



[Member States](#)

POLICY

Strategy Documents

A Global Approach on Cybersecurity and Cybercrime in Africa

African Ministers in charge of Communications and Information and Communication Technologies

- Recalls the African Union Convention on Cybersecurity and personal data protection (The Malabo Convention) and the recommendations of the First Ordinary Session of the Specialized Technical Committee on Communication and ICTs (STC-CICT-1)
- Identifies cybersecurity policy priorities for Africa, outlining:
 - Strategic approach
 - National cyber security framework
 - Fighting all kinds of cybercrime at continental level
 - Personal Data Protection
 - Capacity building and awareness
 - Enhancing Regional and International Cooperation
- Provides a set of recommendations on national, regional and continental level

[Source](#)

September 2016

Other Documents

Internet Infrastructure Security Guidelines for Africa

African Union Commission; Internet Society

- Developed jointly by the African Union Commission (AUC) and the Internet Society (ISOC) with contributions from regional and global Internet infrastructure security experts, government and CERT representatives, and network and ccTLD DNS operators in order to facilitate implementation of the the African Union Convention on Cyber Security and Personal Data Protection
- Aim to provide recommendations and promote principles and solutions to ensure that African Internet infrastructure security meets the requirements of users at large, and that all stakeholders have clear guidelines for achieving what is expected of them
- Put forward four essential principles of Internet infrastructure security:
 - Awareness
 - Responsibility
 - Cooperation, and
 - Adherence to Fundamental Rights and Internet Properties
- Provide recommendations to AU Member States aimed at strengthening the security of their local Internet infrastructure through actions at a regional, national, ISP/operator and organizational levels

[Source](#) [Source 2](#)

30 May 2017

Report on Cyber Security Trends and Government Responses in Africa

African Union Commission; Symantec Corporation and Global Forum for Cybersecurity Expertise (GFCE)

- Developed jointly by the African Union Commission (AUC) and Symantec, as part of the Global Forum for Cyber Expertise (GFCE) Initiative, with additional support from the U.S. Department of State and the Council of Europe
- Incorporates the perspectives of African Union Commission Member State governments and online threat data from Symantec's comprehensive cyber threat monitoring network
- Objectives:
 - Provide an overview of cyber security and cyber crime related developments in Africa
 - Assess the major trends around the world and on the Continent
 - Take stock of the many advances made by government authorities as well as identifies some of the challenges in a rapidly connected and ICT-dependent world
- Explores cybersecurity trends including the overall professionalization of cyber crimes:
 - Rise of Ransomware and Cryptolocker
 - Social Media, Scams, and Email Threats



- Smartphones and the Internet of Things
- Business Email Scams
- Vulnerabilities

[Source Source 2](#)

November 2016

Personal Data Protection Guidelines for Africa

African Union Commission; Internet Society

- Developed jointly by the African Union Commission (AUC) and the Internet Society (ISOC) with contributions from regional and global Internet infrastructure security experts, government and CERT representatives, and network and ccTLD DNS operators in order to facilitate implementation of the the African Union Convention on Cyber Security and Personal Data Protection
- Emphasize the importance of ensuring trust in online services, as a key factor in sustaining a productive and beneficial digital economy
- Offer guidance on how to help individuals take a more active part in the protection of their personal data, while recognising that in many areas, positive outcomes for individuals depend on positive action by other stakeholders
- Set out 18 recommendations, grouped under three headings:
 - The foundational principles to create trust, privacy, and responsible use of personal data
 - Eight recommendations for action by the following stakeholders
 - Governments and policymakers
 - Data Protection Authorities (DPAs)
 - Data controllers and data processors
 - Eight recommendations on the following themes
 - Multi-stakeholder solutions
 - Wellbeing of the digital citizen
 - Enabling and sustaining measures

[Source Source 2](#)

9 May 2018



Communications

Declaration on Internet Governance and Development of Africa's Digital Economy (Assembly/AU/Decl.3(XXX))

African Union Assembly

- Reaffirms commitment to the need for stability, for the safety of citizens and enterprises, confidentiality of online data security, through the AU Convention on Cybersecurity and Personal Data Protection
- Includes sections and provisions on:
 - Internet Governance Principles
 - Africa's Participation in Internet Governance
 - Development of Africa's Digital Economy
 - Management of Domain Names
 - Global Internet Governance

[Source](#)

28-29 January 2018

Communique on Mitigating the Threats of Cyber Security to Peace and Security in Africa

