Government of Malawi

NATIONAL CYBERSECURITY STRATEGY

CONTACT INFORMATION

For more information, please contact:

Secretary for Information, Civic Education and Communications Technology
Central Office of Information
Private Bag 310,
Lilongwe 3.
Tel: 01 772 702
Fax: 01 770 650
Email: principal.secretary@information.gov.mw

FOREWORD

Information Communications Technology (ICT) has become a critical driver for socio-economic development, with the deployment and adoption of ICTs across the nation resulting in noteworthy improvements in all aspects of life and institutional operations in the nation. Improvements in telecommunications infrastructure in Malawi has contributed to the ever increasing over-all adoption of ICTs thereby contributing to an emerging digitally enabled society. Furthermore, the Malawi Government recognizes the significance of ICT to achieving inclusive and sustainable growth and development. It is against this background that the Malawi Growth and Development Strategy (MGDS) identifies ICT as one of its key pillars among the priority sectors for economic growth. In addition, Government has put in place further instruments such as National ICT Policy (2013), National ICT Masterplan (2014), The Electronic and Cybersecurity Act (2016) to enable inclusive growth of the sector.

The recent deployment of a nationwide fiber-optic network infrastructure further underscores the commitment that the Government has to ensure interconnectivity. Such developments provide a plethora of opportunities to the once "unserved peripheral communities" to join the bandwagon of the digital world and effectively take part in the global ICT revolution. The public and private sectors have embraced technology at the center of their business leveraging improved availability of higher capacities of bandwidth and better ICT innovations. Innovations in ICT contribute to efficient service provisioning, enable e-commerce and enhanced collaboration to curb geographical barriers in knowledge transfer and sharing of ideas.

However, a number of risks and threats exist or have emerged in the cyber space. The threats range from mere real time hacking of systems, phishing, mobile money fraud, organised online human trafficking, child pornography, bullying among other threats perpetrated over the internet. These restrict the smooth operation and resilience of ICT systems, and consequently the socio-economic development of the nation.

The Government is committed to keep the nation safe from cyber threats. I therefore call upon all stakeholders in the sector to join hands in the implementation of this Strategy.

Hon. Gospel Kazako
MINISTER OF INFORMATION

PREFACE

This National Cybersecurity Strategy (NCS) 2019 – 2024 aims to provide a national framework for ensuring secure, safe and resilient cyberspace, as well as fostering trust and confidence in cyberspace by Malawians. This has been achieved by describing the high level Strategic Goals and Specific Objectives that provide the basis of the nation's direction with respect to cybersecurity, and establishes the Actions that need to be taken for each. It is a bold and ambitious approach to tackling the many threats our country faces in cyberspace. The Government recognizes its special responsibility to lead the national efforts in managing and mitigating cyber threats.

The Strategy defines Malawi's cybersecurity vision, key objectives, and ongoing commitment to support national priorities by encouraging ICT growth while aggressively protecting critical information infrastructures. Government is committed to the safety, security, and prosperity of our nation and its partners. In order to achieve this, cybersecurity is a key component in providing organizations and citizens with confidence in online and mobile transactions. Furthermore, foreign investment will be greatly encouraged and a broader set of trade opportunities within the global marketplace will be opened. Successful implementation of the Strategy will further enable Malawi to achieve its economic and societal goals.

The formulation of this Strategy followed a participatory process that involved various stakeholders, including Government, private sector, the academia, development partners and the general public. As such, Government will also rely on these partners to implement this Strategy in the most efficient and effective way possible.

The Government is committed to ensuring that the commitments set out in this Strategy are carried out and accurately monitored and regular reports are produced. As a Ministry responsible for ICTs, we are determined to see this Strategy implemented. I, therefore, call upon all stakeholders to work with Government to achieve the goals that have been set in this Strategy.

Mr Francis Bisika
SECRETARY FOR INFORMATION

TABLE OF CONTENTS

Contents

ACRONYMS

CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
ICT	Information and Communications Technology
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol version 6
ISP	Internet Service Provider
LTE	Long-Term Evolutions
M&E	Monitoring and Evaluation
MDF	Malawi Defence Forces
MACRA	Malawi Communications Regulatory Authority
MGDS	Malawi Growth and Development Strategy
MICECT	Ministry of Information, Civic Education and Communications Technology
NCS	National Cybersecurity Strategy
SOP	Standard Operating Procedures
R&D	Research and Development
WiMax	Worldwide Interoperability for Microwave Access

EXECUTIVE SUMMARY

Communication services in Malawi have been governed by the Communications Act (1998) which was developed during the era of second generation (2G) technologies. Malawi has seen the growth of access and usage of ICT services, including an increasing number of online transactions for services. The increasing demand for the ICT applications and services coupled with the provision of high-capacity fibre backbone connectivity across the nation has resulted in the creation of substantial opportunities for further growth in the ICT sector. It is also expected that these developments will drive significant socio-economic growth in Malawi. Consequently, and in an effort to create a conducive environment for the sustained growth and use of ICTs in Malawi, as well as address the threats that come with increased adoption of ICTs, the Government of Malawi undertook a review of existing legislation and developed the Communications Act (2016) and the Electronic Transactions & Cyber Security Act (2016).

ICT has become a critical driver for socio-economic development, with the deployment and adoption of ICTs across the nation resulting in noteworthy improvements in all aspects of lives and institutional operations in the nation. However, a number of risks and threats exist or have emerged that restrict the smooth operation and resilience of ICT systems, and consequently the socio-economic development of the nation. This Strategy aims to provide a national framework for ensuring secure, safe and resilient cyberspace, as well as fostering trust and confidence in cyberspace by Malawians, by describing the high level strategic goals and specific objectives that provide the basis of the nation's direction with respect to cybersecurity, and establishes actions that need to be taken.

Chapter 1 of the Strategy provides an introduction to cybersecurity in Malawi while chapter 2 details the guiding principles upon which the Strategy is built on, and which will underpin the implementation of the Strategy. Chapter 3 outlines the core components of the National Strategy including the vision mission statement, high-level strategic goals and specific objectives. It further describes the various actions necessary for achieving the Specific objectives and strategic goals of the strategy. Chapter 4 describes the roles and responsibilities of the key stakeholders in the implementation of the strategy and further proposes an approach for monitoring and evaluating the implementation of the strategy. The implementation logical frameworks for the strategy which provide details on Deliverables, Key Performance Indicators (KPI), Timeframes, Lead Organisations and Funding options are described in the Appendix.

This Strategy therefore outlines the Government of Malawi's approach to ensuring a safe and secure cyberspace that can be fully leveraged by citizens and institutions. Consequently, driving further growth of the ICT sector, as well as socio-economic development across Malawi.

1. INTRODUCTION

1.1. Background

Major reforms in the ICT Sector of Malawi go as far back as the 1990s with the advent of sector liberalisation through the separation and commercialisation of the then incumbent Telecommunications operator, Malawi Posts and Telecommunications Corporation (MPTC) into the Malawi Telecommunications Limited (MTL) and Malawi Posts Corporation (MPC). Subsequent major reforms include the implementation of the Communications Sector Policy (1998) and the Communications Act (1998) that led to the establishment of the Malawi Communications Regulatory Authority (MACRA). Due to advances in technology over the years, the Communications Act (1998) was reviewed in 2016 and also the Electronic Transactions and Cyber Security Act (2016) were enacted. These are the two current legislations for the sector.

Currently, the mobile penetration rate in Malawi is quite low in comparison to the average African penetration rates, highlighting the tremendous potential for further growth in Malawi. Currently, the mobile penetration rate is at 45 percent compared to the African region average of 77.8 percent. The broadband access prices in Malawi are among the highest in the region due to high cost and limited availability of international bandwidth. However, the internet sector has about 50 licensed ISPs out of which only 20% are active.

The mobile penetration and broadband are expected to grow exponentially over the next couple of years. Since, the current mobile market in Malawi is a duopoly, the Government of Malawi has introduced a converged licensing regime in an effort to encourage further market competition and growth. It is expected that the converged licensing regimes will introduce new entrants into the sector and enhance competition resulting in lower prices. In addition, service providers in Malawi have launched 3G services, invested in LTE infrastructure or continued to extend their WIMAX wireless broadband networks. Furthermore, Malawi gained access to international submarine cables recently following the completion of a transit link via neighbouring countries and is currently deploying a national fibre backbone.

As a result of these recent developments within the sector, as well as the high potential for further rapid proliferation of ICTs within Malawi, it is evident that Malawians will increasingly get connected to the Internet and use ICTs overtime. This increased connectivity and use of ICT's come with increased threats to activities of businesses and people in Malawi. If Malawi is to fully leverage ICTs to spur socio-economic development of the nation, it has to be ready and capable of addressing these threats.

NCS 2019-2024 sets out a multi-stakeholder framework for ensuring Malawians can access and use cyberspace with trust and confidence, and ensuring the nation responds to threats to ICT systems and services in a coherent and effective manner.

1.2. Situational Analysis

1.2.1. National Development and the Role of ICT

The Malawi Growth and Development Strategy (MGDS III) recognizes how critical a well-developed ICT system is in the development of Malawi. Currently, ICT contributes about 5 percent to the country's GDP while the sector's growth rate is at 6.4 percent. The telecom sector accounts for 95 percent of the ICT sector employment and revenue. The Government embarked on implementing a number of strategies resulting in a number of desired outcomes including improved ICT broadband infrastructure; increased access and usage to ICT services; improved postal and broadcasting services; improved ICT governance; and enhanced ICT capacity for the general public. This is consistent with the Government's current overarching Policy Goal for ICTs in Malawi, as described within the National ICT Policy (2013) which is "to contribute to socio-economic development through maximum integration of ICT in all sectors and the provision of ICT services to the rural areas".

