CYBERSECURITY CAPACITY REVIEW

Malawi

September 2020

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Kenneth Herman (World Bank), Óscar Noé Ávila (World Bank)
Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Professor Basie Von Solms, Professor Federico Varese, Dr Jamie Saunders, all members of the Technical Board of the Global Cyber Security Capacity Centre (GCSCC).
Approved by: Professor Michael Goldsmith (GCSCC)

Version	*Date*	*Notes*
1	*26/10/2020*	*First draft submitted to GCSCC Technical Board*
2	*22/11/2020*	*Submitted to Digital Malawi Project for review*
3	*01/02/2021*	*Submitted to Digital Malawi Project for final review*
4		

LIST OF ABBREVIATIONS

AU	African Union
ARIPO	African Regional Intellectual Property Organisation
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
COP	Child Online Protection
CTO	Commonwealth Telecommunications Organisation
CYBER4DEV	Cyber Resilience for Development (EU-funded project)
DoDMA	Department of Disaster Management Affairs
ETCSA 2016	Electronic Transactions and Cybersecurity Act of 2016
EU	European Union
FCDO	Foreign, Commonwealth and Development Office
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
GSMA	Global System of Mobile Communications Association
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technologies
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunications Union
IWF	Internet Watch Foundation
MACRA	Malawi Communications Regulatory Authority
MDF	Malawi Defence Force
MICT	Ministry of Information and Communications Technology
MOD	Ministry of Defence
MOJ	Ministry of Justice and Constitutional Affairs
MPS	Malawi Police Services
MUST	Malawi University of Science and Technology
MW CERT	Malawi Computer Emergency Response Team
NCRA	National Cyber Risk Assessment
NCS	National Cyber Security Strategy

NIST	National Institute of Standards and Technology, US Department of Commerce
PKI	Public Key Infrastructure
SSL	Secure Sockets Layer (a protocol used for website security)
SADC	Southern African Development Community
SANS	(SysAdmin, Audit, Network and Security), an American internet security training company
SARPCCO	Southern African Regional Police Chiefs Cooperation Organisation
TLS	Transport Layer Security (a protocol used for website security)
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNICEF	United Nations Children's Fund
WIPO	World Intellectual Property Organisation
YONECO	Youth Net and Counselling

EXECUTIVE SUMMARY

1. At the invitation of the Ministry of Information and Communications Technology, the World Bank undertook a review of the maturity of cybersecurity capacity in the Republic of Malawi. The objective of this review is to enable the country to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

2. Over the period of August 17 to September 10, 2020 the following stakeholders participated in virtual 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 as well as international partners.

3. The consultations took place using the Cybersecurity Capacity Maturity Model (CMM), developed by the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre'), a part of the Oxford Martin School of the University of Oxford in the United Kingdom. The model defines five *dimensions* of cybersecurity capacity:

    - *Cybersecurity Policy and Strategy*
    - *Cyber Culture and Society*
    - *Cybersecurity Education, Training and Skills*
    - *Legal and Regulatory Frameworks*
    - *Standards, Organisations, and Technologies*

4. Each dimension contains a number of *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]

5. Figure 1 below provides an overall representation of the cybersecurity capacity in Malawi 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]Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (accessed 25 February 2018).

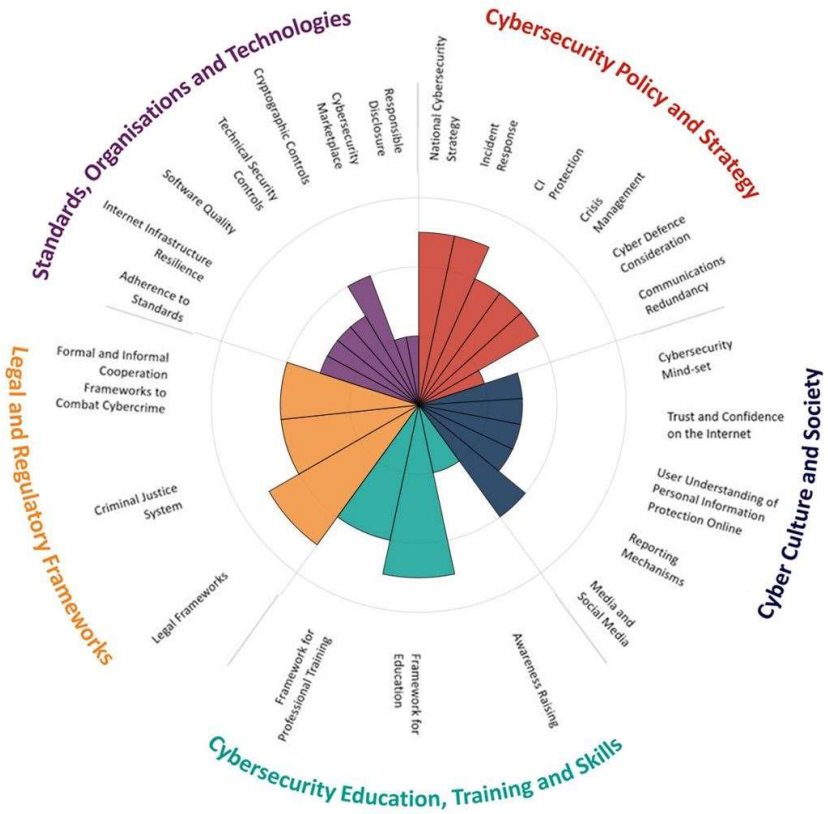

Figure 1: Overall representation of the cybersecurity capacity in Malawi

Cybersecurity Policy and Strategy

6. Overall, the Cybersecurity Policy and Strategy dimension of Malawi is assessed as Start-Up to Established.

7. In 2019, Malawi adopted the National Cybersecurity Strategy 2019-2024 (NCS), which contains a very ambitious Action Plan. When the NCS was drafted, multi-stakeholder consultation processes were followed, and observations fed back to coordinating agencies. The NCS was developed with the financial and technical support of the UK Government, through the Commonwealth Telecommunications Organisation (CTO).

8. The NCS strategic goals have several specific objectives and actions that are linked to national risks, priorities, and objectives, as well as economic and social development plans. The NCS explicitly states that its activities are aligned with national policies, laws and programmes. The NCS contains a detailed Monitoring and Evaluation Plan.

9. Malawi has not established a well-organised programme for cybersecurity coordination with clear objectives and goals. The NCS expressly recognises MACRA as the NCS implementing authority and that the MICT will monitor and evaluate the NCS implementation process. However, MACRA has been informally acting as national coordinator for cybersecurity matters. This has yet to be developed into a coordinated government effort with clear goals and objectives. MACRA took control of the national coordination role, in a “de facto” way, due to the lack of leadership, expertise and financial resources of other ministries and government agencies.

10. MW CERT was legally created in 2016 with the adoption of the Electronic Transactions and Cyber Security Act, which clearly defines its legal mandate, scope and functions. However, to date, MW CERT's incident response operations have not yet started. Some management staff have been hired and trained, and more technical staff will be hired soon. Equipment will be purchased shortly with the support of the ITU. MW CERT's facilities have to be remodelled - construction work is currently suspended due to Covid 19.

11. Malawi already identified fifteen national critical sectors: water, transport, tourism, research and development, mining, manufacturing and industry, ICT, health, government, food and agriculture, finance, environment, energy, education and defence and security. However, the list of CI sectors has not yet been officially published.

12. MACRA recently conducted a National Cyber Risk Assessment (NCRA) with the support of the Foreign, Commonwealth and Development Office (FCDO). The objective of the NCRA was to identify the critical assets and resources within those fifteen critical sectors. Currently, there is no legal or regulatory framework (currently under development) which regulates the CI providers' operation in terms of cybersecurity issues.

13. The NCS sets out a couple of activities related to crisis management at the national level. Currently, cybersecurity is not part of the national crisis management structure, policies or laws. MACRA and MW CERT will play an active role in this domain. Some government officials have been trained in cyber crisis management issues and have been part of regional cyber drills. No cyber drill has been conducted at the national level. MW CERT and other stakeholders had planned to conduct a national cyber drill between May and June 2020, but this exercise had to be postponed due to Covid 19.

14. The Malawi Defence Force (MDF) is responsible for the cyber defence matters in the country. The MDF has a good level of awareness and understanding concerning the need to enhance the cyber defence capacities of the nation. The NCS sets out the development of the National Cyber Defence Strategy, which will contemplate, amongst other aspects, the different approaches to address cyber-related threats to national security. This strategy has not yet been drafted. Within the defence structure, there is a Defence CERT (55% operational) which is responsible for protecting the military ICT infrastructure from cyber threats.

15. Internet network operators have been taking measures to enhance the communications redundancy capacity in the country. However, Government agencies (mainly crisis management agencies, first responders and ISPs), have not convened to assess and identify the main gaps and overlaps in terms of emergency response assets communications and the roles and responsibilities of the authorities to maintain communications stability during a national crisis.

Cyber Culture and Society

16. The Cyber Culture and Society dimension of Malawi was judged to range between the Start-Up and Formative stages.

17. The government of Malawi has demonstrated a commitment to cybersecurity in recent years through the publication of a series of reports studying ICT in general, which include aspects of cybersecurity, as well as reports focused on cybersecurity.

This commitment, however, has not resulted in substantial changes to the mind-set of public or private sector workers, or the general public. Awareness of cybersecurity is most prevalent within the financial and telecommunications industries. While the public mind-set of cybersecurity remains limited, it has improved in recent years.

18. Noting the trusting nature of Malawian society, the assessment participants confirmed that only a limited number of Internet users in Malawi understood the risks and threats posed by insecure web sites. The government offers only a limited range of e-government services, although there is ambition, expressed in the government's cybersecurity strategy, to expand these offerings. There is little to no e-commerce in the country.

19. Notwithstanding the passage of the Electronic Transaction and Cyber Security Act of 2016, which includes provisions for the protections of personal data, Internet users lack an understanding of how personal information is handled by the online services they use.

20. The country does not currently have a formal and well-established mechanism for reporting cybersecurity incidents. It relies mainly on the police services for capturing this information although there are services available for reporting cases of child abuse.

21. News coverage of cybersecurity activities is limited but does occur on occasion. However very little discussion of cybersecurity appears on social media channels.

Cybersecurity Education, Training and Skills

22. The assessment revealed that the Cybersecurity Education, Training and Skills capacity in Malawi ranges from the Start-Up to Established stages.

23. Malawi does not have a coordinated cybersecurity awareness programme, although there are some activities organized by the telecommunications regulator, MACRA. No programmes exist for educating executives on cybersecurity issues.

24. The NCS recognises the need to enhance cybersecurity education in primary and secondary schools and universities.

25. At the school level, public schools only provide IT courses with basic cybersecurity elements at the secondary level. All private schools deliver IT courses with basic cybersecurity components at the primary and secondary level. The NCS sets out some activities in this area, including the review of the existing material and integration of more cybersecurity components into the school curricula.

26. In tertiary education, some universities in Malawi offer accredited cybersecurity-related laboratories or courses within their degree programmes - undergraduate, graduate and post-graduate/doctoral. The MSc. and PhD programmes in Information Theory Coding and Cryptography and the BSc. programme in Computer Systems and Security are the only degree programmes in cybersecurity. The NCS also recognises the need to strengthen cybersecurity education by developing more cybersecurity focused degree programmes.

27. There is a small cadre of cybersecurity educators in Malawi. Hence, there are not sufficient academics to supply the current demand for cybersecurity-related courses. Qualification programmes for cybersecurity educators do not exist in the country. Universities and other education bodies are not currently offering seminars nor

lectures on cybersecurity issues aimed at the non-specialist. A couple of universities are presently conducting research and development projects in cybersecurity, but still have low impact.

28. Different sectors have recognised the need to enhance the professional training capacity in cybersecurity. The NCS, which was adopted in 2019, sets out various activities in this field, including the development of a national career progression policy which aims to promote continuous training and education.

29. ICT professional certifications with some security modules or components are available in Malawi, such as ITIL Foundation, Lean IT, Cisco, Microsoft, Linux, Oracle, Sun, LPIC, and others. Internationally accredited IT Security and Governance training and certification courses are offered in Malawi, such as Ethical Hacking Foundation Training and Certification, COBIT 5 Foundation Certification Training Course, CGEIT Course, CRISC Course, COBIT 5 Assessor Certification Training Course, COBIT 5 Implementation Certification Training Course. CompTIA certifications are also available.

Legal and Regulatory Frameworks

30. Overall, the Legal and Regulatory capacities of Malawi is assessed as Formative to Established.

31. Malawi has developed ICT legislative and regulatory frameworks addressing cybersecurity and cybercrime concerns. However, two issues remain to be addressed: (i) better implementation and enforcement of existing domestic laws and the Constitution; and (ii) some specific topics, such as the protection of the national CI and CII, incident reporting obligations, data protection, cybercrime procedural provisions, child protection online, require either new regulations or the strengthening of the current frameworks. Legislation protecting the rights of individuals and organisations in the digital environment has been adopted.

32. ***Electronic Transactions and Cyber Security Act of 2016*** (ETCSA 2016) addresses cybersecurity-related issues, such as the establishment and administration of the MW CERT, formation and validation of electronic transactions (electronic signature, admissibility and evidential weight of electronic messages, the validity of contracts in electronic form, etc.), consumer protection, the liability of online intermediaries and content editors and protection of online users, electronic commerce, security and digital economy, data protection and privacy, domain name and management, electronic government transactions, cybercrime offences.

33. There is a Cyber Investigation Unit under the Malawi Police Services (MPS). This Unit has two investigators for the entire country who have basic skills, but more training is required, especially in the digital forensic field. This Unit is seeking to enhance its basic office equipment and acquire their first equipment and tools to deal with digital forensics. This Unit does not have sufficient technological, financial and human resources to effectively operate. MACRA will fund the establishment of the Digital Forensic Laboratory.

34. The Directorate of Public Prosecution has no specialised unit for prosecuting cybercrime cases. There are a few prosecutors who understand the fundamentals, but they may struggle with complex and cross-border cybercrime cases. More capacity building is required - occasional training sessions are not enough. Training has to aim

at the specialisation level. Prosecutors dealing with cybercrime cases are well versed in the general procedural aspects, but investigating and prosecuting cybercrime cases require specialised skills and knowledge. That is what has to be developed.

35. The Court System does not have a specialised unit for cybercrime cases. Judges and magistrates are not fully aware of the cybercrime environment in the country nor the content and interpretation of the ETCSA 2016, so they are not fully capable of judging cybercrime cases. Since training has not been adequately delivered, the capacity is minimal.

36. During the CMM review sessions, it was recognised that there is a need to enhance informal and formal cooperation mechanisms, both domestically and internationally.

Standards, Organisations, and Technologies

37. Malawi's capacity in Standards, Organisations and Technologies was assessed to range from the Start-Up to the Formative stages.

38. The adoption of cybersecurity standards in Malawi is limited and uncoordinated, with only a few public or private sector entities deploying internationally recognized standards. A few companies are implementing the ISO 27000 standard, but most of the larger companies and critical infrastructure operators report having policies and procedures in place that have cybersecurity components. The government does not apply any international standards but has in place a "Public Service ICT Standards," developed in 2014, that includes some cybersecurity components.

39. Neither the financial nor the telecommunications regulators require any cybersecurity standards from the companies they regulate. However, the financial regulator, the Reserve Bank of Malawi, does have guidelines for financial institutions that include some measures intended to protect their technology environments.

40. The Internet in Malawi is reported to be reliable and resilient, with multiple independent connections to the global Internet though different providers. However, the cost of access remains one of the highest on the African continent, and rural access remains limited.

41. Catalogues of secure software are not generally applied in Malawi. However, the government and many of the larger private sector organizations, as well as critical infrastructure operators, reported the use of automated update capabilities for their users.

42. Basic technical security controls, such as password management policies and procedures, the use of firewalls, regular backups with some off-site storage are reportedly in use by most public and large private sector organisations. Very few controls are reported to be in use by small and medium sized enterprises.

43. Institutions in both the public and private sector reportedly apply cryptographic controls to data at rest and in transit, however, the deployment of these controls is inconsistent and ad-hoc. These services are not required by any regulator, although the Electronic Transactions and Cyber Security Act has some provisions targeting personal data protection which includes encryption. About half of the most accessed web sites in Malawi (i.e., those that use the dot-mw top level domain) utilize cryptographic web security with TLS, although not all are configured for the latest TLS version.

44. Malawi does not have a domestic cybersecurity development capability, and no market for cyber insurance exists in the country.

