Protection Online (Start-up to formative)

There is evidence that discussions on the protection of personal information or data online have begun in the country. According to the focus-group discussion participants, public debates on personal information protection online, privacy and security are taking place but are limited.

The country has recognised and protected the right to privacy of its citizens through its constitution. The Data Protection Act of 2011 provides guidelines for the regulation of the use of personal information.[87] The Act aims to protect users' personal information and imposes restrictions and obligations on both the private and public organisations as well as individuals when dealing with individual's data or information.[88] However, several legislative mechanisms in the country such as the draft Compliance Monitoring and Revenue Assurance Regulations of 2021, are perceived to undermine individual data protection and privacy. Furthermore, the country has not yet ratified the AU Convention on Cybersecurity and Personal Data Protection.[89]

A limited number of internet users recognise the importance of protecting personal information. Users have minimal knowledge about how personal information is handled online and how to adequately protect their personal information. However, some corporations such as the Lesotho Tourism Development Corporation have developed Data Protection Policy to sensitise users on the use of personal data.[90]

[87] *Data protection Act No. 5 of 2011*. (Lesotho). https://www.centralbank.org.ls/images/Legislation/Principal/Data_Protection_Act_2011.pdf

[88] Lex Africa. (2020, August 26). *Overview of data privacy and protection in Lesotho.* https://www.lexafrica.com/2020/08/overview-to-data-privacy-and-protection-in-lesotho/

[89] CIPESA. (2021, August). *Online privacy at stake in Lesotho with the adoption of the Compliance Monitoring and Revenue Assurance Regulations, 2021*. http://cipesa.org/?wpfb_dl=464

[90] Lesotho Tourism Development Corporation. (n.d.). *Data protection policy*. https://www.visitlesotho.travel/information/data-protection-policy

D 2.4 REPORTING MECHANISMS

This Factor explores the existence of 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 incidents.

Stage: [Start-up]

User Reporting (Start-up)

There are no formal reporting mechanisms for internet users to report incidents relating to privacy and security breaches in the country. The focus-group discussion participants indicated that the absence of formal reporting mechanisms was due to the lack of cybersecurity and cybercrime legislation. LCA has made it possible for consumers to register their complaints regarding communication issues on its website.[91] It has also published a consumer complaints manual called the "Communications Sector Consumer Complaints Procedure" and is available in both Sesotho and English.[92]

Reporting Mechanism (Start-up)

The country has no formal reporting mechanisms for cyberbullying, child abuse online or identity theft. However, ISPs such as Econet Telecom Lesotho (ETL) provide tips on the use of social media available on mobile phones and on how to deal with cyberbullying for teens.[93] Commercial banks in the country introduced security centres to report fraudulent emails, identity theft and other digital fraud.[94] In addition, multinational companies such as TNT Lesotho and DHL Lesotho encourage their customers to report online fraud to the local police.[95] The cost of cybercrime in Lesotho has been estimated at US$ 2 million, with the banking sector, public sector and microfinance.[96] According to a report for 2017/18 by Serianu, 6% of the citizens did not know how to report cybercrime to the police. One estimate is that more than 94% of the incidents are either not reported or not resolved.[97]

---

[91] Lesotho Communications Authority. (2022). *Lodge a complaint*. https://lca.org.ls/lodge-a-complaint/

[92] Lesotho Communication Authority. (2018). *Consumer complaint procedure*. https://www.lca.org.ls/complaints/

[93] Econet Lesotho. (2019, March 18). *Mobiles and Cyber bullying Tips for Teens.* Facebook.https://www.facebook.com/EconetLesotho/posts/mobiles-and-cyber-bullying-tips-for-teens-only-give-your-mobile-number-and-usern/1161831743998786/

[94] First National Bank. (n.d.). *Security centre| report fraud.* https://www.fnb.co.ls/security-centre/index.html

[95] TNT Lesotho. (2017). *Internet fraud.* https://www.tnt.com/express/en_ls/site/support/fraud.html

[96] Serianu. (2018). *Africa cyber security report-Lesotho*. https://www.serianu.com/downloads/LesothoCyberSecurityReport2018.pdf

[97] Serianu. (2018). *Africa cyber security report-Lesotho*. https://www.serianu.com/downloads/LesothoCyberSecurityReport2018.pdf

Metrics on reported incidents (Start-up)

There are no formal metrics on reported incidents in the country. According to the Serianu report for 2018, about 90% of cybercrime incidents are not reported. In addition, there are no mechanisms in place to monitor cybersecurity risks despite the country being vulnerable to cyberattacks.[98] This was confirmed by the focus-group discussion participants, that no metrics exists on reported cyber incidents.

Social media Channels (Start-up)

Internet users rarely use social media channels to inform other users about cybersecurity matters. The country's internet penetration stood at 47.9% in January 2021, and 24.6% of internet users were using social media.[99] According to the focus-group discussions, internet users mostly use social media channels to communicate and share information on general social issues but not specifically on cybersecurity. The main purpose for using the internet is social networking (46.7%), followed by education purposes (23.9%).[100]

Response-Coordination (Start-up)

There are no mechanisms in place to coordinate reported incidents between stakeholders such as law enforcement agencies and national or sectoral incident response teams. According to participants in the focus-group discussions, these mechanisms can only be developed once the Computer Crime and Cyber Security Bill has been passed. Repeatedly, a number of actions appears to have been delayed by a sense that they must await formal legislation.

D 2.5 MEDIA AND ONLINE PLATFORMS

This Factor explores whether cybersecurity is a common subject of discussion across mainstream media, and an issue for broad discussion on social media. Moreover, this Factor looks at the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: [Start-up to Formative]

[98] Symantec. (2016). *Cybercrime & cybersecurity trends in Africa*. https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

[99] Kemp S. (2021, February 11). Digital 2021: Lesotho. Datareportal. https://datareportal.com/reports/digital-2021-lesotho

[100] LCA. (2017). *The state of ICT in Lesotho: Demand side facts and figures*. https://lca.org.ls/ict-research/

Media role (Start-up to formative)

There is limited but growing coverage of cybersecurity issues in the media. Local newspapers such as Metro Maseru and Kingdom Digital News publish articles on cyberattacks and cybersecurity-related issues.[101,102] The focus-group discussions indicated that since the outbreak of the COVID-19 pandemic and the tabling of the Computer Crime and Cyber Security Bill, there has been an increase in the coverage of cybersecurity both on radio and television. In addition, the focus-group discussion participants stated that there are newspaper articles or social media posts on cybersecurity. However, the coverage of cybersecurity issues remains in an early stage of development.

Media cybersecurity information (Start-up to formative)

Cybersecurity information such as about cyberbullying, online child protection, cybercrime and security breaches are reported in the media on an ad-hoc basis. The coverage of this information depends on the most burning issue in the country at the time or when there is an organised event to raise awareness. For instance, at the beginning of the year, the Lesotho Times reported on a tournament organised to raise awareness on gender-based violence and cyberbullying.[103]

Social Media Discussion (Start-up)

Cybersecurity is a rare topic of discussion in the social media among consumers and citizens in the country. Many Internet users are thought to be using social media to cause harm to others, often in the form of cyberbullying. The Post newspaper reported on how most of the Basotho population have been traumatised on social media.[104] Nevertheless, according to the focus-group discussion participants, discussions about cybersecurity on social media are rare.

Discussion Informing Policy-Making (Start-up)

There is limited discussion on cybersecurity in the mainstream media and social media. Therefore, it is not known whether these discussions inform policymaking. In addition, the lack of mechanisms to encourage cybersecurity discussions in the mainstream media demonstrates that the government cannot rely significantly on mainstream media and social media channels for informing policymaking.

---

[101] Metro newspaper. (2020, February 29). *Malicious and nuisance cyberattacks worry Lesotho*. Metro News. https://www.maserumetro.com/news/business/malicious-and-nuisance-cyberattacks-worry-lesotho/

[102] Mosala, M. (2021, September 14). *Parliament asked to prohibit "Draconian" computer, cybersecurity and communications laws*. Kingdom Digital News. https://kdnews.co.ls/parliament-asked-to-prohibit-draconian-computer-cybersecurity-and-communications-laws/

[103] Thuseho, L. (2022, January 7). *Sportspersons tackle GBV, cyberbullying*. Lesotho Times. https://lestimes.com/abc-abandons-gnu-plans/

[104] Motsopa, M. (2020, November 3). *The trauma of cyber-bullying.* The Post. https://www.thepost.co.ls/news/the-trauma-of-cyber-bullying/

Whistleblowers (Start-up to formative)

Whistleblowing is accepted and encouraged in the country. According to the focus-group discussions, some organisations in the country have policies on whistleblowing. The Lesotho Revenue Authority developed the whistleblowing policy to encourage citizens to raise concerns regarding fraud, corruption, or any misconduct; and in line with this, the policy protects whistleblowers.[105] There is also a Facebook page entitled "Whistleblowing Media" aimed at providing news on whistleblowing. However, the Facebook page has 132 followers only and appears to be inactive. Focus-group discussions indicated that whistleblowing focuses more on corruption activities rather than cybersecurity issues and is more prevalent in the private sector.

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *Cybersecurity Culture and Society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MINDSET

R2.1 Ministry of Information, Communications, Science, Technology and Innovation (MICSTI) together with the Lesotho Communication Authority (LCA) and the national and sectorial CSIRTs should create awareness on cybersecurity risks to enhance cybersecurity mindset in the country.

R2.2 Government agencies, and all relevant stakeholders, at all levels should prioritise cybersecurity.

R2.3 The MICSTI, in collaboration with LCA, should strive to promote good cybersecurity practices across all sectors in the country.

R2.4 The MICSTI, in collaboration with relevant stakeholders, should generate more systematic evidence, such as surveys or targeted studies, on the attitudes, beliefs and practices of Internet and social media users across all sectors.

[105] Lesotho Revenue Authority. (n.d.). *Lesotho Revenue Authority whistle blowing policy*. https://www.lra.org.ls/sites/default/files/2017-03/LRA%20Whistle%20Blowing%20Policy.pdf

TRUST AND CONFIDENCE IN ONLINE SERVICES

R2.5 The government in collaboration with civil society and other stakeholders should continue to develop and support multimedia literacy programmes in the country.

R2.6 MICSTI should coordinate digital literacy programmes between ISPs, private sector, regulators and civil society.

R2.7 MICSTI, together with the ISPs, private sector and regulators, should promote and build trust when introducing online services.

R2.8 MICSTI and LCA should develop measures to assess users' trust and confidence in the use of online services.

R2.9 MICSTI, LCA, private sector and civil society should develop measures and initiatives to address online disinformation, mal-information and misinformation.

R2.10 MICSTI should publicly promote the security of e-government services in the country to increase uptake and instil confidence in the use of these services.

R2.11 MICSTI, regulators, National CSIRT and sectorial CSIRTs should encourage the use of secure e-commerce services such as the use of SSL encryption and authentication services.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.12 The LCA, ISPs and CSIRTs should create more awareness to sensitise internet users on how they can protect their personal information online.

R2.13 The government should encourage discussions regarding the protection of personal information online and privacy rights through various initiatives and programmes in the mainstream media.

REPORTING MECHANISMS

R2.14 MICSTI, LCA and LMPS should collaborate and develop mechanisms for reporting cybersecurity incidents in the country and raise awareness about these reporting channels.

R2.15 MICSTI, LCA and LMPS should establish and improve coordination mechanisms that will enable citizens to report cybercrime cases.

MEDIA AND ONLINE PLATFORMS

R2.16 The government through MICSTI should encourage and promote the use of mass media to disseminate information on cybersecurity issues.

R2.17 MICSTI, LCA, civil society groups and the media organisations should raise awareness on cybersecurity topics for media and social media actors.

R2.18 Government agencies, ministries and all stakeholders should continue to encourage whistleblowing for transparency and accountability.

DIMENSION 3

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

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, and relate to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes (See Figure 8). The results of the evaluation are summarised in Figure 9 and further elaborated in the subsequent sections.

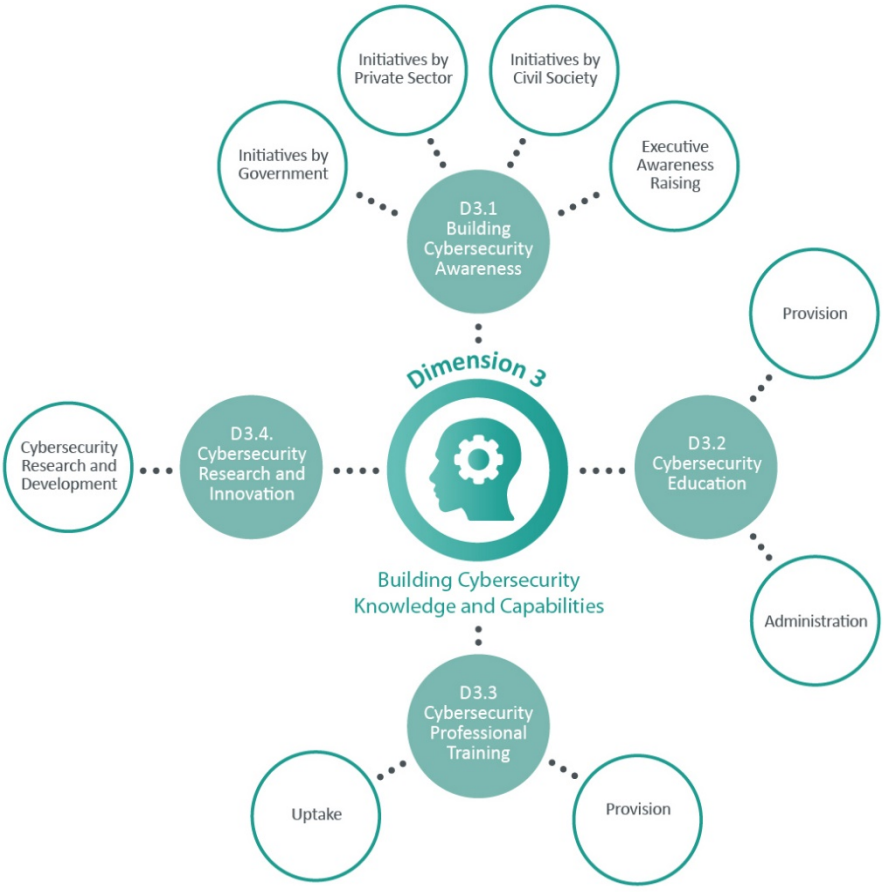

Figure 8: Factors and aspects of the Dimension 3 of the CMM

Overview of results

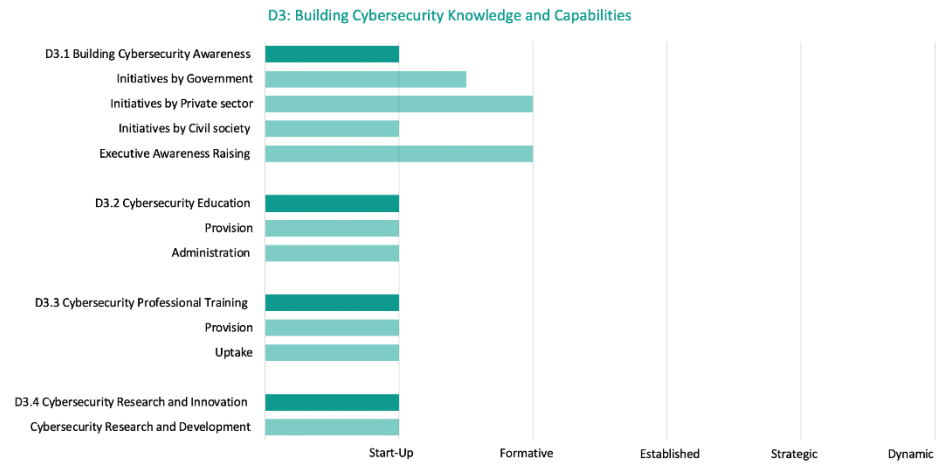

Figure 9: Result of the assessment of building cybersecurity knowledge and capabilities of the Kingdom of Lesotho

D 3.1 BUILDING CYBERSECURITY AWARENESS

This Factor focuses on the availability of programmes that raise cybersecurity awareness throughout the country, concentrating on cybersecurity risks and threats and ways to address them.