The development of the MGDS follows a phased approach to address the ICT development needs of the country in support of the prevailing policies and the legal framework. The MGDS was developed to be the overarching operational medium-term strategy for Malawi in the attainment of its set vision. The main thrust of the MGDS is to create wealth through sustainable economic growth and infrastructure development as a means of achieving poverty reduction. The MGDS I was developed to lay the framework while MGDS II was tasked with putting in place the operational mechanism. The NCS therefore builds on initiatives implemented in MGDS II as well as feed into MGDS III thereby addressing Government goals of universal ICT access within a safe and secure operational environment.

This policy direction is quite consistent with global research studies and evidence that clearly demonstrates the connection between ICT adoption and usage of ICT services with national GDP growth. In fact, the World Bank has demonstrated the greater development impact of broadband specifically on emerging economies as compared to high-income countries. Currently, Malawi's broadband penetration has risen from 6% in 2013 to around 17.1% in 2016, which is relatively low compared to other Southern African

Development Community (SADC) countries and the rest of the world. However, with the rapid development of the ICT sector, the Government of Malawi through the MGDS III, recognizes the potential broadband growth which puts the users of ICT services at a cyber risk. Thus, the Government of Malawi needs to be prepared and deploy effective strategies or measures to create a conducive environment that builds trust and confidence in the use of ICTs by Malawian businesses and citizens.

1.2.2. Cybersecurity in Malawi

Understanding the current cybersecurity-related activities of Malawi is critical to ensuring the effective cooperation between Malawi's stakeholders and their cybersecurity-related mandates and activities. Therefore, this Strategy considers the various functions and activities of the different stakeholders in Malawi relating to cybersecurity. Noteworthy cybersecurity-related activities undertaken in Malawi over the past year include the recent approval of the Electronic Transactions and Cyber Security Act (2016) and the development of this National Cybersecurity Strategy. The recently promulgated Electronic Transactions and Cyber ecurity Act (2016) address a number of ICT security issues like cybercrime, data protection, and privacy among others. For instance, the Electronic-Transactions and Cybersecurity Act (2016) will enable citizens to undertake various electronic transactions with the full protection of the law, as well as ensure citizens are protected from computer related harms like cybercrimes, viruses and hacks. Part 6 of the Electronic-Transactions and Cyber Security Act (2016) provides details of offences; Clause 87, for instance, addresses events where an individual knowingly introduces or spreads a software code that damages computer, computer system or network. Other issues addressed in the Act include cryptography, Country Code Top Level Domain (ccTLD), the establishment of the Malawi National CERT and the appointment of cyber inspectors.

However, efforts to address challenges within the cyberspace in Malawi were fragmented due to the absence of a coordinated strategic approach by all key stakeholders. This Strategy will therefore provide a link among all these stakeholders to provide effective solutions to the identified challenges. The NCS as an overarching strategy provides a platform for: the Ministry of Justice to deal with the legal issues related to the cyberspace in conjunction with all law enforcement agencies; the regulatory authorities to review the effectiveness of the legal and regulatory framework; and the academia to review the curricula and offer training suited to the trends in addressing challenges in the cyberspace.

The extent of cybersecurity issues entails generic actions to specific sectors that eventually feeds into the national strategy. For instance the banking sector has embarked on sector

specific training to address the needs of the banks, likewise the academia has also incorporated various courses for cybersecurity in order to enhance the level of knowledge and awareness for cybersecurity.

1.2.3. Cybercrime in Malawi

The high levels of ICT access and usage in the country coupled with the absence of specific legislation dealing with cybersecurity issues in Malawi is a big challenge in the fight against common forms of cybercrime. The Government's position on cybercrime, like other nations across the world, continues to be a real threat and facet of life in Malawi. Cyber criminals continue to commit cybercrimes of larger scales and sophistication across various countries. Many of these cyber criminals seek to make use of confidential and sensitive information and usually have detrimental effects on individuals, businesses and Government institutions. Consistent with global trends, a major sector targeted by cyber criminals in Malawi is the financial sector. Other notable cybercrime incidents that have been observed in the country include and not limited to child pornography, sexual harassment, fraud, forgery, crime recorded, mobile money fraud, Government Websites defacement, identity theft, email scams, distribution of compromising images, attacks on computer data and systems.

In the National ICT Policy (2013), the Government set out to establish sufficient national capacity to deal with national security, the violation of human rights, and the undesirable impacts of ICTs. Furthermore, the enactment of the Electronic Transactions & Cyber Security Act (2016) has provided a platform to harness all the efforts that were being hampered by lack of appropriate legislation. Malawi is also benefiting from regional initiatives and harmonization of strategies to provide a model standard for the region.

Therefore, it is critical that Malawi develops a Strategy that protects its citizens and institutions from these cyber criminals and enhances the nation's ability to detect, prosecute and prevent cybercrimes.

1.2.4. Linkages with other National Policies and Programmes

The National Cybersecurity Strategy is aligned with and will complement the following key strategic documents:

- The National ICT Policy (2013) - The policy recognizes that Malawi needs to establish adequate capacity to deal with undesirable impacts of ICTs including the violation of privacy, spread of undesirable materials, cyber-crimes, digital frauds and terrorism.

- The National ICT Master Plan (2014 – 2031) - this is to operationalize the National ICT Policy.
- Electronic Transaction and Cybersecurity Act (2016) - This makes provision for criminalizing offences related to computer systems and information communication technologies.
- The Payment Systems Act (2016) - This act provides for the regulation, management and supervision of payment systems and electronic money transfer in Malawi.
- Malawi Growth and Development Strategy III (2017 -2022) – This highlights the need to have developed ICT infrastructure and improved e-governance a system that is conducive to business operations; and enacting appropriate legislation that promotes interest of new entrants in ICT sector.
- Vision 2020 - Vision 2020 has acknowledged in its mission statement of Malawi being a technologically driven middle-income economy and has highlighted the need for improved communications infrastructure promoting the effective use of information technology as a tool to facilitate better management and access to information resources
- Communications Act (2016) - This provides for the regulation of the provision of services in the electronic communications sector, posts, information society.
- Science and Technology Policy (2002) – This aims at attaining sustainable socio-economic development through the development and application of science and technology in order to improve the standard and quality of life of Malawians.

2. METHODOLOGY

The development of the Cybersecurity Strategy was highly participatory and consultative to ensure full ownership of the outputs. All key critical information infrastructure stakeholders in terms of their interest, power and influence were identified in order to involve them in the development of the Strategy. The consultative process included workshops, working groups; and steering committee meetings.

3. THE STRATEGIC ANALYSIS

The strategic analysis examines the operating environment of the country in relation to cybersecurity and seeks to identify key issues that will affect the implementation of the strategies spelled out in the NCS.

3.1. Capability Maturity Model

The Capability Maturity Model (CMM) was employed to critically assess the internal and external environmental factors facing the country in terms of cybersecurity and the table below gives a summary of the results.

Dimension	Constituent Factors of Each Dimension	Findings
Dimension 1 – Cybersecurity Policy and Strategy	D1-1: Documented or Official National Cybersecurity Strategy	• No published national cybersecurity strategy document • No institution that coordinates cybersecurity issues • No budget assigned to address cybersecurity issues • Developing a NCS has commenced • Key stakeholder/working groups established • Consultations on development NCS underway
	D1-2: Incident Response	• Need for creation of Malawi CERT • lacking CERT's role in reporting and management of cybersecurity incidents • No catalogue in a central registry for incidents at national level • No regulation in force that mandates incidents to be reported • Institutions, critical to national cybersecurity have been identified • No formal coordination mechanisms have been established
	D1-3: Critical National Infrastructure (CNI) Protection	• No formal categorisation of Critical Infrastructure • Critical sectors identified • No institution responsible for overseeing CI • Little interaction among owners of CIs and Government ministries • No formal collaboration mechanism. • No coordinated response • No protection procedures • No formal procedures for information sharing • No coordinated approach to detect, identify, protect, respond and recover from cyber threats • Some training and awareness has been provided
	D1-4: Crisis Management	• No planning for crisis management • Little understanding of crisis management from a cybersecurity perspective • No evaluation of cybersecurity cybersecurity crisis management protocols
	D1-5: Cyber Defence Consideration	• National Security Policy under development • No national cyber defence policy or strategy • No central command and control structure for cybersecurity in the armed forces • National security forces do consider cybersecurity dimensions in their operations • Limited capacity for national armed forces
	D1-6: Digital Redundancy	• No National Contingency plans • No standard operating procedures • Redundancy systems established by operators • Emergency response assets have been mapped and identified • No proper communication channels

