

AFRICAN UNION

الاتحاد الأفريقي



UNION AFRICAINE

UNIÃO AFRICANA

P.O. Box: 3243, Addis Ababa, Ethiopia, Tel.:(251-11) 551 38 22 Fax: (251-11) 551 93 21
Email: situationroom@africa-union.org

PEACE AND SECURITY COUNCIL

627TH MEETING

26 SEPTEMBER 2016

ADDIS ABABA, ETHIOPIA

PSC/PR/BR.(DCXXVII)

PRESS STATEMENT

PRESS STATEMENT

The Peace and Security Council of the African Union (AU), at its 627th meeting, held on 26 September 2016, in Addis Ababa, dedicated an open session to the theme: “The crucial role of cybersecurity in the promotion and maintenance of peace and security in Africa”.

Council listened to a statement that was delivered by the Head of the Defense and Security Division in the Department of Peace and Security, as well as to a presentation by the Department of Infrastructure and Energy of the AU Commission. Council also listened to statements that were delivered by representatives of AU Member States, bilateral and multilateral partners, as well as international organizations and civil society organizations.

Council recalled the recommendations of the First Ordinary Session of the Specialized Technical Committee on Communication and Information and Communication Technologies (STC-CICT-1) held in Addis Ababa, Ethiopia, from 31 August to 4 September 2015, in which the AU Commission was requested to follow up on the signature and ratification, by Member States, of the AU Convention on Cybersecurity and Personal Data Protection. Council also recalled that, as part of the same recommendations, Member States were urged to develop national cybersecurity legislations and to create national and regional computer emergency response teams (CERT) and/or computer security incident response teams (CSIRT).

Council and participants highlighted the importance of information and communication technologies (ICTs), in general, and the internet, in particular, in the promotion of socio-economic development. In this context, Council and participants stressed the need for effective internet governance as a matter of strategic importance.

Council and participants noted, with deep concern, the increasing global cyber threats and attacks, which constitute a serious threat to national, regional and international peace and security. They also noted that cybersecurity concerns are broader than national security and that they can become a planetary emergency with the potential of amplifying the traditional security threats that include terrorism and violent extremism. Furthermore, they acknowledged that a safe and secure cyber space is a necessary condition for reaping the benefits of the digital transformation of Africa and for ensuring the positive impact of ICTs on human and economic development throughout the continent. In this regard, they stressed the importance of regional and global frameworks for promoting security and stability in the cyberspace.

Council and participants underscored the importance of promoting a culture of cybersecurity among all stakeholders. In this context, they urged governments, public and private enterprises, as well as civil society organizations, to work together in the process of

capacity building to combat cybercrimes, as well as sensitizing their citizens in this regard, and exchanging of experiences related to cybersecurity and combating cybercrimes.

Council and participants emphasized the need for the AU Commission to establish mechanisms and platforms, such as the regional forums dedicated to discuss cybersecurity issues, with a view to facilitating an efficient platform for sharing experiences, lessons learnt and best practices related to cybersecurity issues among AU Member States, as well as to further enhance regional and international cooperation in this area.

Council and participants underscored the importance of regional and international cooperation in the promotion of security and stability in the global cyberspace. In this context, Council and participants welcomed the ongoing consultations of the United Nations Group of Governmental Experts (UNGGE) on the establishment of a global cybersecurity framework based on international regulations and responsible state behavior in the cyberspace. Furthermore, they encouraged Member States to take full advantage of the benefits from the different capacity building initiatives organized by the Global Forum on Cybersecurity Experts (GFCE), in which the AU Commission is a member and Co-Chair of its Advisory Board.

Council urged Member States to develop, in collaboration with all stakeholders, national cybersecurity policies and adopt other necessary measures to more effectively secure their cyberspaces. In the same context, Council also appealed to Member States to urgently scale up efforts to effectively combat all kinds of malicious use of ICTs and internet in the African cyberspace. Furthermore, Council stressed the need for formulation of policies and regulatory frameworks to prevent and counter all criminal activities carried out in the internet, with special emphasis on the activities of radical terrorist groups in the cyberspace, including, inter-alia, recruiting new fighters.

In addition, Council emphasized the need for Member States to ensure that all employees, both, in government, the private sector and civil society organizations are sufficiently trained in cybersecurity. Council also underscored the importance of maintaining national statistics and regular reports on the incidences and threats of cybercrime affecting Member States.

Furthermore, Council urged Member States to develop cyber diplomacy capabilities and to actively participate in international meetings and debates on the governance of the internet and cybersecurity issues. Council urged all Member States, which have not yet done so, to sign, ratify and fully domesticate the AU Convention on Cybersecurity and Personal Data Protection.

Council welcomed the proposal to create a special unit within the Peace and Security Department, which will be solely devoted to preventing and effectively fighting cybercrime at

continental level, including by coordinating all continental efforts and initiatives to promote cybersecurity related issues and working closely with the relevant ministries in the Member States.

Council welcomed the proposal made by Egypt, Chairperson of the Council for the month of September 2016, to host an African Event to further discuss the Egyptian Initiative previously proposed during the Specialized Technical Committee of Telecommunication and ICT to start an African Dialogue aiming at combating terrorism online and securing cyberspace based on the following pillars:

- I. To pave the way for international principles on how to coordinate and cooperate with the relevant stakeholders in addressing new threats.
- II. To raise the level of confidence and security in the use of ICTs and take necessary actions to fight abuses, while promoting mutual understanding between governments and stakeholders to tackle the issue.
- III. To discuss protection of infrastructure and networks that might raise security challenges faced by countries.
- IV. To prevent the occurrence of any online accident by government authorities at the national, sub-national and regional levels (including the establishment of national Computer Incident Response Teams), and through collaboration with the private sector.
- V. To promote and encourage a linkage between the African Computer Emergency Response Teams and exchange information.

Council agreed to remain seized of the matter.