Stage: [Start-up to Formative]

Awareness-raising initiatives by Government (Start-up)

Most people in Lesotho are unaware of the cybersecurity risks associated with using e-services.[106] The participants in the focus-group discussions emphasised the need for cybersecurity awareness initiatives in the country. According to the participants, government agencies are not actively involved in developing cybersecurity awareness initiatives. Despite the recommendations of the 2019 CMM review, the country is yet to have an overarching cybersecurity awareness-raising programme or a framework to guide the government in developing cybersecurity awareness initiatives. Currently, not much has been done to develop and implement cybersecurity awareness programmes. The focus-group discussions also noted that the government was only active in cybersecurity awareness during the launch of the *Computer Crime and Cyber Security Bill*. The news about the *Computer Crime and Cyber*

[106] Mosola, N. N., Moeketsi, K. F., Sehobai, R., & Pule, N. (2019). Cybersecurity Protection Structures: The Case of Lesotho. *International Journal of Computer and Information Engineering*, *13*(3), 158-163. https://doi.org/10.5281/zenodo.2643673

Security Bill was disseminated via radio, television, social media and other news outlets, which helped raise some cybersecurity awareness among the public.[107,108]

The focus-group discussion participants indicated that some government sectors provide cybersecurity awareness initiatives in silos, making it difficult for the sectors to collaborate and harmonise the initiatives. The 2019 CMM review recommended establishing a government agency responsible for developing and implementing cybersecurity awareness programmes in the country. However, by 2022 no government agency was assigned to develop cybersecurity awareness programmes in Lesotho. The *Computer Crime and Cyber Security Bill* states the establishment of National Cybersecurity Advisory Council (NCAC) which will be responsible for cybersecurity awareness in the country.

Awareness-raising initiatives by Private Sector (Formative)

Companies in the telecommunication and banking sectors conduct cybersecurity awareness-raising initiatives for clients and staff. The review also identified one insurance company raising awareness among its customers.[109] According to the focus-group discussion participants, most private sector organisations have drafted cybersecurity awareness strategies in their internal Information Technology (IT) policy. They conduct robust cybersecurity awareness-raising programmes for employees. The programmes cover cybersecurity risks and how these risks can be mitigated. The participants also added that cybersecurity awareness programmes differ from organisation to organisation. In cases where the organisation serves clients through digital channels, for instance, as is the case in telecommunication and banking sectors, on an ad-hoc basis, they send messages to their clients through text messages on mobile phones, email or other media outlets to alert their clients of the current threats (e.g., phishing, spam, and disclosure of information). Organisations without digital channels focus awareness-raising on their employees. However, from the discussions, it is unclear whether the private sector has developed metrics to measure the impact and effectiveness of cybersecurity awareness strategies for both clients and employees.

The focus-group discussion participants noted that the private and the public sector work in silos. The participants further highlighted that the public sector had not created platforms to collaborate with the private sector; therefore, the private sector does the cybersecurity awareness initiatives without involvement or collaboration with government entities.

---

[107] Lesotho National Broadcasting Service. (2019, June 8). *Computer Crime & Cyber Security Bill. This* [Video attached] [Status update]. Facebook. https://sw-ke.facebook.com/LesothoTv/videos/computer-crime-cyber-security-bill/2121125964861206/?__so__=permalink&__rv__=related_videos

[108] MISA Lesotho. (2021, July 8). *Media Statement on Computer Crime and Cyber Security Bill.* https://lesotho.misa.org/2021/07/08/media-statement-on-computer-crime-and-cyber-security-bill/

[109] Minet Lesotho. (2020, April 29). *Being a cybersecurity champion for the company you work for.* https://www.minet.com/wp-content/uploads/2020/04/Thought-leadership-Being-a-cybersecurity-champion-for-the-company-you-work-for.pdf

Awareness-raising initiatives by Civil Society (Start-up)

Civil society organisations (CSOs) play a critical role in many developing countries. However, there is little involvement in cybersecurity issues by CSOs in the kingdom of Lesotho. According to the focus-group discussion participants, many CSOs in the country are unaware of their potential role and contribution to cybersecurity. This is attributed to a lack of tailored cybersecurity awareness initiatives in the country. In addition, the participants stated that cybersecurity is not a hot topic; as a result, CSOs hardly participate. As such, participants in the focus-group discussions highlighted a need for government to conduct cybersecurity awareness programmes for CSOs to promote their participation in cybersecurity discourse.

Few CSOs in the country are participating in cybersecurity issues. The focus-group discussion participants indicated that some CSOs were training the media houses on reporting news, such as gender-sensitive news. The participants also highlighted that the CSOs had developed an application called *Nokaneng App*.[110,111] The application provides a platform for women and girls in the country to create awareness of gender-based violence, cyberbullying and reporting cases relating to gender-based violence and cybercrime.

Executive Awareness Raising (Formative)

It was evident from the focus-group discussions that the executives are becoming more aware of the cybersecurity risks compared to the previous years. Focus-group discussion participants stated that, during the COVID-19 pandemic, there was an increase in cyber threats. This forced many executives in the country to be more vigilant in protecting their critical infrastructures and assets. Cybersecurity is now being incorporated into their strategic plans. For instance, the Central Bank of Lesotho has formulated a *2022-2024 strategic plan* which points out cybersecurity threats as one of the emerging issues in the country.[112] To counteract cyber threats, the strategic plan indicates a need to enhance cybersecurity resilience. The participants further stated that the Central Bank had drafted the *cybersecurity strategic framework* to achieve the objective stated in the *2022-2024 strategic plan.*

The executives in the private sector are aware of their cybersecurity role both to their employees and customers. For instance, the participants in the focus-group discussions from the private sector stated that they receive cybersecurity training on an ad hoc basis. And for their customers, this is reflected through cybersecurity awareness-raising programmes being conducted in the country. However, according to the discussions, this does not apply to the executives in the public sector.

---

[110] Gender Links for Equality and Justice. (2019, February 26). *Lesotho: Nokaneng App- Going Digital on GBV.* https://genderlinks.org.za/casestudies/lesotho-new-app-to-prevent-gbv/

[111] Mainlevel Development Team. (2021). *Nokaneng (Lesotho)* [Mobile App]. Google Play Store. https://play.google.com/store/apps/details?id=ls.nokaneng.app&hl=en_ZA&gl=US

[112] Central Bank of Lesotho. (2022). *2022-2024 Strategic Plan Promoting a Stable Monetary.* https://www.centralbank.org.ls/images/Publications/Research/Reports/CENTRAL_BANK_OF_LESOTHO_2022_-_2024__STRATEGIC_PLAN_-_Online.pdf

D 3.2 CYBERSECURITY EDUCATION

This Factor addresses the availability and provision of high-quality cybersecurity education programmes and sufficient qualified teachers and lecturers. Moreover, this Factor examines the need to enhance cybersecurity education at national and institutional levels and the collaboration between government and industry to ensure that educational investments meet the needs of the cybersecurity education environment across all sectors.

Stage: [Start-up]

Provision (Start-up)

The country's education system is structured as follows:

- primary school: runs for seven years;
- the junior secondary level is three years, and the students sit for the Junior Certificate Examination (JCE);
- senior secondary level; runs for two years. After completion, the students sit for either the Lesotho General Certificate of Secondary Education (LGCSE) or the International General Certificate of Secondary Education (IGCSE);
- after completing the LGCSCE or IGCSE, students have the option to sit for Advanced Subsidiary (AS) /Advanced (A) Levels.

After senior secondary school, students can pursue a career at universities or other tertiary institutions.[113] The country has fourteen higher education institutions: eight public and six privately owned.[114] The leading higher education institutions in the country are the National University of Lesotho (NUL), Lerotholi Polytechnic and Lesotho College of Education.[115]

The kingdom of Lesotho recognises that technology adoption is the driving force for economic transformation. In 2004, the country introduced computer education at the secondary level as a subject through the National Curriculum Development Centre (NCDC), which is responsible for the development of the curriculum of basic education in the country.[116] The need for ICTs in the education sector is still a priority for the government. The revised *2018*

[113] Lerotholi, L.M. (2001). Tuition fees in primary and secondary education in Lesotho: the levels and implications for access, equity and efficiency. https://unesdoc.unesco.org/ark:/48223/pf0000123535/PDF/123535eng.pdf.multi

[114] Tlali, S.B., & Hapazari, I. (n.d.) *Financing Higher Education and A Selection of Other SADC Countries.* www.che.ac.ls/wp-content/uploads/2018/12/Prof_Tlali_Conference_Paper.pdf

[115] Council on Higher Education. (2010). *Report on the state of higher education in Lesotho.* https://www.che.ac.ls/wp-content/uploads/2019/02/State-of-Higher-Education-Report-2011-12.pdf

[116] Lisene, L.N. (2017). *The integration of information and communication technologies into teaching of physical science in Lesotho.* [Masters dissertation, University of the Free State]. University of free state Repository. https://scholar.ufs.ac.za/handle/11660/7006?show=full

National Strategic Development Plan[117] and the *Education Sector Plan 2016-2026*[118] further acknowledge that the government needs to work towards increased technology adoption in the education sector to leverage economic growth. Despite the emphasis on the need for ICT adoption in the education sector, the sector has not clearly outlined strategies to secure the ICTs for both the learners and the school administration. With the rise in cyber threats, there is a need for the sector to inform students on how to protect themselves.

The focus-group discussion participants stated that privately owned primary and secondary school students are more likely to be aware of cyber threats. However, it is still a challenge for public schools. The participants suggested that the NCDC should revise the curriculum to incorporate cybersecurity in the end-user application studies that are taught in lower grades so that students become aware of cyber threats and develop a cybersecurity mindset. The suggestion for revising the curriculum agrees with the *Curriculum and Assessment Policy of 2009* which stipulates the need for quality and relevance in the education sector for the country.[119]

The 2019 CMM review noted that no cybersecurity degree courses were offered in Lesotho. According to the focus-group discussions, the Universities have not yet implemented cybersecurity-specific courses. Currently, the institutions in the country are offering a Bachelor of Science (Hons) in Information Technology [120] or a Bachelor of Engineering in Computer science and networks.[121,122] According to the desktop study and the 2019 CMM review, NUL established a cybersecurity research centre which was meant to commence in January 2019. The centre was meant to provide short cybersecurity courses and cybersecurity awareness programmes.[123] However, the participants in the focus-group discussions had not seen any activities being run at the centre.

According to the focus-group discussion participants from the education sector, there is a need for cybersecurity-specific courses. They indicated that the Ministry of Education and Training (MoET) and NCDC are not engaging with the Council of Higher Education to ensure that the developed courses meet the country's needs. The Council of Higher Education

---

[117] The Government of Lesotho. (2018). National Strategic Development Plan II 2018/19-2022/23. https://www.gov.ls/wp-content/uploads/2021/06/National-Strategic-Development-Plan-II-2018-19-2022-23.pdf

[118] The Government of Lesotho. (2016). *Education Sector Plan 2016 –2026.* https://www.globalpartnership.org/sites/default/files/education_sector_plan_2016-2026._lesotho_0.pdf

[119] Raselimo, M., & Mahao, M. (2015). The Lesotho curriculum and assessment policy: Opportunities and threats. *South African Journal of Education, 35*(1). https://www.researchgate.net/publication/276788778_The_Lesotho_curriculum_and_assessment_policy_Opportunities_and_threats

[120] Limkokwing University. (2022). *Bachelor of Science (Hons) in Information Technology.* https://www.limkokwing.net/lesotho/academic/courses_details/bachelor-of-science-hons-in-information-technology

[121] National University of Lesotho. (2021). *Undergraduate Prospectus 2021/2022.* www.nul.ls/wp-content/uploads/2021/04/Undergraduate-Prospectus-2021-2022-1.pdf

[122] Botho University. (2022). *Prospectus 2022/23.* https://lesotho.bothouniversity.com/wp-content/uploads/sites/4/2022/03/LESOTHO-Prospectus-A5-Resize-1_compressed.pdf

[123] IST-Africa. (2022). N*ational ICT Research Capacity and Priorities for Cooperation-Kingdom of Lesotho*. www.ist-africa.org/home/default.asp?page=doc-by-id&docid=5189

regulates the national qualifications in the country and has developed the *Lesotho Qualification Framework* (LQF).[124] The LQF is a guide on the development of qualifications and evaluation of foreign qualifications in the country. However, the LQF does not provide for the development and evaluation of guidelines for cybersecurity qualifications.[125] Therefore, the focus-group discussions recommended that the Council on Higher Education develop a cybersecurity qualification framework to guide the education sector in developing and evaluating cybersecurity programmes in the country.

Administration (Start-up)

The kingdom of Lesotho has one of the lowest per capita supports for higher education students.[126] Most of the students in the country are funded by the government through the National Manpower Development Secretariat (NMDS).[127] NMDS offers grants and loans to students enrolled in higher learning institutions in the country. In addition, the government of Lesotho receives scholarship offers from other countries for students to pursue their qualifications. The participants in the focus-group discussions indicated that NMDS offers scholarships and grants to students pursuing Computer Science and Information Technology-related degrees and that these courses were on the NMDS priority list. The courses on the priority list include Computer Engineering, Systems Engineering and Information & Communications Technology.[128] Therefore, there is a need for NMDS to revise their priority list to include cybersecurity courses.