45. No framework currently exists in Malawi for the reporting of vulnerabilities or incidents, although that is addressed in the country's national cybersecurity strategy. There also is no informal or formal community of cybersecurity specialists for sharing of cybersecurity knowledge and information.

Additional Reflections

46. The government of Malawi has clearly made cybersecurity a priority. The CMM team is thankful for the support of the Malawi Communications Regulatory Authority (MACRA), the Malawi Public Private Partnership Commission, and active participation of all the stakeholder groups.

INTRODUCTION

47. At the invitation of the government of Malawi, the World Bank conducted a review of cybersecurity capacity of the Republic of Malawi. The objective of this review was to enable the government of Malawi to determine areas of capacity in which the government might strategically invest in order to improve their national cybersecurity posture.

48. Over the period August 17 to September 10, 2020, stakeholders from the following sectors participated in a consultation process conducted virtually utilizing a web-based conferencing system:

- Public sector entities
  Ministry of ICT, Department of E-Government
  Public Procurement & Disposal of Assets
  National Registration Bureau (NRB)
  Accountant General
  Malawi Revenue Authority
  Department of Immigration
  Malawi Defence Force
  Malawi Police Service
  Ministry of Education, Science and Technology
  Ministry of Agriculture and Food Security
  Ministry of Forestry and Natural Resources
  Ministry of Homeland Security
  Ministry of Local Government
  National Intelligence Service
  Malawi Energy Regulatory Authority
  Energy Generation Company
  Accountant General
  Malawi communications regulatory Authority
  Public Private Partnership Commission (Digital Malawi Project)
  Registrar General
  Office of the President and Cabinet
  Ministry of Justice

- Finance sector
  Malawi Stock Exchange
  Old Mutual
  Vanguard Life Insurance
  Reserve Bank of Malawi
  Ecobank
  Natswitch

- Private Sector
  Malawi SNDP (Sustainable Network Development Corporation)
  ICT Association of Malawi (ICTAM)

Simbanet
Skyband
Malawi Telecommunications Ltd
TNM
Candlex
Sparcs Systems Africa
TechNet
Business Machines Ltd
NeuroTech
TechNet
Business Machines Ltd
Nico Technologies
mHub
access communication LTD

- Utility Companies
  Northern Region Water Board
  Central Region Water Board
  Airport Development Limited
  Blantyre Water Board
  Lilongwe Water Board

- Academia
  College of Medicine
  Malawi Polytechnic
  Malawi University of Science and Technology
  Chancellor College
  National College of Science and Technology

DIMENSIONS OF CYBERSECURITY CAPACITY

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

50. Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions together with the factors which each presents:

DIMENSIONS	FACTORS
Dimension 1 Cybersecurity Policy and Strategy	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2 Cyber Culture and Society	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3 Cybersecurity Education, Training and Skills	D3.1 Awareness Raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4 Legal and Regulatory Frameworks	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 Standards, Organisations, and Technologies	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

[2] See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, *https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition*(accessed 25 February 2018).

STAGES OF CYBERSECURITY CAPACITY MATURITY

51. Each dimension contains a number of *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 dynamically adapt or change against environmental considerations. The five stages are defined as follows:

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

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

iii. **Established:** the indicators of the aspect are in place, and functioning. However, there is not well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.

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

v. **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g., cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in-stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

52. 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 the assessment team. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Malawi and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

METHODOLOGY - MEASURING MATURITY

53. During the country review specific dimensions are discussed with the relevant group of stakeholders. Each stakeholder cluster is expected 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 and Dimension 3 of the CMM.

54. In order to determine the level of maturity, each aspect has a set of indicators corresponding to all five stages of maturity. In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions stakeholders should be able to provide or indicate evidence regarding the implementation of indicators, so that subjective responses are minimised. If evidence cannot be provided for all of the indicators at one stage, then that nation has not yet reached that stage of maturity.

55. The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[3] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[4] It is this interaction and tension that offers advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[5]

56. With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to the data generated by focus groups.[6] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use."[7]

---

[3] Relevant publications: Williams, M. (2003). *Making Sense of Social Research*. Sage Publications: London; Knodel, J. (1993). "The Design and Analysis of Focus Group Studies: A Practical Approach". in *Successful focus groups: Advancing the state of the art*. Morgan, D. L. (Ed.). SAGE Publications: Thousand Oaks, CA; Krueger, R.A. and Casey, M.A. (2009). *Focus Groups: A Practical Guide for Applied Research*. Sage Publications: London.

[4] Relevant publications: Kitzinger, J. (1994)."The Methodology of Focus Groups: The Importance of Interaction between Research Participants. "*Sociology of Health & Illness*, 16(1). Available at https://doi.org/10.1111/1467-9566.ep11347023 (accessed 25 February 2018); Kitzinger, J. (1995). "Qualitative Research: Introducing Focus Groups". *British Medical Journal*, 311(7000). Available at https://doi.org/10.1136/bmj.311.7000.299 (accessed 25 February 2018); 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). Available at https://doi.org/10.1177%2F002224378201900101 (accessed 25 February 2018).

[5] Kitzinger, J. (1995).

[6] Krippendorff, K. (2004).*Content Analysis: An Introduction to its Methodology*. Sage Publications: Thousand Oaks, CA; Hsieh, H.F. and Shannon, S.E. (2005). "Three Approaches to Qualitative Content Analysis." *Qualitative Health Research*, 15(9). Available at https://journals.sagepub.com/doi/pdf/10.1177/1049732305276687 (accessed 25 February 2018); Neuendorf, K.A. (2002). *The Content Analysis Guidebook*. Sage Publications: Thousand Oaks, CA.

[7] Fern, E.F. (1982).

57. There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[8] The process is repeated, and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[9] Dey explains that this process categorises data as "belonging together."[10]

58. The second approach is deductive content analysis which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.[4]

59. In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or by prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly these novel categories that offer a refined perspective may be neglected. This is the reason why the GCSCC research team opts for a third, blended approach in the analysis of the data collected by the Centre, which is a mixture of deductive and inductive approaches.

60. After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each factor of the CMM. The GCSCC adopts a blended approach to analyse focus group data and use the indicators of the CMM as criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor the Centre's recommendations.

61. In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc.

62. For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is 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.

63. Using the GCSCC CMM methodology, this report presents results of the cybersecurity capacity review of Malawi and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

---

[8] *Elo, S. and Kyngäs, H. (2008). "The Qualitative Content Analysis Process."Journal of Advanced Nursing, 62(1). Available at* ***https://doi.org/10.1111/j.1365-2648.2007.04569.x*** *(accessed 25 February 2018); H.F. and Shannon, S.E. (2005).*

[9] Downe-Wamboldt, B. (1992)."Content Analysis: Method, Applications, and Issues."*Health Care for Women International*, 13(3). Available at https://doi.org/10.1080/07399339209516006 (accessed 25 February 2018).

[10] Dey, I. (1993).*Qualitative Data Analysis: A User-friendly Guide for Social Scientists*. Routledge: London.

CYBERSECURITY CONTEXT IN MALAWI

64. The Republic of Malawi is a landlocked country in south-eastern Africa of just over 118 thousand square kilometres. It has a population of just over 12 million, the majority of which reside in the southern half of the country.[11] By some estimates,[12] Malawi has the 7th youngest populations in the world, with a median age of 16.8. Malawi is also one of the least developed countries, scoring 0.485 on the UNDP Human Development Index,[13] placing it 172 out of 189 countries listed.

65. In terms of technology, according to ITU statistics, the percentage of the population using the Internet in Malawi has grown substantially in recent years, going from 2% in 2010 to 13% in 2017,[14] although these are small numbers compared to other countries in Sub-Saharan Africa, which averages 18% in 2017. Malawi places as 167 (out of 176 countries) on the 2017 International Telecommunications Union (ITU) Global ICT Development Index[15] and 30th out of 38 Sub-Saharan African countries on that index.

66. According to the World Economic Forum's Global Information Technology report for 2016, Malawi ranked 132nd out of 139 countries on their Network Readiness Index. The statistics from the WEF report shows that Malawi has a mobile subscription rate of 33% of the population, with a mobile broadband rate of 4.1% of the population and 6.2% of households with internet access.

67. Malawi has, over the years, created strategies to guide its economic and social development. The first Malawi Growth and Development Strategy (MGDS)[16] covered the years from 2006 – 2011 as the "overarching operational medium-term strategy for Malawi to attain the nation's Vision 2020." It included information and communication technology as part of its infrastructure development theme and included a goal to create an "effective, affordable and efficient telecommunications system" as well as a "developed ICT infrastructure and improved e-governance."

68. The first MGDS was followed by MDGS II to cover the period from 2011 – 2016. This plan also included a section on ICT calling for the implementation of "strategies that will facilitate E-services, increase public efficiency and grant citizen access to public services" and entail, *inter alia*, "developing a reliable, fast, adaptive and robust national ICT infrastructure that feeds into international networks; improving efficiency in delivering postal services; and developing public online services." It was

[11] https://www.cia.gov/library/publications/the-world-factbook/geos/mi.html

[12] https://www.cia.gov/library/publications/the-world-factbook/fields/343rank.html#MI

[13] http://hdr.undp.org/sites/default/files/hdr2019.pdf

[14] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[15] https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017rank-tab

[16] https://www.mitc.mw/images/downloads/other-documents/Malawi-Growth-and-Development-Strategy-August-2006.pdf

during this period, in 2013, that Malawi developed its first National ICT Policy[17] to "give direction on ICT development in the country."

69. The third MDGS covers the period from 2017 – 2022. This plan also includes goals for the further development of the ICT sector.

70. To assist its ICT development goals, the Government of Malawi, working with the World Bank and the Public Private Partnership Commission of Malawi, commissioned a report in 2018 titled "Malawi Digital Government Strategy" with an objective to create a "comprehensive e-Government Strategy which will position Malawi to reap digital dividends with the aim of transforming the country into a modern information society."

71. Telecommunications became unregulated and the independent telecommunications regulator, the Malawi Communications Regulatory Authority (MACRA)[18] was established with the communications act in 1998. MACRA's mandate was further revised in 2016 with the Electronic Transaction and Cyber Security Act (ETCSA), which also called for the establishment of a national CERT to be housed at MACRA.

72. In terms of cybersecurity, in the 2018 ITU Global Cybersecurity Index,[19] Malawi registers a score of .275, which places the country at a global rank of 106 (out of 175) and 19th (out of 42) for sub-Saharan African region.

73. Even before the 2016 ETCSA, information security featured in Malawi government publications, notably through a "Public Service ICT Standards" document published in 2014 which contained a section on security. This was followed by an assessment in 2016 using an early version the Cybersecurity Maturity Model. This unpublished report was prepared by the Commonwealth Telecommunications Organisation (CTO) as part of a technical assistance project funded by the Foreign and Commonwealth Office (FCO) of the United Kingdom and contributed substantially to the 2019 Malawi "National Cybersecurity Strategy". Also contributing to the development of a Malawi capacity for cybersecurity is a 2018 CIRT readiness assessment, conducted by the International Telecommunications Union as part of a plan to establish a national computer incident response capability and more recently a "National Cybersecurity Risk Assessment" conducted by the CTO intended "to identify a national risk assessment framework of assets and resources in critical sectors and institutions that could be vulnerable to cyber security intrusion, attacks, hacking and destabilization."

[17] https://www.macra.org.mw/?wpdmpro=malawi-ict-policy-2013#

[18] https://www.macra.org.mw

[19] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

REVIEW REPORT

OVERVIEW

74. This section provides an overall representation of the cybersecurity capacity in Malawi. 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.

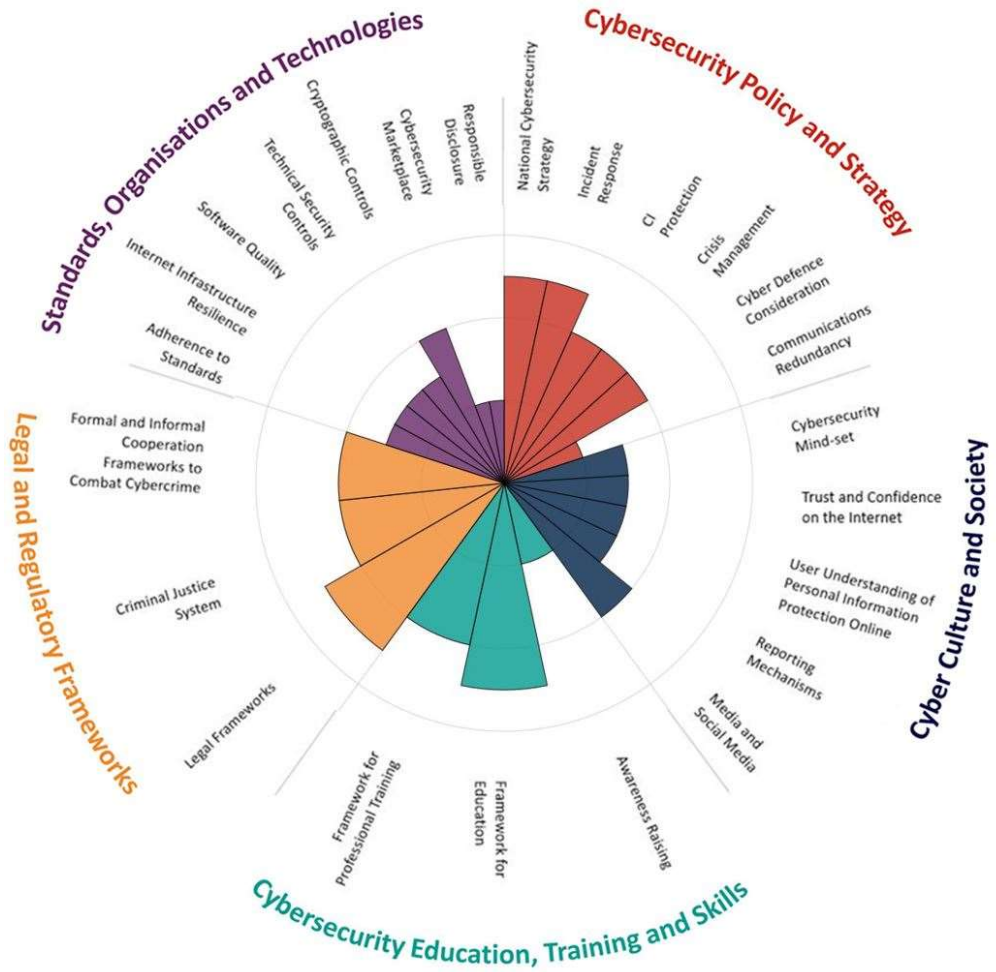

Figure 2: Overall representation of the cybersecurity capacity in Malawi

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

75. The factors in Dimension 1 gauge Malawi's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The Cybersecurity policy and strategy dimension also includes considerations for early warning, deterrence, defence and recovery. This dimension considers effective policy in advancing national cyber-defence and resilience capacity, while facilitating the effective access to cyberspace increasingly vital for government, international business and society in general.

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 government and non-governmental cybersecurity actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities

Stage: Formative to Established

76. In 2019, Malawi adopted the first-ever National Cybersecurity Strategy 2019-2024 (NCS). It was noted that the NCS contains a very ambitious Action Plan which describes the specific objectives, strategies and actions; deliverable outputs; leading implementing agencies; timeframes; key performance indicators (KPI); and possible funding sources and mechanisms for the implementation stage.

77. During the drafting process, which began in 2016, multi-stakeholder consultation processes were followed, and comments and observations were submitted to MACRA (as lead agency) and other established working groups. During the CMM review, some participants pointed out that more than 160 stakeholders from government, private sector, civil society and other relevant sectors participated in the drafting and consultation processes.

78. It was noted that NCS was developed with the financial and technical support of the UK Government, through the Commonwealth Telecommunications Organisation

(CTO). Some government stakeholders stated that no other international partners participated in the NCS development.

79. The NCS sets out general roles and responsibilities for some government actors, such as the Office of President, MACRA, MICT, MoJ, law enforcement agencies, MoD, Malawi Police Service, Malawi Defence Force, as well as for the CII operators, academia, civil society, private sector organisations and citizens. The above suggests that the cybersecurity leaders in Malawi clearly understand that the NCS implementation requires the active participation of all key stakeholders, including the private sector, academia and civil society. Some participants pointed out that NCS was conceived to be promoted and implemented with the cooperation of all key stakeholders across government and other sectors. For that reason, one of the guiding principles of the NCS is the multi-stakeholder approach to ensure active participation from the ecosystem actors and full ownership of the outputs.

