United Nations
Economic Commission for Africa

Guidelines for a model law on computer-enabled and computer-related crimes in African Union member States

United Nations
Economic Commission for Africa

Guidelines for a model law on computer-enabled and computer-related crimes in African Union member States

To order copies of ***Guidelines for a model law on computer-enabled and computer-related crimes in African Union member States*** by the Economic Commission for Africa, please contact:

Publications and Conference Management Section
Economic Commission for Africa
P.O. Box 3001
Addis Ababa, Ethiopia
Tel: +251 11 544-9900
Fax: +251 11 551-4416
E-mail: eca-info@un.org
Web: www.uneca.org

First printing: April 2023

Designed and printed in Addis Ababa by the ECA Printing and Publishing Unit. ISO 14001:2015 certified.
Printed on chlorine free paper.

Cover photo: Shutterstock

Tables and Figures

PART I: Introduction

These guidelines provide guidance to member States of the African Union in designing cybersecurity legislation and on the key features and benefits of a standardized cybersecurity law.

1. Background

The implementation of cybersecurity legislation is an essential component of the regional response to ensuring cybersecurity in Africa. The fourth recommendation set out in the Road Map for Digital Cooperation of the United Nations (A/74/821) is to promote digital trust, security and stability. Following a declaration adopted by the African Union Commission Specialized Technical Committee on Communication and Information and Communications Technology in 2019 (AU/STC-CICT-3/MIN//Decl.), the African Union Commission developed a Digital Transformation Strategy for Africa for the period 2020–2030, which highlights the need for a greater capacity to detect and mitigate cyberattacks and the fundamental responsibility of African Governments to create an enabling environment with policies and regulations that promote digital transformation across foundational pillars, including cybersecurity.[1] In the Strategy, it is also stated that collaborative regulatory measures and tools in the field of information and communications technology (ICT) are the new frontier for regulators and policymakers as they work towards maximizing the opportunities afforded by digital transformation across industries.[2] Digital transformation offers Africa tremendous opportunities; however, effective, and efficient digital transformation in Africa can only be achieved with cybersecurity.

It is necessary to develop guidelines for a model law that can provide assistance to African Union member States in the drafting of cybersecurity legislation that is compatible with best practices. In order to ensure a minimum set of baseline standards by which African Governments can address cybersecurity, the present guidelines have been produced with due consideration of existing national cybersecurity legislation in Africa, the African Union Convention on Cyber Security and Personal Data Protection of 2014, the Council of

1 African Union, "The digital transformation strategy for Africa (2020–2030)", p. 7.
2 Ibid.

Europe Convention on Cybercrime of 2001, and the United Nations Norms of Responsible State Behaviour in Cyberspace established by the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. The guidelines also draw on other current and proposed regional and international efforts in the field of cybersecurity, including efforts to develop a United Nations global convention on countering the use of ICT for criminal purposes.

2. Scope of the guidelines

The guidelines are a set of non-binding guiding principles that African Union member States may follow as they begin to establish standards for ensuring cybersecurity and for cybercrime laws. The guidelines do not limit the operation of any existing or future national or regional law that expressly or implicitly regulates cybersecurity or prohibits activity regarded as a cybercriminal offence in a given jurisdiction. The guidelines do not provide specific legislative language for stipulating the provisions of cybersecurity or cybercrime laws or the implementation of such laws; rather, in recognition of the sovereignty of States and the variation in their national legal systems, the precise language of such laws is left to the discretion of States.

3. Purpose of the guidelines

Cybersecurity legislation covers the regulation, maintenance and promotion of cybersecurity activities, critical national infrastructure and computer-related services. The guidelines are designed to assist African Union member States in drafting, reforming and modernizing their cybersecurity laws so as to take into account the particular features and needs of promoting cybersecurity in the region. The guidelines are for use by African States and African policymakers and legislators who wish to understand the valuable components of a model cybersecurity law.