Students who would like to pursue cybersecurity-specific degrees do so through international institutions. Although the stakeholders are aware of the gap in cybersecurity programmes in the country, the government has not made efforts for stakeholder consultations in cybersecurity educational programme development in the country. In addition, there is a lack of cybersecurity experts to assist in developing the courses. Due to the lack of consultation between higher learning institutions and relevant stakeholders in the country, the programmes that are being developed do not meet the needs of the country. Currently, only private higher learning institutions collaborate with universities in the Republic of South Africa.

---

[124] Malunga, B. (2020, March 25). *Lesotho Qualifications Framework (LQF) is disseminated (March 2020).* Council on Higher Education. https://www.che.ac.ls/lesotho-qualifications-framework-lqf-is-disseminated-march-2020/#:~:text=The%20Lesotho%20Qualifications%20Framework%20(LQF,from%20primary%20to%20doctoral%20qualifications.

[125] Ministry of Education and Training. (2019). *The Lesotho Qualifications Framework (LQF) Procedures Manual.* https://www.che.ac.ls/wp-content/uploads/2020/02/Procedures-Manual_LQF-Approved-1.pdf

[126] Tlali, S.B., & Hapazari, I. (n.d.) *Financing Higher Education and A Selection of Other SADC Countries.* www.che.ac.ls/wp-content/uploads/2018/12/Prof_Tlali_Conference_Paper.pdf

[127] National Manpower Development Secretariat. (2013). *NMDS scholarship portal.* www.scholarships.manp.gov.ls/Home/Download

[128] National Manpower Development Secretariat. (2019, August 2). [Images Attached] [Status update]. Facebook. https://web.facebook.com/National-Manpower-Development-Secretariat-1476476602641711/photos/pcb.2397972473825448/2397971513825544

D 3.3 CYBERSECURITY PROFESSIONAL TRAINING

This Factor addresses and reviews the availability and provision of affordable cybersecurity professional training programmes to build a cadre of cybersecurity professionals. Moreover, this Factor reviews the uptake of cybersecurity training, and horizontal and vertical cybersecurity knowledge and skills transfer within organisations, and how this transfer of skills translates into a continuous increase of cadres of cybersecurity professionals.

Stage: [Start-up to Formative]

Provision (Start-up to formative)

The 2019 CMM review noted that the National University of Lesotho (NUL) was the only higher education institution offering professional training courses. NUL offers Cisco Certified Network Associate (CCNA) training. The focus-group discussion participants highlighted that a few higher education institutions have also started offering professional training. However, they emphasised that it is still limited due to a lack of cybersecurity professionals in the country to develop and deliver the content. Lerotholi Polytechnic offers CCNA Cyber Operations, Cybersecurity Essentials and CISCO IT Essentials 1.[129] In addition, MoET, through Technical and Vocational Education and Training (TVET), established a cybersecurity certification course at the Catholic Comprehensive Community College (CCCC). The participants also stated that the course offered at the Catholic Comprehensive Community College (CCCC) has more practical content for students to have hands-on experience that equips them with cybercrime mitigation strategies. It is unclear whether the relevant stakeholders were consulted during the development of the professional training courses and whether the current courses meet the country's demands.

According to the participants, the private sector, especially the telecommunication sector, provides employee training, generally conducted through online platforms. The 2019 CMM review noted that one private training institution based in the United Kingdom was advertising cybersecurity professional training courses. Based on the current desk research, the courses are still being offered, and more private training companies are advertising cybersecurity professional training in the country. There is still no local professional training for certifications such as COBIT, ISO or ISACA. The participants noted that the online courses were expensive. Therefore, they recommended that NMDS should also provide scholarships for cybersecurity professional training; the current grants are limited to degrees, masters and PhD programmes.

[129] Lerotholi Polytechnic School of Continuing Education-SOCE. (2019, October 3). *Hi everyone, let's help each other, tell a friend to tell a friend. Afternoon classes available.* [Image attached] [Status update]. Facebook. https://web.facebook.com/103470707730072/photos/hi-everyone-lets-help-each-other-tell-a-friend-to-tell-a-friend-afternoon-classe/103476154396194/?_rdc=1&_rdr

Uptake (Start-up)

The focus-group discussion participants highlighted that the demand for cybersecurity professionals is high. However, they were unsure whether MoET had developed metrics to evaluate the number of professionals enrolled on the courses. Such metrics would inform the government of the current demand of the courses in the country. The public and private sector participants in the focus-group discussions emphasised the need for MoET to collaborate with the sectors in identifying the skill set needed in the country and providing cybersecurity professional training.

D 3.4 CYBERSECURITY RESEARCH AND INNOVATION

This Factor addresses the emphasis placed on cybersecurity research and innovation to address technological, societal and business challenges and to advance the building of cybersecurity knowledge and capabilities in the country.

Stage: [Start-up]

Cybersecurity Research and Development (Start-up)

There is currently no cybersecurity research and development in the country. The focus-group discussion participants noted that MoET is not engaging with higher education institutions in the country to promote cybersecurity research and development. This is evident because of the few research outputs in the country. Recently, the Ministry of Communications, Science and Technology (MICSTI), in collaboration with the Organisation of Africa, Caribbean and Pacific States (OACPS), launched the Research and Innovation Policy.[130,131] The implementation of the policy recommendations is expected to commence in 2022. The policy's medium-term recommendation stipulates a need for prioritising scientific research and development in the country:

> *The government will intensify investment in scientific research and development (R&D) and strengthen local innovation and technological capabilities. Proposed programmes should embed the need to develop and strengthen sustainable*

[130] Government of Lesotho. (n.d.). *Science Launches Research and Innovation Policy.* https://www.gov.ls/science-launches-research-and-innovation-policy/

[131] Mokhethi, M. (2021). *Research Fuels Innovation.* Ministry of Communications, Science and Technology. https://www.communications.gov.ls/single_news.php?news=123456797

financing mechanisms, and improve effective collaboration between government, academia, industry and society.[132]

The policy, however, has not specified cybersecurity research and development but a general need for R&D in the country.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *Building Cybersecurity Knowledge and Capabilities*, the following set of recommendations are provided to Lesotho. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

BUILDING CYBERSECURITY AWARENESS

R3.1 Until the National Cybersecurity Advisory Council (NCAC) is established by the Computer Crime and Cybersecurity legislation and becomes operational, the Ministry of Communications, Science and Technology (MICSTI) should take responsibility for the design, implementation and coordination of national cybersecurity awareness-raising programmes. These programs must cater for different target groups.

R3.2 MICSTI should ensure that cybersecurity awareness is comprehensively included in any National Cybersecurity Strategy or other relevant policy documents.

R3.3 MICSTI should involve key stakeholders from the private sector, civil society and international partners when developing and implementing cybersecurity awareness-raising programmes.

R3.4 MICSTI should develop national portals as a single point of contact for the dissemination of cybersecurity awareness content for specific targeted groups.

[132] Thamae, Z.L., Sekota, M., Darboe, M.M.Y., & Galvin, D. (2022). *OACPS R&I PSF Research and Innovation Policy Recommendation Report for Lesotho.* https://www.researchgate.net/publication/357958422_OACPS_R_I_PSF_Research_and_Innovation_Policy_Recommendation_Report_for_Lesotho

R3.5 MICSTI in collaboration with Lesotho Communications Authority (LCA) and other relevant stakeholders, should develop and implement cybersecurity awareness-raising programmes for executives in both the private and public sectors.

CYBERSECURITY EDUCATION

R3.6 MICSTI, in collaboration with MoET and relevant stakeholders, should develop metrics to determine cybersecurity requirements in Lesotho. This will assist in informing the supply and demand in the country.

R3.7 The government, through MoET, should incorporate cybersecurity into primary and secondary school computer application curriculums.

R3.8 MICSTI, in consultation with MoET, should ensure that cybersecurity education is comprehensively included in any future National Cybersecurity Strategy or relevant policy documents.

R3.9 Higher education institutions in Lesotho should hold cybersecurity seminars and lectures for non-specialists.

R3.10 MoET, in collaboration with the Council of Higher Education and the educational institutions, should develop cybersecurity-specific degree programmes. The development of the programmes should be informed by international standards and best practices.

R3.11 Institutions, in consultation with industry, should review the Law, Business, Health, Education and Computer Science-related degrees and masters programmes in the country to integrate the cybersecurity component. This will assist in speeding up the process as they are waiting for the development of cybersecurity-specific programmes.

R3.12 The Council on Higher Education, should develop Cybersecurity Qualification Framework. The development of the framework will assist in the development and the evaluation of cybersecurity programmes in recommendation 3.10.

R3.13 National Manpower Development Secretariat (NMDS) should provide scholarships for cybersecurity qualifications. This could be achieved by amending the priority list of courses to include cybersecurity programmes.

R3.14 Ministry of Public Service, Labour and Employment, should develop incentives to attract and retain cybersecurity experts in Lesotho.

R3.15 MoET should ensure the involvement of professionals in cybersecurity content development for primary and secondary schools.

CYBERSECURITY PROFESSIONAL TRAINING

R3.16 The government should appoint a dedicated government body, MICSTI (and once established the NCAC), to take responsibility for cybersecurity professional training in Lesotho. MICSTI should ensure that cybersecurity professional training is comprehensively included into any National Cybersecurity Strategy or other relevant policy documents.

R3.17 National Manpower Development Secretariat (NMDS) should amend its scholarship policy to encourage continuing professional development for professionals in the public sector to enrol on cybersecurity professional training programmes offered locally or internationally.

R3.18 MoET should develop metrics to track the supply and demand for professional cybersecurity programmes. This data will assist in informing MoET and the training institutions on whether the training meets the country's needs.

CYBERSECURITY RESEARCH AND INNOVATION

R3.19 MICSTI should take responsibility for cybersecurity research and innovation in Lesotho and ensure that cybersecurity research and innovation is comprehensively included into any future National Cybersecurity Strategy or other relevant policy documents.

R3.20 MICSTI, in collaboration with relevant stakeholders, should develop a cybersecurity research and development strategy. The strategy should contain incentives to promote cybersecurity research and innovation.

R3.21 MICSTI, in collaboration with relevant stakeholders, should develop a cybersecurity research and innovation metrics to determine the requirements needed to develop the cybersecurity research and development strategy in recommendation 3.20.

R3.22 MICSTI should set aside a budget for cybersecurity research and development.

DIMENSION 4

LEGAL AND REGULATORY FRAMEWORKS

This Dimension examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis on 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, this Dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

Figure 10: Factors and aspects of the Dimension 4 of the CMM

Overview of results

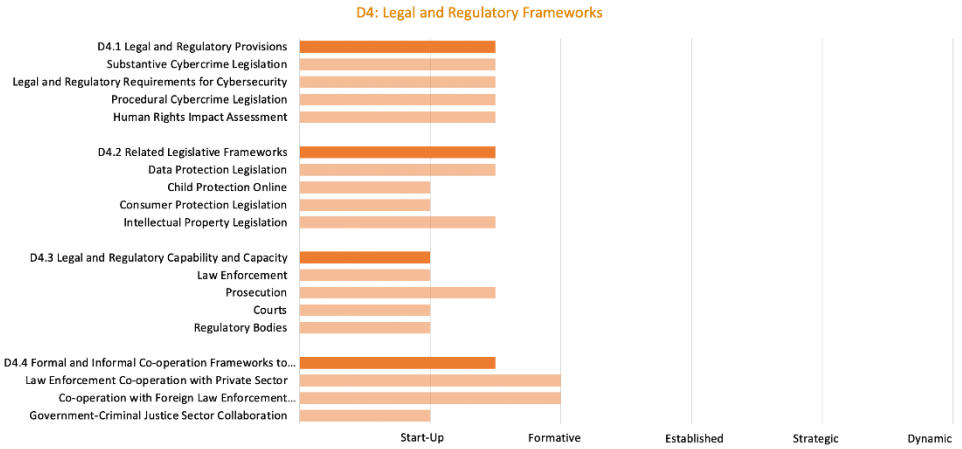

Figure 11: Results of the assessment of the Legal and Regulatory Frameworks of the Kingdom of Lesotho

D 4.1 LEGAL AND REGULATORY PROVISIONS

This Factor addresses various legislation and regulatory provisions relating to cybersecurity, including legal and regulatory requirements, substantive and procedural cybercrime legislation, and human rights impact assessment.

Stage: [Start-up to Formative]

Substantive Legal Provisions on Cybercrime (Start-up to Formative)

Lesotho began addressing criminal activities carried out through computers or the internet, commonly referred to as cybercrimes, in 2012 with the promulgation of the Penal Code Act of 2012.[133] While there is no data on cybercrimes in the country, there are reports of cybercrimes in digital financial services. The media has reported about several incidents of mobile money fraud, e-commerce fraud and forex trading scams.[134,135] Computer-enabled harms such as the

[133] *Penal Code Act 2010* (Lesotho). Act No. 6 of 2012., s 62(2). http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/91506/106148/F-1732401516/LSO91506.pdf

[134] Central Bank of Lesotho. (2019, December 12). *Mobile Money Public Awareness by the Central Bank of Lesotho and Mobile Money Issuers (Vodacom Lesotho, Econet Telecom Lesotho and Lesotho Post Bank)*. [Press Release]. https://www.centralbank.org.ls/images/Public_Awareness/Press_Release/Mobile_Money_12_pg_Press_Release_12_Dec_2019_ENG.pdf

[135] Mahao, S. (2022, June 17). Online shoppers warned against surging cybercrime. *Newsday*. https://www.newsdayonline.co.ls/online-shoppers-warned-against-surging-cybercrime/

sharing of malicious information[136], cyberbullying[137] and the non-consensual publication of intimate images[138] have also been reported in the media. However, existing legislation has been found inadequate to address these crimes. Having noted the deficiencies in the legal framework, 2019 CMM review recommended for Lesotho to review and pass the cybercrime draft law that existed at the time and develop and adopt a comprehensive legislative framework for IC, which covers. However, no law has been passed since the 2019 review.

The current legal provisions on cybercrime are contained in the Communications Act of 2012 and the Penal Code Act of 2012. The Communications Act of 2012 defines two cybercrimes. Section 44 (a) prohibits the use of the telephone service to abuse, threaten or make obscene calls, (e) criminalises the act of modifying or interfering with the content of a message by means of a communications service.[139] Section 44 (f) prohibits the interception of communications on public networks unless authorised by a court of competent jurisdiction.[140] Section 62 (b) of the Penal Code Act of 2012 makes it a crime for a person to access a computer or storage device to extract data without authorisation or to interfere with data on the computer or storage "*with the intention of securing an advantage for himself or herself or causing damage to the electronic data or programmes.*"[141]

The Communications Act of 2012 and the Penal Code Act of 2012 regulate cyber offences. Still, they are limited in scope and do not encompass the range of offences in modern cyberspace. The pending Computer Crime and Cyber Security Bill of 2022 contains detailed provisions on a broad set of cybercrimes, including a full range of relevant data breach activities and espionage. Such as denial of service/distributed denial of service attacks, malware deployment, distribution of illegal digital material and general crime utilising computer systems. The law provides a broad and solid legal basis for prosecuting offences perpetrated in cyberspace and employing ICT.