80. Since the NCS is not publicly available, it is highly recommended that MACRA and the other implementing agencies ensure that the NCS is published and broadly disseminated, so the general public understands the purpose of the NCS and the roles and responsibilities of the key stakeholders, mainly higher levels of government.

81. The NCS clearly articulates its ***vision*** ("A nation with a secure, trusted, resilient and safe cyberspace that promotes a knowledge-based society and socio-economic development") and ***mission*** ("To develop and deliver effective cybersecurity capacity, services and infrastructure that instils confidence in cyberspace").

82. The NCS also sets out several guiding principles, as well as six strategic goals and fourteen specific objectives and actions which define the roadmap to enhance the cybersecurity capacity in Malawi. The strategic goals are:

- *Identification, management and protection of critical information infrastructures,*
- *development and enhancement of cybersecurity-related capacity, infrastructure and regulatory framework,*
- *promotion of awareness-raising and information sharing and collaboration mechanisms,*
- *improvement of the safety of vulnerable groups, such as children,*
- *enhancement and coordination to fight against all forms of cybercrime, and*
- *promotion of the use of cyberspace to drive social and economic development.*

83. Those strategic goals also break down into multiple specific objectives and actions that are linked to national risks, priorities and objectives, as well as economic and social development plans. The NCS explicitly states that its activities are aligned with national policies, laws and programmes, such as the National ICT Policy (2013), the National ICT Master Plan (2014-2031), the Electronic Transaction and Cyber Security Act (2016), the Payment System Act (2016), the Malawi Growth and Development Strategy (2017-2022), the Vision 2020, the Communication Act (2016) and the Science and Technology Policy (2002). As stated above, the content of the NCS seeks to advance the country in critical cybersecurity aspects, such as the protection of critical information infrastructure, awareness raising, fight against cybercrime, cybersecurity education, the establishment of the MW CERT, among others.

84. Some participants pointed out that the CMM model positively influenced the content of the NCS. The specific objectives and actions of the NCS were defined following the

dimensions, factors and aspects of the CMM model. In 2016, the CMM model was deployed by CTO in Malawi; therefore, the outcomes and recommendations of this CMM review helped the local authorities to identify the existing national gaps and priorities which then were integrated into the NCS.

85. It was noted that NCS is a very ambitious project which covers several relevant actions within different dimensions. It means that NCS requires not only the active participation of key stakeholders but also sufficient financial resources to ensure its implementation. MACRA and other implementing authorities understand that sufficient funds and resources are critical for the success of the NCS implementation (Section 6 of the NCS).

86. Some government representatives pointed out that the NCS implementation has been affected by the pandemic. The new President of Malawi was inaugurated in June 2020, so this may also delay the NCS implementation process because the order of priorities of the new government may change. Despite the above, MACRA and other stakeholders have been working closely to advance some NCS projects and also called the attention of the new government to the continuity of the NCS implementation.

87. The establishment of the MW CERT is one of the most important NCS projects that has been delayed. Other programmed activities affected by Covid 19 are the implementation of a national cyber drill which was postponed until new notice, the deployment of the National Cyber Risk Assessment (mainly the last sessions and the validation workshop), and the present CMM Review which had to be conducted remotely.

88. The NCS expressly recognises the importance of the monitoring and evaluation process. The NCS sets out the assessment of operational issues and long-term impact and outcomes of the NCS based on periodic reviews. The NCS Monitoring and Evaluation Plan provides mechanisms for data collection and reporting, and further information on the roles and responsibilities of stakeholders, and frequency of reports. MACRA and MICT should work closely on the monitoring and review aspects to ensure an efficient implementation process.

89. Some participants pointed out that Malawi has not established a well-organised programme for cybersecurity coordination with clear objectives and goals. Even though the roles and responsibilities of some government agencies and ministries, which are part of the national cybersecurity governance structure, are clearly defined in the NCS (institutional framework), some participants pointed out that MACRA has been informally acting as national coordinator for cybersecurity matters. This has yet to be developed into a coordinated government effort with clear goals and objectives.

90. It was noted that MACRA has three specific mandates within the cybersecurity domain: (i) NCS expressly recognises that MACRA is responsible for leading, planning and coordinating the NCS implementation; (ii) MACRA is the authority of the ETCSA 2016 (section 2); and (iii) the same legal body also establishes that MW CERT is managed by MACRA (section 6.1), being MW CERT the focal point for national coordination to respond to information and communication technology security threats (section 6.3). However, there is no specific legal mandate which empowers MACRA to coordinate cybersecurity matters under an overarching national cybersecurity programme (coordinated government effort) with clear goals and objectives. Based on our review, it is important to clarify that the scope of section 6.3 of the ETCSA is clear, the national coordination is limited to national incident response management, which is the core function of MW CERT, not of MACRA.

91. The fact that MACRA is the MW CERT administrator and that MW CERT has been empowered by law to serve as a base for national coordination to respond to information and communication technology security threats, has led to confusion. Some participants pointed out that the national cybersecurity coordination role falls to MW CERT, not to MACRA. Other participants stated that this coordination role is under MACRA. Moreover, other participants questioned why the national cybersecurity coordination role and the MW CERT's administration is under the aegis of MACRA, suggesting a potential conflict of interest with MACRA as the telecom regulator. Those participants also stated that the national cybersecurity coordination function should be in the hands of the MICT or another multi-stakeholder body.

92. Some government representatives recognised this situation and that while the 2016 ECTSA authorizes MW CERT to coordinate incident response, MW CERT has led some national cybersecurity initiatives and coordination activities which are not typically under the competences of the telecommunications regulators or the National CERT. However, since no other body is explicitly charged with overall coordination of activities, MW CERT assumed this national coordination role, in a "de facto" way, due to the lack of leadership, expertise and financial resources of other ministries and government agencies.

93. It was noted that MACRA has been clear that both functions, the MW CERT's administration and the national cybersecurity coordination role, may be taken over by other government agencies or ministries in the future. It is also important to highlight that the majority of the interviewed participants recognised MACRA's efforts to strengthen the cybersecurity capacities of Malawi.

94. It was also noted that each government agency or ministry has an independent budget line for its internal cybersecurity issues, which includes funds for the implementation of the NCS initiatives that they manage. Some participants also pointed out that international partners will provide technical and financial support to address some specific NCS initiatives, e.g., the ITU committed to providing some funds which will be allocated for the acquisition of equipment for the MW CERT. The EU funded-project, Cyber Resilience for Development (Cyber4D), will also fund some activities, mainly in the capacity building arena. Other international organisations will likely provide more technical and financial support for the NCS implementation.

95. It was also noted that half of the NCS projects and initiatives would be funded by MACRA, which could represent a significant surcharge in MACRA's budget, especially in times of crisis. MACRA committed to funding some projects, which in principle are out of its scope, such as the establishment of the Digital Forensic Laboratory within the Malawi Police Service (MPS). The CMM review team observed that one of the main challenges of the NCS implementation could be the financial resources, but it will be tested and eventually revised until the NCS implementation process gets back on track. MACRA and the other implementing agencies should take advantage of this pause, caused by Covid 19, to explore and seek cooperation arrangements, including financial resources, to ensure that the NCS activities are adequately implemented.

D 1.2 INCIDENT RESPONSE

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, coordinate, and operationalise incident response.

Stage: Formative to Established

96. ETCSA 2016, in its section 6, legally established the MW CERT, as the national CERT, and also details its legal mandate, scope, services to be offered and that MACRA will be its administrator. Despite the above, currently, there is no operational national computer-related incident response organisation that would serve as the coordinating body for the reporting and management of cybersecurity incidents in the country. Such organisations mostly take the form of Computer Security Incident Response Teams (CSIRT) or Computer Emergency Response Teams (CERT).

97. Due to the lack of a central organisation, there is no single entity holding a central registry of national-level incidents. However, it was said that MW CERT, with limited resources, has been able to categorise and record a few cyber incidents as national-level threats. It was noted that most public and private organisations are keeping track of the cyber incidents that affect their systems and networks, but this information is not shared with the MW CERT or other government agencies.

98. In 2018, the International Telecommunications Union (ITU) conducted a readiness assessment in Malawi to establish a national CSIRT. During this assessment, key stakeholders were consulted and interviewed, and also relevant information was gathered regarding the readiness of the country to establish a national CSIRT. Since then, MACRA has worked closely with ITU to implement the Action Plan (output of the assessment) to establish the MW CERT. This Action Plan includes several activities which will be conducted in three stages: (i) design; (ii) establishment; and (iii) enhancement. It was noted that the establishment of the MW CERT is currently between the design and establishment stages. Some government representatives pointed out that multi-stakeholders helped to define how the MW CERT should be designed and operated.

99. As part of such an assessment, the ITU committed to providing (i) assistance for the technical implementation; and (ii) some financial resources to procure the MW CERT technical equipment. Both activities have not been started yet due to Covid 19; however, the ITU will begin the procurement process soon to purchase the needed equipment and also engage some external consultants to support the establishment process. It was also noted that MACRA has allocated within its facilities some physical space for the MW CERT; however, these facilities are not ready yet and requires some construction work which is currently suspended due to Covid 19.

100. MW CERT currently has three staff members in place, including the CERT director and manager, but the plan is to hire three more highly skilled experts by mid-2021. It was noted that the ITU assessment report sets out what kind of skillsets the MW CERT staff should have, and those hiring guidelines have been followed so far. It was noted that the existing MW CERT staff is taking advantage of any training opportunity, including those programmed training activities that are now delivered remotely. Some capacity-building activities have been provided through the World Bank

("Digital Malawi Project") and the UK Government. It was also said that after the CMM working sessions, MW CERT's staff would have some virtual training sessions provided by experts from the Cyber4Dev project. It was also said that MACRA allocated some funds for MW CERT's staff training.

101. Before Covid 19, MACRA expected to have the MW CERT duly established by December 2020; however, the conditions changed early in March, and now it is uncertain when it will be operationally established. Some government representatives forecasted that MACRA might need some additional months (maybe by mid-2021) to finally established the MW CERT.

102. In the meantime, MW CERT is developing the incident response management procedures and defining clear roles and responsibilities according to its legal mandate and ITU guidelines. MW CERT already identified specific digital tools for the incident response management, and these will be purchased in the next few months. MW CERT has also established lines of communication with the domestic public and private organisations and other international and regional incident response bodies. The increasing cyber incidents caused by Covid 19 forced MW CERT to take further actions in this regard. Some participants pointed out that MW CERT's management staff is aware of the need to establish formal sharing mechanisms and procedures with public and private sector organisations. Currently, information-sharing practices are conducted on an ad-hoc basis.

103. Some government representatives pointed out that public and private sector organisations are not obliged to report their cyber incidents to MW CERT or any other government agency. Some participants recognised that Malawi must adopt an incident reporting framework, so that MW CERT is in a better position to constrain its constituents and the general public to report their cyber incidents as they occur. Some government representatives pointed out that this incident reporting framework could be developed with the support of the World Bank ("Digital Malawi Project").

104. Some participants pointed out that private sector organisations are maybe one step ahead of the government in the cybersecurity arena. In several CMM sessions, it was noted that some public and private sector organisations have the capability to detect and respond to a limited number of cyber incidents as they occur. It was noted that some private sector organisations, especially the multinational organisations operating in Malawi, have their own IT security team which takes care of the incident response management process or they engage cybersecurity service providers to assist them to prevent and contain cyber incidents. It was noted that the organisations within the telecommunications and financial sectors have enhanced their incident response management capacity while SMEs have very little or no capacity at all to handle cyber incidents. Some participants pointed out that SMEs require both technical assistance from MW CERT and a lot of capacity building.

105. It was also noted that that certain government agencies have already faced cyber-attacks, such as DDoS, ransomware attacks, and they have been able to handle those cyber incidents. It was noted that the lack of skilled staff and equipment are two of the main challenges that they face. Some participants pointed out that public sector organisations require more capacity building on incident response management. It was also noted that their incident response management capacity would be enhanced once the MW CERT is operationally established.

106. Some participants also pointed out that there are plans to establish various public and private sector CERTs in the country. It was mentioned that the Government CERT

would be established soon as part of the "Digital Malawi Project" and also the Banking and Telecommunications sectors are considering establishing their sectoral CERTs.

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This factor studies the government's capacity to identify CI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

Stage: Formative

107. Some government representatives pointed out that Malawi, through MACRA, organised a three-day workshop with key stakeholders (more than 100 participants from different critical sectors) to identify the Critical Infrastructure (CI) sectors. There, the following fifteen Critical Infrastructure (CI) sectors were identified: water, transport, tourism, research and development, mining, manufacturing and industry, ICT, health, government, food and agriculture, finance, environment, energy, education and defence and security. It was also said that during this workshop a CI matrix (methodology) was used to identify and categorise those CI sectors. However, the list of CI sectors has not yet been officially published, but MACRA plans to do so once the CIP regulatory framework is finished (currently under development)

108. In various CMM review sessions, stakeholders pointed out that MACRA recently conducted a National Cyber Risk Assessment (NCRA) with the support of the Foreign, Commonwealth and Development Office (FCDO). The objective of the NCRA was to identify the critical assets, systems and resources within those fifteen critical sectors which could be vulnerable to cybersecurity intrusions, attacks, hacking and destabilization.

109. During the NCRA deployment, more than forty stakeholders from different sectors and organisations, such as government, private sector, academia, civil society, including CII operators, participated in several in-country and remote workshops which took place from November 2019 to March 2020. During the first NCRA survey, the participants identified and rated a total of 109 CII systems which are exposed to cyber risks. It was noted that 37 of those 109 CII systems were rated and placed into the highest risk category and 38 CII systems were placed into the second-highest risk category. It was also noted that the majority of those critical systems are part of the energy sector. Some government representatives pointed out that the Government, through MACRA or MW CERT, plans to carry out NCRA every year since this is a continuous process.

110. The NCRA report states that in the ICT, energy and finance sectors, the cybersecurity prominence is very good, but in the transport and education sectors it is very low. It was noted that the NCRA report is not available to the general public yet, and the final validation workshop has not taken place due to Covid 19. It is unclear when the validation workshop will be rescheduled.

111. Some government representatives stated that currently there is no legal or regulatory framework (currently under development) which regulates the CI providers' operation in terms of cybersecurity issues. However, the plan is to enact a new law which obliges the CI providers to fulfil certain legal and technical obligations, including but not limited to incident reporting, regular risk management activities, threat and vulnerability disclosure and information sharing practices. It was also noted that the plan is that the MW CERT will be the national focal point for the CI and CII community; however, it may change in the future when sectoral CERTs (e.g., Government CERT, Banking Sector CERT, etc.) are established. It is unclear if sectoral regulators will play an active role in the supervision of the CI & CII assets.

112. It was noted that there are informal threat and vulnerability disclosure practices among the CI owners and administrators, as well as between CI owners and administrators and certain government agencies. However, any disclosure practices are conducted voluntarily since no formal incident reporting and information sharing frameworks are in place. It was further noted that CI owners and administrators now understand the importance of beginning to share information for the benefit of their organisations, the sector itself and the cyber resilience of the nation. Some participants pointed out that there is an informal group with a broader audience (cybersecurity experts from banks, telcos, government, etc.) that share cybersecurity information via WhatsApp and regularly get together via Zoom and other digital platforms. It is recommended that this group at least follows some information sharing rules (e.g., the traffic light protocol) to build trust amongst the participants.

113. Some CI owners and administrators, mainly those from regulated sectors, report some cyber incidents to the sectoral regulator as part of their compliance obligations, but nothing happens after the incident is reported - no technical support is provided. It was also noted that other utility organisations within regulated sectors do not report any cyber incidents.

114. It was noted that the Malawi Reserve Bank does not have the technical capacity to assist the regulated organisations in the event of a major cyber incident. Some participants pointed out that there is a Financial Intelligence Authority in the country, but incident response issues are not part of its scope of work. It was noted that MACRA, as the regulator for the telecommunications sector, is not doing anything different to what the Malawi Reserve Bank is doing. MACRA will likely adopt a preventive and supportive approach when MW CERT starts operations. In general, sectoral regulators in Malawi are not taking any appropriate measures to oversee and enhance the cybersecurity capacity of their regulated organisations. Some participants pointed out that it is an issue because many of those organisations are within the critical sectors described above.