The guidelines are aimed at linking best practices regarding substantive offences, powers and mutual legal assistance, such as those enunciated in regional and international cybersecurity treaties, with specific examples of standards, principles and measures that define the various elements that need to be included in cybersecurity legislation. They also provide guidance on provisions relating to respect for human rights, law enforcement stand-

ards, and judicial or other types of oversight. Poorly drafted cybersecurity laws that diverge from international best practices can have a negative effect on efforts to promote cybersecurity and on regional and international cooperation. Ineffectively drafted model laws can also cause countries to enact inadequate cybercrime legislation, while at the same time criminalizing and labelling conduct as cybercrime that other countries may not view as cybercrime. It is therefore important that countries follow an appropriate model for developing cybersecurity legislation.

The guidelines contain a discussion of standard cybersecurity measures, including those aimed at recognizing offences, and provide definitions of the types of acts than can be criminalized under a model cybersecurity law. States, lawmakers and regulators are encouraged to provide guidance for creating cybersecurity programmes that are flexible, scalable, practical and consistent with global best practices. Ultimately, the guidelines provide recommendations on standards for cybersecurity laws and regulations in African jurisdictions. They also provide guidance on law enforcement activities that can be undertaken to ensure cybersecurity while prioritizing respect for human rights in accordance with international and regional human rights standards.

4. Definition of terms

(1) "Competent authority" shall mean a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorize or undertake the execution of measures under the national cybersecurity legislation with respect to specific criminal investigations or proceedings.

(2) "Computer data" shall mean any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program designed to cause a computer system to perform a function.

(3) "Computer extortion" shall mean an attack or a threat of an attack accompanied by a demand for money or some other response in return for remediating or stopping the attack.

(4) "Computer system" shall mean any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

(5) "Corporation" shall mean a limited liability undertaking within the meaning of the applicable national legislation of a State.

(6) "Critical infrastructure" shall mean all the assets, systems and networks – physical and virtual – that are essential to the proper functioning of a country's economy, public health, safety and security, or any combination thereof.

(7) "Cybercrime" shall mean, for the purpose of these guidelines, conduct as defined in Part II. General offences.

(8) "Cybersecurity" shall mean the state of protection against the criminal or unauthorized use of computer systems and data, the measures taken to ensure such protection and the activities necessary to protect network and information systems, the users of such systems and other persons affected by cyberthreats.

(9) "Cybersquatting" shall mean registering, selling or using a domain name with the intent of profiting from the goodwill associated with another person's trademark or business reputation.

(10) "Cyberthreat" shall mean any potential circumstance, event or action that could damage, disrupt or otherwise have an adverse impact on network and information systems, the users of such systems and other persons.

(11) "Data controller" shall mean a natural or legal person, public authority, agency or other body that, alone or with others, determines the purpose and means of processing personal data.

(12) "Denial of service attacks" shall mean activities that prevent a rightful user from accessing a computer system, or rapid and continuous online requests that are sent to a targeted server in order to overload the server.

(13) "Fraudulent inducement" shall mean deceitful practices designed to persuade another party to act against their own best interest and to the advantage of the party engaging in the deceitful practice.

(14) "Guidelines" shall mean suggested cybersecurity legislative content for African Union member States, designed by the Economic Commission for Africa, that is not part of any country's body of legislation and that is aimed at supporting the introduction of new legislation or reforming existing law.

(15) "Interception" shall mean the monitoring, modifying, viewing or recording of non-public transmissions of data to or from a com-

puter system over a telecommunications system, and, in relation to a function of a computer system, includes listening to or recording such a function or acquiring the substance, meaning or purport of such function.

(16) "Malware and viruses" shall mean a set of computer instructions that are designed to infect computer programs or computer data, modify, destroy, record or transmit data, or disrupt the normal operation of a computer system.

(17) "Officer", in relation to a corporation, shall mean any director, partner, chief executive, manager, secretary or other similar officer of the corporation, and includes any person purporting to act in such capacity; for a corporation whose affairs are managed by its members, the term shall refer to any of those members in their capacity as officers of the corporation as defined in this paragraph.

(18) "Personal data" shall mean information relating to an identified or identifiable natural person.

(19) "Personal or human identifier" shall mean a subset of personally identifiable information and data elements that identify an individual and can permit another person to assume that individual's identity without his or her knowledge or consent.

(20) "Ransomware" shall mean computer malware that is installed covertly in a computer system, computer program or computer data to prevent access to it.