Focus-group discussion participants indicated that, on May 17th, 2022, the Lesotho National assembly approved new extensive legal provisions on cybercrime and cybersecurity through the Computer Crime and Cyber Security Bill. The bill amends and vastly expands regulatory provisions on cybercrimes enacted through the Communications Act of 2012 and the Penal Code Act of 2012. Sections 21 to 56 defines acts and behaviours that constitute offences, which include illegal access to a computer, distribution of child pornography, interception of electronic messages or money transfers, cyber extortion, computer fraud and forgery and the

---

[136] Moremoholo, R. (2019, December 17). The scourge of cybercrime. *The Post Newspaper.* https://www.thepost.co.ls/news/the-scourge-of-cybercrime/

[137] Motsopa, M. (2020, November 3). The trauma of cyber-bullying. *The Post Newspaper.* https://www.thepost.co.ls/news/the-trauma-of-cyber-bullying/

[138] Shale, T.R. (2018 June 8). Show us the money! *MNN Centre for Investigative Journalism*. https://lescij.org/2018/06/08/show-us-the-money/

[139] *Communications Act of 2012*. (Lesotho). Act 4 of 2012. s 44 (a) & (e) https://sherloc.unodc.org/cld/uploads/res/document/lso/2003/communications-act_html/communications_act_2012.pdf

[140] *Communications Act of 2012*. (Lesotho). Act 4 of 2012. s 44 (f). https://sherloc.unodc.org/cld/uploads/res/document/lso/2003/communications-act_html/communications_act_2012.pdf

[141] *Penal Code of 2012* (Lesotho). Act 6 of 2012. *S 62(2).* https://lesotholii.org/ls/legislation/num-act/6

distribution of data message of intimate image without consent. The bill also establishes a legal basis for punishing perpetrators of a broad range of cybercrimes with fines and prison sentences. The bill has not been enacted in lieu of further steps in the legislative process. The enactment of the bill is a crucial determinant of whether the maturity of the legal and regulatory provisions in Lesotho should be considered at the start-up or formative stage. Because the bill has not entered into effect, the substantive legal provisions on cybercrime in Lesotho should be considered between Start-up and Formative.

Effective June 24th, 2022, every network subscriber must register their Subscriber Identity Module (SIM) cards with their network service provider.[142,143] The mandate to register is stipulated in sections 7 and 8 of the *Communications (Subscriber Identity Module Registration) Regulations of 2021* (SIMR)[144], passed by the Minister responsible for communications in terms of section 55 of the Communications Act of 2012. The provisions in these regulations are meant to eliminate the anonymity enjoyed by unregistered prepaid subscribers, an make it easier for law enforcement to investigate crimes committed using mobile devices.[145] Registration could also provide better conditions for combatting cybercrime.[146]

For cross-border cybercrimes, Lesotho does not have instruments such as treaties or mutual legal assistance agreements to facilitate criminal investigations and prosecution as it has not yet completed the promulgated the Computer Crime and Cyber Security Bill of 2022, which has provisions for international corporation on cybercrime. Lesotho started but did not complete the process of adopting international instruments combatting cybercrime. The Computer Crime and Cyber Security Bill of 2022 is derived from harmonised model law developed through the HIPSSA (Harmonization of ICT Policies in Sub-Sahara Africa), a legal and policy framework that sets out fundamental principles for legislation on cybercrime.[147] In addition, the content of the pending cybercrime legislation complies with the African Union's (AU) *African Convention on Cyber Security and Personal Data Protection* and the *Budapest Convention on Cybercrime* (ETS 185).[148] The focus-group discussion participants indicated that

---

[142] Latela, M. (June, 2022). *Sim card registration starts*. https://www.thereporter.co.ls/2022/06/27/sim-card-registration-starts/?amp=

[143] African Wireless Communications. (2022). *Lesotho: telecom operators to begin SIM card registration.* https://www.africanwirelesscomms.com/news-details?itemid=4853#

[144] The Communications (Subscriber Identity Module Registration) Regulations, 2021. s. 7 & 8 https://lca.org.ls/wp-content/uploads/filr/3229/SIM%20CARD%20REGISTRATION%20REGULATIONS%202021%20(2).pdf

[145] Mpaki, B. (2022, May 17). Unregistered Subscribers to Be Cut Off. *Lesotho Times*. https://lestimes.com/unregistered-subscribers-to-be-cut-off/

[146] Macdonald, A. (2022, July). *Lesotho, Namibia join trend of SIM card registration with biometrics*. https://www.biometricupdate.com/202207/lesotho-namibia-join-trend-of-sim-card-registration-with-biometrics

[147] ITU. (2013). Data Protection: Southern African Development Community (SADC) Model Law (Establishment of Harmonized Policies for the ICT Market in the ACP Countries). International Telecommunications Union. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwio2Lyl2e_9AhUEiFwKHdyJBDcQFnoECAwQAQ&url=https%3A%2F%2Fwww.itu.int%2Fen%2FITU-D%2FProjects%2FITU-EC-ACP%2FHIPSSA%2FDocuments%2FFINAL%2520DOCUMENTS%2FFINAL%2520DOCS%2520ENGLISH%2Fsadc_model_law_data_protection.pdf

[148] Computer Crime and Cybersecurity Bill 2022 (Lesotho).

there are intentions by Lesotho authorities to adopt the AU African Convention on Cyber Security and Personal Data Protection and the Budapest Convention at a later date. This signifies Lesotho's intent on harmonizing its laws on cybercrime with international legal instruments. Therefore, it could contribute to the ongoing efforts to tackle global cybercrime.

Legal and Regulatory Requirements for Cybersecurity (Start-up to Formative)

Lesotho has limited cybersecurity requirements set out in regulation or law. The focus-group discussion participants indicated that they were not aware of the existence of regulatory requirements for cybersecurity, such as minimum-security standards, breach notification requirements or vulnerability disclosure. Requirements such as these are contained in the Computer Crime and Cybersecurity Bill of 2022. While awaiting the promulgation of the bill, a few regulatory provisions are contained in the Data Protection Act of 2011, the Communications Act of 2012, the Lesotho Communications Authority (Administrative Rules) 2016 and the SIMR rules.

The Data Protection Act of 2011 has some regulatory provisions for cybersecurity. Section 20 requires data controllers to *"...secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical measures..."* to prevent damage, loss, or unlawful access to personal information under their control.[149] Section 23 requires data controllers to notify both the Data Protection Commission and the affected data subject in case of a security compromise.[150] However, Lesotho has not yet established the Data Protection Commission envisaged by the law. As a result, this assessment could not establish the extent of compliance of data controllers. The study could not establish the extent to which existing regulatory bodies enforce security requirements contained in the Data Protection Act.

There are no civil and criminal liabilities for the failure to comply with this requirement. The Communications Act of 2012 also gives some remit to the LCA over the security of telecommunications infrastructure. Section 44 (g) makes it an offence to damage communication faculties belonging to another person. Furthermore, section 5 (a) of the SIMR indicates that *"...all reasonable precautions in accordance with interna-tional best practice to preserve the integrity and prevent any corruption, loss or unauthorised disclosure of sub-scriber information obtained pursuant to these Regula-tions..."*[151]

The relevant legal and regulatory frameworks are under development. The pending Computer Crime and Cyber Security Bill of 2022 sets out foundational cybersecurity requirements for the government and regulatory authorities of Lesotho. The requirements can be found in part two, sections 3 through 17 the bill, which also includes establishing a National Cyber Security Incident Response Team (CSIRT) and a National Cybersecurity Advisory Council (NCAC) to coordinate cybersecurity matters. In part 3, sections 18 through 20, the bill provides for the

[149] *Data Protection Act 2011* (Lesotho) Act 5 of 2012. https://new.lesotholii.org/akn/ls/act/2012/5/eng@2012-02-22

[150] *Data Protection Act 2011* (Lesotho) Act 5 of 2012 https://new.lesotholii.org/akn/ls/act/2012/5/eng@2012-02-22

[151] *The Communications (Subscriber Identity Module Registration) Regulations*, 2021 (Lesotho) Legal notice 141 s.5. https://lca.org.ls/wp-content/uploads/filr/3229/SIM%20CARD%20REGISTRATION%20REGULATIONS%202021%20(2).pdf

identification and protection of critical of critical information infrastructure, including the obligations of critical infrastructure owners. Obligations include the use of recognised good cybersecurity practices, incident report and cybersecurity audits. However, the bill can potentially be in violation of human rights.[152]

Lesotho does not regularly update its regulation to keep up with emerging technologies. As indicated, Lesotho does not have substantive law on cybercrime. During focus-group discussions, participants indicated that incidents as cyberbullying or and digital scams were reported to the police, but cases were not prosecuted due there are not covered by the existing law and the principle of "no crime without law" applies.

Lesotho does not currently have regulatory requirements for general cybersecurity measures. Elements of e-commerce and how technologies underpinning them can be operated are regulated through the Electronic Transactions and Commerce Act of 2021.[153] The legislation should in principle contribute to providing Lesotho citizens with a well-functioning digital economy. However, it is very limited in scope regarding non-technical aspects of digital economic activity. The Lesotho regulatory provisions for more advanced emerging digital technologies like quantum computing, neural networks, and artificial intelligence (AI) can be considered lacking.

Procedural Cybercrime Legislation (Start-up to Formative)

Specific procedural criminal law for cybercrime does not exist but is under development. The Computer Crime and Cyber Security Bill of 2022 regulates how Lesotho authorities and law enforcement can access the digital information belonging to citizens. Focus-group discussion participants commented that Lesotho law enforcement can experience uncertainty on how to apply the law on crimes committed in cyberspace and that this is linked to the country's cybersecurity culture. The procedures related to gathering digital evidence are formulated. However, the letter of the law is unclear on investigative procedures for cybercrimes related to sabotage activity like obfuscated attacks deploying malware and DDoS-attacks.

Human Rights Impact Assessment (Start-up to Formative)

No human rights impact assessments were carried out during the development of Lesotho's procedural cybercrime legislation and cybersecurity regulations. The Computer Crime and Cyber Security Bill of 2022 and the SIMR have received criticism from media and analysts for being too intrusive into the privacy and freedom of expression of Lesotho citizens and violating

[152] Moyo, H. (2022, May 19th). Cyber law not well thought-out, potentially violates human rights: Analysts. *Lesotho Times*. https://lestimes.com/lesothos-cyber-law-not-well-thought-out-potentially-violates-human-rights-analysts/

[153] Electronic Transactions and Commerce Bill 2021 (Lesotho).

provisions of the country's constitution and international agreements. The criticism targets both the content of the laws and the legislative process in drafting and passing them.[154,155]

The provisions of the SIMR regulations can be considered partly in violation of the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples' Rights (ACHPR). This is due to its infringement on privacy, freedom of expression and surveillance without proper legal procedure. A key reason for this is the vague standard for data collection established in the Law, leading to it not adhering to the legality standard.[156]

D 4.2 RELATED LEGISLATIVE FRAMEWORKS

This Factor addresses the legislative frameworks related to cybersecurity including data protection, child protection, consumer protection, and intellectual property.

Stage: [Start-up to Formative]

Data Protection (Start-up to Formative)

Lesotho has some related legislative frameworks that work in synergy with its legal provisions on cybersecurity and cybercrime. The Data Protection Act of 2011 provides extensive legal provisions for data protection. The financial and telecommunications sectors also have specific legal provisions contributing to cybersecurity. The Communications Act of 2012 designates regulatory responsibility to LCA for an extensive range of telecommunications issues, including cyber-related offences. The Data Protection Act of 2011, the pending Computer Crime and Cybersecurity legislation of 2022, the Communications Act of 2012, the Financial Consumer Protection Act of 2022 and the Electronic Transactions and Commerce Act of 2021 contain the provisions directly regulating data protection, child protection, consumer protection, and intellectual property in Lesotho.

The Data Protection Act of 2011 provides comprehensive legal provisions for the protection of access to data and privacy for Lesotho citizens and organisations. This includes the requirements and conditions necessary for processing personal information and valid exemptions. The legislation also sets out the functions and mandate of the Lesotho Data Protection Commission. The core tasks of the Commission are to promote knowledge about

[154] ICNL. (2022, May 30th). Lesotho's Communications Regulations (Legal Analysis). https://archive.org/details/icnl-legal-analysis-lesotho-computer-crimes-act;

[155] Moyo, H. (2022, May 19th). Cyber law not well thought-out, potentially violates human rights: Analysts. *Lesotho Times*, https://lestimes.com/lesothos-cyber-law-not-well-thought-out-potentially-violates-human-rights-analysts/

[156]Moyo, H. (2022, November 18). Lesotho's amendments to mobile phone regulations welcome but not enough. *Lesotho Times*. https://lestimes.com/lesothos-amendments-to-mobile-phone-regulations-welcome-but-not-enough/

information protection principles through education and awareness-raising, monitoring and enforcement of compliance with the Act's provisions, and various types of cooperation with relevant stakeholders to ensure good data protection in Lesotho.[157]

While the Data Protection Act of 2011 has been in existence for over 10 years, Lesotho has not yet established the Data Protection Commission. As a result, there is no oversight for compliance. During the focus-group discussions, participant gave examples potential violations of the Data Protection Act in different sectors, particularly during the height of the COVID-19 pandemic where individuals were required to register their names, mobile number and address at every establishment that they visited. According to participants, the malpractice around personal data protection was pervasive in Lesotho.

The Financial Consumer Protection Act of 2022 also provides regulatory provisions that protect financial data belonging to Lesotho citizens. Section 44 in the Act regulates Privacy Policy and in subsection 2 stipulates that; "A policy referred to in subsection (1) shall ensure confidentiality, security and integrity of a data stored in a database of a financial service provider...".[158] This is important in supporting the legal provision that contributes to enhanced cybersecurity in financial matters for Lesotho institutions and citizens.

The Communications Act of 2012 contains provisions that regulate telecommunications and the confidentiality, integrity and accessibility of data for users. Furthermore, section 41(1) of the Lesotho Communications Authority (Administrative) Rules of 2016[159] and Sections 5 and 6 of the SIMR set out requirements for network service providers to ensure the protection of personal data of registrants; it also set out conditions for the sharing of such data is third parties.[160] A focus-group discussion participant commented that these regulations were necessary for the privacy of Lesotho citizens since it ensures that mobile network operators apply appropriate measures to protect customers' information.

In the pending Computer Crime and Cybersecurity legislation, data protection is regulated comprehensively and in detail. In part IV, sections 21 through 24 and 33 describe offences related to data stored on individuals' devices. Data protection from surveillance and collection is regulated in part VI, section 59 through 66 and part VI, section 67 through 74. The ability of law enforcement to access data is according to a court order, as is the norm in most countries of the world.

