

African Union Cyber Security Expert Group

Terms of Reference (ToR)

1. Background

The African community is increasingly embracing ICTs in general and the Internet in particular as key enablers for social and economic development. Member states of the African Union recognize the untapped potential of the digital transformation and its power to further the prosperity and wellbeing of their citizens.

However, the rapid growth of the Internet has also created new opportunities for perpetrating cyber-attacks and cybercrime on a global scale. Therefore, ICTs and Internet cannot be fully used for the benefit of Africans unless they can be trusted. This is why the African Union recognizes that cybersecurity must be an integral and indivisible part of technological and digital revolution. In 2014, the African Union Commission adopted the Malabo Convention [on Cyber Security and Personal Data Protection](#) to provide fundamental principles and guidelines to ensure an effective protection of personal data and create a safe digital environment for citizens, security and privacy of individuals' data online. This is considered an important first step in **establishing** a uniform system of data processing and determine a common set of rules to govern cross-border transfer of data to avoid divergent regulatory approaches between the African Union Member States and ensure a safe digital space for Africans. This will also facilitate any data transfer agreement involving other continents/states.

In January 2018, the 32nd Ordinary Session of the Executive Council endorsed the decision of the Specialized Technical Committee on ICTs, EX.CL/Dec.987(XXXII) to create an Africa Cyber Security Collaboration and Coordination Committee to advise the AUC and policy makers on the Cyber strategies. This committee shall be called the African Union Cyber Security Expert Group (AUCSEG) and will advise the AUC in matters related to Cyber security, Cybercrime, Cyber-legislations, Online privacy and data protection as well as digital policy related issues. The expert group will help facilitate coordination and information sharing among African countries & regions and different stakeholders, help identify cyber security areas where resources are needed, and advise African Union policymakers on national, regional and continental strategies and initiatives that should be prioritized. The Committee would be an evolving, compact, and trusted network of experts formed by the AUC in collaboration with the African Internet community.

2. Rationale

Africa has made major headway in developing its digital ecosystem in the past decade. Nonetheless, there is still an evident gap among AU Member States in terms of awareness, understanding, knowledge and capacity to deploy and adopt the proper strategies, capabilities and programmes to mitigate cyber threats. The ongoing digital transformation in Africa will not provide the desired social and economic benefits unless Africans have access to a secure and trusted Internet. Unfortunately, rapid Internet growth in Africa in the last few years has also brought about increased cyber-criminality. While digital technologies expand the possibilities for people to enjoy freedoms and the right to access information and knowledge, reacting to emerging threats such as cybercrime and Cyber terrorism has become a top priority for all governments. It is in this context, the AUC will establish the AUCSEG with the main objective of advising the AUC and AU Policy makers to actively deal with cyber-security concerns in the region. The focus of the Group will be to provide guidance and recommend strategies and solutions taking into account the international and regional dynamics and needs

3. General Objective of the AUCSEG

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.

4. Role and function of the AUCSEG

The AUCSEG will be established by and reports to the African Union Commission / Department of infrastructure and Energy / Information Society Division. The responsibilities of the AUCSEG will be to provide advice to AU on technical, policy, legal and other related Cyber security matters at a national, regional and continental levels; this includes but is not limited to:

- a) strategies for collecting synthesizing, and disseminating information on cyber security for member states;
- b) guidance on Cyber security programs for Member States, such as:
 - (i) establishing systems and mitigating programmes e.g. CERTs/CIRTs or CSIRTs to counter criminal activities committed over the Internet
 - (ii) Evaluating the impact of cyber security interventions and programmes;
 - (iii) Assisting member states to develop cyber security national strategies and legislations;
 - (iv) Assisting with the planning of content and structure of the AUC yearly cybersecurity conference;
 - (v) Establishing the cyber security month in all Members States;
 - (vi) Enhancing the capacities of criminal justice authorities, such as law enforcement, Prosecutors and Judges, in order to enable them to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence and computer forensic;
 - (vii) Ensuring the dissemination of best practices in the fight against existing and emerging cybercrime through the cyber security Month and the yearly cybersecurity conference institutions.
- c) Promoting accuracy and integrity of ICT data at the national, regional and continental levels and identifying gaps in evidence and suggesting priority research areas in the field of cyber security.
- d) Design a model for cybersecurity capacity building which takes in consideration all aspects (policy, technology, skills development...) and can be easily adapted to Member State's needs;
- e) Providing guidance and advise on the online privacy and personal data protection issues raised by Member States;
- f) Develop comprehensive and detailed national sensitization programs including public awareness campaigns and preventives measures at all levels to mitigate Cyber risks for Internet users, small businesses, schools and children;

The AUCSEG will be specifically tasked with:

- Advising the AUC on cyber security issues and policies, such as capacity building initiatives;

- Proposing solutions to facilitate the ratification and domestication of the Malabo Convention into national laws;
- Sharing best practice on critical and Internet infrastructure security and how to mitigate current and new threats;
- Identifying areas of research needed for the formulation of policies, guidelines, etc., which can be general or sector-specific, for instance, cyber security for smart grid technologies in the electric power industry, for financial systems, and for equipment monitoring tools
- Identifying ways to support Computer Security Incident Response Teams (CSIRTs), in the area of capacity building and information sharing at the regional and African Union level;
- Encouraging close collaboration among AU Member States and stakeholders, including in responsible and coordinated disclosures;
- Proposing ways to increase the skills of information systems and cyber security professionals in Africa (e.g. by fostering trusted certification programs)
- Supporting AUC in formulating strategies for cyber security and capacity building programs;
- Supporting AUC and Member States on international cooperation matters regarding cyber security, personal data protection and combating cybercrime.