(21) "Requested State" shall mean the State being requested to provide legal assistance.

(22) "Requesting State" shall mean the State requesting legal assistance and may include an international entity to which a State is obligated.

(23) "Safe harbour" shall mean a national legal provision that will shield an individual or entity in certain circumstances from being held liable for activities.

(24) "Service provider" shall mean a public or private entity that provides, to users of its services, the means to communicate by use of a computer system, and any other entity that processes or stores computer data on behalf of that entity or the users of its services.

(25) "State of mind" of a person shall mean the knowledge, intention, opinion or belief of the person and the person's reasons for the intention, opinion or belief.

(26) "Unauthorized access" shall mean trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing, computer resources without lawful consent.

(27) "Vulnerable person" shall mean a natural person who is susceptible to being disadvantaged, owing to particular characteristics, including age, disability, gender or location.

5. General scope

(1) The cybersecurity legislation of States must be focused on the prevention, investigation and prosecution of cyberdependent and cyberenabled offences that are criminalized under statutes established in accordance with national legislation.

(2) Such legislation must be drafted with a view to responding to, managing and preventing cybersecurity threats or incidents that occur within and outside the country and that may threaten the lives and property of citizens and residents and the national security and defence of the State.

(3) Generally, cybersecurity law covers cyberservices that are essential for the functioning of society, State and local authorities, network and information systems and critical infrastructure, and should be aimed at imposing adequate measures to ensure organizational, physical and information security and to prevent, mitigate and resolve cyberthreats and incidents.

(4) States must ensure that, in national cybersecurity legislation, the protection of human rights and fundamental freedoms is prioritized, public-private partnerships are ensured and States are encouraged to engage in public education, research and training to enhance knowledge and skills pertaining to cybersecurity.

PART II: General offences

6. Illegal and unauthorized access

(1) States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without authorization or exceeding authorization, gaining access to the whole or a part of a computer system, including access in relation to a computer system that is connected to another computer system, or any action that obtains, alters or prevents authorized access.

(2) States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without authorization or exceeding authorization, any act causing a computer to perform any function to obtain, secure or prevent access to a computer program, system or data held in that computer.

7. Illegal interception

States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, without authorization and without lawful excuse or justification, the interception of computer data being transmitted to, from or within a computer system, including in relation to a computer system that is connected to another computer system.

8. Misuse of computer devices and access codes

States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without justification, the production, sale, procurement for use, possession, importation and distribution of the following:

a) A device, including a computer program, designed or adapted primarily for the purpose of committing any offence established in the national legislation as a cybercriminal offence;

b) A computer password, access code or similar data through which the whole or any part of a computer system is capable of being

accessed, with the intent that it be used for the purpose of committing any offence established in the national legislation as a cybercriminal offence.

9. Unauthorized modification of a computer program or data

(1) States shall adopt such legislative and other measures as may be necessary to establish as criminal offences the intentional and direct or indirect unauthorized modification of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

(2) A modification of a computer program or data will be considered as such if:

a) A program or data held in the computer are damaged, altered or erased without authorization;

b) A program or data are added to or removed from a program or electronic record held in the computer system;

c) An act is carried out that impairs the normal operation of any computer or program therein or causes normal operation to deteriorate.

(3) It shall be immaterial whether the unauthorized modification or interference is, or is intended to be, permanent or temporary.

10. Unauthorized interference in computer systems

(1) States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, without authorization and without lawful excuse or justification, the interference in the functioning of a computer system or the hindering of a person who is lawfully using or operating a computer.

(2) Interference or hindrance includes but is not limited to:

a) Preventing the functioning of a computer system by any means;

b) Causing electrical, electronic or electromagnetic interference to a computer system;

c) Causing denial-of-service attacks;

d) Defacing websites;

e) Corrupting a computer system by any means, including through the use of malware and viruses.

(3) It shall be immaterial whether the unauthorized interference is, or is intended to be, permanent or temporary.

11. Child pornography

(1) States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally or negligently in relation to the protection of children, the following acts:
   a) Publishing child pornography through a computer system;
   b) Distributing child pornography through a computer system;
   c) Producing child pornography for the purpose of its publication or distribution through a computer system;
   d) Possessing child pornography in a computer system or on a computer-data storage medium.