---

[157] *Data Protection Act 2011* (Lesotho), Act 5 of 2012, https://new.lesotholii.org/akn/ls/act/2012/5/eng@2012-02-22

[158] *Financial Consumer Protection Act* 2022 (Lesotho) Act 7 of 2022. https://www.centralbank.org.ls/images/Legislation/Supervision/Acts/Financial_Sector_All/Financial_Consumer_Protection_Act_7_of_2022.pdf

[159] *Lesotho Communications Authority (Administrative Rules) 2016* (Lesotho) Legal Notice 77 of 2016. https://lca.org.ls/wp-content/uploads/filr/2274/LCA%20Administrative%20Rules%202016.pdf

[160] *Communications (Subscriber Identity Module) Regulations 2021* (Lesotho) Legal Notice 77, https://lca.org.ls/wp-content/uploads/filr/3229/SIM%20CARD%20REGISTRATION%20REGULATIONS%202021%20(2).pdf

Child Protection Online (Start-up)

Lesotho regulates the general protection of children through the Children's Protection and Welfare Act of 2011. The legislation provides extensive legal provisions for children's rights in society but not specifically in cyberspace. With regards to on the legislative protection of children online, including the protection of their rights online and the criminalisation of child abuse online, Lesotho has limited provisions. The focus-group participants asserted that such issues could be solved at the policy level and that the ITU Guidelines on Child Online Protection could be a well-suited point of departure.

The country has other pieces of legislation have provision for the protection of children online, but they are limited in application. For example, the abuse of The Counter Domestic Violence Act of 2022 criminalises technological abuse, which it defines as "…an abusive act where a person by means of technology device, supplies, sends, shares, exposes or displays violence, nude or semi-nude material, photos or videos and sexually suggestive messages to another person", among other things to protect children from domestic abuse.[161] Furthermore, Part IV, section 32 of the Computer Crime and Cybersecurity Bill of 2022 defines what material is considered unlawful depictions of children and sets out the unlawful acts associated with such material. In addition, the section defines the facilitating of children accessing unlawful material as a crime. The punishment for such crimes is also stipulated up to twenty years imprisonment.

The application of child protection online needs to be better understood and reflected in the relevant legislation. Lesotho does not have legislation to protect children online, such as provisions to manage the risk of children accessing harmful and age-inappropriate content or to provide parents and children with clear and accessible ways to report problems online when they do arise.

Consumer Protection (Start-up)

Legislation related to consumer protection is limited and its application in the online environment was drafted in 2013, but never promulgated. The Consumer Protection Bill of 2022 was passed and approved by parliament[162]. However, it has no provisions for the online environment. As a result, Lesotho does not have a comprehensive legal and regulatory framework necessary to enable online transactions; there are no regulation covering critical areas such as e-transactions, cybercrime, consumer protection and competition law.[163] Focus-group discussion participants commented that Lesotho is missing proper regulatory provisions on Consumer protection in general, and especially for digital products and services.

---

[161] *Counter Domestic Violence Act, 2022* (Lesotho) Act 14 of 2022, s. 3(k). https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwil4IzBiPD9AhUCRsAKHRDMDTIQFnoECAoQAQ&url=https%3A%2F%2Fwww.webbernew.com%2Fuploads%2FGG%2520No.%252072%2520of%25202022.pdf&usg=AOvVaw06zXXobm9dbYy0HYk-SPVV

[162] Senoko, N. (2022, May). *Consumer law in the pipeline.* Metro. [Business]. https://www.maserumetro.com/news/business/consumer-law-in-the-pipeline/

[163] United Nations Conference on Trade and Development. (2019). Lesotho Rapid eTrade Readiness Assessment. https://unctad.org/system/files/official-document/dtlstict2019d8_en.pdf

The Financial Consumer Protection Act of 2022 provides regulatory provisions that protect the rights of consumers of financial products and services.[164] While digital commerce in Lesotho is generally low, digital financial services are growing, spurred by digital wallet services. Therefore, the Act could become more important as digital financial activity grows further. The purpose of the Electronic Transactions and Commerce Act of 2021 stipulates that it shall contribute to a; "...safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions.".[165] However, the sections of the legislation do not provide meaningful regulation related to consumer protection in the digital economy. Therefore, this is a regulatory area where Lesotho can improve.

Intellectual Property (Start-up to Formative)

Legislation related to intellectual property protection is limited and its application in the online environment is yet to be considered. Intellectual property protection is regulated by the Industrial Property Order of 1989[166] and the Copyright Act of 1989[167], which conform to the standards set out in the Paris Convention and Berne Convention. They protect patents, industrial designs, trademarks, and grant of copyright. Digital Intellectual property rights are also enshrined in the Computer Crime and Cyber Security Bill of 2022. Part IV, section 41 stipulates that any person that wilfully utilizes digital technology to violate such rights for commercial purposes is committing an unlawful act and is liable for fines and/or prison sentences.[168]

D 4.3 LEGAL AND REGULATORY CAPABILITY AND CAPACITY

This Factor studies the capacity of law enforcement to investigate cybercrime, the prosecution's capacity to present cybercrime and electronic evidence cases, and the court's capacity to preside over cybercrime cases and those involving electronic evidence. Finally, this Factor reviews the existence of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations.

Stage: [start-up]

---

[164] *Financial Consumer Protection Act of 2022* (Lesotho) Act No. 7 of 2022. https://www.centralbank.org.ls/images/Legislation/Supervision/Acts/Financial_Sector_All/Financial_Consumer_Protection_Act_7_of_2022.pdf

[165] Electronic Transactions and Commerce Bill 2021. (Lesotho).

[166] *Industrial Property Order 198* (Lesotho) Ordinance 5 of 1989. https://new.lesotholii.org/akn/ls/act/ord/1989/5/eng@1989-12-31

[167] *Copyright Order 1989* (Lesotho). Order no. 13 of 1989. https://lesotholii.org/ls/legislation/act/13/copy%20right%20order%201989.pdf

[168] Computer Crime and Cyber Security Bill 2022 (Lesotho). s.41

Law Enforcement (Start-up)

According to the participants of the focus-group discussions, the institutional capacity of law enforcement in cybercrime is limited. However, in anticipation of the promulgation of Computer Crime and Cybersecurity legislation of 2022, in June 2022, the Lesotho Mounted Police established a cybersecurity unit to focus on combating cybercrime.[169] Members of the unit received are reported to have received expert training.[170] The focus-group discussion participants highlighted that while police tend to receive cybersecurity training, prosecutors and judges do not receive the relevant training to enable them to prosecute and try cybercrime cases. As such, there is human, procedural and technological misalignment in investigating cybercrime cases.

In 2015, law enforcement experts from nine southern African countries, including Lesotho took part in a workshop for law enforcement. The purpose of this workshop was to provide law enforcement in these countries with the tools that can be used "to build better, stronger, and more effective law enforcement in those countries and across southern Africa".[171]

> *"In this workshop, you will learn about techniques for using cyber tools and methods to investigate crime and to collect and analyse digital evidence associated with criminal networks. In particular, you will be presented information on online investigations, forensic analysis, and methods for seizing and searching computers and cell phones involved in criminal activity. Additionally, you will have an opportunity to explore legal and procedural issues related to using electronic evidence in criminal proceedings."*

However, participants in the focus-group discussions stated that while some law enforcement officers may received training, cyber-related crimes are still not fully understood. This is a problem for the Lesotho police because Investigating cybercrime requires specialised skills and technology that are not universally available such as malware profiling, darknet tracing and cryptocurrency analysis.[172] Participants from Lesotho Mounted Police confirmed that the police have not been addressing cybercrime, even those provided for in the penal code, due to lack of capacity. In addition to limited skills, the police lack relevant technological infrastructure to handle cybercrime cases.[173]

In addition, according to the focus-group participants, crimes are generally categorised by the police. A respondent from the Department of Correctional services indicated that the produce

---

[169] Liphoto, N. (2022, August 16). New police unit to fight cybercrime. *The Post Newspaper.* https://www.thepost.co.ls/news/new-police-unit-to-fight-cybercrimes/

[170] Ibid.

[171] U.S. Embassy in Namibia. (2015). *U.S. Ambassador Thomas F. Daughton Remarks for the Opening of the Southern Africa Regional Cyber Investigations & Electronic Evidence Workshop*. https://na.usembassy.gov/u-s-ambassador-thomas-f-daughton-remarks-opening-southern-africa-regional-cyber-investigations-electronic-evidence-workshop/

[172] World Economic Forum. (2021). *Global police must partner up to prevent a ransomware crisis - here's how*. https://www.weforum.org/agenda/2021/11/police-agencies-must-partner-up-to-prevent-a-ransomware-crisis-heres-how/

[173] Moremoholo, R. Lesotho - The scourge of cybercrime. *The Post Newspaper.* https://menafn.com/1099439154/Lesotho-The-scourge-of-cybercrime

daily reports, weekly and monthly reports; they also have quarterly, and annual reports on different crimes committed by inmates. Inmates are categorised according to the offences they have committed, and other manner of categorisation. However, a different respondent in the discussions added that there are no specific categories for cybercrimes cases, or cybercrimes civil lawsuits and that crimes of that nature are often categorised under other cases.

Prosecution (Start-up to formative)

Prosecutors do not receive training to prosecute cybercrimes and no consultation has started to address this. According to focus-group discussion participants, prosecutors fall behind in the training of how to deal with cybercrimes. Participants also expressed that there is a shortage of skills when prosecuting cybercrimes. However, Lesotho lacks the capacity to successfully prosecute cases; as such cybercrimes would not be an exception from this problem. Media reports had indicated that the Chief Justice and other judges had determined that justice was not being served due to "inefficient and unprofessional" police and public prosecutors.[174, 175]

A participant from the prosecutor's office detailed how evidence from cybercrimes is captured and used in cases. To avoid alterations of the evidence, digital forensics techniques are used such as capturing images of devices used in cyber-related crimes and hashing these images to avoid tempering of evidence. The conclusion from that discussion was that the procedure used did not comply with recognised best practices or standards such as the ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence[176] or standards developed by the Scientific Working Group on Digital Evidence, a grouping of organisations involved in the field of digital and multimedia evidence.[177] The assessment could not find a record of cases prosecuted under section 62(2) of the Penal Code of 2012, which criminalises unauthorised access to a computer without authorisation, and/or the extraction of data without authorisation.

---

[174] Tsiane, M. (2022, April). Sakoane chides police and prosecution failures in achieving justice. *Lesotho Times*.

[175] Tsiane, M. (2022, April). *Nthane Walks Free*. https://sundayexpress.co.ls/nthane-walks-free/

[176] ISO/IEC 27037:2012. https://www.iso.org/standard/44381.html?browse=tc

And:

- ISO/IEC 27037 Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence
- ISO/IEC 27041 Guidelines on Assuring Suitability and Adequacy of Incident Investigative Method
- ISO/IEC 27042 Guidelines for the Analysis and Interpretation of Digital Evidence
- ISO/IEC 27043 Incident Investigation Principles and Processes

[177] Scientific Working Group on Digital Evidence (SWGDE). (2023). *Published.* https://www.swgde.org/documents/published-complete-listing

Courts (Start-up)

There is little to no training of judges or magistrates. According to focus-group discussion participants, because of poor understanding of cybercrimes, the courts sometimes fail to prosecute cybercrimes appropriately.

Regulatory Bodies (Start-up)

There is no cross-sector body for cybersecurity regulation. There is no information relating to sector-specific regulators, e.g., financial sector regulator, energy and water regulator, regulators for professions like institute for auditors, regulators in the education sector (CHE, Examinations Council), Government itself (e.g., the Auditor General's office).

According to the focus-group discussion participants, there has not been any discussions between the regulators on the issues of cybersecurity. There are some other areas where regulators in Lesotho collaborate (for example, the communications sector and the financial sector regulators) through a memorandum of understanding (MOU). In this instance, the LCA and the Central Bank of Lesotho have agreed to share information.

D 4.4 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This Factor addresses the existence and function of formal and informal mechanisms that enable co-operation between domestic actors and across borders to deter and combat cybercrime.

Stage: [start-up to formative]

Law Enforcement Co-operation with Private Sector (Formative)

There is limited information on the level of cooperation between the public and private sectors to combat cybercrime in Lesotho. However, the Communications Act of 2012[178] allows for data sharing provided there is an order from a competent court. Media reports indicate that law enforcement agencies obtained call record data from Vodacom Lesotho in a case relating to the murder of the wife of a former prime minister, but it is not clear whether due process was followed.[179] In addition, in the gazetted Computer Crime and Cybersecurity Bill

[178] *Communications Act 2012,* (Lesotho). Act 4 of 2012. S. 44 (f). https://new.lesotholii.org/akn/ls/act/2012/4/eng@2012-02-17

[179] DigiWatch. (2020, February). *Murder mystery haunts Vodacom Lesotho.* https://dig.watch/updates/murder-mystery-haunts-vodacom-lesotho

of 2022, there is provision for establishing a cybersecurity council which will enable the cooperation of law enforcement and the private sector.[180]

Although Lesotho is a member of Southern African Regional Police Chiefs Co-operation Organisation (SARPCCO), Asset Recovery Inter-Agency Network Southern Africa (ARINSA), and INTERPOL, it is not clear from the literature if the government is actively promoting public/private partnership and/or the development of international public/private partnership platforms. This is unlikely given the government's history of limited transparency and accountability mechanism.

Evidence needed by the police to investigate crimes involving digital evidence often lies with industry players such as network service providers, content hosting provider and financial services providers. Nevertheless, according to the focus-group discussions, there are no formal or standard cooperation mechanisms such as a memorandum of understanding (MOU)s or cooperation agreements between law enforcement agencies and industry players regarding cybercrime. The focus-group discussions also indicated that cooperation existed in the form of information sharing between entities or institutions. This information sharing may relate to different types of crime, excluding cybercrime, because it is a new phenomenon for many Lesotho organisations. Information sharing is guided by MOUs whenever possible.

When organisations (for example, network service providers) report cybercrimes and digital records involving customer data have to be collected, a court order is required before a referral code is given. At this point, the evidence that may be needed to prosecute someone can be collected from the network providers.

Co-operation with Foreign Law Enforcement Counterparts (Formative)

The Lesotho Mounted Police Service is a member of INTERPOL[181] and the SADC INTERPOL bureau. The INTERPOL National Central Bureau (NCB) in Maseru is Lesotho's lead agency for national investigations requiring cooperation with police forces in other countries. Located at the Police Headquarters in the Maseru district, the NCB is part of the Lesotho Mounted Police Service.[182] The 2019 CMM review established that INTERPOL Maseru works with national central bureaus "globally in tackling the transnational crime groups which affect Lesotho's national security. They share intelligence, monitor emerging trends and work together in targeted regional police operations. NCB Maseru comprises 22 crime desks which specialize in crime areas ranging from cybercrime to fugitive investigations and terrorism, with a larger desk for tackling regional organized crime linked to trafficking in human beings."[183] However, the lack of cybercrime laws in Lesotho means that some cooperation is impossible or not fruitful.