Peace and Security Council (PSC) of the African Union

- Adopted at the 850th meeting of the Peace and Security Council (PSC) of the AU held on 20 May 2019 on Mitigating the Threats of Cyber Security to Peace and Security in Africa
- Addresses the increasing cyber threats
- Underscores the needs for the AU Member States to:
 - Undertake regular cyber security risk assessments and to further enhance their national cyber security capacities
 - Redouble the investments in education and public awareness raising campaigns on the growing threat of cyber-crime
 - Adopt a multi-disciplinary, multi-sectoral, multi-stakeholder and public-private partnership approaches in preventing and mitigating the risks posed by cyber-crimes
 - Take necessary steps to own national information, ICT infrastructure, in order to reduce their vulnerabilities to cyber-attacks
- Encourages Member States to:
 - Take full advantage of the various capacity building initiatives of the Global Forum on Cyber Expertise (GFCE)



- Establish synergies and enhance national, regional and continental coordination
- Harmonize their laws and excise mutual legal assistance in cases of cyber-crimes

[Source Source 2](#)

20 May 2019

Press Statement on the Crucial Role of Cybersecurity in the Promotion and Maintenance of Peace and Security in Africa

Peace and Security Council of the African Union

- Issued in follow-up to the 627th meeting of the AU Peace and Security Council (PSC) held on 26 September 2016, in Addis Ababa
- The PSC and participants:
 - Addressed the increasing global cyber threats and attacks
 - Stressed the importance of regional and global frameworks for promoting security and stability in cyberspace
 - Underscored the importance of promoting a culture of cybersecurity among all stakeholders
 - Emphasized the need for the AU Commission to establish mechanisms and platforms, such as the regional forums dedicated to discuss cybersecurity issues
 - Underscored the importance of regional and international cooperation in the promotion of security and stability in the global cyberspace

[Source](#)

26 September 2016

STRUCTURE



Specialized Agencies

(proposed) Africa Cybersecurity Collaboration and Coordination Committee (ACS3C) (or the African Union Cyber Security Expert Group (AUCSEG))

Executive Council of the African Union; the African Union Commission

- Proposed by the Special Technical Committee (STC) on ICT in its Report to the Executive Council
- The STC's decision endorsed at the 32nd Ordinary Session of the Executive Council (EX.CL/Dec.987(XXXII)) on 25-26 January 2018
- Proposed general objective: to provide guidance and recommendations on Cyber policies and strategies to AU with the aim to adopt, monitor, prevent, mitigate and address current and emerging cyber threats and data misuse.
- Proposed responsibilities: to provide advice to AU on technical, policy, legal and other related Cyber security matters at a national, regional and continental levels
- The Committee will be called the African Union Cyber Security Expert Group (AUCSEG) and will be established by and report to the AU Commission / Department of infrastructure and Energy / Information Society Division

[Source Source 2](#)

25 - 26 January 2018 (decision to establish endorsed)

Specialized Technical Committee on Communication and ICT (STC CICT)

AU Executive Council

- Established in 2009 by the Decision of the AU Assembly ([Assembly/AU/Dec.227\(XII\)](#)) to reconfigure the previous structure of STCs
- Functions include:
 - overseeing development and implementation of policies on access to information and freedom of expression
 - overseeing promotion of the capacity of African media
 - developing common African e-strategies
 - discussing resource mobilisation and capacity building for implementation of the African Regional Action Plan on the Knowledge Economy
 - promoting public investment in ICT infrastructure; and
 - developing frameworks for ICT policy and regulation harmonisation in Africa
- The [Second Ordinary Session](#) of the STC CICT took place on 20-22 November 2017 in Addis Ababa, Ethiopia

[Source Source 2](#)

1991 (established)

Department of Infrastructure and Energy (DIE)



Amani Abou-Zeid (Commissioner for Infrastructure and Energy); Cheikh Bedda (Director)

- Coordinates the implementation of several [Agenda 2063](#) infrastructure programmes and projects, including:
 - [Cyber Security](#): Incorporating emerging technologies in Africa's development plans and ensuring their use for the benefit of African individuals, institutions and nation states by ensuring data protection and safety online
- Coordinates the implementation of the AU's activities aimed at promoting, coordinating, implementing and monitoring programmes and policies at the regional and continental levels on:
 - Infrastructure development
 - Transport
 - Energy resources
 - ICTs (including cybersecurity)
 - Postal services, and
 - Tourism
- Facilitates private sector initiatives on infrastructure development and advocating among development partners for programme implementation

[Source](#)



Key Positions

Commissioner for Infrastructure and Energy

African Union Commission

- The position of Commissioner for Infrastructure and Energy is currently held by H.E. Amani Abou-Zeid, Egyptian, who was elected for the term from January 30, 2016 to January 30, 2020

[Source](#)

January 30, 2016 (current Commissioner elected)

LEGISLATION



Regulations and Directives

African Union Convention on Cyber Security and Personal Data Protection (The Malabo Convention)