(2) Child pornography includes material that visually depicts:
   a) A child engaged in sexually explicit conduct;
   b) A person who appears to be a child engaged in sexually explicit conduct;
   c) Images representing a child engaged in sexually explicit conduct;
   d) Unauthorized images of nude children.

(3) "Child" shall mean a person under the age of 18 or as otherwise defined in national legislation.

(4) "Publish" shall mean to transmit, disseminate, circulate, deliver or exhibit.

(5) "Distribute" shall mean to exchange, barter, lend, sell or offer for sale, let on hire or offer to let on hire, offer in any other way or make available in any way.

(6) "Possession" shall mean to have in possession or custody or under control.

(7) "Produce" shall mean to print, photograph, copy or make in any other manner.

12. Misleading content targeted at children

States may adopt such legislative and other measures as may be necessary to establish as criminal offences the use of misleading words or digital images on the Internet targeted at children and aimed at grooming children to enable the commission of criminal acts, including the creation of domain names on the Internet to deceive minors to enable the commission of acts that may be considered criminal under national legislation.

13. Offences in relation to identity

States may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the following acts:

a) Assuming the identity of another person (whether living, deceased, natural or corporate) with or through access to a computer system or in relation to other standards stipulated in national law;
b) Obtaining, disclosing or procuring the personal data or personal or human identifier of a living or deceased person in order to assume the identity of such person with the intent to commit or facilitate the commission of a criminal offence with or through access to a computer system.

14. Denial of service attacks

States may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the following acts:

a) Flooding the bandwidth or resources of a targeted computer system or servers with traffic, thereby preventing the legitimate users from accessing information or services;
b) Compromising and taking control of multiple computers with security flaws in order to use them to commit the act described in subparagraph (a) above.

15. Ransomware and computer extortion

States may adopt such legislative and other measures as may be necessary to establish as criminal offences the intentional covert installation of malware or viruses on a computer system, thereby preventing access to it, followed by demands for a ransom payment in exchange for returning access or not publishing or exposing data held on the computer system.

16. Fraudulent inducement

States may adopt such legislative and other measures as may be necessary to establish as criminal offences the intentional and fraudulent sending of unrequested or unsolicited messages by electronic means, or the creation of deceptive websites or Internet hyperlinks, to elicit personal or financial information from unsuspecting victims, with the intent to use such information for fraudulent purposes or other purposes of beneficial interest to the perpetrator.

17. Online infringement of copyright and related rights

States may adopt such legislative and other measures as may be necessary to establish as criminal offences the online infringement of copyright, including defining the liability of intermediaries when they act outside the scope of safe-harbour provisions.

18. Cybersquatting

States may adopt such legislative and other measures as may be necessary to establish as criminal offences the intentional taking or making use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the Internet or any other computer network, without authority or right and with the intent to benefit therefrom.

19. Unlawful obtention of personal data

(1) States may adopt such legislative and other measures as may be necessary to establish as criminal offences any act committed by a person knowingly or recklessly with the intent to:

a) Obtain or disclose personal data without the consent of a data controller;
b) Elicit the disclosure of personal data to another person without the consent of a data controller;
c) Retain the personal data without the consent of the person who was the data controller when the data were obtained;
d) Sell or offer to sell personal data that were obtained in the circumstances stated in the present paragraph.

(2) Paragraph (1) above may not apply if the obtention, disclosure, procurement or retention of personal data:
a) Was necessary for the purposes of preventing or detecting crime;
b) Was required or authorized by the enactment of a law, a rule or the order of a court or tribunal;
c) Was justified as being in the public interest.

PART III: Criminal Procedure and Determination of Liability

20. Criminal intent

States shall adopt such legislative and other measures as may be necessary to establish intent where a person through computer enablement, whether in part or in whole, is deemed to intend to cause or contributes to causing an offence established under the national legislation that results from the use of or intervention in a computer system.

21. Criminal negligence

States shall adopt such legislative and other measures as may be necessary to establish criminal negligence where a person through computer enablement, whether in part or in whole, is deemed to have negligently caused an event, if, without intending to cause the event, the person causes it by voluntary action from the use of or intervention in a computer system without due care, as would be reasonably necessary under such circumstances.