Lesotho is a member of several regional and international such as the Southern African Regional Police Chiefs Co-operation Organisation (SARPCCO), a cooperation and information-

[180] Computer Crime and Cybercrime Bill 2022, s.3.

[181] INTERPOL. https://www.interpol.int/en/Who-we-are/Member-countries/Africa/LESOTHO

[182] INTERPOL. (n.d.). *How INTERPOL supports Lesotho to tackle international crime*. https://www.interpol.int/en/Who-we-are/Member-countries/Africa/LESOTHO

[183] The World Bank & GCSCC (2019). *2019 Lesotho CCM* para 1 pg. 70

sharing forum for cybercrime issues in the Southern African region.[184] Cybercrime is one of SARPCCO's priority areas[185], and SARPCCO has two regional initiatives for its members, which include Lesotho:[186]

1. *Inception of regional Cybercrime Course for law enforcement officers. This course is delivered once a year putting together police officers from the 16 Member States dealing with cybercrime.*
2. *Establishment of a Regional Cybercrime Centre of Excellence in line with the INTERPOL Global Cybercrime Strategy. The centre is meant to assist member countries in terms of capacity building, investigative and operational support*

Lesotho is also a member of Asset Recovery Inter-Agency Network of Southern Africa (ARINSA) a multi-agency, informal network of practitioners between participating countries for exchanging information, model legislation and country laws in asset forfeiture, confiscation[187] UNODC Southern Africa, through ARINSA, provided training and retreats for over 3000 investigators, prosecutors and judicial officials in 2014/18. The training was primarily in the form of regional and national workshops. The training has included, inter alia: specialised judicial retreats, terrorist financing and cybercrime.[188]

Participants in the focus-group discussions confirmed that Lesotho law enforcement cooperates with INTERPOL for crimes. It is uncertain, however, whether this applies to cybercrimes. In addition, participants indicated that they rely on the Legal Mutual Assistance legislation between the Republic of South Africa and the Government of Lesotho on Extradition and the Treaty on Mutual Assistance in Criminal Matters.[189]

Government-Criminal Justice Sector Collaboration (Start-up)

There is no evidence on whether the government and criminal justice actors (prosecutors, judges and law-enforcement agencies) exchange information to combat cybercrime and; whether the country actively contributes to the international promotion of efficient and timely exchange of information between government and criminal-justice actors.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following recommendations are provided to Lesotho. These

[184] SARPCCO: https://sarpcco.com/member-country/

[185] SARPCCO. (2019). *Background information.* https://sarpcco.com/priority-crime-areas/

[186] SARPCCO. (2019). *SARPCCO initiatives.* https://sarpcco.com/cyber-crimes/

[187] Asset Recovery Inter-Agency Network Southern Africa (ARINSA). (2019). *Taking the Proceeds from Crime: The Story of ARINSA.* https://www.unodc.org/documents/southernafrica/The_story_of_ARINSA.pdf

[188] Ibid.

[189] Parliamentary Monitoring Group. (2001). *Mutual Legal Assistance on Criminal Matters Treaty & Extradition Treaty with Lesotho; Statute of Hague Conference on Private Int*. https://pmg.org.za/committee-meeting/996/

recommendations aim to provide advice and steps to be followed for enhancing existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL AND REGULATORY PROVISIONS

R4.1 The government should pass the Computer Crime and Cybersecurity Bill, which establishes structures for cybersecurity coordination in Lesotho.

R4.2 In anticipation of the passing of the Computer Crime and Cybersecurity Bill, the government should start planning the formation of the National Cybersecurity Advisory Council, including making budgetary provisions for its establishment.

R4.3 The envisaged Cybersecurity Council should formulate requirements for cybersecurity measures for non-Critical Infrastructure actors to deter cybercrime and protect citizens from cyber harms.

R4.4 As envisaged in the Computer Crime and Cybersecurity Bill, MICSTI should expedite the promulgation of regulations for critical information infrastructure protection to ensure that the national CSIRT is empowered to identify, protect, detect, and respond to cyber-attacks and provide recovery services for public, private and civil society actors to ensure effectiveness once established.

R4.5 The Lesotho Government, through MICSTI, should develop policy and regulations that can underpin a cyber task force within Lesotho Law Enforcement. This task force could work exclusively on cybercrime and attract talented individuals competent in relevant technical fields such as Information systems, Information Technology and Computer Science.

RELATED LEGISLATIVE FRAMEWORKS

R4.6 The Lesotho Government, through the Ministry of Local Government, Chieftainship, Home Affairs and Police in collaboration with MICSTI, should provide further legal provisions on Data Protection that establish requirements for security measures across all government sectors and the private sector when participating in government projects.

R4.7 The Lesotho Government, through the Ministry of Trade, Industry, Business Development and Tourism in collaboration with MICSTI, should review the

current Consumer Protection legislation and implement more comprehensive consumer protection legislation for e-Commerce, digital products and services.

R4.8 The Lesotho Government, through Ministry of Gender, Youth, Sports, Arts, Culture and Social Development in collaboration with MICSTI, should adopt the ITU Guidelines on Child Online Protection and adapt them into Lesotho Law and/or policy.

LEGAL AND REGULATORY CAPABILITY AND CAPACITY

R4.9 MICSTI should prioritise building threat intelligence capabilities in order to have the capacity for analysing data about threats and attacks.

R4.10 The Deputy Prime Minister and Minister of Justice, Law and Parliamentary Affairs, in collaboration with the ministries and agencies responsible for law enforcement, should allocate additional resources to courts to enable the adjudication of cybercrimes and crimes involving digital evidence. This should include ensuring law enforcement's roles in combating cybercrimes are understood and prioritised.

R4.11 The Ministry of Justice, Human Rights and Correctional Services should collaborate with the institutions of higher learning and training providers in the private sector to develop cybersecurity training programmes for law enforcement, judges, magistrates, and prosecutors. These programmes must be consistent with international standards of prosecuting cybercrimes.

R4.12 The Ministry of Justice, Human Rights and Correctional Services should develop regulations and mechanisms for maintaining evidence and integrity when investigating cybercrime cases in line with internationally recognised digital cyber forensic chain-of-custody practices.

R4.13 The Lesotho Mounted Police Service should maintain a register of cases, which classifies crimes to enable the tracking of crime trends, including cybercrime trends, to inform decisions on resource allocation to address cybercrime. This register may be shared among parties involved in prosecution and litigation.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

R4.14 To facilitate and encourage the exchange of information between the public and private sectors, MICSTI should prioritise the establishment of the national

cybersecurity incident response team once the Computer Crime and Cybersecurity Bill of is promulgated.

R4.15 MICSTI should continuously evaluate the effectiveness of legislation on cybersecurity and cybercrime and monitor adherence.

R4.16 MICSTI should develop public/private collaboration frameworks that they regularly adapt to take into account new technologies and emerging forms of cybercrime.

R4.17 Ministry of Foreign Affairs and International Relations, in collaboration with relevant stakeholders, should ensure that Lesotho actively participate in international public/private partnership platforms on cybersecurity.

R4.18 The Ministry of Justice, Law and Parliamentary Affairs and the Ministry of Local Government, Chieftainship, Home Affairs and Police should capacitate law enforcement agencies to work jointly with foreign counterparts through joint task forces for successful cross-border cybercrime investigations and prosecutions.

R4.19 The Minister and Minister of Justice, Law and Parliamentary Affairs should ensure that extradition laws that exist between Lesotho and other countries begin to take into consideration cybercrime cases explicitly.

R4.20 The government and criminal justice actors (prosecutors, judges, and law-enforcement agencies) should develop formal mechanisms that encourage and enforce the exchange of information to combat cybercrime between themselves. These mechanisms must also be assessed regularly to enhance their effectiveness.

DIMENSION 5
STANDARDS AND TECHNOLOGIES

This Dimension addresses the 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 to reduce cybersecurity risks (See Figure 12). The results of the evaluation are summarised in Figure 13 and further elaborated in paragraphs afterwards.

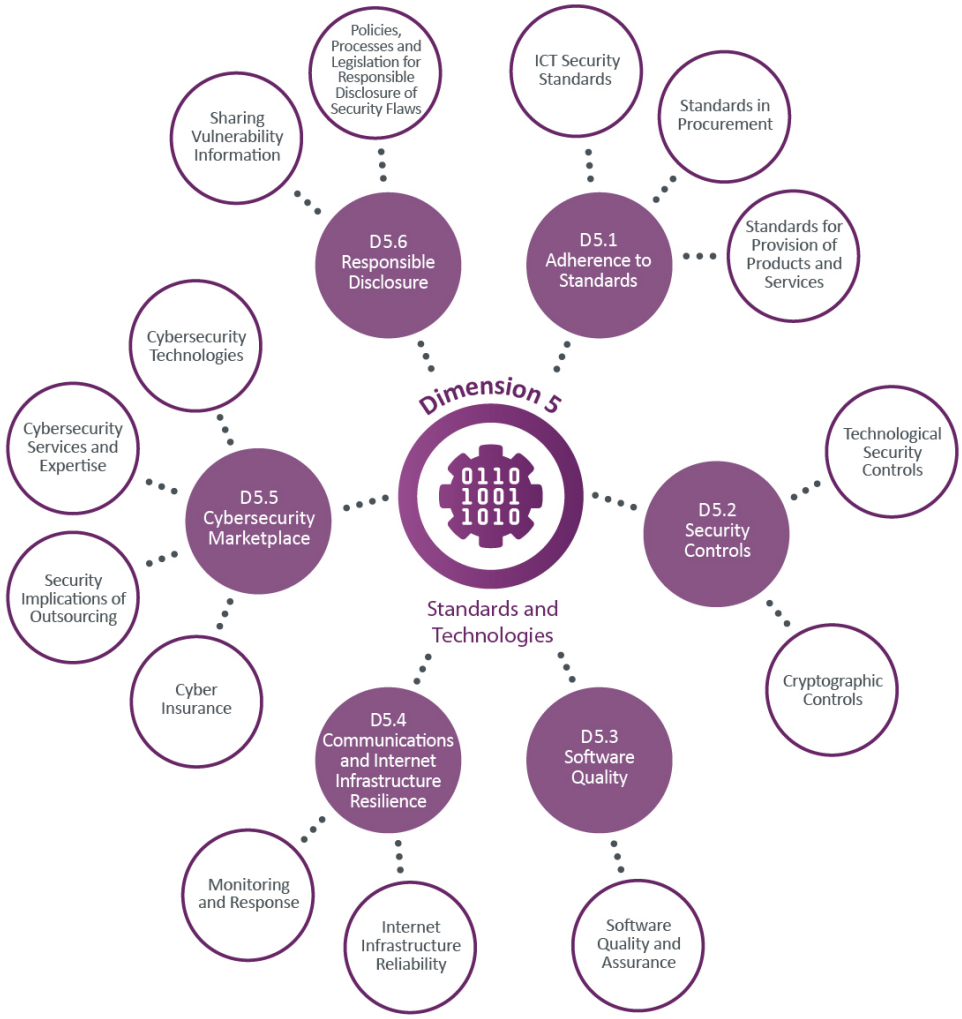

Figure 12: Factors and aspects of the Dimension 5 standards and Technology of the CMM

Overview of results

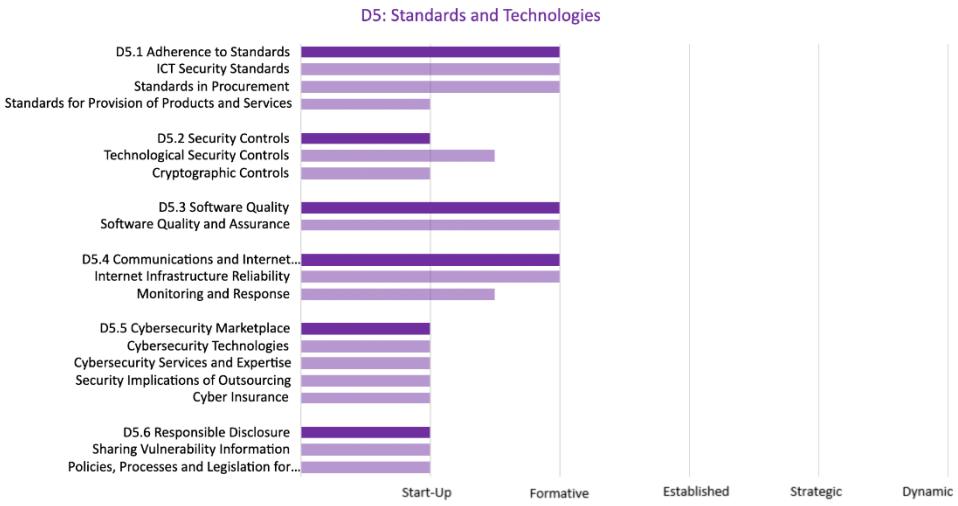

Figure 13. Results of the assessment of the Standards and Technologies of the Kingdom of Lesotho

D 5.1 ADHERENCE TO STANDARDS

This Factor reviews the government's capacity to promote, assess implementation of, and monitor compliance with international cybersecurity standards and good practices.

Stage: [start-up to formative]

ICT Security Standards (Start-up to Formative)

No Information risk management standards have been identified at the national level. Practices differ by organisation and sector. According to focus-group discussion participants, there is no promotion and take-up of cybersecurity risk management standards within the government Information Technology (IT) ecosystem in which the MICSTI is a critical player. The MICSTI manages the Lesotho Government Data Network (LGDN), hosts the government's IT systems and provides services to government ministries and agencies.[190] The MICSTI's ICT Department also leads a public services digitisation project, which started in 2013 as e-Government Phase 1 and is now in e-Government Phase 2.[191] As a result of the project, more public service processes are digitised, and citizen services are provided online. However, the MICSTI has not established information risk management standards. According to focus-group discussion participants, the MICSTI does not have an IT governance framework or an IT policy

[190] Ministry of Communications Science and Technology. (n.d). *Three (3) year (2020/21 - 2022/23) strategic plan*. https://www.communications.gov.ls/document/MCST%20STATEGIC%20PLAN%20FOR%20THE%20YEAR%202020%20-%2021%20%20-%202022%20-23.PDF

[191] African Development Bank. (2021). *Lesotho - e-government infrastructure - project complétion report.* https://www.afdb.org/en/documents/lesotho-egovernment-infrastructure-project-completion-report

defining the rules, regulations, and guidelines for the proper usage, security, and maintenance of the public sector's technological assets, including things such as computers, mobile devices, servers, internet and applications.

