AFRICAN UNION
الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

Addis Ababa, Ethiopia, P.O. Box: 3243 Tel.: (251-11) 551 7700 Fax: (251-11) 5519 321
Email: situationroom@africa-union.org

PEACE AND SECURITY COUNCIL
850TH MEETING
ADDIS ABABA, ETHIOPIA
20 MAY 2019

PSC/PR/COMM. (DCCCL)

COMMUNIQUÉ

COMMUNIQUÉ

Adopted by the Peace and Security Council (PSC) of the African Union (AU) at its 850th meeting held on 20 May 2019 on Mitigating the Threats of Cyber Security to Peace and Security in Africa.

The Peace and Security Council,

Recalling its previous communiqués and press statements on cybersecurity in Africa, particularly, Communique [PSC/AHG/COMM. (DCCXLIX)] adopted at its 749th meeting held at the level of Heads of State and Government, on 27 January 2018 and Press Statement [PSC/PR/BR (DCXXVII)] adopted at its 627th meeting, open session, held on 26 September 2016;

Also recalling the African Union Convention on Cyber Security and Personal Data Protection (The Malabo Convention), the African Union Declaration on Internet Governance and Digital Economy and the Budapest Convention on Cybercrime;

Further recalling the Executive Council Decision [EX.CL/ Dec.986-1007 (XXXII)] requesting the Commission "to undertake, among others, the following: (i) implement Cyber Security as a flagship project of the African Union Agenda 2063; (ii) form an Africa Cyber Security Collaboration and Coordination Committee (ACS3C) to advise the Commission and policymakers on Cyber strategies; develop guidelines on Personal Data Protection; organize a yearly AU Conference on Cyber Security in collaboration with Industry and Academia and establish a continental Cyber Security awareness month" and also the United Nations General Assembly (UNGA) Resolution A/RES/73/266 on advancing responsible State behaviour in cyber space in the context of international security;

Noting the opening remarks made by the Permanent Representative of the Republic of Rwanda to the African Union, H.E. Ambassador Hope Tumukunde Gasatura, in her capacity as the PSC Chairperson for the month of May 2019; the introductory remarks of AU Commissioner for Infrastructure and Energy, H.E. Dr. Aman Abou-Zeid, as well as the statement made by the Special Representative of the Secretary-General of the United Nations to the African Union, H.E. Madam Hanna S. Tetteh;

Also noting the presentations made by the representatives of the AU Commission Department of Infrastructure and Energy, the United Nations (UN) International Telecommunications Union (ITU) and the Committee of Intelligence and Security Services of Africa (CISSA);

Mindful of the immense opportunities offered by advancements in information and communication technologies (ICT) and artificial intelligence to national economic development and improvements in the living standards and general wellbeing of the African people, as well as the attendant risks to peace and security in the Continent;

Also mindful of the increasing vulnerability of the entire Continent to the growing threat of cyber-crimes/cyber-attacks being committed by criminals, as well as extremist and terrorist

groups; Confirming that ICTs are dual-use technologies and can be used for both legitimate and malicious purposes;

Expressing concern that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in future conflicts between States is becoming more likely;

Underlining the importance of respect for human rights and fundamental freedoms in the use of ICTs; and

Acting under Article 7 of its Protocol, the Peace and Security Council:

1. ***Expresses deep concern***, over the increasing global threats to Cyber Security, which constitute serious threats to national, regional, continental and international peace and security;

2. ***Re-affirms,*** that a safe and secure cyber space is a necessary condition for reaping the dividends of the digital transformation of Africa and the world, and for promoting a positive impact of ICTs on human and economic development throughout the Continent;

3. ***Stresses the urgent need*** for Member States to undertake regular cyber security risk assessments and, working in close collaboration with the AU Commission, to further enhance their national cyber security capacities, in order to more effectively address cyber security challenges and combat cyber-crimes including the abuse and misuse of the internet;

4. ***Underscores the need*** for Member States to redouble their investments in education and public awareness raising campaigns on the growing threat of cyber-crimes, as well as to adopt a multi-disciplinary, multi-sectoral, multi-stakeholder and public-private partnership approaches in preventing and mitigating the risks posed by cyber-crimes;

5. ***Also underscores the need*** for Member States to take necessary steps to own national information, communication technologies (ICT) infrastructure, in order to reduce their vulnerabilities to cyber-attacks, and in this context, ***encourages*** Member States to take full advantage of the various capacity building initiatives of the Global Forum on Cybersecurity Experts (GFCE), in which the AU Commission is both, a member and Co-Chair of its Advisory Board;

6. ***Encourages*** Member States to establish synergies and enhance national, regional and continental coordination, among others, through harmonizing and updating national cyber security strategies, cyber security emergency responses and policies;

7. ***Also encourages*** Member States to harmonize their laws and excise mutual legal assistance in cases of cyber-crimes;

8. ***Commends*** the efforts of the Smart Africa Alliance Initiative towards having Africa's telecommunication traffic remaining in Africa and encourages Member States, which have not yet joined the Smart Africa Alliance Initiative to do so, in order to ensure maximum benefits for Africa;

9. ***Reaffirms, once again****, the need* to counter the use of ICT technologies by terrorist groups,

whether in their fundraising, narrative promotion, and recruitment of others to commit terrorist acts;

10. ***Commends*** all Member States that have already signed and ratified and are implementing the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention of 2014) and encourages those Member States, which have not yet done so, to also do the same without further delays;

11. ***Also commends*** the AU Mechanism for Police Cooperation (AFRIPOL) and the International Criminal Police Organization (INTERPOL) for their continued technical support to the efforts being deployed by Member States towards preventing and mitigating the risks posed by cybercrimes;

12. ***Reiterates its request*** for the AU Commission to establish mechanisms and platforms, such as regional forums dedicated to discussing cyber security-related issues, with a view to facilitating sharing of experiences, lessons learnt and best practices, as well as promoting regional and international cooperation in the area of cyber security;

13. ***Also requests*** the AU Commission, Department of Infrastructure and Energy, working in close collaboration with the Department for Peace and Security, Member states and the RECs/RMs, to expeditiously develop a Continental Cyber Security Strategy and a cyber security Model Law, and to report to the PSC before the early 2020 Ordinary Session of the AU Assembly of Heads of State and Government;

14. ***Decides*** to dedicate an annual session on cyber security; and

15. ***Decides*** to remain actively seized of the matter.