22. Attempt, aiding and abetting, and conspiracy

(1) States shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, an attempt to commit any cyberoffence established in the national legislation.

(2) States may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, aiding or abetting in the commission of any offence established as a cybercriminal offence in accordance with national law.

(3) (3) States may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, conspiracy to commit any offence established as a cybercriminal offence in accordance with national law, whether the medium used in whole or in part was cyberenabled.

23. Liability of persons

(1) States shall ensure compliance and effective enforcement of cybersecurity legislation by imposing convictions, sentencing and punitive measures for the commission of offences outlined in legislation.

(2) States shall adopt such legislative and other measures as may be necessary, consistent with and subject to their domestic laws, to ensure that legal persons other than the State and public institutions can be held liable for offences established in national cybersecurity legislation that are committed on their behalf by their organs or representatives.

(3) Such liability may be criminal, civil or administrative and shall not exclude or be without prejudice to the criminal liability of the natural persons who have committed such offences.

(4) States shall hold liable both natural and legal persons for the commission of offences established in accordance with their national cybersecurity laws through the application of sanctions that are effective, necessary and proportionate.

24. Offences by corporations

(1) States may ensure that, in a proceeding for an offence under national cybersecurity legislation, it shall be evidence that the corporation had a particular state of mind in relation to a particular act where there is evidence that:

a) An officer, employee or agent of the corporation acted within the scope of his or her actual or apparent authority;

b) The officer, employee or agent had that state of mind.

(2) Where a corporation commits an offence stipulated as a cybercriminal offence under national legislation, a person shall be liable for the same offence as the corporation if that person is either:

a) An officer of the corporation, or a member of the corporation (in the case where the affairs of the corporation are managed by its members);

b) An individual involved in the management of the corporation and in a position to influence the conduct of the corporation in relation to the commission of the offence.

(3) Where a corporation commits an offence stipulated as a cyber-criminal offence under national legislation, a person shall be liable for the same offence as the corporation if that person either:

a) Consented, connived or conspired with others to cause the commission of the offence;

b) Is in any other way, whether by act or omission, intentionally party to the commission of the offence by the corporation;

c) Knew or ought reasonably to have known that the offence by the corporation would be or was being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence.

PART IV: Criminal Procedure and Law Enforcement

25. Procedural and substantive powers

States shall develop and maintain an effective and rule-of-law-based national criminal justice system that can ensure that any person prosecuted for offences covered in the national cybersecurity legislation is brought to justice, while ensuring full protection of human rights and fundamental freedoms in accordance with the African Charter on Human and Peoples' Rights and other international human rights instruments.

26. Scope of procedural measures

(1) States shall adopt such legislative and other measures as may be necessary to establish the powers and procedures required for the purpose of specific criminal investigations or proceedings.

(2) States shall apply such powers and procedures to:

a) The offences established in their national legislation as cybercriminal offences;

b) The collection of evidence in electronic or digital form of a criminal offence established in their national legislation as a cybercriminal offence.

27. Conditions and safeguards

States shall ensure that the establishment, implementation and application of powers and procedures are subject to conditions and safeguards provided for under their domestic laws, which shall provide for the total protection of human rights and fundamental freedoms, in line with international and regional human rights standards, including rights arising pursuant to the obligations that States may have undertaken pursuant to the African Charter on Human and Peoples' Rights.

28. Preservation and disclosure of computer data

Subject to appropriate standards and legal domestic considerations, States may adopt such measures as may be necessary to enable their competent authorities to order the preservation and disclosure of data that have been stored by means of a computer program or system, in particular where such data are relevant for investigation purposes, law enforcement or judicial processes.

29. Production and obtention of computer data

States shall adopt such measures as may be necessary to empower their competent authorities to order:

a) Persons in their territory to submit specified computer data in the person's possession or control;
b) A service provider offering its services in their territory to submit data or information on services or service users that is in the service provider's possession or control.

30. Search and seizure of stored computer data

(1) States shall adopt such measures as may be necessary to empower their competent authorities to search or access:
   a) A computer system or part of it and computer data stored therein;
   b) A computer-data storage medium in which computer data may be stored on their territory.