Some government agencies also do not have IT policies, including cybersecurity standards. A participant from a law-enforcement agency indicated that their department did not have a cybersecurity policy. Some participants from parastatals, which operate more independently from the MICSTI IT infrastructure and services, stated that they had developed IT policies based on cybersecurity-related standards and internationally recognised good practices. Participants from civil society organisations and small and medium enterprises indicated that their organisations did not have codified information risk management policies or standards.

There are signs of uptake of information risk management standards in a few agencies in the public and private sectors. These are entities providing telecommunication and financial services. During the focus-group discussions, some participants from the financial and telecommunication sectors indicated that they have developed corporate cybersecurity policies, standards and frameworks which are based on elements of the ISO 27000 family of information security standards or series, the United States Department of Commerce's National Institute of Standards (NIST) framework and several other cybersecurity standards. Some of the participants indicated that, due to the international nature of their business, their companies are required to comply with personal data privacy laws, such as the Data Protection Act of 2011, the European General Data Protection Regulation (GDPR), and the South African Privacy of Personal Information Act (POPIA). As a result, their cybersecurity policy baseline aims to meet the privacy requirements in addition to managing their cybersecurity risks. In the public sector, a participant from a government agency indicated that they have also developed internal controls based on the NIST and ISO 27000 family of standards.

Standards in Procurement (start-up)

No standards or best practices have been identified for use in guiding procurement processes by the public sector. Focus-group discussion Participants stated that the government of Lesotho does not have a policy or regulation that sets out security requirements for hardware, software or cloud vendors selling digital goods and services to the government. However, the government has general procurement policies that apply across the public sector and which are more applicable to general goods and services, not cyber goods and services.[192]

Large private companies and parastatals indicated that their organisations' procurement policies include the requirement for cybersecurity risk assessment where the procurement of digital goods and services was concerned, and they were audited for compliance. Participants

[192] Public procurement regulation (2007) Government of the Kingdom of Lesotho. http://www.finance.gov.ls/documents/laws%20and%20regulations/PUBLIC_PROCUREMENT_REGULATIONS_2007.pdf

http://www.finance.gov.ls/documents/laws%20and%20regulations/Public%20Procurement%20Amendment%20Regulations,%202018.pdf

from small enterprises indicated that they did not have standards per se, but they still did some due diligence as part of their procurement processes.

Standards for the provision of products and services (start-up)

The use of standards and good practices by local suppliers of goods and services, including software, hardware, managed services, and cloud services, varies from supplier to supplier. No standards or best practices have been identified to secure digital products and services developed or offered by providers in Lesotho. The application of standards and best practices in the provision of products and services varies by sector and type of service. Providers of services such as internet access and financial services have adopted cybersecurity standards or best practices.

Government IT, which the MICSTI leads, has not yet established cybersecurity standards in software development, hardware quality assurance, or provision of managed services and cloud security. Through the e-Government project, the government has commissioned the development of several web applications like the e-portal.[193] However, according to focus-group discussion participants, no security standards were stipulated in the application development processes; developers were at liberty to apply security best practices or not. Focus-group discussion participants observed that several e-services have been developed but they are not being used due to lack of support; the quality of the applications is uncertain as the MICSTI did not have software development standards before commissioning developers. In the development of applications, security risks were considered, but there were no mandatory cybersecurity standards or government policy to follow.

D 5.2 SECURITY CONTROLS

This Factor reviews evidence regarding the deployment of security controls by users and public and private sectors, and whether the technological cybersecurity control set is based on established cybersecurity frameworks.

Stage: [Start-up to Formative]

Technological security controls (Start-up to Formative)

Up-to-date technological security controls are deployed by users, public and private sectors, but not consistently across all sectors. Focus-group discussion participants from the telecommunication and financial sectors indicated that they have different types of security controls in place. Some participants from the public sector indicated that their organisational ICT policy included some security controls although their application was not uniform. For example, some entities, such as the Lesotho Millennium Development Agency and LCA, reported implementing security controls based on international standards and internally recognised best practices. In the focus-group discussions, government agencies indicated that

[193] Government of Lesotho e-portal: https://www.gov.ls/services/

they relied on MICSTI as their internet and ICT services provider to provide a framework for security controls. However, MICSTI had not yet developed such a framework.

Focus-group discussion participants from telecommunications companies and the financial sector indicated the deployment of security controls based on the ISO 27000-series and similar industry standards. Examples of controls that service providers in the banking sector uses include multi-factor authentication for digital channels. Participants from the focus-group discussions reported that the ISPs did not provide upstream controls for their end-users by default. Some service providers offer optional security controls such as intrusion prevention systems, IP/URL blacklists, and on-demand malware detection to customers. One hosting service provider was offering enhanced email security as extras. This review found that some organisations are looking for ways to strengthen their cybersecurity controls through the acquisition of technology and recruitment of talent. [194,195]

Cryptographic Controls (start-up)

While businesses and individuals deploy cryptographic controls for protecting data at rest and in transit, the use of cryptographic controls in Lesotho is ad hoc and limited. According to the 2020 data, Lesotho had 150 secure servers per 1 million people.[196] A secure internet server is a server that uses encryption technology in internet transactions. Critical services such as the country code Top-Level Domain (ccTLD) have not yet implemented Domain Name System Security Extensions DNSSEC.[197] Some private and government service providers deploy tools such as TLS (Transport Layer Security) to secure communications between servers and users; others do not. For example, local banks providing online banking services have secure websites. Yet, some e-service sites, such as the Ministry of Tourism's licensing portal, have not implemented encryption even though it collects personally identifiable data.[198]

Secure communication services, such as encrypted or signed email, are limited. According to focus-group discussion participants, within the public service, top-secret communication is transmitted in hardcopy through trusted messengers instead of using encrypted email, sharing a link to an encrypted file.

[194] Econet Telecom Lesotho. (2021, July). *Tender notice*. https://www.etl.co.ls/tenders/tender-notice-cyber-security.pdf

[195] Lesotho Post Bank. (2019, February). *Vacancy*. https://www.lpb.co.ls/wp-content/uploads/2020/01/Information-Security-Admin-Advert.pdf

[196] World Bank. (2022). *Secure internet servers: Lesotho*. https://data.worldbank.org/indicator/IT.NET.SECR?locations=LS

[197] Internet Society. (2022). *DNSSEC Deployment Maps: AF ccTLD DNSSEC Status on 2021-06-14* https://www.internetsociety.org/deploy360/dnssec/maps/

[198] Ministry of Tourism. (2022). *Sign up.* http://tourism.ecitizen.gov.ls/index.php/apply

D 5.3 SOFTWARE QUALITY

This Factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this Factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the critical nature of services.

Stage: [start-up]

Software Quality and Assurance (start-up)

The quality and performance of software used in the country vary by the type and size of the organisation. There are few software development firms in Lesotho. Some of the larger organisations develop some applications in-house. However, most software applications are imported from other countries as standalone software or as Software-as-a-service (SaaS).

In the public sector, the MICSTI has commissioned several web applications[199] as part of the e-Government project to improve public service delivery.[200] However, some web applications, such as online visa applications, do not function.[201] The user registration page on the Ministry of Tourism's website lacks encryption, and the registration form allows simple passwords, such as "1234567".[202] The website also seems incomplete; for example, the links on the front page lead to nowhere.[203] According to focus-group discussion participants, MICSTI did not build security requirements into the application requirements specification for most e-Government commissioned applications and website development. MICSTI has not generally integrated security requirements analysis into the software development lifecycle processes as the government does not have a written cybersecurity policy. Furthermore, there is no catalogue of assured software platforms and applications within the public sector. Procedures and processes regarding software application updates and maintenance (including patch management) have not been formulated yet. However, participants from MICSTI indicated that they often apply security patches for operating systems and applications.

Public entities, such as parastatals and state-owned enterprises, that do not rely on infrastructure and service provided by MICSTI have different software quality practices since they have IT and security policies that inform their application security requirements and software assurance.

---

[199] Government of Lesotho. e*Services*. https://www.gov.ls/services/, archived: https://web.archive.org/web/20230323070010/https://www.gov.ls/services/

[200] African Development Bank. (2020). Lesotho - eGovernment Infrastructure Project https://projectsportal.afdb.org/dataportal/VProject/show/P-LS-G00-001

[201] Government of Lesotho. (n.d). *Online visa applications*. http://www.homeaffairs.gov.ls/online-visa-applications-suspended/, archived: https://web.archive.org/web/20230323065631/http://www.homeaffairs.gov.ls/online-visa-applications-suspended/

[202] Ministry of Tourism. (2022). *Register*. http://tourism.ecitizen.gov.ls/index.php/apply, archived: https://web.archive.org/web/20230323065428/https://tourism.ecitizen.gov.ls/index.php/apply

[203] Ministry of Tourism. (2022). *Welcome to Ministry of Tourism e-services portal.* http://tourism.ecitizen.gov.ls/

D 5.4 COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

This Factor addresses the existence of reliable Internet services and infrastructure in the country, as well as rigorous security processes across private and public sectors. Also, this Factor reviews the control that the government might have on its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: **[Formative]**

Internet Infrastructure Reliability (formative)

Lesotho has followed a clear strategy for ICT sector development, including market competition, private sector participation, and independent sector regulation.[204] The internet infrastructure is available to serve internet users and mobile communication. However, the number of internet users is still lower than that of mobile communication users. This may have been attributed to the high prices of internet connectivity and the affordability of mobile devices. Most people in Lesotho have limited ICT skills and lack awareness of the benefits of the internet. In addition, the level of technology adoption in research and development is low. In 2017, Lesotho's competitive ranking on ICT by the World Bank was 115 and 125 on innovation and technology readiness (NSDP, 2020).[205]

Internet service in Lesotho is dominated by two companies, Vodacom and Econet Telecom Lesotho (ETL). Vodacom Lesotho controls the mobile market, while ETL dominates the fixed data services. Other players in the fixed market are Comnet and Leo, which compete with Vodacom and Econet. However, their footprint is limited to a few places.[206] The Lesotho Electricity Company Communications (LECC) also provides transmission network facilities to the market through its limited footprint.[207]

Over 90% of the population lives in areas that have either Third Generation UMTS (3G) network or Long-Term Evolution (LTE).[208] Both Econet and Vodacom have significantly invested in mobile network extension in the country. They have covered most of the rural, hard-to-reach areas with the assistance of the Universal Service Fund (USF). According to the Lesotho Communications 2019/2020 data, 97% of the mobile sites were on 3G and 64%

[205] Reva, Anna (2018). *Unlocking the potential of Lesotho's private sector : a focus on apparel, horticulture, and ICT (English)*. Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/832751537465818570/Unlocking-the-potential-of-Lesotho-s-private-sector-a-focus-on-apparel-horticulture-and-ICT

[206] Lesotho Communications Authority. (2020). *2019/20 Annual Report*. https://lca.org.ls/wp-content/uploads/filr/2328/LTA%20Report2002-3.pdf

[207] Ibid.

[208] Gillwald, A., Deen-Swarray, M, & · Mothobi, O. (2017). *The State of ICT in Lesotho.* https://researchictafrica.net/publication/the-state-of-ict-in-lesotho/

provided LTE access.[209] However, 63% of all LTE sites located in Maseru.[210] LTE and 3G are the main access technologies through which most of the population access the internet in Lesotho.[211] Fixed broadband internet penetration is below 1%.

There are mixed views on Internet service quality and affordability. Most of the focus-group discussion participants believed that the Internet is unaffordable. In contrast, others reported internet access to be affordable compared to other services such as electricity. Participants agreed that internet services in Lesotho are unreliable and that rural communities lack access. The education sector is particularly affected as most schools do not have internet access, even in areas with access infrastructure such as FTTx and mobile broadband. Participants indicated that access was also impeded by the lack of electricity in some rural areas. In 2020, the World Bank estimated that 47% of the population had access to electricity.[212]

Monitoring and response (start-up to formative)

Internet infrastructure owners conduct risk assessments are able to identify vulnerable assets and prioritise protective actions. Internet infrastructure owners in Lesotho include internet access providers (Comnet, LECC, Econet, Vodacom, Leo), the Lesotho Internet eXchange Point (LIXP), the dot LS registry (LSNIC), and accredited domain name registrars and web hosting service providers. The MICSTI provides internet access and hosting services to government departments and agencies.

Some of the focus-group discussions participants from the private sector indicated that they have risk assessments as part of the overall corporate risk management. They also have network monitoring and response mechanisms for their services. In the public sector, according to focus-group discussion participants, MICSTI monitors parts of the LGDN that provide internet infrastructure. However, the study did not find evidence of incident response plans and the frequency with which they are tested and reviewed.

D 5.5 CYBERSECURITY MARKETPLACE

This Factor addresses the availability and development of competitive cybersecurity technologies, cyber-insurance products, cybersecurity services and expertise, and the security implications of outsourcing.

Stage: [start-up]

[209] Lesotho Communications Authority. *(2020). 2019/20 Annual Report*. https://lca.org.ls/wp-content/uploads/filr/2328/LTA%20Report2002-3.pdf

[210] Ibid.

[211] Gillwald, A., Deen-Swarray, M, & Mothobi, O. (2017). *The State of ICT in Lesotho.* https://researchictafrica.net/publication/the-state-of-ict-in-lesotho/

[212] The World Bank. (2022). *Access to electricity (% of population) - Lesotho*. https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?locations=LS

Cybersecurity technologies (start-up)

There is no domestic production of cybersecurity technologies. Participants in focus-group discussions indicated that cybersecurity technologies are imported. Participants gave examples of instances where services were outsourced to companies in South Africa, Lesotho's largest trading partner. There is no information on whether the country has considered the security implications of using foreign cybersecurity technologies.

Cybersecurity services and expertise (start-up)

According to focus-group discussions, Lesotho has a small number of certified cybersecurity professionals. The country does not monitor the demand or supply of cybersecurity skills, and as such, there is no data on the availability of cybersecurity experts. There are firms that include cybersecurity consulting services in their portfolios. However, participants indicated that they have not been satisfied with the performance of the few local cybersecurity firms. As a result, large organisation outsources some of their cybersecurity work to vendors outside the country. Participants gave examples of instances where their organisations have outsourced work to vendors in South Africa and elsewhere.

Cyber Insurance (Start-up)

There is an emerging market for cyber insurance in Lesotho. Participants in focus-group discussions mentioned that two insurance service providers, Alliance and Minet Lesotho, were known to offer comprehensive insurance that included cybersecurity incidents. Minet Lesotho also lists cybercrime under its products and services on its website.[213] Despite the availability of cyber insurance cover, there is little awareness of cyber insurance products in Lesotho.

D 5.6 RESPONSIBLE DISCLOSURE

This Factor explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors, and whether there is sufficient capacity to continuously review and update this framework.