Dimension 2 – Cyber Culture and Society	D2-1: Cybersecurity Mind-set	• Government or the private sector have begun to place priority on cybersecurity • Government institutions and the public sector were more informed on the need for cybersecurity when compared to non technical personnel • Cybersecurity mindset was emerging across the nation • Need improvements especially among vulnerable groups like women and children.
	D2-2: Cybersecurity Awareness	• Need for awareness • National cybersecurity awareness campaigns have not been launched or deployed • Identify institutions to lead on the execution of national awareness
	D2-3: Confidence and Trust on the Internet	• Minimal use of online services across Malawi. • Need to highlight features of e-commerce services to promote trust • adoption of e-Government services across the nation • Need for security measures to promote trust in e-services being recognised • Minimal E-Commerce services
	D2-4: Privacy Online	• E-Transactions and Cybersecurity Act to handle privacy online • Malawi would have the right legislative frameworks to address cyber
Dimension 3 – Cybersecurity Education, Training and Skills	D3-1: National Availability of Cyber Education and Training	• Some education in cybersecurity at the national and institutional level • A number of training programmes are offered across the nation
	D3-2: National Development of Cybersecurity Education	• No formal national programme exists to promote cybersecurity education • National education and skill focus areas have been identified • Incentives for training and education exist
	D3-3: Training and Educational Initiatives within the Public and Private Sector	• Knowledge transfer occurs in an ad hoc among trained employees • Number of cybersecurity training programmes exist • No gaps analysis for technical training
	D3-4: Corporate Governance, Knowledge and Standards	• Understanding of cybersecurity issues vary at Board Level across institutions

Dimension 4 – Legal and Regulatory Frameworks	D4-1: Cybersecurity Legal Frameworks	• E Transactions and Cyber-Security Act in place • Need to develop regulatory instruments relating to ICT Security • Partial legislation regarding privacy
	D4-2: Legal Investigation	• Limited capacity for police and judiciary • Law enforcement forces do possess some investigative capacity • Lack formal collaboration mechanisms with law enforcement. • Limited number of judges who have capacity to preside over cyber case
	D4-3: Responsible Reporting	• No formal and official responsible vulnerability disclosure framework exists
Dimension 5 – Standards, Organisations and Technologies	D5-1: Adherence to Standards	• No information security standards • Public Service ICT Standards available
	D5-2: National Infrastructure Resilience	• Low resilience of the internet services infrastructure • Limited availability of technology to support e-commerce • No formal approach has been established to address these issues. • Minimal control of their technology infrastructure by Government • Dependent on unreliable third party markets for cybersecurity related products
	D5-3: Cybersecurity Marketplace	• No cybersecurity related products or services from Malawi • No cyber insurance

3.2. Key Strategic Issues

Following the above analysis, the following emerge as key strategic areas for intervention:

1. Identifying and managing the critical information infrastructure of Malawi
2. Developing and enhancing cybersecurity-related capacity, infrastructure and regulatory frameworks.
3. Promoting awareness, information sharing and collaboration on cybersecurity.
4. Enable and continuously improve the safety of vulnerable groups[1] in cyberspace, especially the safety of children.
5. Enhancing and coordinating the fight against all forms of cybercrime
6. Promoting the use of cyberspace to drive social and economic development

4. BROAD DIMENSIONS FOR NATIONAL CYBERSECURITY STRATEGY

This section of the Strategy articulates Malawi's Vision and Mission Statements for Cybersecurity as well as the core elements of Malawi's approach to improving the cybersecurity posture.

4.1. Vision

Malawi's vision is:

"A nation with a secure, trusted, resilient and safe cyberspace that promotes a knowledge-based society and socio-economic development"

4.2. Mission

Malawi's mission is:

"To develop and deliver effective cybersecurity capacity, services and infrastructure that instills confidence in cyberspace"

4.3. Guiding Principles

The National Cybersecurity Strategy is built on the following Guiding Principles:

i. **Risk-based approach:** The Cybersecurity Strategy will ensure that a risk-based approach is adopted by the private sector, the Government, academia and civil society in assessing and responding to cyber-related threats or issues.

ii. **Multi-stakeholder approach:** The Cybersecurity Strategy will seek to enhance the effectiveness of all key stakeholders in improving the cybersecurity posture of Malawi by recognizing the various roles and responsibilities of different stakeholders and promoting national cooperation and coordination for cybersecurity-related activities amongst stakeholders.

iii. **External Co-operation:** The Strategy will also promote bilateral, regional and international cooperation, recognizing the borderless nature of cyberspace.

iv. **Respect for the rule of law and human rights:** The Cybersecurity Strategy is aligned with the laws in force in Malawi. It is also aimed at facilitating the promotion, protection and enjoyment of fundamental human rights and freedoms of Malawian citizens.

v. **Capacity development:** The Cybersecurity Strategy will seek to enable the continuous development of the Malawi's capacity to address fast changing cybersecurity issues and developments.

vi. **Socio-economic development:** The National Cybersecurity Strategy will ensure cyberspace is fully leveraged by Malawi to spur broader socio-economic development, facilitate sustainable socio-economic development across the entire nation.

vii. **Addressing Cybercrime:** The National Cybersecurity Strategy will promote and facilitate both individual and collective action in tackling cybercrime, recognizing both the individual responsibility and collective responsibility in taking steps in combating cybercrime.

4.4. Strategic Goals

To achieve the above mentioned Vision, the Government of Malawi will work to achieve the following Six Strategic Goals:

1. Identify and manage the critical information infrastructure of Malawi
2. Develop and enhance cybersecurity-related capacity, infrastructure and regulatory frameworks.
3. Promote awareness, information sharing and collaboration on cybersecurity.
4. Enable and continuously improve the safety of vulnerable groups[2] in cyberspace, especially the safety of children.
5. Enhance and coordinate the fight against all forms of cybercrime
6. Promote the use of cyberspace to drive social and economic development

The following section details the Specific Objectives and Actions required to achieve the above mentioned Strategic Goals of the Strategy.

4.5. Specific Objectives and Actions

I. Strategic Goal (i): Identify and manage the Critical Information Infrastructure of Malawi

Protecting the information infrastructure of Malawi is of critical to the Government of Malawi, especially as successful cyber attacks on them will have severe impacts on the country. These impacts could include destabilization of Malawi's economy, national security risks and stability or reputational damages to individuals. Therefore, it is vital that Malawi prioritizes the cybersecurity of its critical information infrastructures (CIIs) which are key for the provision of essential services to Malawi by ensuring these CIIs

are secure and resilient. The protection of Malawi's information infrastructure including CIIs necessitates collaboration of all relevant stakeholders including public and private institutions that own or operate the information infrastructure which supports the well-functioning of the Malawian society. Consequently, the Government of Malawi will work with all relevant stakeholders to identify and understand the vulnerabilities and levels of cybersecurity of Malawi's information infrastructure, especially CIIs. The Government will also work with relevant stakeholders to establish measures that will address current and future cyber threats and risks to the national information infrastructure, and drive improvements where necessary.

4.5.1. Specific Objective 1: Identify the Critical Information Infrastructure of Malawi.

Actions:

4.5.1.1. Establish a National CII Register

4.5.1.2. Create a National Vulnerability Register and Framework for regular vulnerability monitoring and disclosure for CII

4.5.1.3. Establish a National Risk Register and Regulations and/or Guidelines that promote continuous risk assessment and management across CIIs in Malawi

4.5.2. Specific Objective 2: Protect the Critical Information Infrastructure of Malawi.

Actions:

4.5.2.1. Develop a National CII Governance Framework which provides details on CII protection procedures and processes

4.5.2.2. Establish Mandatory Equipment Specifications, Mandatory Guidelines, Regulations, Security Requirements, Procedures relating to the management of risks by CIIs

4.5.2.3. Undertake continuous monitoring and regular testing to detect errors, vulnerabilities, and intrusions in CII

4.5.2.4. Promote and enhance regional and international cooperation in the protection of the critical information infrastructure (CII)

4.5.3. Specific Objective 3: Continuously manage cyber threats and risks to enhance incident response.

Actions:

4.5.3.1. Expedite the establishment and operationalization of a national CERT with clear processes, defined roles and responsibilities

4.5.3.2. Continuously develop the capacity of staff at Malawi National CERT to address the fast changing technical requirements, and develop abilities to actively obtain information in cyberspace, about current cyber risks and threats

4.5.3.3. Develop a national incident reporting, information sharing and coordination mechanisms to address reporting of incidents and coordination in incident response

4.5.3.4. Create and continuously update cybersecurity incidents register, assess incidents, and suggest measures to resolve issues and mitigate threats and risks

4.5.3.5. Specify minimum and mandatory log/register requirements necessary for dependable cybersecurity incident analysis

4.5.3.6. Continuously monitor, analyse and assess cyber threats and potential risks and be able to provide a real time overview of the state of cybersecurity across the country

4.5.3.7. Develop a Cybersecurity Governance Framework for defining roles and responsibilities of all stakeholders in the cybersecurity ecosystem as well as describe SOPs and Code of Conduct in responding to incidents

4.5.3.8. Establish a call center/help line for reporting incidents or seeking assistance with incidents

4.5.3.9. Develop and implement cybersecurity incident simulation scenarios and programs that can be used during the national exercises

4.5.3.10. Develop and continuously update cybersecurity contingency plans, which will include roles of the military/security forces during cyber-attacks and emergencies

4.5.3.11. Develop and test requisite crisis management measures during frequent cyber drills

4.5.3.12. Evaluate cyber drills to develop options on how to improve crisis management measures

4.5.3.13. Develop a Cyber Defence Strategy that details approaches to addressing threats to national security in cyberspace

4.5.3.14. Establish a Central Defence Command and Control Centre for cybersecurity in Malawi

II. Strategic Goal (ii): Develop and enhance cybersecurity - related capacity, infrastructure, Legal, regulatory and other related frameworks

The limitation of cybersecurity capacity, infrastructure, and other related frameworks is recognized as a key challenge for Malawi which impairs the nation's efforts in ensuring high levels of cybersecurity. Aligned to the national vision of creating information driven and knowledge based society, the Government of Malawi will seek to ensure that there is an available pool of highly skilled and knowledgeable cybersecurity professionals in Malawi. The Government will also seek to promote research and development in cybersecurity as well as create an enabling environment where innovation and creativity in cybersecurity can be fostered.