(2) States shall adopt such measures as may be necessary to ensure that, where its authorities search or similarly gain access to a specific computer system or part of it, and have grounds to believe that the data sought are located or stored in another computer system, or are connected to or form part of another computer system in their territory, and such data are lawfully accessible from, or available to, the initial system, the authorities shall be granted powers within lawful standards to extend the search or gain access to that other computer system.

(3) States shall adopt such legislative and other measures as may be necessary to empower their competent authorities to seize or

take into their possession where necessary such computer data as have been accessed. These measures shall include the power to:

a) Seize or similarly secure a computer system or part of it or a computer-data storage medium;
b) Make and retain a copy of those computer data;
c) Facilitate the integrity of the relevant stored computer data;
d) Render inaccessible or remove those computer data in the accessed computer system.

31. Authorized warrants

(1) States shall authorize competent authorities, upon application to a competent court of appropriate jurisdiction, to issue an interception warrant to facilitate the demand for, collection of and/or recording of computer data, where such specified data are necessary for law enforcement, criminal investigation or criminal proceedings.

(2) States shall provide that, upon satisfaction on the basis of an application to a court of competent jurisdiction by a law enforcement officer that a specified item of computer data is reasonably required for the purpose of a criminal investigation or criminal proceedings, the court may order that:

a) A person in control of a computer system produce the specified computer data;
b) An Internet service provider produce specified computer data or produce information about persons who subscribe to or otherwise use the service.

32. Blocking, filtering and removal of illegal content

Taking into account the principles of legitimacy, necessity and proportionality, States may adopt such legislative and other measures as may be necessary to provide powers to competent authorities for the blocking, filtering and removal of illegal content on the order of a court, on certain specified legal grounds, for the purpose of ensuring cybersecurity, or for the purpose of ensuring the respect of the rights of citizens in relation to cyberenabled criminal activities.

33. Jurisdictional scope

(1) States shall adopt such measures as may be necessary to exercise criminal jurisdiction over the cyberenabled offences established in accordance with their national laws if either:

a) The offence is committed in the territory of that State;

b) The offence is committed on board a vessel that is flying the flag of that State or an aircraft registered under the laws of that State at the time the offence is committed;

c) The offence is committed by one of its nationals, if the offence is punishable under the national cybercrime law in the place where it was committed, or if the offence is committed outside the territorial jurisdiction of any State.

(2) States may also establish their jurisdiction over any such offence when:

a) The offence is committed against a national of that State;

b) The offence is committed by a national of that State or a stateless person who has his or her habitual residence in its territory.

(3) States may also adopt such measures as may be necessary to establish jurisdiction over the offences covered by their national cybersecurity legislation when the alleged offender is present in the State's territory and the State does not extradite the offender on the grounds of nationality pursuant to a request for extradition.

(4) Having regard to the principle of double criminality, States intending to exercise jurisdiction over cybercriminal offences established in their national cybersecurity legislation in cases where one or more States are already conducting an investigation, prosecution or judicial proceeding in respect of the same conduct shall, without prejudice to norms of general international law, consult one another with a view to coordinating their actions in respect of the exercise of jurisdiction.

PART V: Cybersecurity Cooperation

34. Cooperation and mutual legal assistance

(1) States shall develop appropriate policies for coordinating the sharing of cybersecurity information among relevant security sectors to increase the volume, timeliness and quality of cyberthreat information-sharing so that States may better protect and defend themselves against cyberthreats.

(2) States shall develop appropriate policies to coordinate voluntary programmes for sharing information among public and private sector entities with a view to enhancing classified cyberthreat and technical information-sharing among law enforcement bodies and other stakeholders that provide cybersecurity services.