115. It was noted that most organisations from the financial sector have developed different ways to manage their incident response management issues. For instance, some organisations have their own IT security teams, but also hire cybersecurity service providers to help them manage their cyber incidents. Other organisations, mainly multinational companies, receive incident response support from satellite offices or regional headquarters. It was said that in the telecommunications sector, both ISPs and Telcos have also developed incident response management capacities. Some telecommunications companies also receive incident response support from their regional headquarters.

116. It was noted that most financial sector organisations have adopted international security standards and best practices (e.g., ISO 27.000) to protect their critical assets and also to be aligned with the industry standards and headquarters' security policies. However, the level of cybersecurity awareness among their employees is still low.

117. It was noted that most financial institutions in Malawi conduct risk management assessments on an annual basis, and cybersecurity is one of the components of this type of assessments. Some participants pointed out that issues are identified, but recommendations are not always implemented because there is not a real commitment from senior management to provide the appropriate resources to fix those issues. Despite the above, senior management within the financial sector has a better appreciation for cybersecurity since some major cyber incidents have occurred in the sector. It was noted that the financial institutions are required to conduct internal cyber simulations and penetration testing exercises and that the Malawi Reserve Bank supervises that those activities are carried out. It was noted that no cyber drills have been conducted at the sectoral level.

118. Some participants from the telecommunications sector pointed out that they regularly conduct risk assessments, and cybersecurity is also part of this risk analysis. It was noted that virtual and physical access controls are implemented. No cyber exercises have been conducted at the sectoral level. Most telecommunications organisations responded that they are not conducting cyber simulations at the organisational level.

119. Some participants stated that most actors within the energy sector conduct annual risks management assessments which also cover an extensive cyber risk analysis and that this type of assessments are based on their internal security and business policies. It was noted that as part of these risk management activities, some organisations provide cybersecurity training to their staff, as well as to senior management. These activities have driven cybersecurity to be a priority now within their organisations. It was also noted that some organisations within the energy sector regularly organise internal cyber exercises and penetration testing to close existing gaps.

120. Until the issues mentioned above are adequately addressed, including the adoption of an incident reporting framework, the development of a robust CIIP regulatory framework and real incentives to comply with that regulatory framework, it is unlikely that the Government (MACRA, MW CERT) will be able to provide a high level of assurance that the critical infrastructure assets in the country are adequately protected.

D 1.4 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, coordinate, and operationalise incident response.

Stage: Formative

121. It was noted that Malawi has established the Department of Disaster Management Affairs (DoDMA),[20] whose legal mandate is to coordinate and direct the implementation of disaster risk management programmes in Malawi. DoDMA's mission is to effectively coordinate the implementation of disaster risk management programmes through overseeing disaster prevention, mitigation, preparedness, response and recovery activities.[1] Even though there is an established DRM institutional framework and there are various laws and policies related to the national DRM system, it was noted that DoDMA is not currently equipped with any official mandate to manage and coordinate cyber-related incidents. Some participants pointed out that it is likely that DoDMA's role within the cyber crisis management area will be limited to supporting other organisations, such as MACRA, MW CERT, etc.

122. Some government representatives recognised that there is an adequate level of awareness about the need to incorporate cybersecurity components into the national crisis management structure, policies and frameworks. It was also noted that in 2016 key stakeholders already had this discussion and decided to integrate some cyber crisis management activities into the NCS.

123. It was noted that the NCS Action Plan contemplates the following two activities within the crisis management area: (i) develop and test requisite for crisis management measures during cyber drills, and (ii) evaluate cyber drills to develop options on how to improve crisis management measures. MACRA and MW CERT will lead the first activity, and the second activity will be led by MW CERT and Malawi Defence Force (MDF). The NCS Action Plan also states the development and continuous update of contingency plans, which will include roles (and responsibilities) of the military and security forces during cyber-attacks. This specific activity will be led and funded by MACRA, MW CERT and MDF.

124. In various CMM review sessions, stakeholders stated that no cyber drill has been conducted at the national level. However, MW CERT and other stakeholders had planned to conduct a national cyber drill between May and June 2020. Unfortunately, this exercise had to be postponed until new notice due to Covid 19. It was also noted that the ITU and Cyber4 Dev project are committed to supporting and guiding MACRA and other stakeholders during this exercise.

125. According to some government representatives, some officials from the Malawi government attended the 2018 SADC Capacity Building Workshop on Cyber Security and Regional Cyber Drill in Mauritius. There, those government officials participated, among other activities, in a real-time simulation of cyber-attacks, and also learned how to manage that type of crisis in a national-level context. Even though Malawi has

[20] https://www.dodma.gov.mw/index.php/pages/who-are-we

not made much progress on managing the cyber crisis management matters at the national level, it was noted that in Malawi there is a basic understanding and training at the government level on how to manage the national cyber-related crisis.

126. It is recommended that MACRA, MDF, DoDMA or any other high-level agency, integrate cyber crisis management mechanisms and activities within the national crisis management structure, laws and policies. When established, MW CERT can support the leading agency to conduct regular cyber exercises to ensure (i) that the national crisis management structure is capable of dealing with the likely consequences of major cyber incidents; and (ii) that the participants and stakeholders of the crisis management community, who are not likely to be IT or cybersecurity experts, understand the dynamic and main related issues, and that they are adequately prepared to face the different cyber-related crisis scenarios.

D 1.5 CYBER DEFENCE

This factor explores whether the government has the capacity to design and implement a cyber Defence strategy and lead its implementation, including through a designated cyber Defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Stage: Formative

127. Malawi Defence Force (MDF) is responsible for the cyber defence matters in the country. MDF has a good level of awareness and understanding concerning the need to enhance the cyber defence capacities of the nation.

128. Some government representatives pointed out that the existing national security and national defence strategies and policies do not contemplate any cybersecurity-related activity or operation. However, the NCS Action Plan sets out the development of a Cyber Defence Strategy, which will contemplate, amongst other aspects, the different approaches to address cyber-related threats to national security. It was noted that this specific strategy has not been drafted yet, but the process will be led by MDF in collaboration with other stakeholders.

129. Some participants pointed out that MDF already identified several specific threats to national security in cyberspace, such as external threat actors (both state and non-state actors), insider threats, supply chain vulnerabilities and threats to military operational capacity. The identification of these cyber threats took place as part of the recent NCRA carried out by MACRA and FCDO. It was also said that MDF not only identified cyber threats but also defined the strategy of how to contain them.

130. Some stakeholders pointed out that MDF established the Defence CERT (55% operational) which aims to monitor and protect the military ICT infrastructure and will also collaborate with the MW CERT. It was noted that the Defence CERT does not have any specific mandate to oversee and protect the national CI and CII assets and it is unclear if such a collaboration with the MW CERT will also cover that specific function. It is recommended that both the Defence CERT and the MW CERT collaborate with

the protection of the national CI and CII assets because any disruption to these assets may cause severe consequences to national security and stability and well-functioning of the society.

131. Even though the Defence CERT is not fully functional, it was noted that MDF is working around the clock to reach an operational level early next year. In that line, the Defence CERT already hired highly skilled officials who are continuously trained locally and internationally. It was noted that better equipment and tools would be delivered soon.

132. Some government representatives also pointed out that the MDF does not have any central command nor control structure conducting cyber operations. However, the NCS Action Plan sets out the establishment of a Central Defence Command (CDC) for cybersecurity operations in Malawi. It is unclear the scope of the CDC and if the CDC and the Defence CERT are the same body.

133. Some government representatives said that the MDF has organised a few internal cyber drills with the cooperation of the Defence CERT. They plan to conduct a new cyber exercise soon and expect to invite the U.S., German, UK and the Netherlands Defence Forces and other domestic stakeholders to this exercise.

134. Some participants pointed out that both the MDF and the Defence CERT collaborate actively with public and private sector stakeholders (ISPs, telcos, banks, law enforcement, MACRA) to protect the nation from cyber threats and their adverse impact to the national and international security. It was noted that MDF has trained some private sector organisations to enhance their cybersecurity capacity and national cyber resilience.

135. It was noted that the MDF usually shares information informally with other stakeholders of the domestic ecosystem. MDF is an active participant of the national debate on cybersecurity issues. At the regional level, it was noted that MDF has built collaboration channels with regional organisations (e.g., SADC, ITU, CTO) but those links have been focused on capacity building. At the international level, MDF has established a robust collaboration network with the U.S., German and UK Defence Forces which have provided capacity building and support in other military areas.

136. Some government representatives pointed out that MDF has to implement the following actions to enhance their cybersecurity capacity and tackle most of their existing challenges: (i) more capacity building opportunities and more trained staff; (ii) better technology and tools to run the Defence CERT; (iii) build robust international and domestic collaboration channels; and (iv) more financial resources to cover all the activities indicated above and new challenges.

D 1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Start-Up

137. It was noted that digital redundancy measurers might be considered by public and private sector organisations, but not systematically or comprehensively.

138. Some government representatives pointed out that no emergency assets have yet been identified.

139. At the national level, the Government, mainly crisis management agencies, first responders and ISPs, have not convened to assess and identify the main gaps and overlaps in terms of emergency response assets communications and authorities' roles and responsibilities to maintain the communication stable during a national crisis. Indeed, establishing communication channels and backups (digital and non-digital) and which authorities are in charge of managing and coordinating this type of matters is highly important in case of a national crisis regardless of its nature - cyber or non-cyber incidents.

140. Even though the NCS is very ambitious and sets out several projects in different areas, there is no initiative or project which aims towards the enhancement of the digital and non-digital communication redundancy aspects at the national level. Therefore, the Malawi Government, through MACRA and other stakeholders, should integrate this specific issue in the national cybersecurity agenda.

RECOMMENDATIONS

141. 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 Malawi. 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

R1.2 Ensure that the NCS is publicly available on MACRA's website or other sources. Also, ensure that NCS is promoted and broadly disseminated.

R1.3 MACRA, as lead agency, should consider the following actions to ensure an adequate implementation process of the NCS:

1. *Ensure that MACRA and MICT are working closely to implement the Monitoring and Evaluation Plan described in the NCS.*
2. *Monitor and evaluate the current roles and responsibilities of the relevant stakeholders, including the identification of gaps and duplication of functions.*
3. *Gauge implementing partners' performance and managing and implementing capabilities.*
4. *Revise budget allocation to ensure sufficient funds for the implementation of the NCS projects and initiatives. Seek additional technical and financial resources from international, regional and domestic partners to ensure a successful NCS implementation.*

R1.4 Ensure that the existing national cybersecurity governance structure (e.g., MACRA, MW CERT, MICT, MDF, etc.) has clear roles and responsibilities and that the whole ecosystem, including the general public, understands their roles and functions and how cyber incidents, risks and issues get escalated to higher levels of government.

R1.5 As a national coordinated effort, appoint a dedicated National Cybersecurity Coordinator (NCC) to lead the national cybersecurity programme. NCC could be either MACRA, MICT, any other *government* agency or multi-stakeholder committee.

R1.6 Ensure that the NCC has the pertinent legal mandate to perform its functions and responsibilities, accordingly, including the authority to consult stakeholders across public and private sectors and civil society. Ensure that the overarching national cybersecurity programme has clear objectives and goals and an adequate budget to operate.

INCIDENT RESPONSE

R1.7 Develop a centralised operational registry, possibly hosted by the MW CERT, to analyse, categorise and record national-level cyber adverse incidents. Also, conduct regular, systematic updates to the national level incident registry.

R1.8 Ensure that the MW CERT's technological, financial and human resources are adequate to initiate operations. Establish clear processes and defined roles and responsibilities.

R1.9 Establish regular training for the MW CERT employees and design metrics to assess the result of this training.

R1.10 Develop and implement a national cyber incident reporting framework and platform for incident reporting and information sharing across sectors with robust lines of communication prepared for times of crisis.

R1.11 Create a specific mandate for the MW CERT to compel public and private sector organisations, including national CI and CII operators, to report cyber incidents.

R1.12 Strengthen the existing mechanisms for regional and international cooperation for incident response between domestic and international organisations to resolve incidents as they occur.

R1.13 When incident response operations begin, establish metrics to monitor and evaluate the effectiveness of the MW CERT.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.14 Ensure that the identified national critical infrastructure sectors are officially published and broadly disseminated. Regularly re-appraise both CI and CII ecosystems following international standards to capture changes in the threat environment.

R1.15 Ensure that the public and private CIP/CIIP operators are implementing robust incident prevention, detection and response protocols, policies and standards. Allocate sufficient resources for conducting emergency response scenario exercises at the organisational level, at least once a year.

R1.16 Develop a CIP/CIIP legal framework which obliges CI and CII operators to meet specific legal and technical standards, such as the implementation of internationally recognised security standards, incident reporting requirements, regular risk management activities, threat and vulnerability disclosure practices, and information sharing mechanisms, etc. to ensure that CI/CII operators are adequately protecting the national CI/CII assets.

R1.17 Establish clear instructions concerning which government agency or multi-stakeholder body (MACRA, MW CERT, the sectoral regulators, etc.) is responsible for monitoring and enforcing the CIP/CIIP regulatory framework. Also, ensure that this supervising authority has sufficient financial, human and technological resources to comply with these functions.

R1.18 As Malawi develops the relevant CNI governance mechanisms and CIP/CIIP regulatory framework, the following best practices in CNI management should be considered:

1. *Ensure that the CI sectors and assets are regularly audited.*
2. *Establish a mechanism for regular vulnerability disclosure and information sharing between CI assets owners, operators and government.*
3. *Establish a regular dialogue between tactical and executive strategic levels regarding cyber risks practices and encourage communication among CI operators and government.*
4. *Establish information protection and risk management procedures and processes within CI, supported by adequate technical security solutions, which inform the development of an incident response plan for cyber adverse incidents.*
5. *Identify internal and external CI communication strategies with clear points of contact.*
6. *Establish standard processes and procedures to assess and measure the capability of CI assets owners and operators to detect, identify, respond to and recover from, cyber threats.*

CRISIS MANAGEMENT

R1.19 Consider equipping DoDMA, MACRA or any other agency with a specific legal mandate to manage and coordinate with relevant actors, including the MW CERT, cyber crisis management issues at the national level. Also, integrate cybersecurity components and activities into the existing national crisis management system, policies and structures.

R1.20 Allocate cybersecurity exercise planning to relevant authorities, such as DoDMA, MACRA, with the support of the MW CERT when established. The planning process includes engagement of participants, outlining roles in the exercises and the articulation of benefits and incentives for participation.

R1.21 Allocate sufficient resources for conducting cyber drills at the national level, at least once a year. Also, identify metrics to evaluate the success of the exercises and feed the findings back into the decision-making process.

CYBER DEFENCE

R1.22 Strengthen the cyber defence capacity within the MDF, including the Defence CERT, by allocating sufficient human, financial and technological resources to protect the country's stability from major cyber incidents and protect the sovereignty of the nation in cyberspace.

R1.23 Ensure that the Defence CERT protects and monitors the military ICT infrastructure, as well as the national CI/CII sectors and assets from adverse cyber

threats. If the Defence structure will also be responsible for monitoring the protection of the wider CNI, this has to be appropriately documented and communicated to the stakeholders.

R1.24 Consider integrating the following aspects into the National Cyber Defence Strategy: (i) cyber defence activities and operations within the existing MDF structures; (ii) clear roles and responsibilities in terms of the broader cybersecurity needs of the country; and (iii) the country's position in its response to different types and levels of cyber-attacks.

R1.25 Develop incident reporting and information sharing mechanisms between the government, the military structures and the CI/CII operators. Also, establish international cooperation mechanisms to exchange cyber intelligence information with allies and other regional platforms.

R1.26 Establish robust training programmes for the Defence CERTs, armed forces, and national security's staff members working on cyber defence issues in the country and develop awareness campaigns.

COMMUNICATIONS REDUNDANCY

R1.27 Consider assessing the resilience of the overall Internet infrastructure.

R1.28 Establish a consultation process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response assets communications and authority links, and also identify and map emergency response assets, priorities and standard operating procedures in case of communication disruption.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

142. Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including Internet users. The days in which cybersecurity was left to experts formally charged with implementing cybersecurity have passed with the rise of the Internet. All those involved with the Internet and related technologies, such as social media, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of users in achieving cybersecurity but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, cybersecurity experts need to build systems and programmes for users – systems that can be used easily and be incorporated in everyday practices online.