5. Membership and structure of the AUCSEG

- The AUCSEG shall be multi-stakeholder and would include experts from relevant Africa-wide, regional and national level organizations, institutions, academia, the technical community, civil society, and law enforcement agencies & legal institutions.
- The AUCSEG will appoint its chair and co-chairs; and define working modalities
- Through its multi-stakeholder network structure, the Expert group would more flexibly adapt to the new and emerging security challenges facing Africa.
- The AUCSEG will have up to 15 members. AUCSEG members will serve in a voluntary, independent, personal, and individual capacity.
- The AUCSEG composition should strive for appropriate regional representation and gender balance and should comprise individuals representing different areas of expertise and experience within the cyber security and ICT sector.
- Members of the AUCSEG must represent the 5 African regions namely Northern, Southern, Central, Eastern and Western. Two seats will be reserved for each region. The Head of the Information Society division of the African Union Commission will serve as a permanent member and a secretariat of the group.
- The Experts must have excellent technical knowledge, expertise in the subject area and proven evidence of work in similar roles such as scientific publications in peer-reviewed journals, and more than 7 years' experience in at least one of the cyber related areas listed below:
 - Online Privacy
 - Cybersecurity policy
 - ICT technology, capacity building and training
 - Internet Governance
 - Data protection

- Emerging issues, Internet of Things, Artificial Intelligence
 - Cyber-Crime investigations & legislations
 - Critical Infrastructure protection (CIP)
 - Internet and jurisdiction
- The AUCSEG shall include diverse members who have worked or are currently working for the following, Academic, Technical Community, Civil Society, Law Enforcement, Policy, Private corporates, National security and personal data protection agencies, Private companies in the technology space with experience in cyber security issues, as well as ICTs in general.

Following an open call to submit nominations, AUCSEG members will be appointed by the African Union Commission based upon the recommendations from a panel composed of the AUC senior officials and African ICT community Experts. The panel may also consult with other relevant technical community organizations.

6. Term of service

- Members of the AUCSEG shall be appointed to serve for an initial term of up to two years, renewable once, for a period of up to an additional two years.
- However, in order to allow staggering of committee members, the working modalities will define the number of expert to serve for 3 years.
- Membership of the AUCSEG may be terminated by AUC (the members of the AUCSEG) for any of the following reasons:
 - failure to attend 50% of AUCSEG meetings;
 - change in affiliation resulting in a conflict of interest;
 - a lack of professionalism involving, for example, a breach of confidentiality.
- In addition, AUCSEG members have an ongoing obligation throughout their tenure to inform AUC of any material changes to the information that they have disclosed prior to appointment.

7. Responsibilities of AUCSEG members

- Members of the AUCSEG have a responsibility to provide AUC with high quality, well considered, evidence-informed advice and recommendations on matters described in these ToR.
- The AUCSEG has no executive or regulatory function. Its role is to work with the AUC secretariat to provide recommendations to the AUC and STC. AUCSEG members may be approached by non-AUC sources for their views, comments, and statements on matters within AUCSEG and asked to state the views or details related to AUCSEG discussions. AUCSEG members should refer all such enquiries to AUC.

8. AUCSEG Operating Procedures

- The AUCSEG will meet at least once a year in face-to-face meetings and have additional meetings and/or teleconferences at least once a month as needed. Open meetings can be attended by anyone interested in AUCSEG issues and are intended for discussion of new tools, technologies and approaches and issues related to the agenda item(s) of the closed meeting. All meetings are open except for meetings discussing confidential African Union issues.
- AUC will organize the AUCSEG meetings (provide support for travel and accommodation for the members). Decisions on AUCSEG recommendations will, as a rule, be taken by consensus. In the

exceptional situation that consensus cannot be reached the chairperson shall report the majority and minority views. It is also the chairperson's responsibility to ensure there is clarity for AUCSEG members on what exactly is being decided.

- Additional experts might be invited to participate in meetings, also as appropriate, to ensure that a sufficiently broad base of expertise is available for the specific agenda items at each meeting.
- Recommendations from the AUCSEG will be used to reinforce the work and support the strategies of AUC.

9. Principles of the committee

The committee should work by embodying principles that will earn it confidence and respect from AU, Member States and African citizens.

In particular, it should be:

- Open and inclusive
- Transparent
- Impartial
- Fair
- Accountable
- Evidence-based
- Consensus-based
- Guided by public interest
- Guided by the African spirit and AU Vision

10. Change of the ToR

These terms of reference shall be reviewed at least one every two years by the AUCSEG. Any proposed changes in the ToR must be submitted to and approved by the AUC.

11. Dissolution of the AUCSEG

The AUC can dissolve the AUCSEG if it considers it is no more relevant