Considering that all ICT users including individuals, public or private sector are required to take necessary steps in ensuring their cybersecurity including investing in infrastructure or technology, the Government will facilitate the deployment of, and usage of requisite infrastructure/technology necessary to ensure good levels of cybersecurity nationwide.

The Government will also seek to establish and strengthen a range of cybersecurity-related frameworks which will enhance the cybersecurity of Malawi. For instance, the Government will seek to strengthen the legal and regulatory framework of Malawi to support the cybersecurity landscape and create a conducive environment for the effective use of cyberspace by individuals, the public and private sector.

4.5.4. Specific Objective 4: Strengthen Malawi's legal and regulatory frameworks

Actions:

4.5.4.1. Undertake a gap analysis to identify gaps in current ICT Security Legal and Regulatory Framework and develop requisite instruments to address Gaps including issues relating to privacy and data protection.

4.5.4.2. Develop and publish a cybersecurity policy and standards consisting of general and sector-specific cybersecurity controls that would be recognized as a national standard

4.5.4.3. Create a national programme to promote the adaptation and adoption of cyber standards across Government institutions and CII in Malawi

4.5.5. Specific Objective 5: Build capacity of law enforcement agents and the judiciary

Actions:

4.5.5.1. Identify needs and then provide training and education to develop the capacities of the law enforcement agencies, judiciary and the legal fraternity on how to interpret and enforce the policy, legal and regulatory frameworks on cybersecurity in Malawi

4.5.6. Specific objective 6: Enhance technical and procedural measures for CIIs

4.5.6.1. Establish mandatory and minimum technology and security requirements for CIIs

4.5.6.2. Develop a national Government programme to deploy and manage Government ICT infrastructure

4.5.6.3. Develop a national programme to enhance internet infrastructure development and resilience.

4.5.6.4. Develop National Contingency plans which identify emergency response asset priorities and standard operating procedures (SOPs)

4.5.6.5. Review and update the map of current emergency response assets

4.5.6.6. Ensure communication channels are deployed across emergency response functions, geographic areas of responsibility, public and private responders, and command authority.

4.5.7. Specific Objective 7: Continuously develop cybersecurity technical capacity in Malawi

Actions:

4.5.7.1. Revise the National Research Agenda to promote R&D in cybersecurity in Malawi
4.5.7.2. Establish a National Centre of Excellence for Cybersecurity Training & Research
4.5.7.3. Review and update primary, secondary and tertiary level education curriculum to include cybersecurity elements
4.5.7.4 Support cybersecurity competitions and R & D projects in Universities and Schools
4.5.7.5. Support national enterprises providing cybersecurity solutions, and undertaking R & D in cybersecurity
4.5.7.6. Collaborate with universities, colleges and the private sector to create new studies and internship programs on cybersecurity
4.5.7.7. Collaborate with the private sector and academia to support participation of Government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity
4.5.7.8. Develop standards in cybersecurity training and education
4.5.7.9. Train ICT personnel of various Government ministries and institutions on how to detect incidents, report incidents, and collaborate with the national CERT and institutions from other sectors on cybersecurity

4.5.8. Specific Objective 8: Facilitate retention of cybersecurity expertise within Malawi

Actions:

4.5.8.1. Develop National and Career Progression Policy promoting continuous training and education for Incident Response and addressing issues relating to cybersecurity
4.5.8.2. Identify the staffing requirements for Government agencies and CII operators
4.5.8.3. Develop a national recruitment and retention strategy
4.5.8.4. Develop and implement cybersecurity training and capacity building training plans for Government personnel.

III trategic Goal (iii): Promote awareness, information sharing and collaboration on cybersecurity

A significant proportion of cybersecurity incidents can be prevented by being aware of, and understanding the threat. It is critical that individuals and organizations in Malawi are aware of the threat, and are taking the appropriate measures to protect themselves from cyber attacks. It is paramount that the Government of Malawi and other stakeholders aim to undertake various awareness building programmes which not only provide information and advice to individuals and organizations on how to protect themselves but also create a national cybersecurity culture and mindset.

Recognizing the shared responsibilities of various stakeholders in improving cybersecurity in Malawi, as well as the borderless nature of cyberspace, it is imperative the Government of Malawi promotes information sharing and collaboration in the nation's efforts in addressing cyber threats and cyber incidents. The Government of Malawi will seek to establish measures that promote a culture of information sharing and collaboration across all relevant stakeholders nationally, regionally or internationally.

4.5.9. Specific Objective 9: Enhance cybersecurity awareness across the general public and national institutions

Actions:

4.5.9.1. Undertake a nationwide assessment to determine level of awareness of cybersecurity across the nation

4.5.9.2. Develop and implement a national roadmap for improving awareness of current cybersecurity trends and threats

4.5.9.3. Develop and disseminate National Cybersecurity Best Practices to ingrain a cybersecurity mindset in the public

4.5.9.4. Undertake mandatory training of Board Members of different organizations to enhance their understanding of cyber issues and how their organizations address these threats.

4.5.10. Specific Objective 10: Promote collaboration and information sharing on Cybersecurity.

Actions:

4.5.10.1. Create a national forum to enhance and promote information sharing and collaboration nationally on cybersecurity

4.5.10.2. Continuously update the citizens, the private sector and the public sector, on information related to cyber threats, vulnerabilities, incidents, activities across the nation to foster trust.

IV. Strategic Goal (iv): Enable and continuously improve the safety of vulnerable groups in cyberspace, especially the safety of children

The Government of Malawi recognizes its responsibility in protecting vulnerable groups, especially children as they usually lack the capacity to do so themselves. For instance, children are susceptible to cyber bullying, pornography, and other harmful content, and meeting online contacts offline, sexual solicitation and grooming. Therefore, the Government will seek to ensure that vulnerable groups, especially children, use ICTs and cyberspace in a safe and responsible manner. The Government will deploy measures that ensure that vulnerable groups especially children, as well as their minders or guardians, are informed and aware of cyber threats and risks. Furthermore, it will collaborate with relevant stakeholders to develop and deploy measures and tools to protect the vulnerable and ensure they stay safe online.

4.5.11. Specific Objective 11: Strengthen online safety for vulnerable groups, especially children

Actions:

4.5.11.1. Develop and disseminate online safety guidelines and best practices to protect vulnerable groups in Malawi, especially children, from cyber threats

4.5.11.2. Deploy special awareness programmes to target and inform children and other vulnerable groups about safe and responsible use of the internet

4.5.11.3. Promote the deployment of technical measures or web filtering tools that prevent access to harmful content by children and other vulnerable groups

4.5.11.4. Encourage ISPs and other services providers to make their clients, especially parents and guardians aware of how to leverage available tools, technologies to manage potential risks to vulnerable groups while accessing services online

V. Strategic Goal (v): Enhance and coordinate the fight against all forms of cybercrime

It is evident that cybercrime has several detrimental effects on the Malawi nation. Some of these impacts include economic losses, reputation damage, reduced confidence in ICT services, etc. The Government of Malawi appreciates the severity of the evolving threat of cyber crime to the nation and the numerous challenges in combating cybercrime across the nation. The Government aims to enhance the detection, investigation, and prosecution of cybercrimes in Malawi. This will

require Malawi to strengthen the relevant legal and regulatory frameworks relating to Cybercrime in Malawi, as well as to build the capacity of the stakeholders responsible for the detection, investigation, and prosecution of cyber crimes. The Government also recognizes the need for coordination and collaboration in the national response to cybercrime, and will develop strong partnerships to combat cybercrime.

4.5.12. Specific Objective 12: Strengthen Cybercrime detection

Actions:

4.5.12.1. Establish the requisite framework and operationalize a Digital Forensics Laboratory

4.5.12.2. Develop mandatory digital forensics and evidence handling courses for the judiciary, law enforcement and personnel from other related agencies involved in the detection and prosecution of cybercrime

4.5.12.3. Build and enhance capacity to detect cybercrime incidents

4.5.13. Specific Objective 13: Promote national and international collaboration in the fight against cybercrimes

Actions:

4.5.13.1. Develop and continuously update an information sharing, governance and collaboration framework for the fight against cybercrime which will include links that ensure direct and timely collaboration between judiciary, law enforcement and personnel from other related agencies, service providers, CII entities, Malawi CERT and other Government institutions on issues that concern cybercrime and Cybersecurity

4.5.13.2. Strengthen collaboration with regional, international states and partners in combating cybercrime through treaties, conventions (e.g. Budapest) and bilateral agreements, especially through frameworks such as the 24/7 cybercrime Network, mutual legal assistance frameworks.

4.5.13.3. Develop a clear plan that outlines how to manage international collaboration across multiple strategy areas such as law enforcement, incidence response, research and innovation in cybersecurity.

4.5.13.4. Subscribe to and participate in all relevant regional and international forums on cybersecurity.

VI. Strategic Goal (vi): Promote use of secure cyberspace to drive social and economic development

The Government of Malawi recognizes the multiplier effect of the cyberspace on several aspects of its society, including social and economic development. In fact, with more and more individuals and organizations adopting and utilizing ICT technologies and applications, there is extensive evidence that illustrates the positive impacts of ICTs including cyberspace. The Government seeks to create a secure and reliable environment which facilitates the secure use of cyberspace, promotes trust in cyberspace, increased usage of e-Government and e-commerce services, and consequently driving further social and economic development in Malawi.