35. Measures to enhance law enforcement cooperation

(1) States may take appropriate measures to ensure law enforcement cooperation. States shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat cybercriminal offences covered under their national cybersecurity legislation. States shall in particular, adopt effective measures:

a) To enhance and, where necessary, to establish channels of communication among their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered under their national cybersecurity legislation;

b) To cooperate with other States in conducting inquiries with respect to offences covered under their national cybersecurity legislation, including:

i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;

ii) The movement of proceeds of crime or property derived from the commission of such offences;

iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

c) To provide, where appropriate, necessary information for analytical or investigative purposes;

d) To facilitate effective coordination among their competent authorities, agencies and services and to promote the exchange of personnel and other experts, subject to bilateral or multilateral agreements or arrangements between the States concerned;

e) To exchange information and coordinate administrative and other measures taken, as appropriate, for the purpose of early identification of the offences covered under their national cybersecurity legislation.

(2) With a view to ensuring cybersecurity, States may consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them to incorporate cybersecurity objectives.

36. International cooperation

(1) The operation of domestic cybersecurity legislation shall occur in conjunction with, and with consideration of, provisions established by international agreements and mechanisms.

(2) States shall establish regimes to provide mechanisms to ensure a single point of contact for incidents and their resolution in cooperation with other governmental, law enforcement and sectoral efforts at the international level.

(3) States shall make use of existing means for international cooperation with a view to responding to cyberthreats, improving cybersecurity and stimulating dialogue between stakeholders. These means may be international, regional, intergovernmental or based on public-private partnerships.

37. Public-private partnerships

(1) States shall develop multi-stakeholder engagement models for public-private partnerships for cybersecurity monitoring, preven-

tion and mitigation and to enhance cyber-resilience and trust in the African region.

(2) In furtherance of public-private partnerships, States may establish entities that are charged with setting cybersecurity standards for the private sector relating to security and welfare, including monitoring and implementation agencies, such as a national cybersecurity committee, to administer the implementation of public-private partnerships.

PART VI: Cybersecurity Management

38. Critical infrastructure

(1) States shall ensure that national cybersecurity legislation imposes strict obligations for the maintenance and protection of computer networks that, if compromised, could cause significant disruption, destruction and interference to critical infrastructure and information systems.

(2) States shall identify critical infrastructure at greatest risk of cyberthreats.

(3) States shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic and financial security, or national security.

(4) Each State shall ensure that its national cybersecurity legislation lists and defines what will be considered as "critical infrastructure" and provides a regulatory framework for the maintenance and protection of that "critical infrastructure".

39. Computer emergency response

(1) States shall establish specialized cybersecurity management bodies and teams responsible for cybersecurity management and formulate emergency response plans.

(2) States may also direct the establishment of national and sectoral teams for the purpose of responding to computer network emergency incidents and coordinate such responses along national and/or sectoral lines. The national and sectoral teams will work in coordination to respond to and mitigate cybersecurity incidents and threats.

(3) States may mandate the national and sectoral emergency response teams to establish a cyberincident registry or database in their respective jurisdictions for the collection and collation of data on cybersecurity incidents, analysing cybersecurity incidents and performing cybersecurity supervisory functions.

40. Cybersecurity points of contact

To ensure expedited operational cooperation on cybersecurity in the African region, States shall take appropriate measures to designate a point of contact, equipped with trained personnel to facilitate the operation of the network, that is available twenty four hours a day, seven days a week to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning offences established as cybercriminal offences in national legislation, or for the collection of electronic evidence necessary for investigative or law enforcement purposes.

41. Cybersecurity strategies and framework

(1) States shall design and develop appropriate cybersecurity strategies and frameworks to identify, assess, monitor, prevent and mitigate cyberthreats in their respective jurisdictions.

(2) The cybersecurity strategy and framework shall include a set of standards, methodologies, procedures and processes that align policy, business and technological approaches to address cyberthreats in the State's jurisdiction.

(3) The cybersecurity strategy shall incorporate global and regional consensus standards and best practices. The cybersecurity strategy shall focus on identifying cross-sectoral security standards and guidelines that are applicable to cybersecurity.

(4) The cybersecurity strategy shall also identify areas for improvement to enable technical innovation and the monitoring and measuring of organizational standards and shall provide guidance that enables national cybersecurity sectors to provide services that are aligned with the standards, methodologies, procedures and processes developed to address cyberthreats.