Stage: [start-up]

Sharing vulnerability information (start-up)

Focus-group discussion participants mentioned that there were no formal or informal mechanisms through which stakeholders share information about the technical details of

[213] Minet Lesotho. (2022). *Products and services*. https://www.minet.com/lesotho/products-services/

vulnerabilities. They do not have sectoral CSIRTs to assist with guidelines for reporting vulnerabilities found on applications. The review found two instances where a member of the Lesotho technical community identified vulnerabilities relating to organisations based in Lesotho. The publications were articles from 2020 and 2021, written by an author named Moima, a technical engineer through Medium, an online publish platform. In the 2020 article, Moima reported vulnerabilities identified on SR political party's website. However, the article did not state whether a report had been logged to the site owners.[214] In addition, the 2021 article discussed a vulnerability on the Lesotho Bureau of Statistics website and wrote:

> *"All in all, I call upon the IT engineers at bureau of statistics (SIC) to fix this problem. These (SIC) article is non offensive (SIC) but a matter of cyber awareness campaign through practical demonstrations."* [215]

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws (start-up)

According to focus-group discussions, Lesotho does not have a responsible disclosure policy or regulation. No organisation in the public or private sector has published a responsible disclosure policy. Currently, there is no legal provision protecting those disclosing security flaws. However, the Computer Crime and Cybersecurity Bill of 2022, which was undergoing promulgation at the same time as this CMM review was taking place, might have such provisions.

RECOMMENDATIONS

Following the information presented on the maturity of cybersecurity Standards and Technologies review, the following set of recommendations are provided to the kingdom of Lesotho. These recommendations aim to provide advice and steps to be followed for enhancing existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1 Through a multi-stakeholder process led by MICSTI, Lesotho should adopt a nationally agreed baseline of cybersecurity-related standards and good practices across the public and private sectors.

[214] Moima, T. (2020). *How to hack a website*. Medium. https://busyh27.medium.com/how-i-hacked-sr-politics-website-97379b097071

[215] Moima. T. (2021). *How I found anon login on Shodan*. Medium. https://busyh27.medium.com/how-i-found-anon-login-on-shodan-529143635e77

R5.2 MICSTI, in collaboration with government ministries and agencies, should promote the adoption of security standards in the private sector by ensuring that accredited government technology suppliers adhere to internationally recognised security standards.

R5.3 MICSTI should develop and implement IT governance and cybersecurity frameworks or adopt an international IT governance framework such as the Control Objectives for Information and Related Technologies (COBIT) and a cybersecurity framework such as the United States Department of Commerce's National Institute of Standards (NIST), ISO 27000 family of standards or Service Organization Control 2 (SOC 2).

5.4 In collaboration with the Office of the Auditor General and other government ministries, MICSTI should ensure annual IT audits of government IT to ensure adherence to standards.

SECURITY CONTROLS

R5.6 Through MICSTI, the government should establish national policy supporting cryptography and other cybersecurity controls to secure Lesotho's information infrastructure.

R5.7 MICSTI, in collaboration with other ministries, should establish a unit responsible for enhancing the ICT infrastructure resilience across the public sector (a public sector Security Operation Centre (SOC)).

R5.8 MICSTI, in consultation with LCA, should regularly review international standards and guidelines and evaluate local internet security infrastructure based on such reviews.

SOFTWARE QUALITY

R5.9 MICSTI should develop a catalogue of accredited, secure software applications and cloud services for use in the public sector.

R5.10 MICSTI should adopt and regularly review a secure software framework, such as one developed by the Secure Software Alliance (SSA), for commissioned or in-house application development in the public sector.

R5.11 MICSTI should promote software quality and security requirements across the public sector and ensure adherence.

R5.12 All government ministries and agencies should ensure security and privacy are built into design and development processes and that government websites and web-based systems are fit for purpose from the conception.

R5.13 MICSTI should develop an information security manual for government websites based on internationally recognised security principles such as the Open Web Application Security Project (OWASP) principles.

COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

R5.14 MICSTI, in collaboration with LCA and the private sector, should review the existing ICT policy to ensure that it enables the development of reliable Internet services that are widely available and used. Furthermore, LCA should enhance the current quality of service regime to include quality assessments and enforcement for internet services.

R5.15 LCA, in collaboration with government and industry players, should assess and identify the critical weaknesses in Lesotho's internet infrastructure and develop risk mitigation plans.

R5.16 MICSTI should ensure that critical national infrastructure is formally managed with documented network maps, processes, roles and responsibilities.

R5.17 MICSTI, in collaboration with stakeholders in government and industry, should review existing legal and regulatory mechanisms to ensure that providers of critical internet services in both public and private sectors conduct risk assessments, monitor and test network resilience, and respond to incidents.

CYBERSECURITY MARKETPLACE

R5.18 The government should promote collaboration between academia, private and public sectors to undertake research and develop cybersecurity technology products.

R5.19 MICSTI should encourage local production by supporting research and innovation and partnering with businesses related to developing cybersecurity applications, services, and solutions.

R5.20 Sector regulators should promote sharing information and best practices among organisations to explore potential cybercrime and cyber insurance coverage.

R5.21 Working with the SADC secretariat and member countries, work towards establishing a regional CSIRT and a protocol for the regional sharing of vulnerability and threat information.

RESPONSIBLE DISCLOSURE

R5.22 MICSTI should develop a responsible vulnerability-disclosure framework or policy within the public sector and facilitate its adoption in the private sector.

R5.23 MICSTI, in collaboration with key stakeholders, should develop a system to enable threat intelligence sharing among critical infrastructure partners. Importantly, the Central Bank of Lesotho should promote sharing of threat intelligence in the financial sector and incentivise companies to participate actively.

R5.24 MICSTI should review the existing Computer Crime and Cybersecurity Bill to ensure that it does not criminalise the work of cybersecurity researchers.

ADDITIONAL REFLECTIONS

The CMM review of the Kingdom of Lesotho was conducted by the C3SA in collaboration with the GCSCC and NUPI. The C3SA team was hosted by the MICSTI in collaboration with the LCA. Developing this report was rewarding and challenging for the research team. The process encompasses a thorough desktop study, engaging focus-group discussions, critical analytical work, and meticulous writing. The desktop study provided a good point of departure for the focus-group discussions and the analysis. Even though the level of stakeholder engagement in the review was more limited than we might have hoped, the representation and composition of stakeholder groups were overall balanced and broad. In addition, the focus-group discussion participants contributed vehemently to acquiring knowledge by being very generous with their time and thoughts.

The focus-group discussions for the review took place, in person, in Maseru between 10th and 12th May 2022. The workshops were publicised on local media and other Internet platforms. LCA gathered the main cybersecurity stakeholders in the country. The civil society, public and private sectors were represented and generously contributed to discussions. The discussions involved representatives of non-profit organisations protecting children and women. Most government departments expressed themselves, security agencies were present, financial institutions made essential points, and telecommunication operators brought clarity about the infrastructure and the quality of service they were providing. Also, some focus-group discussion participants expressed themselves in Sesotho, which is the main language spoken Lesotho.

Amongst the few challenges encountered, there was an issue with the completeness of evidence. It was not easy to find information about the different dimensions of the CMM. It was hard to find online digital documents and soft copies. Many documents were not available online, including the relevant governmental websites. We had to contact the person responsible for sending the related information. The use of Sesotho, while it enabled participants to express themselves freely, was a challenge for the only one team member spoke it. That team member had to translate contributions into English so that the rest of the team could follow the discussions. Further, it was impossible to engage with international partners in the country regarding cybersecurity.

Overall, it was a wonderful experience to meet the people of the Kingdom of Lesotho. The CMM review presented many opportunities for both the host country and C3SA. Amongst the opportunities was the interest of most public sector entities to improve their cybersecurity posture. The overwhelming attendance demonstrated this throughout the exercise, and most attendants were eager to contribute to the discussions. Another opportunity this engagement presents is collaboration talks between the C3SA and the host country to contribute to various cybersecurity capacity-building initiatives.

We are grateful for the heart-warming welcome we received in Lesotho and for the engouement of stakeholders to contribute to the discussions. From that interaction, it is easy to believe that the country has reached that point where the need for change is acknowledged, and there is a solid commitment among the stakeholders. We hope and believe that profound insights for establishing and maintaining cybersecurity in Lesotho can be garnered from our report.

APPENDICES

METHODOLOGY - MEASURING MATURITY

Deploying the CMM involves data-gathering through in-country stakeholder consultation (typically over three days) and remotely through desk research. It is designed to produce an evidence-based report which is submitted to the government representatives for the country being studied and will include recommendations to:

- benchmark the maturity of a country's cybersecurity capacity;
- provide a detailed set of pragmatic actions to contribute towards the advancement of cybersecurity capacity
- identify maturity gaps; and
- identify priorities for investment and future capacity-building.

During the review of a country, specific dimensions are discussed with relevant groups of stakeholders. Each group of stakeholders is asked to respond to one or two dimensions of the CMM, depending on their expertise. For example, Academia, Civil Society, and Internet Governance groups would all be invited to discuss both Dimension 2 'Cybersecurity Culture and Society' and Dimension 3 'Building Cybersecurity Knowledge and Capabilities' of the CMM.

Data collection

The Review Team gathers the evidence necessary to identify the stages of maturity across the CMM through desk research, in-depth interviews, and modified-focus-group discussions, utilising the CMM Structured Field Coding (SFC) Tool to capture the results. The Review Team's functions include a facilitator to lead the group sessions and a note-taker.

The CMM uses a **modified focus-group discussion methodology** that elicits data that complements and helps validate in-depth interviews and desk research.[216] As with interviews, focus-group discussions are an interactive methodology with the advantage that during collecting data, diverse viewpoints and conceptions can emerge as participants follow the discussion. Rather than posing questions to specific participants, the researcher(s) facilitate a discussion among the participants, encouraging them to adopt, defend or explain different

[216] Williams, M. (2003). Questionnaire design. In *Making sense of social research* (pp. 104-123). SAGE Publications, Ltd, https://www.doi.org/10.4135/9781849209434; Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 35-50). SAGE Publications, Inc., https://www.doi.org/10.4135/9781483349008; Richard A. Krueger, R. A., & Mary Anne Casey, M. A., (2009) Focus-groups: A Practical Guide for Applied Research. SAGE Publications, London.

perspectives.[217] This interaction offers advantages over other methodologies, making it possible for the participants to reach a mutual understanding and raise everyone's awareness of cybersecurity practices and capacities.[218] During CMM reviews, the Review Team leads the discussion to get onto all the aspects within the relevant dimensions.

To determine the level of cybersecurity capacity maturity, each *Aspect* has a set of indicators corresponding to all five stages of maturity. A consensus method is used to drive the discussions within sessions, for the stakeholders to provide evidence on how many indicators have been implemented by the country and to determine the maturity level of every aspect of the model. During focus-group discussions, researchers use semi-structured questions to keep discussions around relevant indicators. The discussion among stakeholders provides evidence regarding the implementation of indicators. In gauging the maturity level, if there is no evidence for all the indicators being met at a particular stage, then that country has not yet reached that stage of maturity.

Inconsistencies between stakeholders will inevitably occur. Equally, information known to a stakeholder in one sector might not be familiar in other sectors. Accordingly, it will fall to the Review Team to perceive these information gaps and investigate them.

Desk research and modified focus-groups inevitably raise some additional questions and possible inconsistencies. For this reason, and to gain a more in-depth understanding of critical and sometimes unique policies and practices, a set of in-depth interviews are also conducted during and occasionally following the field research.

Data analysis

With the prior consent of participants, all sessions are recorded. Individual responses are treated as confidential with the Chatham House Rule applied in reporting our results.[219] After conducting a country review, the **data collected during consultations** with stakeholders and the notes taken during the sessions are used to find evidence and **define the stages of maturity** for each *Aspect* of the CMM. The CMM report aggregates this information and determines the maturity of each Factor of the CMM.

In the course of the review, further desk research is undertaken to bridge any gaps that emerge during the in-country data-collection process and to validate the evidence provided. While drafting the **CMM report**, further desk research and interviews are often necessary to address any missing information and to validate and verify the results. For example,

---

[217] Kitzinger, J. (1994). The methodology of focus groups: the importance of interaction between research participants. Sociology of health & illness, 16(1), 103-121. https://doi.org/10.1111/1467-9566.ep11347023; Kitzinger, J. (1995). Qualitative research: introducing focus groups. Bmj, 311(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299;

Fern, E. F. (1982). The use of Focus Groups for Idea Generation: The Effects of Group Size, Acquaintanceship, and Moderator on Response Quantity and Quality. Journal of Marketing Research, 19(1), 1–13. https://doi.org/10.1177/002224378201900101

[218] Kitzinger, J. (1995). Qualitative research: introducing focus groups. *Bmj*, *311*(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299

[219] https://www.chathamhouse.org/about/chatham-house-rule

stakeholders might not always be aware of recent developments in their country, or if the country has signed a particular convention on personal data protection policy. Therefore, official government or ministry websites, annual reports of international organisations, university websites, in-depth interviews, etc. can be used as supplementary sources for information. This type of additional research helps to ensure that the report accurately reflects the Host Country's cybersecurity capacity. In each case, the team does not privilege any particular source of information but seeks to reach a consensus on the most valid status of each indicator of the model.

Developing recommendations

For each *Dimension*, **recommendations** are provided for the next steps to be taken for the country to enhance its cybersecurity capacity. If a country's capacity for a certain *Aspect* is, for example, at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders. The recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the CMM. The recommendations are provided specifically for each *Factor.*

After a review by the GCSCC Technical Board, the draft report is submitted to the Local Host to secure feedback. If new evidence arises, the draft report is revised and the maturity stages of each *Aspect* and *Factor* in the CMM are updated correspondingly. Once all parties approve the draft report, the Local Host will take the lead in the publication process. Publication approval rests with the Host Country and if this is agreed the Local Host is encouraged to publish it via an official government portal or other outlets.

Data management and ethical considerations

Focus-group discussions are conducted online on Microsoft Teams™ and Zoom™ platforms. *(Depending on platforms preferred by each nation)* The discussions are recorded using external recorders to guarantee the confidentiality of the data and information collected, and for future transcription for the purpose of writing the CMM report. The recordings remain anonymised. The findings from the desktop study, in-depth interviews, and focus-group discussions are consolidated during the analysis.






C3SA Researchers:

Professor Wallace Chigona, Dr Enrico Calandro, Dr Laban Bagui, Dr Shallen Lusinga, Ms Nthabiseng Pule, Ms Chimwemwe Queen Mtegha, Mr Teofelus Tuyeni, and Mr Ihab Alagha.

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.co.za/

NUPI Researchers:

Eskil Jakobsen

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, Professor Federico Varese, Professor Basie Von Solms, Professor David S. Wall, Dr Jamie Saunders, Dr Patricia Esteve-González, Dr Eva Nagyfejeo, and Mrs 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/