4.5.14. Specific Objective 14: Enhance trust and confidence in cyberspace, especially in applications relating to e-Government and e-commerce.

Actions:

4.5.14.1. Create, and continuously update the general public and public sector on how cyberspace is securely used in Malawi to deliver e-Government and e-commerce services in Malawi, highlighting the various security features deployed to foster trust

4.5.14.2. Encourage the use of Public Key Infrastructure (PKI) for transactions to/from Government Ministries, Departments and Agencies to enhance high cybersecurity levels and trust in delivering public services.

4.5.14.3. Appoint cybersecurity inspectors whom among other duties will serve as focal points of contacts to support small and medium enterprises in addressing cybersecurity needs and method of mitigating cyber threats.

4.5.14.4. Undertake the transition from IPV4 to IPV6 protocol and disseminate information on the benefits of the transition, especially IPV6 security features relating to confidentiality, authentication and data integrity

4.6. FOCUS AREAS

The main focus areas of this strategy are:

1. Critical information infrastructure
2. Cybersecurity capacity
3. Cybersecurity awareness and collaboration.
4. Vulnerable groups in cyberspace.
5. Cybersecurity coordinate
6. Secure usage

5. INSTITUTIONAL FRAMEWORK

5.1. Roles and Responsibilities

The section below describes the roles and responsibilities of key actors involved in the implementation of the strategy:

5.1.1. Office of the President

The Office of the President's will champion cybersecurity in Malawi and will provide support and leadership at the executive level to ensure the successful implementation of the National Cybersecurity Strategy of Malawi.

5.1.2. Ministry of Information, Civic Education and Communications Technology (MICECT)

The MICECT will be responsible for creating a conducive legal and regulatory environment for the safe use of ICTs and confidence in cyberspace, by developing relevant policies, laws, and regulations that enable the smooth functioning of the ICT sector of Malawi.

5.1.3. Malawi Communications Regulatory Authority (MACRA)

The Malawi Communications Regulatory Authority (MACRA) will be responsible for leading, planning and coordinating the implementation of the National Cybersecurity Strategy through collaboration with other stakeholders. MACRA will through CERT, continuously monitor the cyberspace to provide pro-active and reactive responses to cyber threats and risks.

MACRA provides regulatory oversight of the ICT sector of Malawi and ensures compliance to relevant cybersecurity-related frameworks within the ICT sector. MACRA will also host the Malawi CERT.

5.1.4. Ministry of Justice and Constitutional Affairs

The Ministry of Justice will lead in the prosecution of cybercrime and provide legal guidance on cybersecurity issues.

5.1.5. Ministry of National Defence & Ministry of Home Affairs and Internal Security

These Ministries will be responsible for setting up security related policies to guide the implementing agencies i.e. Malawi Defence Force and Malawi Police Service respectively to undertake their cyber-related activities in line with the policy direction.

5.1.6. Malawi Police Service (MPS) and other law enforcement agencies

The Malawi Police Service (MPS) and other law enforcement agencies will be responsible for the investigation of cybercrimes and enforcement relevant laws in Malawi. They will also play a vital role in collaborating with national and international stakeholders and law enforcement agencies in combating cybercrime.

5.1.7. Malawi Defence Force

The Malawi Defence Force, in collaboration with the Malawi CERT will continuously monitor the cyberspace sphere to identify and address cyber threats and risks to the National Security. They will also work with other security forces and stakeholders to safeguard and combat cyber-terrorism and maintain law and order during nationwide incidents or emergencies.

5.1.8. Critical Information Infrastructure (CII) Owners and Operators

CII owners and/or operators in Malawi will be responsible for protecting their infrastructure from cyber threats and vulnerabilities. To this end, they will ensure that various mitigation measures are implemented to protect the CII. They will also be responsible for ensuring that they comply with various cybersecurity-related frameworks in force in Malawi.

5.1.9. The Academia

The Academia in Malawi will play a key role in the nation's efforts in developing capacity and expertise in cybersecurity to address Malawi's requirements for skilled and knowledgeable cybersecurity professionals of Malawi, at present and in the future. The Academia will also play a key role in undertaking cybersecurity-related R&D.

5.1.10. Civil Society

The Civil Society will work with other stakeholders to promote effective engagement, promote transparency and accountability of the public and private sector institutions, and strengthen knowledge and awareness of cybersecurity related issues across Malawi.

5.1.11. Private Sector

The Private Sector will be responsible for protecting the data, services and systems they own, provide and operate respectively, and as such will be responsible for ensuring their compliance with national laws, policies, standards, procedures and frameworks relating to cybersecurity.

5.1.12. Citizens

The citizens will be expected to take appropriate steps in order to safeguard themselves in cyberspace against cyber threats and attacks. They will further be expected to utilize the information and messages available on the safe use of the cyberspace.

6. CRITICAL SUCCESS FACTORS (CSFS)

The CMM that was used to assess cybersecurity posture of Malawi revealed a number of critical success factors that will lead to successful achievement of cybersecurity goals of Malawi. These factors include:

6.1. Political Will

- Enhancing Malawi's cybersecurity posture needs to be a top priority for the Government.
- Cybersecurity requires adequate organizational and political support.
- At the national level, cybersecurity has to be driven from the highest office to provide a unified agenda that will guide all relevant national stakeholders.
- At organization level, the success of cybersecurity efforts depend mainly on the commitment and support of top management to get stakeholders support and secure budget for cybersecurity.
- security governance should be led by competent security managers

6.2. Funding and Resources

- The successful implementation of Malawi's NCS will depend on adequate funds and resources. Considering that ICTs and Cyberspace spur socio-economic growth, the National Cybersecurity Strategy implementation logical frameworks have identified possible lead organization and funding sources for various measures proposed in the NCS.

6.3. Effective coordination of efforts

- Cybersecurity is a shared responsibility among different players with different responsibilities and abilities requiring unified coordination across a wide spectrum of stakeholders.
- Successful implementation of the NCS will therefore, require developing a comprehensive national structure that will facilitate national cohesion at all levels and meaningful participation by all stakeholders, working together toward a common goal of securing Malawi's cyberspace.

6.4. Awareness, education and training

- The success of cybersecurity depends on availability of the requisite knowledge, awareness, trust to use information systems and reduced exposure to risks.
- It is important to inform, educate and raise awareness of public and private organizations, owners of critical infrastructures and the civil society of their security responsibilities.
- Security awareness among ICT professionals and users can prevent them from becoming easy and soft target for cyber criminals. It is also important for the nation to provide qualified human resources with enhanced technological capabilities of dealing with

complex challenges of cybersecurity.

6.5. Collaboration and networking

- The world today is highly linked and interdependent as such cybersecurity requires close cooperation and collaboration among national, regional and international partners, based on mutual trust.
- Effective response to challenges of cyberspace security requires a networked approach among stakeholders in various fields to facilitate information and resource sharing.

6.6. Protection of Critical information infrastructure

- ICT infrastructure supporting critical societal functions must be secure, robust and reliable so that adverse incidents are avoided or mitigated as much as possible.

6.7. Innovation, Research & Development

- Cyber threats continue to evolve in complexity and gravity requiring new solutions and approaches. Research and Development will provide a platform for innovation and creativity to deal with emerging issues in cyberspace.

7. MONITORING AND EVALUATION

The Monitoring and Evaluation Plan will enable the assessment of the operational issues encountered during the implementation of the strategy, as well as the assessment of the long-term impact and outcomes of the strategy based on periodic reviews. The Monitoring and Evaluation Plan will also provide mechanisms or tools for data collection and reporting, and further information on the roles and responsibilities of stakeholders, and frequency of reports.

The implementation of the NCS will require a Monitoring and Evaluation Framework that:

- Supports the attainment of the NCS Vision and Strategic Goals; and
- Enables accurate reporting on progress and identification of lessons learned and challenges encountered for informed decision making and effective planning.

This can be used to elaborate new measures as well as amend and tailor existing initiatives under the strategy. This section of the Strategy details the proposed systematic approach to monitoring and evaluating progress as an integral part in implementing the NCS of Malawi. The monitoring is scheduled to be periodic in order to track the progress of implementation of the NCS. The monitoring will, therefore, focus on periodic and objective assessment of progress towards the attainment of the set objectives.

The key objectives of the monitoring and evaluation approach are:

- Establishment of Performance Targets for various Government institutions or relevant stakeholders responsible for implementing specific actions of the NCS.
- Development of performance plans to establish a shared understanding of the expected end results, the approach to achieving these end results and identify the resources necessary to ensure a successful implementation. The plans will be based on the KPIs, Performance Targets and Deadlines provided in the Implementation Logical Framework
- Monitoring and reporting performance and progress in achieving expected end results by identifying and promptly reporting observed or likely deviations.
- Periodically evaluating institutional or individual performance against established performance targets

7.1. Monitoring

Implementation of this Strategy will be through annual work plans and budgets. The tasks detailed in the NCS implementation plan will form the basis for preparing annual work plans and budgets. In this regard, the Ministry of Information and Communications Technology and all relevant stakeholders will ensure that annual work plans and budgets are prepared within the framework of the Strategy.

Activities of this strategy will be continuously monitored and monthly performance reports will be prepared by all implementing agencies and submitted to MoICT. The Ministry will in turn submit to the National Steering Committee quarterly performance reports highlighting the progress made towards the achievement of key performance indicators (KPIs) in general and quarterly targets. Furthermore, quarterly monitoring exercises will be conducted. Lastly, a comprehensive annual progress report will be produced highlighting the progress made towards achievement of the KPIs in general and annual targets. The purpose of periodic reporting is to account for the resources utilized and output/results.