143. This dimension reviews important elements of a responsible cybersecurity culture and society such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. This dimension also entails the existence mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this dimension reviews the role of media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D 2.1 CYBERSECURITY MIND-SET

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 mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Start-Up - Formative

144. The government of Malawi has clearly prioritized cybersecurity, at least in principle. Over the past 10 years the government has produced a series of reports and strategies related to ICT, all demonstrating recognition of the importance of ICT as a critical enabler of the country's development ambitions. These reports frequently include

security as a component of a comprehensive ICT strategy. In recent years, the government has focused more specifically on cybersecurity, which has resulted in a broad range of recommendations intended to improve the security posture of both the government's ICT environment as well as to advocate for cybersecurity across the country more generally.

145. According to assessment participants, the recent focus on cybersecurity by the government has led to an improving cybersecurity stance within the government. That is, participants noted that key agencies of the government were beginning to recognise the importance of a secure environment. For example, it was noted that recent moves to centralize the administration of all government systems into the Office of E-Government was designed to allow for better monitoring and control of access. Several participants in the technology field mentioned also the growing, albeit at a slow pace, of opportunities for cybersecurity specialists, with one noting that he had been working as a systems analyst for just a few months before he was encouraged to start working as an information security officer in government.

146. All these developments demonstrate that within the Government of Malawi there is a growing interest and understanding of the importance of cybersecurity. However, this is only prominent within the leading agencies and with less indication that it is currently based on an awareness of risks and threats. For example, there is no indication that the government is developing any internal capacity to monitor systems or to create a senior position to lead government cybersecurity efforts.

147. Within the private sector there is a more substantial mind-set for cybersecurity developing, but mainly within leading firms, and mostly in the telecommunications and financial industries, as well as some of the critical infrastructure operators. Participants report that the private sector cybersecurity mind-set has improved over the past 5 years, suggesting that incidents related in the press sent a signal to the private sector to be responsive and proactive in this area. Nevertheless, participants note that most executives are more results focused and only when presented with specific incidents does there develop an interest to invest in cybersecurity. However, as noted above, firms in some industries, most notably finance, but also others, have taken steps to implement policies and procedures that secure their environments. This includes training for their employees which, for one reported institution, involves testing and removal of access if the results of training are not satisfactory. The situation is different in smaller enterprises where, due to either the level of leadership comprehension of the risks or the lack of resources or both, a cybersecurity mind-set has not developed nor have security measures been implemented.

148. Amongst the general population in Malawi, participants noted that the level of cybersecurity awareness needs substantial improvement, with only a limited number of individuals being aware of the risks and taking steps to protect themselves. However, some participants noted that the legislation passed in the last several years, along with the creation of a cybersecurity strategy, were milestones in the development of a more secure technology environment for the country. As a result, the beginnings of awareness have taken root, even if much more work is needed.

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Stage: Start-Up - Formative

149. Participants in the focus group discussions generally agreed that, overall, only a limited number of users in Malawi approached the Internet with an understanding of the risks and threats. They noted that Malawian culture is trusting by nature and the Internet users trusted much of what they saw on the Internet and that the service providers they used, such as the mobile money companies, would keep them safe. However, participants also expressed that the environment was changing, with more people becoming aware of the risks and threats, mainly through exposure to the limited number of news stories that they have seen or through information available on social media posts.

150. E-government services in the country are extremely limited, although they are slowly growing, and the NCS indicates an ambition to continue to develop these services. Participants noted that some immigration services were available online and the Malawi Revenue Authority[21] has links on its web site for taxpayer related services. In addition, some of the utility companies, such as the electrical authority (ESCOM), offer a portal[22] for customers as do some of the water companies.[23] Participants noted that, in their view, these services remain exceptional, but the use is slowly diffusing and growing as users gain experience and learn to trust them.

151. In the area of e-commerce, Malawi has none in the traditional sense of consumers conducting online purchasing of goods and services. This fact is illustrated by both the UNCTAD E-Commerce index,[24] where Malawi ranked 140 out of 152 countries listed, as well as in comments by assessment participants. However, commerce facilitated by the Internet does exist through individuals selling products through social media services such as Facebook and WhatsApp groups, according to focus group participants, who also note that this has been observed to have increased in recent years. The number of mobile money accounts in use has also increased, according to reports by the Reserve Bank of Malawi. For example, the RBM "National Payments System (NPS) Report - Fourth Quarter 2018" notes an increase in the number of mobile network operator (MNO) subscribers as follows:

> "The number of registered subscribers for MNO-led mobile payments rose to 5.6 million during the period under review representing an increase of 6.8 percent. However, activity rates for subscribers continue to be low as 41.1 percent of the mobile money subscribers used the service during the quarter under review. Although this represents an improvement from 32.6

[21] https://www.mra.mw

[22] https://webportal.escom.mw/iopen/#/login

[23] https://bwb.mw

[24] https://unctad.org/system/files/official-document/tn_unctad_ict4d14_en.pdf

percent recorded at end of December 2017, there is still need for more interventions by all relevant parties to increase activity of customers using mobile money for payment of goods and services."[25]

152. The same report for the second quarter of 2020[26] notes that the number of subscribers has increased to 7.2 million. While these reports note that the majority of transactions is for cashing in and out of the system, the second quarter 2020 report notes that there are substantial transactions for person-to-person and business-to-business. The rise in mobile financial transactions indicates that individuals trust these internet-enabled mobile systems. However, an examination of the web sites for the mobile operators of these systems did not provide clear information regarding the risks associated with using these systems or how to remain safe.

153. Even though the country does not currently have an e-commerce environment and even though e-government services are limited, the country has demonstrated an ambition to create a more robust environment for these services. The NCS includes an objective, number 14, to "Enhance trust and confidence in cyberspace, especially in applications relating to e-Government and e-commerce," which is part of intended for "increased usage of e-Government and e-commerce services, and consequently driving further social and economic development in Malawi."

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 protection of personal information online, and whether they are sensitised to their privacy rights.

Stage: Start-Up - Formative

154. The Electronic Transaction and Cyber Security Act of 2016 established many parameters for the use of online services, including for the management and protection of personal data. The act notwithstanding, the prevailing view of most participants in the assessment indicated that internet users lacked an understanding of how personal information was handled online. Participants pointed out that most users freely share personal information online, with few concerned with the details of user agreements for the services they use. However, some participants suggested, based on anecdotal observation, that awareness of personal data appears to have improved in recent years due to a visible decrease in the amount of personal data appearing in social media. Furthermore, as noted in the Legal Frameworks factor of Dimension 4, any limitations regarding the data protection provisions of the 2016 ETCSA are being addressed as part of more comprehensive data protection act, which is currently under development.

[25] https://www.rbm.mw/Home/GetContentFile/?ContentID=29671

[26] https://www.rbm.mw/Home/GetContentFile/?ContentID=40789

D 2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning 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 - Formative

155. The assessment revealed that there are very few channels for the reporting of Internet-related crimes, such as online fraud, cyberbullying, child abuse online, etc. Participants noted that, overall, these reports go through law enforcement channels. However, the Internet Watch Foundation does operate in Malawi[27] and takes reports of child sexual abuse, and the organization Youth Net and Counselling (YONECO)[28] is also accepting reports of child abuse via a telephone hotline. These services do not appear to be well advertised as not many participants were aware of them. Going forward, the telecommunications regulator, MACRA, was viewed as the most promising channel for future efforts in reporting all incidents. Some participants also noted that the mobile money operators accept reports of fraud through their normal support channels.

D 2.5 MEDIA AND SOCIAL MEDIA

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

Stage: Formative

156. Although there does not appear to be substantial traditional news coverage related to cybersecurity, a search of the major online press sites reveals that occasional coverage does exist. Some stories focus on events outside of the country, such as cyberbullying,[29] however, most of the press coverage has a local connection, including one urging responsibility in the use of social media and other digital platforms[30] and another recounting how prisoners are using mobile telephones to defraud people outside the prisons.[31] A search for the term "cyber" on the Malawi24[32] web site returned more than 10 stories of local cybersecurity and/or cybercrime interest from

[27] https://www.iwf.org.uk/news/malawi-takes-vital-step-to-remove-online-child-sexual-abuse-from-internet-by-launching-a

[28] https://yoneco.org

[29] https://times.mw/girls-demand-action-on-cyber-bullying/

[30] https://times.mw/network-condemns-cyber-crimes-urges-government-to-act/

[31] https://times.mw/when-cyber-criminals-infiltrate-prisons/

[32] https://malawi24.com

the past 4 years, the web site Malawi Voice carried several recent stories,[33] all within the past year, and the Malawi Government's news service,[34] carried several stories about the activities in the public sector related to cybersecurity and cybercrime.

157. A review of the social media channels for several of the major telecommunications and Internet Service companies (TNM, MTL and SkyBand) revealed little or no mention of, or information about, cyber risks. However, several focus group participants mentioned that these companies use their social media accounts to communicate warnings to their followers and that the security and law enforcement services utilize traditional medial to communicate warnings regarding scammers on social media.[35]

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *cyberculture 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 MIND-SET

R2.1 Review and update as necessary the 2014 Public Sector Technology Standards with a focus on the security components of the standards (see D5.1).

R2.2 Intensify efforts across government agencies to enhance the understanding of cybersecurity risks and threats by, initially, ensuring that all public sector employees at all levels of government have reviewed and understood the security components of the 2014 Public Sector standards. Establish a team of focal points across the government who can answer questions about and advocate for the standards.

R2.3 Create and deliver to all senior government officials a briefing on cybersecurity risks and threats to government ministries.

R2.4 Engage with private sector business associations to create and deliver briefings on cybersecurity risks and threats to businesses large and small.

---

[33] http://www.malawivoice.com/2020/04/16/macra-warns-against-covid-19-cyber-crime-offences/; http://www.malawivoice.com/2020/03/07/macra-on-track-in-cybercrime-awareness/; http://www.malawivoice.com/2020/10/11/malawians-warned-against-posting-photos-of-children-on-facebook-whatsapp/;

[34] https://www.manaonline.gov.mw/

[35] https://www.nyasatimes.com/police-warns-malawi-women-on-scammers/

R2.5 Prepare and deliver to small business owners information that clearly outlines the risks and threats that cybersecurity present to their livelihoods and the basic steps they can take for mitigating the risks and threats.

R2.6 Utilize traditional and social media channels to share information on incidents and best practices among organisations and across sectors to promote a proactive cybersecurity mind-set.

TRUST AND CONFIDENCE ON THE INTERNET

R2.7 Encourage internet service providers (ISPs) to establish programmes that promote trust in their services based on measures of effectiveness of these programmes.

R2.8 Promote use of e-government services and trust in these services through a coordinated programme including the compliance to web standards that protect the anonymity of users.

R2.9 Ensure that security measures are in place for existing e-government services for businesses and public organisations.

R2.10 Encourage government leaders to creatively utilize social media channels to promote the use of e-government services.

R2.11 Encourage the development of e-commerce services emphasising the need for security (e.g., use of SSL encryption, post trust certificates/logos of third-party authentication services on the homepage).

R2.12 Ensure that the private sector applies security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.13 As part of awareness campaigns, and in collaboration with civil society and the private sector, promote the understanding of the importance of protecting personal information online among users. Promote the development of their skills to manage their privacy online.

R2.14 Using traditional and social media channels, encourage a public debate regarding the protection of personal information and about the balance between security and privacy.

REPORTING MECHANISMS

R2.15 As a matter of urgency establish a centralized reporting mechanism along with clear channels, including a telephone hotline, a website and, if possible, a localized mobile app for reporting and addressing cyber incidents.

R2.16 Raise awareness about new and existing reporting channels among the wider public and across stakeholder groups and cooperate with the private sector in this regard.

R2.17 Create online and printed guides to educate the public, teachers and parents about the types of cybercrime that can be reported, how to exercise their rights when falling victim to such crimes, and how to report it.

MEDIA AND SOCIAL MEDIA

R2.18 Enhance the understanding of cybersecurity among media providers (e.g., journalists and editors) and facilitate a more active role for media in conveying information about cybersecurity to the public.

R2.19 Encourage media content providers to proactively disseminate information on good cybersecurity practices that users can pursue to protect themselves or to respond to cyber incidents.

R2.20 Engage with leading social media actors to enhance their understanding of cybersecurity topics and issues and encourage and incentivize them to convey good personal protection practices to their audiences.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

158. This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D 3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Stage: Start-Up

159. Malawi does not have a national programme for raising cybersecurity awareness, nor do other structured awareness programmes exist. As noted in dimension 2, awareness of cybersecurity is low in Malawi, but participants suggested that awareness is growing within the country, mostly through exposure to limited media reporting, some initiatives by private sector entities like telecommunications and financial institutions, and personal experience. Some awareness events have occurred, notably around the international Safer Internet Day (SID) initiative. The June 2020[36] issue of "MACRA Magazine" reports that for the third year running Malawi has participated in SID with an event that featured workshops on issues such as cyberbullying and online child trafficking. In addition, the December 2019[37] edition of the magazine featured a story about social media threats. In the private sector, participants indicated that some staff members have received briefings or attended required cybersecurity training offered by their employers. Malawi also does not have any awareness programmes targeting executives.

[36] https://www.macra.org.mw/?page_id=12733#
[37] Ibid

160. While Malawi does not have a structured awareness programme, the NCS recognized the value of awareness by including "Cybersecurity awareness and collaboration" as one of six "focus areas," along with an objective to "Enhance cybersecurity awareness across the general public and national institutions." This objective contains four action items:

- *Undertake a nationwide assessment to determine level of awareness of cybersecurity across the nation*
- *Develop and implement a national roadmap for improving awareness of current cybersecurity trends and threats*
- *Develop and disseminate National Cybersecurity Best Practices to ingrain a cybersecurity mindset in the public*
- *Undertake mandatory training of Board Members of different organizations to enhance their understanding of cyber issues and how their organizations address these threats*

161. In addition, the strategy includes, within its objective to "strengthen online safety for vulnerable groups, especially children" an action to "Deploy special awareness programmes to target and inform children and other vulnerable groups about safe and responsible use of the internet".

162. The activities associated with the actions indicated in the NCS include, *inter alia*, the creation of a web site with information on current cybersecurity threats, risks and vulnerabilities, awareness campaigns, and mandatory trainings for board members. The NCS places the Malawi telecommunications regulator, MACRA, along with the national CERT, as lead or supporting agencies for these activities, along with other ministries and critical infrastructure operators. The indicators for these activities focus mainly on the number of campaigns or training programmes delivered, however the strategy may want to consider assessing the effectiveness of the awareness trainings and adjust the trainings accordingly.

D 3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high-quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Formative to Established

163. Malawi, through the NCS, has recognised the need to enhance the cybersecurity education, training and skills in the country, and in that direction, the NCS has also set out the following actions:

- *Integrate and promote cybersecurity research and development activities within the National Research Agenda.*
- *Creation of a National Centre of Excellence for cybersecurity training and research.*

- *Revise the primary, secondary and tertiary level curricula to integrate cybersecurity components.*
- *Support cybersecurity competitions and research and development projects at the school and university level.*
- *Build collaboration channels between the academia and private sector to develop new degrees, academic programmes and internship programmes on cybersecurity based on their needs.*
- *Develop a national career progression policy to promote continuous training and education.*
- *Develop and implement cybersecurity training and capacity building plans for Government staff.*
- *Develop and implement a national recruitment and retention strategy.*

164. Some participants from academia pointed out that public schools provide IT courses that include only basic elements of cybersecurity to secondary-level students. All private schools deliver IT courses with basic cybersecurity components to both primary and secondary-level students. As mentioned above, NCS sets out some activities in this area, including the review of the existing material and integration of more cybersecurity components into the school curricula.

165. Some participants said that it is unclear how often the material of those courses is revised, and which stakeholders are involved in the review process. Some participants also pointed out that the Ministry of Education should ensure that both public and private schools are delivering the same content and material for those courses, so there is no distinction between private and public education.

166. Currently, there is no national budget focused on the development of cybersecurity education in the country; however, MACRA, the Ministry of Education and other stakeholders plan to allocate sufficient financial resources to implement the NCS activities, including the activities in this particular area. Some participants pointed out that MACRA, as the NCS implementing authority, should approach private sector organisations, such as Microsoft, to obtain technical guidance and financial support to accomplish those activities.

167. At the university level, NCS also recognises the need to strengthen cybersecurity education by developing more cybersecurity-focus degree programmes. It was also noted that some universities in Malawi offer accredited cybersecurity-related laboratories or courses within their degree programmes - undergraduate, graduate and post-graduate/doctoral.