42. Establishment of a central authority for cybersecurity regulation

States shall ensure that their national cybersecurity legislation includes provisions establishing the authority or authorities responsible for regulation of cybersecurity measures in their territory, as well as its or their scope and powers. The national cybersecurity authority shall:

a) Monitor cybersecurity trends such as vulnerabilities, risk management, governance practices and breaches with the potential to affect the domestic cyberspace;
b) Perform long-term strategic analyses of cyberthreats and incidents in order to identify emerging trends and help prevent incidents;
c) Interact with and support government departments that are responding to cybersecurity incidents;
d) Promote communication across cybersecurity-related sectors and departments regarding cybersecurity;
e) Advise the national institutions, bodies, offices and agencies on cybersecurity research needs and priorities to support effective responses to current and emerging risks and cyberthreats;
f) Oversee the development of regulatory cybersecurity response guidance to assist the State in the continued mitigation of cyberthreats;
g) Support the State in the implementation of national cybersecurity laws, policies and strategies and assist in the implementation efforts related to the ratification and adoption of regional and global cybersecurity treaties;
h) Engage with national and international stakeholders in efforts to manage and evaluate cybersecurity;
i) Raise public awareness of cybersecurity risks, and provide guidance on good practices for individual users, organizations and businesses, including cyberhygiene and cyberliteracy.

43. Cybersecurity assistance and support for victims

(1) In fulfilment of their obligation to monitor and prevent cybersecurity threats and oversee the welfare of citizens, States may implement support systems to advise, support and protect the victims of offences established under national cybersecurity legislation, including establishing designated agencies that will be charged with providing support to victims.

(2) Each State shall take appropriate measures within its means to provide assistance and protection to victims of offences covered by national cybersecurity legislation, in particular in cases of threat

of retaliation or intimidation and having particular regard to the most vulnerable groups in society.

(3) Each State shall establish appropriate procedures to provide access to compensation and restitution for victims of offences covered by national cybersecurity legislation.

(4) Each State shall, subject to its national cybersecurity laws, enable the views and concerns of victims to be presented and considered at appropriate stages of the criminal proceedings against the accused in a manner not prejudicial to the rights of those accused and consistent with the protection of their rights under the law.

44. Education and training

(1) States are reminded that cybersecurity regimes impose important duties relating to the maintenance and protection of systems upon governments, the private sector, institutions and citizens; therefore, the importance of public education and awareness shall be considered alongside the important function of regulation.

(2) Each State shall adopt measures to build capacity by providing training covering all areas of cybersecurity to various stakeholders.

(3) States shall promote technical education for information and communications technology professionals, within and outside governmental bodies, through certification and standardization of training, categorization of professional qualifications and the development and needs-based distribution of educational material.

(4) As part of the plan for promotion of public education and training, States may:

a) Develop and implement programmes and initiatives to raise awareness among, educate, train and disseminate information to citizens on cybersecurity issues;

b) Encourage the development of a cybersecurity culture in enterprises;

c) Foster the involvement of civil society;

d) Launch a comprehensive and detailed national curriculum in schools for students.

(5) States, in fulfilment of their obligation to monitor and prevent cybersecurity threats and oversee the welfare of citizens, may implement support systems to advise vulnerable groups of society on cybersecurity matters.

45. Cybersecurity research and development

(1) States shall support research and development programmes to guide the overall direction of national cybersecurity and the development of information technology and networking systems to meet cybersecurity objectives, including with a view to:

a) Designing and building complex software-intensive systems that promote cybersecurity;
b) Building new protocols to enable robust Internet security;
c) Developing and designing cybersecurity solutions locally;
d) Developing solutions that protect critical national infrastructure;
e) Protecting privacy in conjunction with improved security, including the identity of and information on individuals and their lawful transactions when stored in distributed systems or transmitted over networks;
f) Combatting internal and external cyberthreats;
g) Improving consumer education and digital literacy to address the human factors that contribute to cybersecurity;
h) Protecting information processed, transmitted or stored using cloud computing or transmitted through wireless services;
i) Achieving other objectives that are set with input from stakeholders, including national laboratories, industry and academia, as appropriate.

46. Amendments to domestic legislation

States shall also adopt such measures as may be necessary to facilitate the review and amendment of cybersecurity laws to facilitate flexible and appropriate responses to existing and future cyberthreats.