7.2. Joint Annual Reviews

The MICECT in conjunction with other stakeholders shall set the Terms of Reference for the Joint Annual Reviews (JARs). The JARs will start at organizational level, sector and national level in order to allow for wider participation and analysis of implementation bottlenecks. Participation at national level will include representatives from all ICT stakeholders, who will discuss policy recommendations from the organizations as well as sector and achieved Annual Implementation Plan milestones. Emphasis will be placed on challenges being experienced in the achievement of the targets and how these can best be addressed.

7.3. Evaluation

Performance evaluation is very important as it helps in objective comparison of actual against expected results and the resultant impact. In a changing environment, some of the key assumptions in the strategy may dramatically change and affect implementation of the set outcome targets. It is in the course of evaluation that the effects of such changes will be determined and appropriate corrective action taken. The evaluations, therefore, will assess the relevance of the strategic goals and objectives, efficiency and effectiveness of the strategies, assumptions, the strengths and weaknesses in the implementation of the NCS.

A mid-term and full review will be conducted. As such, an independent stakeholder will be commissioned to undertake the mid-term and long- term review of the strategy to determine the short and long-term impact and outcomes of the strategy based on annual reviews, and if necessary effect remedial actions following the mid-term review to keep implementation on track. The mid-term review will be undertaken at the end of 3rd Quarter of Year 3 of the Strategy and the long term review at the end of the 5th year.

APPENDIX A - NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION LOGICAL FRAMEWORKS

This section presents the key elements necessary to successfully implement the strategy detailed in Chapter 3 and these include:

- Strategic Goal: the substantive long term goal that Malawi would like to achieve in each priority area;
- Specific Objective: the specific steps to be undertaken to achieve the Strategic Goal
- Strategies/Actions: The activities that must be undertaken, under this Strategic Plan, in pursuit of the Specific Objective objectives
- Deliverables/Outputs: The formal work products that Malawi will achieve in the pursuit of the objectives and the implementation of the Strategy
- Lead Implementing Agency and Support: The Malawian Institutions with primary responsibility for managing completion of each objective, and the institutions that will provide support.
- Time Period: Period of time within which deliverables/outputs are produced and/or Strategies/ Actions are implemented.
- Key Performance Indicators: The indices, data measurements, and trends that should be monitored to evaluate the progress in implementing the Strategy and achieving the objectives and deliverables
- Possiible Funding Sources and Mechanisms: An overview of different possible funding sources and mechanisms that can be adopted by Malawi to fund the implementation of the NCS.

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Focus Area 1: Critical Information Infrastructure						
Strategic Goal – 1: Identify and manage the Critical Information Infrastructure of Malawi						
4.5.1 Specific Objective 1: **Identify and protect the Critical Information Infrastructure of Malawi**	4.5.1.1. Establish a National CII Register	National CII Register	MACRA/Malawi CERT/MICECT	Jan 2020 – Dec 2020	National CII Register	MACRA/Malawi CERT
	4.5.1.2. Create a National Vulnerability Register and Framework for regular vulnerability monitoring and disclosure for CII	National Vulnerability Register and Vulnerability Disclosure Framework	MACRA/MALAWI CERT CII /MICECT	Jan 2020 – Dec 2020	National vulnerability register	MACRA/Malawi CERT CII
	4.5.1.3. Establish a National Risk Register and Regulations and/or Guidelines that promote continuous risk assessment and management across CIIs in Malawi	Risk assessment and management guidelines for CIIs National Risk Register	MACRA/Malawi CERT Malawi CII/ MICECT	Nov 2019 – July 2020	National Risk Register Regulations /Guidelines on Risk assessment and management for CIIs	MACRA/Malawi CERT Malawi CII
4.5.2. Specific Objective 2: **Protect the Critical Information Infrastructure of Malawi.**	4.5.2.1. Develop a National CII Governance Framework which provides details on CII protection procedures and processes	National CII Governance Framework	MACRA/Malawi CERT Malawi CII/ MICECT	July 2020 – Mar 2021	National CII Governance Framework	MACRA/Malawi CERT
	4.5.2.2. Establish	CII Minimum	MICECT	Feb 2020 –	CII Minimum	MICECT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	Mandatory Equipment Specifications, Mandatory Guidelines, Regulations, Security Requirements, Procedures relating to the management of risks by CIIs	security standards and procedures including security audits, equipment specifications, SOPS, Access Control Mechanisms, etc.	MACRA/MALAWI CERT	Jan 2021	security standards and procedures	MACRA/MALAWI CERT
	4.5.2.3. Undertake continuous monitoring and regular testing to detect errors, vulnerabilities, and intrusions in CII	Security Audits and tests to detect errors and vulnerabilities Intrusion detection systems/exercises	CII MICECT MACRA/Malawi CERT	Jan 2020 – june 2024	Security audits reports Effectiveness of security audits and tests Intrusion detection tests/systems;	CII
	4.5.2.4. Promote and enhance regional and international cooperation in the protection of the critical information infrastructure (CII)	Regional and international collaboration Programmes Enhanced collaboration and information sharing	MICECT MACRA/MALAWI CERT	July 2020 – June 2024	Signed MoUs and agreements	MICECT MACRA/MALAWI CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		mechanism MOUs with international partners on the monitoring, analysis and management of cross border CII				
4.5.3. Specific Objective 3: **Continuously manage cyber threats and risks to enhance incident response.**	4.5.3.1. Expedite the establishment and operationalization of a national CERT with clear processes, defined roles and responsibilities	Establish and operationalize CERT hosted at MACRA	MACRA/Malawi CERT MICECT	Dec 2019 – May 2020	Staff recruitment and retention reports	MACRA/Malawi CERT
	4.5.3.2. Continuously develop the capacity of staff at Malawi National CERT to address the fast changing technical requirements, and develop abilities to actively obtain information in cyberspace, about current cyber risks and threats	Malawi CERT Training Programme	MACRA/Malawi CERT	Jan 2020 – June 2024	Number and frequency of MACRA/Malawi CERT Training sessions; Number of incidents/attacks/threats/risks prevented/mitigated by forensic detection and	MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
					analysis Capacity building plan	
	4.5.3.3. Develop a national incident reporting, information sharing and coordination mechanisms to address reporting of incidents and coordination in incident response	National Incident Reporting and Information Sharing Framework	MACRA/Malawi CERT	July 2020 – June 2021	Number of calls to help line or call center Number of incidents addressed through call line	MACRA/Malawi CERT
	4.5.3.4. Create and continuously update cybersecurity incidents register, assess incidents, and suggest measures to resolve issues and mitigate threats and risks	Real time cybersecurity incident registers; Measures to mitigate threats, risks and resolve incidents	MACRA/Malawi CERT	June 2020 – Dec 2020	Cybersecurity Incidents Register	MACRA/Malawi CERT
	4.5.3.5. Specify minimum and mandatory log/register requirements necessary for dependable cybersecurity incident analysis	Minimum and mandatory log requirements	MACRA/Malawi CERT	Mar 2020 – Aug 2020	Mandatory requirements register	MACRA/Malawi CERT
	4.5.3.6. Continuously monitor, analyse and	Real time overview of the	MACRA/Malawi CERT	Jul 2020 – June 2021	Monitoring Report	MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	assess cyber threats and potential risks and be able to provide a real time overview of the state of cybersecurity across the country	state of cybersecurity				
	4.5.3.7. Develop a Cybersecurity Governance Framework for defining roles and responsibilities of all stakeholders in the cybersecurity ecosystem as well as describe SOPs and Code of Conduct in responding to incidents	Cybersecurity Governance Framework that roles and responsibilities of all stakeholders in the cybersecurity ecosystem as well as describe SOPs and code of conduct in responding to incidents	MICECT MACRA/Malawi CERT	Jul 2020 – Dec 2020	Cybersecurity Governance Framework	MACRA/Malawi CERT
	4.5.3.8. Establish a call center/help line for reporting incidents or seeking assistance with incidents	National Cybersecurity Call Center/Help Line	MACRA/Malawi CERT	July 2021 – June 2022	Number of calls to help line or call center Number of incident reports addressed	MACRA/Malawi CERT
	4.5.3.9. Develop and implement cybersecurity incident simulation scenarios and programs	Cybersecurity incident simulation scenarios and	MACRA/Malawi CERT	feb 2020 – June 2024	Number of cybersecurity incident simulation scenarios and	MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	that can be used during the national exercises	programs			programs	
	4.5.3.10. Develop and continuously update cybersecurity contingency plans, which will include roles of the military/security forces during cyber-attacks and emergencies	Sector specific contingency plans (reviewed annually)	MACRA/Malawi CERT Malawi Defence Force	Jan 2021 – Jun 2021	Number of Cybersecurity contingency plans	MACRA/Malawi CERT Malawi Defence Force
	4.5.3.11. Develop and test requisite crisis management measures during frequent cyber drills	National crisis management Measures for Malawi Frequent cyber drills	MACRA/Malawi CERT	Feb 2020 – June 2024	National Crisis Management Measures	MACRA/Malawi CERT
	4.5.3.12. Evaluate cyber drills to develop options on how to improve crisis management measures	Lessons/Results of cyber drill exercise Frequent cyber drills	Malawi CERT MDF	Feb 2020 – June 2024	Evaluation Report No. of revisions of contingency plans	Malawi CERT MDF
	4.5.3.13. Develop a Cyber Defence Strategy that details approaches to addressing threats to national security in cyberspace	National Cyber Defence Strategy	MDF	July 2020 – June 2024	National Cyber Defence Strategy	MDF