168. Some participants pointed out that the following degree programmes are being offered in Malawi:

- *Mzuzu University: MSc. and PhD programmes in Information Theory Coding and Cryptography*
- *St. John The Baptist University: BSc. in Computer Science and a Diploma in Computer Science*
- *Daeyang University: BSc. In Information*
- *University of Livingstonia: BSc. In Computer Engineering*
- *Malawi University of Science and Technology (MUST): BSc. In Systems and Security which has the following course: Cryptography I & II, Computer Security, Cybersecurity, Ethical Hacking, Information Security, Mobile and Wireless Network Security, Digital Forensics, and Advanced Network Security*
- *Malawi Polytechnic: BSc. In Computer Science and BSc. In Information Systems*

- *University of Malawi: BSc. In Computer Network Engineering and MSc. In Informatics*
- *UNICAF University: BSc. In Computer Science and BSc. Security Systems*

169. Some participants from academia recognised that the MSc. and PhD programmes in Information Theory Coding and Cryptography and the BSc. programme in Computer Systems and Security are the only degree programmes in cybersecurity. It was also noted that one university recently developed a master's degree programme in Information Security and Digital Forensics, but it has not been rolled out yet. This specific master's degree programme was tailored to meet the industry requirements. It was also noted that this type of consultation with the industry and other relevant stakeholders is broadly carried out when new degree programmes are developed.

170. Some participants from academia indicated that cybersecurity courses are in demand. It was noted that one university offers a master's degree programme with specific cybersecurity-related courses. At the graduate level, the Network Engineering programme, which contains some cybersecurity-related courses. It was noted that in some universities, the enrolment rate is restricted due to the lack of academics, limited infrastructure and other factors. In essence, the appetite for cybersecurity education is growing, not exponentially as yet, but the interest is there.

171. Some participants indicated that there is a small cadre of cybersecurity educators in Malawi. Hence, there are not sufficient academics to supply the current demand for cybersecurity-related courses. It was noted that those academics are locals and have been mainly trained in Malawi. Some participants from academia pointed out that universities ensure that their academics hold the best qualifications, at least master's degrees, industry certifications and vast experience in the field. It was noted that in the degree programmes mentioned above, none of the lecturers hold PhD degrees in the field. Some participants indicated that the majority of the existing educators work either for the government or for the industry, and participants suggested that there are limited incentives for cybersecurity specialists to become a full-time lecturer.

172. Some participants from academia pointed out that post-secondary educational institutions in Malawi do not mandate any specific qualification programme for cybersecurity lecturers. They usually pursue either master's degree programmes locally or take industry certification to obtain advanced knowledge in some particular areas. Indeed, this is one aspect of cybersecurity education that needs to be strengthened. MACRA and other stakeholders are aware of this situation.

173. Some participants pointed out that universities and other education bodies are not currently offering seminars or lectures on cybersecurity issues aimed at the non-specialist. However, international and local NGOs and private organisations are regularly organising Webinars targeting a broad audience, including non-specialists, on basic and advanced cybersecurity issues. It was noted that a couple of universities are presently conducting research and development projects in cybersecurity, but still have low impact. NCS also has some activities to enhance the research and development activities in the country.

174. Some participants from the academic sector pointed out that there are no specific scholarship programmes or student loan programmes available for both students and lecturers who want to pursue cybersecurity-related degree programmes. However, there are national scholarship programmes of which both students and lectures interested in those degree programmes can benefit from. Even though the scholarship/student loan components were not considered in the NCS, some

participants pointed out that this issue could be addressed and integrated into the national career progression policy.

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Stage: Formative

175. As noted above, NCS sets out to develop a National and Career Progression Policy, which aims to promote continuous training and education for cybersecurity incident response. Some participants indicated that the Government, through the NCS implementing agencies, has expressly recognised the need for professional training opportunities in cybersecurity matters. Some participants stated that they have high expectations on the development and implementation of this policy to see what kind of benefits and incentives will be granted. It was noted that this policy has not been developed yet.

176. Some participants pointed out that some professional training companies (e.g., 2KO Malawi) and universities (e.g., UNICAF) in Malawi offer ICT professional certifications with some security modules or components, such as ITIL Foundation, Lean IT, Cisco, Microsoft, Linux, Oracle, Sun, LPIC, and others. Some internationally accredited IT Security and Governance training and certification courses are also offered in Malawi, such as Ethical Hacking Foundation Training and Certification, COBIT 5 Foundation Certification Training Course, CGEIT Course, CRISC Course, COBIT 5 Assessor Certification Training Course, COBIT 5 Implementation Certification Training Course. CompTIA certifications are also available. Some participants from academia pointed out that those courses and certifications are in demand, but the Government and the private sector need to work closely to create some incentives to attract more students and professionals to the cybersecurity field.

177. It was noted that the domestic offering is limited, but a lot of IT and security courses and certifications are now offered virtually, so IT and security professionals in Malawi have access to unlimited resources and options. Some participants pointed out that the cost of industry certifications is indeed a constraint. It was noted that some private sector organisations subsidise the registration fee for those certifications. During the CMM review, there was no record that government agencies are doing the same to incentivise their employees.

178. It was also noted that it is hard for the government agencies to retain highly skilled staff, so the Government plans to develop some recruitment and retention policies which are described in the NCS. According to some participants, those actions should consider the creation of a scholarships fund or other type of incentives to incentivise their employees not only to develop a cybersecurity career but also to retain highly skilled staff.

179. Some participants highlighted that cybersecurity professionals occasionally get together in informal and formal activities to discuss internet governance and cybersecurity issues. It was noted that the ICT Association of Malawi is one of the forums available in the country. This association organises annual conferences to discuss relevant topics in different areas, including cybersecurity and privacy. A group called "Cyber Friends" was created in 2019 to share information and provoke debate on cybersecurity issues in Malawi. Last year, this group organised a conference. Due to the pandemic, it was noted that the discussions now take place via WhatsApp or other digital platforms.

180. Some government representatives pointed out that there are no records of any cyber competition or similar activities in the country whose primary purpose is to incentivise and promote cybersecurity careers amongst local students. However, NCS sets out some activities in that direction. MACRA and other local authorities are aware of this situation and will implement some activities to close gaps.

181. It was noted that some private sector companies have implemented knowledge transfer policies. Although there is no official knowledge transfer policy within the government sector, it was noted that some government agencies are starting to implement some knowledge transfer activities.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *cybersecurity education, training and skills*, the following set of recommendations are provided to Malawi. 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.

AWARENESS RAISING

R3.1 Ensure that the awareness roadmap is developed in collaboration with input from relevant stakeholders, including cybersecurity specialists in the private sector, civil society, and academia.

R3.2 Ensure that the content of the awareness roadmap included in the NCS contains modules targeting teachers and be integrated into ICT literacy initiatives in schools.

R3.3 Ensure that the content of the awareness roadmap included in the NCS contains modules targeting media professionals, to allow them to better understand the issues and encourage them to report more frequently and accurately on cybersecurity topics.

R3.4 Establish metrics for assessing cybersecurity awareness raising programmes and ensure that evidence of application and lessons learnt feed into existing and newly-developed programmes.

FRAMEWORK FOR EDUCATION

R3.5 Following the activities on the NCS, leading authorities should ensure that primary and secondary-level students, from both public and private schools, have access to the same IT courses and material and the government should define the minimum level of cyber security education as a national standard for all education institutions. Also, strengthen the cybersecurity content of those courses.

R3.6 Consider creating cybersecurity education programmes for primary and secondary school teachers to ensure that they also have the knowledge and skills necessary to integrate cybersecurity education into training and learning curriculum successfully.

R3.7 At tertiary level, consider developing more formal cybersecurity education programmes for academics and instructors to ensure that skilled staff is available in the country to teach newly formed or existing cybersecurity courses.

R3.8 Leading authorities should consider developing incentives to attract more security professionals to the teaching field.

R3.9 Consider integrating cybersecurity content in all (technical and non-technical) degrees at universities.

R3.10 Develop more specialised cybersecurity courses and degrees in universities and other higher education bodies to supply the domestic market's needs.

R3.11 Expand the availability of cybersecurity and cybercrime courses to students of non-technical study programmes, such as law, criminology or management studies. Also, promote the multi-disciplinary nature of cybersecurity (technical, legal, policy, business, amongst others).

R3.12 Promote efforts by universities and other education bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists.

R3.13 Review regularly the materials of those courses and programmes mentioned above. Develop and collect effective metrics to gather feedback from existing students, teachers, academics and other key stakeholders (including the industry)

and evaluate the present offerings in cybersecurity to define and inform cybersecurity education priorities.

R3.14 Allocate additional financial resources for public universities to expand and enhance their existing infrastructure, including laboratories, equipment and other facilities, to meet the growing demand for formal education in cybersecurity.

R3.15 Develop public-private partnerships for both sustainable and high-level research and development programmes and guidance and support in other areas.

R3.16 Provide more opportunities for individuals (such as students and experts) to gain experience, through internships and apprenticeships, to enhance their expertise by combining education and practical training.

R3.17 Strengthen free-tuition programmes for university education and/or create a national fund for both scholarship and student loan programmes, so that students and professionals who want to initiate or strengthen their security career development can take cybersecurity degree programmes or professional certifications. Ensure that all cyber-related courses and degrees are affordable.

R3.18 Market cybersecurity as an important career option by using different marketing methods. The Government and/or industry should consider creating competitions and initiatives for students to increase the attractiveness of cybersecurity careers.

R3.19 The Government, in collaboration with private sector organisations, should consider creating academic centres of excellence in cybersecurity.

R3.20 Consider creating and maintaining a defined incentive plan to keep experienced and skilled cybersecurity experts not only in the country but also in public services.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.21 Consider appointing a designed body or committee which, in cooperation with all role players, should be responsible, amongst others, for coordinating the development of skills towards building a cadre of cybersecurity-specific professionals. As part of its functions, this body or committee should identify training needs and develop training courses and online resources for targeted demographics, including non-IT professionals.

R3.22 Develop a central platform or portal for coordination and sharing training information for experts.

R3.23 Create a national-level register of cybersecurity experts.

R3.24 Ensure that affordable security professional certifications are offered across sectors within the country. Different forms of professional cybersecurity certification, e.g. ISACA certifications, will provide suitable skills at a faster rate.

R3.25 Consider subsidising the (high) cost of training and certification courses for trainees.

R3.26 Develop metrics to evaluate the take-up and success of cybersecurity training courses to strengthen the current offerings and inform future training programmes. This metric system should be managed by the body described in Recommendation R3.22.

R3.27 Establish job creation initiatives for cybersecurity professionals and students within the organisations and encourage employers to create cybersecurity positions based on their needs and also train their staff to become cybersecurity professionals.

R3.28 Consider creating special initiatives to retain skilled cybersecurity professionals.

R3.29 Consider developing and implementing a formal knowledge transfer policy across all sectors to foster and promote this practice at all levels of government, private sector organisations, CI operators, among others.

R3.30 Promote the creation of networking platforms and/or professional associations which can organise cybersecurity-related events (seminars, workshops, etc.) and get cybersecurity professionals together regularly for training and networking purposes.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

182. This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D 4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Stage: Formative to Established

183. Malawi has developed ICT legislative and regulatory frameworks addressing cybersecurity and cybercrime issues. However, two issues have to be addressed: (i) better implementation and enforcement of existing domestic laws and the Constitution, and (ii) some specific topics require either new law and regulations or the strengthening of the current frameworks, such as: the protection of the national CI and CII, incident reporting obligations, data protection, cybercrime procedural provisions, child protection online, amongst others. Legislation protecting the rights of individuals and organisations in the digital environment has been adopted. Some participants also pointed out the need to regulate the issue of fake news and fake accounts on social media outlets which have caused a great impact in the stability of the country.

184. The most relevant legislative frameworks related to Malawi's Internet and cybersecurity are:

- ***Electronic Transactions and Cyber Security Act (2016)*** **
- ***Communications Act (2016)*** **

** consulted as part of the drafting and enactment process.

185. It was noted that the ***Electronic Transactions and Cyber Security Act of 2016*** (ETCSA 2016) addresses cybersecurity-related issues, such as the establishment and administration of the MW CERT, formation and validation of electronic transactions (electronic signature, admissibility and evidential weight of electronic messages, the validity of contracts in electronic form, etc.), consumer protection, the liability of online intermediaries and content editors and protection of online users, electronic commerce, security and digital economy, data protection and privacy, domain name and management, electronic government transactions, cybercrime offences, amongst others.

186. The ***Communications Act of 2016*** (MACRA-CA 2016) addresses cybersecurity-related issues, such as consumer protection for the communications sector users, cyber-related offences (unlawful intercept, disclosure of content, sabotage and theft, interference with the transmission of electronic communications), amongst others.

187. While Malawi has not adopted specific legislation on human rights online, the Constitution of the Republic of Malawi of 1994,[1] in its Chapter IV, safeguards the following human rights and freedoms:

- *Section 19. Human dignity and personal freedoms*
- *Section 20. Equality*
- *Section 21. Privacy (personal searchers, home or property, seizure of private possessions or interference with private communications-mail and all forms of telecommunications)*
- *Section 32. Freedom of Association*
- *Section 34. Freedom of Opinion*
- *Section 35. Freedom of Expression*
- *Section 36. Freedom of Press*
- *Section 37. Access to Information*
- *Section 38. Freedom of Assembly*

188. Several participants pointed out that both constitutional and ordinary courts protect human rights equally in offline and online settings.[2] ETCSA 2016, in its section 24, sets out that no limitations to online public communications will be established, except for those communications that promote crimes against humanity, human dignity and pluralism in the expression of thoughts and opinions. It was also noted that one of the guiding principles of the NCS is the *"respect for the rule of law and human right" which means that the NCS is aligned with the laws enforced in Malawi and that NCS aims to facilitate the promotion, protection and enjoyment of fundamental human rights and freedoms in online environments.*

189. Some participants also pointed out that the constitutional and legal provisions which protect the human rights both online and offline are there, but it is the Government and other public institutions (e.g., Court System) which have to enable, promote and enforce those provisions to ensure that the citizens are adequately protected.

190. Even though privacy online has become a major concern for Malawians, the reality is that the level of awareness amongst the citizens is still low. During the Presidential election, some participants noted a lot of negative reactions on social media outlets which caused infringements to privacy online. This situation provoked the local legal fraternity to start debating on how to protect privacy online. Some participants also said that they expect awareness-raising campaigns from MACRA, as the ETCSA 2016 authority, to enhance the digital culture of the citizens.

191. Malawi is a signatory of multiple international treaties on human rights, such as International Covenant on Civil and Political Rights, International Covenant on Economic, Social and Cultural Rights, and U.N. Conventions, such as the Geneva Convention relating to the Status of Refugees, the Convention against Torture, the Convention on the Rights of Persons with Disabilities, the Convention on the Rights of the Child, the Convention on the Elimination of All Forms of Discrimination against Women and the Convention on the Elimination of All Forms of Racial Discrimination. Also, standards established by the jurisprudence of the U.N. Human Rights Committee are binding for Malawi.

192. It was noted that the ETCSA 2016 sets out only four data protection legal provisions which seem to be influenced by international standards and best practices; however, their scope is very limited. Those legal provisions regulate the processing of personal data and define the rights of the data subjects and set the obligations of the data controllers. It was noted that there are no clear enforcement mechanisms in place, and no Data Protection Authority was created.

193. During the CMM review, some government representatives pointed out that they are aware of the existing limitations of those data protection provisions in the ETCSA 2016. It was also noted that a consulting firm drafted the "zero draft" of the comprehensive data protection legislation. MACRA has made some preliminary comments, and they will be integrated into this draft. A task force will also review such a draft. Finally, the updated data protection draft will be submitted to public consultation (some workshops will be organised) before heading to Parliament for approval. It was noted that MICT is championing this specific Bill Some participants indicated that this Bill is one of the activities promoted by the "Digital Malawi" project.

194. It was also indicated that this data protection draft would propose the establishment of the national Data Protection Authority (DPA). However, there was some debate on this particular issue because the Government had said that there are no funds to create a new government agency. DPA's functions may likely be delegated to an existing agency, such as MACRA or the Competition Commission.

195. Some participants also pointed out that Malawi has not ratified the Convention on Cybersecurity and Personal Data Protection (known as the "Malabo Convention") developed by the African Union in 2014. It was noted that the only reason why Malawi is not part of this Convention is the lack of knowledge and awareness of the Ministry of Foreign Affairs and International Cooperation and other stakeholders. It is recommended that Malawi adopt a comprehensive data protection legislation first, and then seek to join the Malabo Convention and other internationally recognised conventions, such as the Convention 108+ (Council of Europe).