African Union Assembly of Heads of States and Governments

- Objective: setting the essential rules for establishing a credible digital environment (cyber space) and address the gaps affecting the regulation and legal recognition of electronic communications and electronic signature; as well as the absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems and privacy online
- Aims to set up a minimum standards and procedures to reach a common approach on the security issues in Africa and Address the need for harmonized legislations necessary to enhance cooperation in the area of cyber security in Member States of the African Union
- Requires member states to develop a national cyber security policy and appropriate institutional mechanism for governance; legislation and institutions against cybercrime; ensuring monitoring and a response to incidents and alerts, national and cross-border coordination and global cooperation
- Major sections include:
 - Part I: Organization of Electronic Commerce
 - Part II: Protection of Personal Data
 - Part III: Promoting Cyber Security And Combating Cyber Crime
 - Part IV: Common And Final Provisions
- [As of June 2019](#), signed by 14 AU Member States and ratified by 5 Member States

[Source](#) [Source 2](#)

27 June 2014 (adopted)

Draft African Union Convention on the Establishment of A Legal Framework Conducive to Cyber Security in Africa (or Draft African Union Convention on the Confidence and Security in Cyberspace)

African Union Commission, Economic Commission for Africa



- Proposal of a Convention seeking to harmonize African cyber legislations and establishing a credible framework for cybersecurity in Africa through organization of electronic transactions, protection of personal data, promotion of cyber security , e-governance and combating cybercrime
- Objective: to contribute to the preservation of the institutional, human, financial, technological and informational assets and resources put in place by institutions to achieve their objectives
- Geared to protecting:
 - Institutions against the threats and attacks capable of endangering their survival and efficacy
 - The rights of persons during data gathering and processing against the threats and attacks capable of compromising such rights
- Seeks to:
 - Reduce related institutional intrusions or gaps in the event of disaster
 - Facilitate the return to normal functioning at reasonable cost and within a reasonable timeframe
 - Establish the legal and institutional mechanisms likely to guarantee normal exercise of human rights in cyber space
- The proposal of the Convention was not adopted

[Source Source 2](#)

1 September 2012

COOPERATION

Meetings

Workshop for AU Member States on Cyber-Strategy, Cyber Legislation and Setting up CERTs

African Union Commission

- Organized and conducted by Department of Infrastructure and Energy Information Society Division
- Covered the following topics:
 1. National and regional cyber strategies
 2. CERTs/CIRTs
 3. National and regional cyber legislation and regulatory frameworks

[Source Source 2](#)

23-27 July 2018

Workshop on Cyber Security and Cybercrime Policies

African Union Commission, Department of Infrastructure and Energy

- Jointly organized by the African Union Commission and the Council of Europe's Cybercrime Programme Office as a part of ongoing collaboration between AU and CoE, with support from the European Union through the project "Joint EU-CoE Global Action on Cybercrime extended" (GLACY+)
- Objectives:
 - to bring together the diplomatic community of the African countries
 - to discuss cybersecurity matters, and
 - further raise awareness on the importance of political, legislative and diplomatic efforts, cooperation and commitment necessary in tackling the inherent cross-border nature of cyber-attacks and cyber crime
- The focus was dedicated to legal instruments for cooperation between States, such as, on the regional level, the African Union [Malabo Convention](#) and, on the international level, the CoE [Convention on Cybercrime \(Budapest Convention\)](#)
- Provided an introduction on the impact of the use of digital technologies and Internet on the conduct of diplomacy (e-diplomacy), as well as an overview of international and regional policy discussions and debates over cyber security and cybercrime issues

[Source](#)

12 April 2018

Capacity Building Workshop for International Cyber Security Negotiations

Directorate of Information and Communication at the African Union Commission

- Organised by the African Union Commission in collaboration with the *ICT for peace Foundation (ICT4Peace)*
- Aim and subject: to address the Misuse of ICTs and their potential implication on the national and international security and stability
- Objective: to familiarize African diplomats with the on-going international discussions to acquire a deeper understanding of the most important areas of diplomatic negotiations for a secure and open cyberspace, such as:
 - the application of the international laws for cyberspace
 - norms of responsible state behaviour and confidence building measures (CBMs) in cyberspace

[Source](#)

15-16 February 2016

 **External Cooperation****Joint Statement of the Third Forum on China-Africa Media Cooperation**

African Union Commission, African Union of Broadcasting

- Issued at the closing of the Third Forum on China-Africa Media Cooperation in Beijing, China
- Three areas of focus identified in the agenda of the China-Africa comprehensive strategic partnership:
 - building the capacity of the media through training programs, infrastructure development and institution building
 - enhance industrialization through transfer technology; and
 - *cooperation in cyber security and digitalization*
- The parties commit to to contribute to the promoting of the initiative to jointly build the Silk Road Economic Belt and the 21st Century Maritime Silk Road, develop and promote national and local African contents to fully contribute to digital economy, and enhance our cooperation in cybersecurity and digitalization

[Source Source 2](#)

21 June 2016