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	4.5.3.14. Establish a Central Defence Command and Control Centre for cybersecurity in Malawi	A Central Defence Command and Control Centre for cybersecurity	MDF	Jan 2020 – June 2024	Central Defence Command and Control Centre for Cybersecurity	MDF
Focus Area 2: Cybersecurity Capacity						
Strategic Goal – 2: Develop and enhance cybersecurity-related capacity, infrastructure, legal, regulatory and other related frameworks						
4.5.4. Specific Objective 4: **Strengthen Malawi's legal and regulatory frameworks**	4.5.4.1. Undertake a gap analysis to identify gaps in current ICT Security Legal and Regulatory Framework and develop requisite instruments to address Gaps including issues relating to privacy and data protection.	A gap analysis to identify gaps in current ICT security legal and regulatory framework Requisite instruments to address Gaps including issues relating to privacy and data protection	MICECT Ministry of Justice and Constitutional Affairs MACRA	Jan 2021 – june 2023	Gap analysis reports New/Reviewed policies/legislations	MICECT Ministry of Justice and Constitutional Affairs MACRA
	4.5.4.2. Develop and publish a cybersecurity policy and standards consisting of general and sector-specific cybersecurity controls that would be recognized as a national standard	A Cybersecurity Framework (CSF) consisting of general and sector-specific policies and controls	MICECT MACRA	July 2021 – June 2023	National Cybersecurity policy	MICECT MACRA

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	4.5.4.3. Create a national programme to promote the adaptation and adoption of cyber standards across Government institutions and CII in Malawi	Deployment of national cyber standards across the nation	MICECT MACRA Malawi Bureau of Standards	July 2022 – June 2024	Number of promotion Programmes developed	MICECT MACRA Malawi Bureau of Standards
4.5.5. Specific Objective 5: **Build capacity of law enforcement agents and the judiciary**	4.5.5.1. Identify needs and then provide training and education to develop the capacities of the law enforcement agencies, judiciary and the legal fraternity on how to interpret and enforce the policy, legal and regulatory frameworks on cybersecurity in Malawi	Training programme for law enforcement agencies and judiciary on how to interpret and enforce the policy, legal & regulatory frameworks on cybersecurity in Malawi Strong law enforcement and judiciary capable enforcing the policy, legal & regulatory frameworks on cybersecurity in Malawi	Law Enforcement and Judiciary	July 2021 – June 2024	Needs assessment reports Number of capacity building Programmes conducted Number of personnel trained	Law Enforcement and Judiciary

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
4.5.6. Specific objective 6: **Enhance technical and procedural measures for CIIs**	4.5.6.1. Establish mandatory and minimum technology and security requirements for CIIs	Mandatory and minimum technology and security requirements for equipment of ISPs and end users	MACRA/Malawi CERT CIIs, ISPs and other end users	July 2021 – June 2022	Minimum technology and security requirements Guidelines	MACRA/Malawi CERT CIIs, ISPs and other end users
	4.5.6.2. Develop a national Government programme to deploy and manage Government ICT infrastructure	National programme to deploy and manage Government ICT infrastructure	MICECT	July 2020 – June 2021	National Government programme	MICECT
	4.5.6.3. Develop a national programme to enhance internet infrastructure development and resilience.	National programme to enhance internet infrastructure development and resilience	MICECT	July 2022 – June 2024	National programme	MICECT
	4.5.6.4. Develop National Contingency plans which identify emergency response asset priorities and standard operating procedures (SOPs)	National contingency plan	MACRA/Malawi CERT Malawi Defence Force	July 2021 – June 2023	Number of contingency plans developed	MACRA/Malawi CERT Malawi Defence Force
	4.5.6.5. Review and update the map of current emergency response assets	Emergency response asset map	MACRA/Malawi CERT	June 2021 – July 2022	Reviewed Emergency Response Asset	MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
			Malawi Defence Forces		Maps	Malawi Defence Forces
	4.5.6.6. Ensure communication channels are deployed across emergency response functions, geographic areas of responsibility, public and private responders, and command authority.	Emergency Communication Network	ICT/Communications service providers Malawi Defence Forces	july 2022 – June 2023	Emergency Communication Network	ICT/Communications Service Providers Malawi Defence Forces
4.5.7. Specific Objective 7: **Continuously develop cybersecurity technical capacity in Malawi**	4.5.7.1. Revise the National Research Agenda to promote R&D in cybersecurity in Malawi	Revised National Research Agenda which includes the cybersecurity aspects	Ministry of Education, Science and Technology (MoEST) Academia MICECT National Commission for Science and Technology (NCST)	July 2021 – June 2023	A revised National Research Agenda.	Ministry of Education, Science and Technology (MoEST) Academia MICECT National Research Council
	4.5.7.2. Establish a National Centre of Excellence for Cybersecurity Training & Research	Operational National Centre of Excellence for cybersecurity training &	MICECT Ministry of Education, Science and	July 2021 – June 2024	National Centre of Excellence	Ministry of Education, Science and Technology (MoEST)

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		research	Technology (MoEST) Academia National Commission for Science and Technology (NCST)			Academia Private sector
	4.5.7.3. Review and update primary, secondary and tertiary level education curriculum to include cybersecurity elements	Revised education curriculum which includes aspects about cybersecurity	Ministry of Education, Science and Technology (MoEST) Academia	July 2020 – June 2024	Revised education curriculum	Ministry of Education, Science and Technology (MoEST)
	4.5.7.4. Support cybersecurity competitions and R & D projects in Universities and Schools	Funding and incentive Programmes for universities engaged in cybersecurity R & D competitions in schools on cybersecurity	Academia; Ministry of Education, Science and Technology (MoEST) Private sector National Commission for	July 2022 – June 2024	Number of incentive Programmes for Universities	Academia; Ministry of Education, Science and Technology (MoEST) Private sector

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
			Science and Technology (NCST)			
	4.5.7.5. Support national enterprises providing cybersecurity solutions, and undertaking R & D in cybersecurity	Funding and incentive Programmes for Enterprises engaged in cybersecurity R & D	Academia; Ministry of Education, Science and Technology (MoEST)	July 2020 – June 2024	Number of incentive Programmes for enterprises.	Special incentive Programmes provided by Ministry of finance
	4.5.7.6. Collaborate with universities, colleges and the private sector to create new studies and internship programs on cybersecurity	New tertiary level study and internship programs on cybersecurity	Academia Ministry of Education, Science and Technology (MoEST) Ministry of Labour, Youth, Sports and Manpower development Private Sector	July 2021 – June 2024	Number of new tertiary level study and internship programs; Number of students/graduates on cybersecurity study/internship programme	Academia Ministry of Education, Science and Technology (MoEST) Ministry of Labour Private Sector

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	4.5.7.7. Collaborate with the private sector and academia to support participation of Government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity	Partnerships to support participation of Government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity	Academia Ministry of Education, Science and Technology (MoEST) National Commission for Science and Technology (NCST)	July 2021 – June 2024	Reports on partnerships created supporting participation in national and international research Number of partnerships	Academia Ministry of Education, Science and Technology (MoEST) Ministry of Labour National Commission for Science and Technology
	4.5.7.8. Develop standards in cybersecurity training and education	Standards for cybersecurity training and education	Ministry of Education, Science and Technology (MoEST)	July 2021 – June 2023	Cybersecurity training standards	Academia Ministry of Education, Science and Technology (MoEST)
	4.5.7.9. Train ICT personnel of various Government ministries and institutions on how to detect incidents, report incidents, and collaborate with the national CERT and	Training programme for IT personnel of various Government ministries and institutions	OPC/Department of Human Resources Management and Development(DHRMD)	July 2020 – June 2024	Number of IT personnel trained	OPC/Department of Human Resources Management and Development(DHRMD)

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	institutions from other sectors on cybersecurity		Academia Ministry of Education, Science and Technology (MoEST) Ministry of Labour MICECT			Ministry of Education, Science and Technology (MoEST) Ministry of Labour MICECT
4.5.8. Specific Objective 8: **Facilitate retention of cybersecurity expertise within Malawi**	4.5.8.1. Develop National and Career Progression Policy promoting continuous training and education for Incident Response and addressing issues relating to cybersecurity	National Policy promoting continuous training and education for incident response and addressing countermeasures for CERT and security personnel Career progression strategy that promotes continuous professional	OPC/Department of Human Resources Management and Development(DHRMD) Ministry of Labour	July 2020 – June 2023	National career progression Policy.	OPC/Department of Human Resources Management and Development(DRHRD) Ministry of Labour

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		education				
	4.5.8.2. Identify the staffing requirements for Government agencies and CII operators	Set of staffing requirements for Government agencies and Critical Infrastructure operators Cybersecurity staffing recruitment and retention strategy	OPC/Department of Human Resources Management and Development(DHRMD) Ministry of Labour	July 2021 – June 2024	Staffing requirements Report National recruitment and retention strategy	OPC/Department of Human Resources Management and Development(DHRMD) Ministry of Labour
	4.5.8.3. Develop a national recruitment and retention strategy	National Recruitment and Retention Strategy	OPC/Department of Human Resources Management and Development(DHRMD) Ministry of Labour	Jul 2021 – Jun 2024	National Recruitment and Retention Strategy	OPC/Department of Human Resources Management and Development(DHRMD) Ministry of Labour
	4.5.8.4. Develop and implement cybersecurity training and capacity building training plans for Government personnel.	National cybersecurity training and capacity building training plans for Government	OPC/Department of Human Resources Management and Development(DHRMD)	July 2021 – June 2023	Annual Training Plans Number personnel trained	OPC/Department of Human Resources Management and Development(DHRMD)