196. Currently, Malawi does not have a specific law on child protection online, but some stakeholders pointed out that there is a constitutional provision on children's rights (section 23), and there is also a general law called Child Care, Protection and Justice Act of 2010[4] which sets out a few legal provisions against child sexual exploitation and child pornography.

197. ETCSA 2016 also sets out some provisions related to child pornography in electronic form, punishing the reproduction, sale, purchase, distribution and possession of child pornography material (section 85). It also establishes some restrictions on online public communications, such as the prohibition of child pornography material (section 24).

198. It was noted that in 2017 ITU organised a three-day workshop on child online protection (COP) in collaboration with MACRA. There, MACRA committed to developing robust COP legislation with the support of ITU and other international and local stakeholders. As part of that process, ITU engaged a COP consultant who led some workshops in Malawi and this consultant supposed to prepare the final COP assessment report. However, some participants pointed out that the ITU consultant never delivered this report. Some government representatives during the CMM sessions committed to following up on this report with ITU/MACRA and also expediting the process for the development of the COP legislation. As plan B, some government representatives proposed that MACRA should approach UNICEF, GSMA and other international organisations to provide technical support on developing the COP legislation.

199. In Malawi, the Internet Watch Foundation (IWF), in collaboration with Youth Net and Counselling (YONECO), MACRA, Ministry of Gender and other local authorities, launched in 2018 an online reporting portal (https://report.iwf.org.uk/mw), which is available for web users to report online images and videos of child sexual abuse.[8]

200. YONECO is also managing the national Tithandizane Child Helpline (toll-free number - 116). There, people can report child abuse cases. It was also noted that MACRA delegated this function to YONECO.

201. At the international level, Malawi ratified some international instruments, treaties and conventions which are relevant for this CMM review, including but not limited to, the African Charter on the Rights and Welfare of the Child, ratified in 1999, and the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography; accession in 2009.

202. The generally accepted international benchmarks for child protection from online sexual exploitation are found in the Budapest Convention and the Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse.[5] Although Malawi is not a signatory to these two conventions, they can be used as model laws for implementation in the country.[6]

203. Consumer protection in Malawi is presently regulated through a general law called the Consumer Protection Act of 2003 (CPA 2003). The ETCSA 2016 also establishes some provisions regarding consumer protection on electronic transactions, such as the information that should be provided by the supplier, cooling-off period, formation and performance of electronic transactions, review and cancellation of contracts by consumers, the prohibition of misleading advertising, unsolicited communications, the right to withdrawal from a contract, amongst others. Even though the general public lodges complaints of this nature before MACRA (the authority in charge of enforcing the ETCSA 2016), it was noted that MACRA does not have any dedicated officer or department within its structure that deals with consumer protection online issues.

204. According to the World Intellectual Property Organisation's (WIPO) website, the Copyright Society of Malawi (Ministry of Tourism, Culture and Wildlife) and the Department of the Registrar General (MoJ) are the competent government agencies in Malawi responsible for leading the intellectual property (IP) protection in the country, including the copyright and industrial property matters.[9]

205. The current IP protection framework in Malawi is composed of various laws, but these are two primary laws:

- ***Copyright Act, 2016 (Act No. 26 of 2016).***[10] *It was noted that this legal body sets out the definition of a computer programme and states that computer programmes are protected under the category of literary work.*
- ***Trademarks Act, 2018 (Art No. 2 of 2018)***

206. Some participants pointed out that ETCSA 2016 does not contain any legal provision regarding infringement of intellectual property rights.

207. At the international level, Malawi is also a member of the African Regional Intellectual Property Organisation (ARIPO), which is an inter-governmental organisation that facilitates cooperation among member-states in intellectual property matters to pool financial and human resources and seek technological advancement for economic, social, technological, scientific and industrial development.[11] Malawi is also a party to the following treaties and protocols: Banjul Protocol on Marks since 1993, Harare Protocol on Patents and Industrial Designs since 1982,[12] Berne Convention since 1991, Marrakesh Treaty since 2017, and TRIPS since 1995.[13] It was also noted that Malawi is not part of the WIPO Copyright Treaty and the WIPO Performance and Phonogram Treaty, both are internationally recognised as the 'Internet Treaties.' It is recommended that Malawi join these two conventions to strengthen its IP legislation.

208. Some participants pointed out that ETCSA 2016 sets out several substantives cybercrime provisions which describe the following cybercrime offences: unauthorized access, interception or interference with data (section 84), child pornography (section 85), the prohibition of cyber harassment (section 86), the prohibition of offensive communication (section 87), prohibition of cyberstalking (section 88), the prohibition of hacking, cracking and introduction of virus (section 89), unlawfully disabling a computer system (section 90), the prohibition of spamming (section 91), the prohibition of illegal trade and commerce (section 92), attempting, aiding and abetting crimes (section 93), offences committed by legal persons (section 94) and general offences and penalty (section 95).

209. It was also noted that ETCSA 2016 falls short in the cybercrime procedural provisions; it is almost limited to the search warrant provisions (section 83) and the admissibility of electronic messages in court proceedings (section 16). On the website of the Council of Europe, there is a country profile for Malawi which describes the cybercrime policies, strategies and laws in the country and the Malawi profile reports that limited references to procedural powers in Part X Offences of ETCSA 2016.[14]

210. The CMM review team also reviewed the Criminal Procedure and Evidence Code (Cap 8:01 of the Laws of Malawi), and the main finding is that there are no provisions which explicitly recognised the electronic evidence and that describe the rules of its admissibility in court proceedings. The lack of procedural provisions which recognise electronic evidence in court proceedings is indeed an issue to investigate, prosecute and try cybercrime cases in Malawi. It is a critical area which needs to be strengthened.

211. It was also noted that the existing Extradition Acts (Cap. 8:03 of the Laws of Malawi), including bilateral arrangements, and the Mutual Assistance in Criminal Matters Act (Cap. 8:04 of the Laws of Malawi) have some procedural provisions which may complement the limited procedural powers of the ETCSA 2016, especially in cross-border cybercrime cases. It was noted that Malawi is not yet a signatory of the Budapest Convention and the Malabo Convention, which will strengthen the substantive and procedures powers of the domestic cybercrime legislation in order to

tackle the current cybercrime activities. It was noted that Malawi has not approached the Council of Europe yet (not even for capacity building purposes) to start the discussions on joining the Budapest Convention. MACRA and MoJ are working closely to identify which international treaties and conventions are relevant for Malawi's interests.

212. It is recommended that Malawi authorities conduct, with the support of the Council of Europe or any other international organisation, an exhaustive assessment of the current substantive and procedural cybercrime provisions to identify the existing gaps and harmonise the existing cybercrime legislation with internationally recognised standards and best practices. Joining the Budapest Convention is also a recommended step to strengthen the capacities of the local authorities to fight against cybercrime.

D 4.2 CRIMINAL JUSTICE SYSTEM

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Formative

213. Some participants pointed out that the Malawi Police Services (MPS) established a Cybercrime Investigation Unit. It was noted that this Unit has two investigators for the entire country who have basic skills, but more training is required, especially in the digital forensic field. The last training in digital forensics they had was three or four years ago. Some training has been delivered through the U.S. Federal Bureau of Investigation. Some government representatives also pointed out that international cooperation must be enhanced to obtain additional support from reputable international organisations.

214. In terms of tools and equipment, this Unit is seeking to enhance its basic office equipment and acquire their first equipment and tools to deal with digital forensics. Some participants pointed out that this Unit does not even have computers for its daily operation. In the absence of tools, it was said that those investigators implement internationally recognised standards and procedures to ensure the chain of custody and digital integrity. It was noted that the Cybercrime Investigation Unit depends financially on MPS.

215. Some government representatives indicated that currently there is no Digital Forensic Laboratory in place. MACRA and Malawi Police Service entered into an agreement in which MACRA will fund the establishment of the Digital Forensic Laboratory (DFL) within the MPS. This support will cover the design, supervision and construction of the DFL, which will have high tech equipment to assist the Police to solve highly technical cases using electronic devices and information technology. The DFL will be constructed on the MPS' facilities (headquarters) and is expected to be completed in 2021.

216. To tackle the existing challenges, this Unit urgently requires (i) digital forensic tools, (ii) updated capacity building to be exposed to new skills and ways to conduct digital forensics and digital evidence gathering, and (iii) more personnel, including more investigators (understaffed) to be able to deal with the cybercrime activities for the entire country. Some participants pointed out that this Unit will hire more people soon.

217. It was noted that ETCSA 2016 created what is called Cyber Inspectors – as an alternative to fill the gaps caused by the lack of knowledge and expertise within the domestic law enforcement agencies in Malawi. The cyber inspectors are private companies/persons who are authorized by law to assist the domestic law enforcement agencies during the investigation of cybercrime activities. They are deemed an extended arm of the MPS for cybercrime investigations.

218. Some government stakeholders pointed out that the Directorate of Public Prosecution has no specialised unit for cybercrime cases. However, there are a few prosecutors who understand the fundamentals, but they may struggle with complex and cross-border cybercrime cases. It was noted that more capacity building is required and that occasional training sessions are not enough; therefore, the level of training has to aim at the specialisation level. It was noted that those prosecutors dealing with cybercrime cases are well-versed in the general procedural aspects, but investigating and prosecuting cybercrime cases require specialised skills and knowledge; that is what has to be developed. Some stakeholders pointed out that the level of communication and exchange of information on cybercrime issues between prosecutors and the judges and magistrates is still informal.

219. Some government representatives indicated that the Court System does not have a specialised unit for cybercrime cases. Even though judges and magistrates are highly versed in the application of the domestic substantive and procedural laws, it was noted that they are not fully aware of the cybercrime environment in the country nor the content and interpretation of ETCSA 2016. Therefore, they are not fully capable of judging complex and cross-border cybercrime cases. Since training has not been adequately delivered, their capacity in this specific area is minimal. Indeed, it has to be enhanced in order to increase the level of knowledge and expertise within the Court System.

220. Some participants pointed out that the Judiciary Services Commission of Malawi understands the need for providing more training opportunities to the domestic judges dealing with cybercrime cases, and therefore, they plan to deliver some capacity building sessions to strengthen some specific areas and also dive deeply into the electronic evidence aspects. It was also noted that MACRA understands the urgent need for providing more capacity building for this group, so MACRA is planning to develop a robust training programme for the members of the Criminal Justice System.

221. Even though Malawi has cybercrime legislation since 2016, not much progress has been accomplished in terms of training and capacity building within the Criminal Justice System. It was also said that there are highly skilled professionals within the Criminal Justice System, but knowledge and expertise on cybercrime have to be developed. More training opportunities are required to reach a high level of specialisation in this particular field.

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

Stage: Formative

222. It was noted that NCS is built on seven guiding principles of which three principles seek (i) domestic cooperation under the multi-stakeholder approach, (ii) international cooperation by promoting bilateral, regional and international cooperation arrangements, and (iii) the fight against cybercrime by recognising the individual and collective responsibility to take steps to combat the cybercrime activities in the nation. NCS also recognises the importance of promoting and enhancing regional and international cooperation in the protection of critical information infrastructures. Within the Critical Success Factors section, NCS also sets out that cooperation and networking among national, regional and international partners are based on mutual trust. As noted above, domestic stakeholders have a good degree of awareness regarding the importance of working closely with domestic and international partners to not only implement the NCS projects, but also combat the cybercrime in the nation.

223. Over the CMM review sessions, stakeholders from multiple sectors recognised the need to enhance informal and formal cooperation mechanisms, both domestically and internationally. Even though Malawi has made a significant effort to keep pace regarding the development of domestic cybercrime legislation since 2016, it was noted that the country still has not reached the same level of progress at the implementation and enforcement stages, which indeed must be remedied. Certainly, one of the areas which need to be improved is the creation and formalisation of domestic and international cooperation arrangements.

224. As mentioned, Malawi has not signed the Budapest Convention, but multiple government representatives pointed out that there is an interest in joining this convention. The procedural and international cooperation provisions established in the Budapest Convention would not only complement the existing cybercrime legislation, but also provide additional legal mechanisms and resources to the local law enforcement agencies to investigate and prosecute complex and cross-border cybercrime cases, mainly accessing electronic evidence in other countries. Similarly, Malawi has not signed the African Union Convention on Cybersecurity and Personal Data Protection. Both conventions contain legal provisions concerning international cooperation mechanisms and mutual legal assistance instruments among the signatory countries. It is recommended that Malawi authorities approach the Council of Europe authorities not only to begin the accession process but also join the capacity building activities.

225. As a member of the SADC community, Malawi officers have participated in multiple training events and activities, including the first SADC Cyber Drill in 2018 which served as a platform for cooperation and information sharing, and discussed the current

domestic and regional challenges, incident response capabilities and communications, as well as a hands-on exercise for national CSIRTs.

226. Malawi is also a member of the Southern African Regional Police Chiefs Coordination Organisation (SARPCCO) which is the primary force in Southern Africa for the prevention and fighting of cross-border crime. SARPCCO was formed in 1995 in Zimbabwe and has firmly established itself as a benchmark for international police cooperation. The Sub-Regional Bureau of INTERPOL supports this regional organisation in Harare which coordinates its activities and programmes.[1]

227. SARPCCO has become a cooperation and information sharing forum for cybercrime issues in the Southern Africa region. SARPCCO has been working on two regional initiatives: (i) the creation of a regional cybercrime course for law enforcement officers which is delivered once a year putting together law enforcement officers dealing with cybercrime issues from the 16 member states, and (ii) the establishment of a regional Cybercrime Centre of Excellence in line with the INTERPOL Global Cybercrime Strategy. This Centre is designed to assist member states in terms of capacity building and investigative and operational support.[2]

228. ITU collaborated with financial resources and technical assistance to conduct the CSIRT assessment in 2018, and more recently, MACRA entered into a cooperation agreement with ITU to assist with the establishment of the MW CERT. UNICEF has also worked closely with the Malawi authorities relating to child protection matters.

229. At the domestic level, a group of stakeholders said that there is an adequate level of communication between law enforcement agencies and other stakeholders from the public and private sector regarding cybercrime issues. It was noted that the Cybercrime Investigation Unit has established good communication with local and foreign ISPs and other internet service providers. For instance, it was noted that MACRA and the Cybercrime Investigation Unit work closely with Facebook and other digital platforms to investigate and prosecute cybercrime activities, such as impersonation, defamation and human rights violations (e.g., the persecution of people with albinism during the elections).

RECOMMENDATIONS

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

LEGAL FRAMEWORKS

R4.1 Conduct an assessment of the existing legal and regulatory framework to ensure that the provisions addressing ICT security, child online protection, consumer protection online, intellectual property online and cybercrime provisions are aligned with international best practices.

R4.2 Ensure that (i) the current Legislative Framework ICT Security is implemented and enforced accordingly, (ii) sufficient financial, human and technological resources are allocated to that effect, and (iii) Malawi meets international commitments (e.g., treaties, conventions and directives).

R4.3 Ensure that the domestic legislation and judicial system recognise and protect human rights online. Consider conducting a human rights review or audit to ensure that the existing legislation aligns with international standards which aim to protect human rights in online settings.

R4.4 Ensure that the draft of the Data Protection bill is aligned with international and regional standards and best practices (e.g., EU GDPR, Convention 108+, OCDE's Guidelines, Malabo Convention). Ensure that this legal body also meets Malawi's international commitments (e.g., treaties, conventions). Ensure that this Data Protection bill is broadly consulted with key stakeholders and that their feedback and comments are incorporated into the final draft.

R4.5 Ensure the establishment of the Data Protection Authority not only to enforce the Data Protection Legislation - when enacted - but also to launch a -powerful- awareness-raising campaign for the general public. Allocate sufficient financial, technological and human resources to initiate operations and that metrics and mechanics are in place to enable strategic decision-making and resources planning.

R4.6 Consider ratifying and implementing the Budapest Convention, the Malabo Convention and any other convention which aims to strengthen the substantive and procedural cybercrime provisions and international cooperation mechanisms to combat cybercrime. Ensure that Malawi complies with the international commitments to combat cybercrime, including SADC and UA's commitments and directives.

CRIMINAL JUSTICE SYSTEM

R4.7 Strengthen the domestic law enforcement capacity, mainly the Cybercrime Investigation Unit, by hiring highly skilled investigators. Also, consider developing a training plan for the next two years and incorporating some budget for specialised training, either locally or abroad, for officers and investigators to conduct complex and cross-border cybercrime cases.