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		Personnel	Ministry of Labour			Ministry of Labour
Focus Area 3: Cybersecurity awareness & collaboration						
Strategic Goal – 3: Promote awareness, information sharing and collaboration on cybersecurity						
4.5.9. Specific Objective 9: **Enhance cybersecurity awareness across the general public and national institutions**	4.5.9.1. Undertake a nationwide assessment to determine level of awareness of cybersecurity across the nation	Assessment of national levels of cybersecurity awareness	MACRA/Malawi CERT	July 2020 – June 2024	Situation/ Assessment Report	MACRA/Malawi CERT
	4.5.9.2. Develop and implement a national roadmap for improving awareness of current cybersecurity trends and threats	National roadmap for improving awareness of current cybersecurity trends Up to date and functional website with information current cybersecurity threats, risks, vulnerabilities, etc.; Awareness campaigns to	MICECT MACRA/Malawi CERT	July 2021 – June 2024	National roadmap for awareness of cybersecurity Number/frequency of cybersecurity campaigns Up to date website	MICECT MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		raise awareness of cybersecurity trends and threats				
	4.5.9.3. Develop and disseminate National Cybersecurity Best Practices to ingrain a cybersecurity mindset in the public	National cybersecurity best practices	MACRA/Malawi CERT	July 2020 – June 2022	National Cybersecurity Best Practices.	MACRA/Malawi CERT
	4.5.9.4. Undertake mandatory training of Board Members of different organizations to enhance their understanding of cyber issues and how their organizations address these threats.	Mandatory training of Board Members of different organizations	MACRA CII	July 2020 – June 2022	Number of training Programmes Number of Board members trained	MACRA CII
4.5.10. Specific Objective 10: Promote collaboration and information sharing on Cybersecurity.	4.5.10.1. Create a national forum to enhance and promote information sharing and collaboration nationally on cybersecurity	National Forum for national information sharing and collaboration	MACRA, MICECT	July 2020 – June 2021	National working group	MACRA, MICECT
	4.5.10.2. Continuously update the citizens, the private sector and the public sector, on information related to cyber threats, vulnerabilities, incidents, activities across	Online Platform which provides national cybersecurity-related information	MACRA, MICECT	July 2020 – June 2021	Number of awareness Programmes	MACRA, MICECT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	the nation to foster trust					
Focus Area 4: Vulnerable groups in cyber space						
Strategic Goal – 4: Enable and continuously improve the safety of vulnerable groups in cyberspace, especially the safety of children						
4.5.11. Specific Objective 11: **Strengthen online safety for vulnerable groups, especially children**	4.5.11.1. Develop and disseminate online safety guidelines and best practices to protect vulnerable groups in Malawi, especially children, from cyber threats	Guidelines and best practices to protect children and other vulnerable groups from cyber threats	MACRA, MICECT, CONGOMA	July 2020 – June 2021	Online Safety guidelines	MACRA, MICECT, CONGOMA
	4.5.11.2. Deploy special awareness Programmes to target and inform children and other vulnerable groups about safe and responsible use of the internet	Special online Safety awareness programme for children and other vulnerable groups	MACRA, MICECT, CONGOMA	July 2020 – June 2021	Number of special online safety awareness programme for children and other vulnerable groups Number of children and members of other vulnerable groups with skills on how to use the internet safely	MACRA, MICECT, CONGOMA

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	4.5.11.3. Promote the deployment of technical measures or web filtering tools that prevent access to harmful content by children and other vulnerable groups	Wide deployment of technical measures to prevent access to harmful content by children and other vulnerable groups	Operators; ISPs	Jul 2020 – June 2021	Number of measures deployed	Operators; ISPs
	4.5.11.4. Encourage ISPs and other services providers to make their clients, especially parents and guardians aware of how to leverage available tools, technologies to manage potential risks to vulnerable groups while accessing services online	Knowledge and awareness of tools/technologies that can be deployed by ISPs and other service providers to keep children and other vulnerable groups safe online;	MACRA Operators; ISPs	Jul 2020 – June 2021	Number of awareness Programmes by ISPs	MACRA Operators; ISPs
Focus Area 5: Cybersecurity Coordination						
Strategic Goal – 5: Enhance and coordinate the fight against all forms of cybercrime						
4.5.12. Specific Objective 12: **Strengthen**	4.5.12.1. Establish the requisite framework and operationalize a Digital Forensics Laboratory	Operational digital forensics laboratory Plans and	Malawi Police Services Ministry of Justice and	Jul 2020 – June 2022	l Digital Forensics Laboratory	Malawi Police Services Ministry of Justice and

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Cybercrime detection		budgets to establish Digital forensics lab	Constitutional Affairs			Constitutional Affairs
	4.5.12.2. Develop mandatory digital forensics and evidence handling courses for the judiciary, law enforcement and personnel from other related agencies involved in the detection and prosecution of cybercrime	Training programme on digital forensics and evidence handling	Malawi Police Services, Ministry of Justice and Constitutional Affairs	Jul 2020 – June 2024	Number of training courses. Number of successful prosecutions of cybercrimes	Malawi Police Services Ministry of Justice and Constitutional Affairs
	4.5.12.3. Build and enhance capacity to detect cybercrime incidents	Training Programme and Budget on cybercrime incident detection	Malawi Police Services, Ministry of Justice and Constitutional Affairs.	Jul 2020 – June 2024	Number of capacity building programs	Malawi Police Services Ministry of Justice and Constitutional Affairs.
4.5.13. Specific Objective 13: **Promote national and international collaboration in the fight against**	4.5.13.1. Develop and continuously update an information sharing, governance and collaboration framework for the fight against cybercrime which will include links that ensure direct and timely	Governance Framework for fight against cybercrime	Malawi Police Forces Other Security Forces; Judiciary and Ministry of Justice and Constitutional	Jul 2020 – June 2024	National cybersecurity governance framework	Malawi Police Forces Other Security Forces; Judiciary and Ministry of Justice and Constitutional

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
cybercrimes	collaboration between judiciary, law enforcement and personnel from other related agencies, service providers, CII entities, Malawi CERT and other Government institutions on issues that concern cybercrime and Cybersecurity		Affairs. MACRA/MALAWI CERT			Affairs. MACRA/MALAWI CERT
	4.5.13.2. Strengthen collaboration with regional, international states and partners in combating cybercrime through treaties, conventions (e.g. Budapest) and bilateral agreements, especially through frameworks such as the 24/7 cybercrime Network, mutual legal assistance frameworks.	Signatures of relevant international treaty agreements on cybercrime MOUs between other countries and international partners Participation in international forums on cybercrime	Ministry of Foreign Affairs and International Cooperation Malawi Police Service	Jul 2020 – June 2023	Number of signed MOUs Number of signed international treaties	Ministry of Foreign Affairs Malawi Police Forces
	4.5.13.3. Develop a clear plan that outlines how to manage international collaboration across multiple strategy areas such as law enforcement, incidence response,	International collaboration management plan Improved international	MACRA, MICECT	July 2020 – June 2021	International collaboration management plan	MACRA, MICECT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	research and innovation in cybersecurity.	collaboration				
	4.5.13.4. Subscribe to and participate in all relevant regional and international forums on cybersecurity.	Improved regional and international collaboration on cybersecurity Participation in relevant regional and international fora on cybersecurity	MACRA, MICECT	July 2020-June 2024	Number of regional and international bodies subscribed to	MACRA, MICECT
Focus Area 6: Secure Usage of cyber space						
Strategic Goal – 6: Promote use of secure cyberspace to drive social and economic development						
4.5.14. Specific Objective 14: **Enhance trust and confidence in cyberspace, especially in applications relating to e-Government and e-commerce.**	4.5.14.1. Create, and continuously update the general public and public sector on how cyberspace is securely used in Malawi to deliver e-Government and e-commerce services in Malawi, highlighting the various security features deployed to foster trust	E-Governance and E-commerce services awareness campaign that highlights the security features of	MICECT	July 2020 – June 2024	Number of E-Government and e-Commerce Services Awareness Campaigns.	MICECT
	4.5.14.2. Encourage the use of Public Key	PKI implementation	MICECT	July 2021 – June 2022	Number of Government ICT	MICECT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	Infrastructure (PKI) for transactions to/from Government Ministries, Departments and Agencies to enhance high cybersecurity levels and trust in delivering public services.	plan			systems and applications incorporating usage of PKI	
	4.5.14.3. Appoint cybersecurity inspectors whom among other duties will serve as focal points of contacts to support small and medium enterprises in addressing cybersecurity needs and method of mitigating cyber threats.	Cybersecurity inspectors to support small and medium enterprises on cybersecurity	MACRA	July 2021 – June 20233	Number of Cybersecurity Inspectors	MACRA
	4.5.14.4. Undertake the transition from IPV4 to IPV6 protocol and disseminate information on the benefits of the transition, especially IPV6 security features relating to confidentiality, authentication and data integrity	IPV4 to IPV6 Implementation Plan	MICECT MICECT	July 2021 – June 2022	IPV4 to IPV6 Implementation Plan	MICECT MICECT