R4.8 Establish digital chain of custody and evidence integrity processes, roles and responsibilities within the Cybercrime Investigation Unit and other law enforcement units.

R4.9 Ensure that the Digital Forensic Laboratory within the MPS has sufficient technological, human and financial resources to meet current and projected demands.

R4.10 Strengthen training and education of prosecutors and judges on cybercrimes issues to develop the skills and capacity to investigate, prosecute, and try complex and cross-border cases. Also, allocate additional resources for this purpose.

R4.11 Allocate sufficient financial and technological resources for prosecutors and judges dealing with cybercrime activities.

R4.12 Establish formal mechanisms, protocols and best practices to enable not only information sharing, but also cooperation between prosecutors and judges in order to ensure efficient and effective prosecution of cybercrime cases.

R4.13 Collect and analyse statistics and trends regularly on cybercrime investigations, prosecutions and convictions.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.14 Establish formal international cooperation mechanisms to combat cybercrime based on existing legal assistance frameworks, mutual legal assistance and extradition provisions, and further bilateral and international agreements (e.g., Malabo Convention and Budapest Convention, when ratified, and SADC protocols).

R4.15 Consider establishing a 24/7 point of contact within the Cybercrime Investigation Unit in order to provide instant assistance for mutual legal assistance requests.

R4.16 Facilitate informal cooperation mechanisms within law enforcement and the criminal justice system, and between law enforcement and third parties, both domestically and cross-border, in particular, ISPs. Consider expertise from other areas, such as anti-corruption cooperation.

R4.17 Allocate resources to support information sharing between the public and private sectors at the national level and enhance the legislative framework and communication mechanisms, protocols and standards.

DIMENSION 5 STANDARDS, ORGANISATIONS AND TECHNOLOGIES

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

D 5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Start-Up – Formative

231. The application of cybersecurity standards in Malawi is limited and uncoordinated. A few companies indicated that they either are currently certified as ISO 27000 compliant or are pursuing certification, but most have simply adopted policies and procedures related to cybersecurity standards. Some of these policies and procedures are based on aspects of the ISO 27000 standard or follow another framework, such as the one from NIST. In terms of industry, the finance community members that participated in the assessment noted their adoption of standards either closely based on ISO or certified as ISO. Some of these institutions are branches of international financial entities, and therefore the local entities follow their headquarters' standard. The financial regulator, the Reserve Bank of Malawi, does not require financial institutions to adopt any specific cybersecurity standard.

232. The telecommunications industry is similar to the finance in that some have adopted the ISO standard, even if they have not completed the certification process.

233. The government has not implemented any standard beyond what is described in the "Public Service ICT Standards" which were adopted in 2014. This document outlines

the procedures and policies that all government institutions should apply in eleven areas listed below with detailed descriptions in each:

- Acceptable Use of ICT Facilities in the Public Service
- Electronic Records Management
- Information Asset Classification and Control
- Information System Security Management
- Data Back-Up
- ICT Audit
- ICT Project Management
- System Development
- E-Waste Management
- Strategic and Operational Planning
- Tele-Centers Management

234. The security section includes topics such as Physical and Environmental Security, Communications and Operations Management, and Controlling Access to Information, among others. It was not clear from the interviews the extent to which these standards are applied.

235. In the areas of standards for procurement and software development, participants were not aware of any initiatives that related to either of these activities. However, the "Public Sector ICT Standards" published in 2014 covered both of these areas in substantial detail. For example, the section on "Procurement, development, and maintenance of information Systems" notes that "GoM/Organization systems will be developed in such a way that security is a fundamental element of the development project in accordance with GoM/Organization information security policy and procedures" and that "GoM/Organization shall clearly define and document security requirements of relevant information prior to construction, expansion, or procurement of a new information system."

D 5.2 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 aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Start-Up – Formative

236. Telecommunications services in Malawi are overseen by the regulator, the Malawi Communications Regulatory Authority (MACRA), which was established as an independent body through the Communications Act of 1998. A more recent review led to the passage of the Electronic Transactions and Cyber Security Act in 2016, which enhanced the functionality of MACRA.

237. As a landlocked country, Malawi depends on other countries for access to the global Internet. This connectivity comes mainly through Mozambique to the south and east and Tanzania in the north,[38] with some transit routes through South Africa via Zambia to the west. Participants reported that, over the past several years, the creation of multiple connections through these neighbouring countries has increased the reliability and resilience of connectivity. Within the country Malawi has several wide-area network providers that offer wholesale connectivity services to ISPs and provide redundancy of access to major regions of the country. The mobile market in Malawi is composed of only two operators, with some of the lowest mobile penetration rates in Africa[39] and, while the Internet market lists approximately 50 internet service providers, only about 20% are active.

238. For those who have access to the Internet, either through mobile or terrestrial services, options exist and, according to assessment participants, both from the perspective as users and providers, the service is reliable and resilient. Anecdotes from the focus groups regularly related how, in the past, service disruptions were a regular occurrence and restoration of service was not timely. These same participants related that access to the Internet is rarely interrupted and when it is, the service is normally restored quickly, unlike in the past when service was disrupted it was necessary to wait for an extended period for repair. Some credit this improvement to the redundant nature of the connectivity while others note that there is an increase in the use of service level agreements between operators which penalize downtime, and as a result, the operators have a greater incentive to restore service.

239. Several participants noted that the resiliency and capabilities of the Internet infrastructure has recently been tested as a result of the Covid-19 pandemic when many more customers have relied on the environment for work and school. However, there were reported some complaints amongst students regarding connectivity, mostly due to increased demand on the infrastructure.

240. While MACRA issues the licenses for the operation of telecommunications services, including ISPs, it does not monitor their operation or impose any operating requirements. The 2016 Electronic Transactions and Cyber Security Act does include measures relating to the use of the Internet, and ISPs and other telecommunications operators manage their systems as they see is necessary. The operators that participated in the focus group discussions, however, all indicated that they follow internationally recognized and documented processes standards for maintaining their systems, including redundant capabilities.

241. The cost of access has been the key issue raised by all participants and noted in documents describing the environment. According to a MACRA report, some fees have been lifted, but there does not appear to be any sustained effort to address the cost constraint on Internet access. MACRA maintains a Universal Access Fund, dedicated to enhancing access in underserved areas to all communication services, including telephone, postal and internet. However, several participants expressed disappointment that the fund was not operating more quickly to make additional services available in rural areas. For its part, MACRA, in some of its reports, has

[38] https://afterfibre.nsrc.org

[39] 39% for Malawi vs 76% for Africa according to 2018 ITU statistics at https://www.itu.int/net4/ITU-D/icteye/#/compare

indicated that it is working on incentives for operators to bring mobile services in particular to these underserved regions.

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 criticality of services.

Stage: Start-Up - Formative

242. None of the organisations that participated in the assessment reported the use of catalogues of secure or approved software. When asked about the management of software, almost all large organizations in both the public and private sectors indicated that they deployed automated software management systems. Many of these same institutions also reported that only approved applications were installed on workstations and workstation controls were in place to prevent the unauthorized installation of software. Some organizations also mentioned using license management procedures to avoid software piracy. In the private sector, these conditions did not apply to SMEs, which did not deploy any kind of software management practices.

D 5.4 TECHNICAL SECURITY CONTROLS

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

Stage: Start-Up - Formative

243. Organizations across sectors in Malawi apply a largely consistent, if limited, set of technical security controls, with some small variation depending primarily on industry and institutional size. As mentioned for the Software Quality aspect, public and larger private sector institutions largely control desktop software distribution and automate updates to approved applications. This includes antivirus software, which appears to be widely used amongst these institutions. Password management procedures, implementation of firewalls and regular backup operations also reportedly are in place, and some institutions reported monitoring of local networks for suspicious activities, including the attachment of unapproved devices. Several of the critical infrastructure operators mentioned the use of off-site backup storage and most institutions reported controlled access to data centres. Only the major international institutions, primarily in the financial and telecommunications sector, along with

some of the larger local companies, apply network intrusion detection systems or implement security operations centres.

244. The situation is different amongst the small and medium sized enterprises, which reportedly only rarely apply security controls.

D 5.5 CRYPTOGRAPHIC CONTROLS

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up to date.

Stage: Formative

245. Institutions in both the public and private sector reportedly apply cryptographic controls to data at rest and in transit, however, the deployment of these controls is inconsistent and ad-hoc. Until the creation of the Electronic Transactions and Cyber Security Act in 2016, Malawi did not have any regulation or requirements relating to the protection of personal data through encryption. With respect to encryption, this act includes provisions for the creation and management of a public key infrastructure (PKI) and the rules surrounding the provision of cryptographic services. Some participants mentioned that no national PKI exists in Malawi, however one government entity reported implementing a public key infrastructure for protection of the personal data it collects.

246. Within the public sector, government participants in the assessment noted that encryption was applied to systems, based on requirements for protection of data and confidentiality, therefore, not all systems were encrypted. Representatives noted that encryption is applied to websites and applications, such as financial management systems, which apply to the entire government, whereas other applications which serve specific purposes for a ministry are not encrypted. As noted in the Adherence to Standards aspect, the government issued in 2014 the "Public Service ICT Standards." This document includes guidelines for the protection of official and confidential material by, for example, noting that such material "sent through e-mail should be encrypted." While no mention is made of the type of encryption to be used, it does call for the "organisation responsible for ICT implementation in Malawi" to provide the encryption tools.

247. In the private sector, many organizations reported applying cryptographic controls for some of their applications and for some data in transit but did so as a matter of institutional practice rather than regulator requirement. This was mainly the case for large and multinational companies and mainly in the financial and telecommunications sectors. Small and medium size entities did not generally apply any encryption to systems or data in transit.

248. For the financial industry, as noted in the Adherence to Standards aspect, the Reserve Bank of Malawi, in late 2019, published "Guidelines on Information and Cybersecurity Risk Management for Banks." Encryption is included in these guidelines under the section "Management of Operational Infrastructure Security" which, *inter alia*, calls

for banks to "protect confidential information stored in all types of endpoint devices with strong encryption," "implement appropriate security measures including sending information through encrypted channels or encrypting the email and the contents using strong encryption with adequate key length based on criticality assessment," and "encrypt and protect confidential information stored on IT systems, servers and databases through strong access controls, bearing in mind the principle of least privilege." While none of the financial institutions referred to these standards, all reported applying encryption to their key systems.

249. An examination of the 30 most-visited local web sites (according to one tracking source[40]), indicates that about half utilize SSL and represent a variety of industries. The banking institutions and most of the telecommunications companies utilize secure web sites, as do many of the frequently visited government sites, and about half of the tertiary education institutions listed apply security to their sites.

D 5.6 CYBERSECURITY MARKETPLACE

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Start-Up

250. No domestic capability for cybersecurity product development does not exist in Malawi, and all the products used for cybersecurity come from international suppliers and developers. There are some companies that offer cybersecurity services such as penetration testing, firewall management and training. Some of these companies are local branches of companies[41] based in other countries and some are Malawi-based.[42] No cybersecurity insurance market exists in Malawi, although it was reported that one company recently surveyed the market to explore opportunities.

[40] https://domaintyper.com/top-websites/most-popular-websites-with-mw-domain

[41] https://computersecuritynetworks.mw/index.php

[42] https://www.sparcsystems.africa

D 5.7 RESPONSIBLE DISCLOSURE

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

Stage: Start-Up

251. Until the creation of the national cybersecurity strategy, no requirement or framework for the disclosure or sharing of vulnerability information existed in Malawi. The strategy calls for several actions regarding reporting within its objective to "Continuously manage cyber threats and risks to enhance incident response" including the intention to create "a national incident reporting, information sharing and coordination mechanisms to address reporting of incidents and coordination in incident response."

252. Financial institutions do not currently have a requirement to report incidents or disclose vulnerabilities, although the previously mentioned "Guidelines on Information and Cybersecurity Risk Management for Banks" suggests that these institutions report incidents and risks to internal and external stakeholders.

253. Participants indicated that no specific community of cybersecurity professionals existed in Malawi, although matters of cybersecurity were sometimes raised during discussions of the general ICT community, called the ICT Association of Malawi (ICTAM),[43] and some cybersecurity professionals formed informal groups over platforms like WhatsApp.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity Standards, Organisations, and Technologies, the following set of recommendations are provided to Malawi. 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.

ADHERENCE TO STANDARDS

R5.1 Enhance the adoption of standards and policies intended to improve the cybersecurity environment within the public sector, including the following steps:

- As an initial step, and as a matter of urgency, review and update the 2014 "Public Sector ICT Standards" as necessary and consider alignment with international frameworks such as the NIST or SANS top 20.
- Ensure the wide circulation of the updated standards amongst public sector employees.

[43] http://www.ictam.org.mw

- Ensure the adoption of the ICT standards by applying metrics to monitor compliance and establish periodic audits of the standards.
- Examine which bodies within the public sector should consider adoption of international standards such as ISO 27000.
- Establish compliance with cybersecurity standards as part of senior management performance reviews.
- Establish procurement sures that require private sector organizations that interface with the government also comply with public sector cybersecurity standards

R5.2 Streamline clear guidance for the public sector for the procurement of hardware and software.

R5.3 As part of public awareness campaigns, and in consultation with private sector entities, promote the awareness and implementation of standards, with a particular focus on SMEs.

R5.4 Encourage the regulators, particularly of the financial and telecommunications industries, but also of all critical infrastructure operators, to advocate for, or require, the adoption of international cybersecurity standards or documented frameworks of good practices.

INTERNET INFRASTRUCTURE RESILIENCE

R5.5 Identify and map potential points of critical failure within the Internet infrastructure.

R5.6 Encourage ISPs to establish and publish service level agreements for services and report on service outages to the responsible agency.

R5.7 Raise awareness with end users to enable them to identify services that have successfully implemented defined standards and good practices.

R5.8 Explore measures to reduce the cost of access to the Internet.

R5.9 Explore measures to provide access to remote areas, including through the Universal Service Fund.

SOFTWARE QUALITY

R5.10 Develop a catalogue of secure software platforms and applications used within the public sector, including critical infrastructure operators. Encourage private sector entities to also create or adopt these catalogues.

R5.11 As part of standards review under dimension 5.1, include the development, implementation and enforcement of policies and processes for software updates and maintenance to be applied to public sector. Encourage critical infrastructure operators and private sector entities to also adopt these standards.

TECHNICAL SECURITY CONTROLS

R5.12 Encourage ISPs and banks to offer anti-malware and anti-virus services for clients and ensure that their effectiveness is monitored and assessed.

R5.13 Collaborate with ISPs to raise awareness among end users about the importance of anti-malware software and network firewalls across devices.

R5.14 Institute measures such as Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS), anti-DDoS, Data Loss Prevention measures across the public sector. Encourage or work with regulators to require critical infrastructure operators to do the same.

CRYPTOGRAPHIC CONTROLS

R5.15 Establish or assign an institution responsible for designing a policy, aiming to assess the deployment of cryptographic controls according to their objectives and priorities within the public sector.

R5.16 Ensure the enforcement of encryption requirements within the Electronic Transactions and Cyber Security Act.

R5.17 As part of public awareness campaigns, raise awareness of secure communication services, such as encrypted and signed emails.

R5.18 Promote the deployment of state-of-the-art tools, such as SSL or TLS, by web service providers, to secure all communications between servers and web browsers. Promotion should be not only to service providers, but target in

particular small and medium-sized enterprises and encourage them to insist on these services from their providers.

CYBERSECURITY MARKETPLACE

R5.19 Foster collaboration with the private sector and academia regarding research and development of cybersecurity-technology products.

R5.20 Encourage and support local initiatives in partnership with businesses that aim at developing innovative localized cybersecurity technology, applications, services and solutions.

R5.21 Promote sharing of information and best practices among organisations to explore potential for cyber-insurance coverage.

RESPONSIBLE DISCLOSURE

R5.22 Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution, and an acknowledgement report.

R5.23 Within the responsible vulnerability disclosure framework or policy as described above, include mechanisms that ensure that organisations neither conceal vulnerability information nor are penalized for disclosing vulnerabilities discovered.

R5.24 Encourage sharing of technical details of vulnerabilities across sectors, including critical infrastructure operators, and foster the development of informal information-sharing groups and platforms to build trust.

ADDITIONAL REFLECTIONS

254. The government of Malawi has clearly made cybersecurity a priority. The CMM team is thankful for the support of the Malawi Communications Regulatory Authority (MACRA), the Malawi Public Private Partnership Commission, and active participation of all the stakeholder groups.