AFRICAN UNION

الاتحاد الأفريقي

UMOJA WA AFRICA

UNION AFRICAINE

UNIÃO AFRICANA

UNIÓN AFRICANA

Addis Ababa, Ethiopia. P.O. Box: 3243 Tel.: (251-11) 5513 822 Fax: (251-11) 5519 321
Email: situationroom@africa-union.org

PEACE AND SECURITY COUNCIL
1196TH MEETING

29 JANUARY 2024
ADDIS ABABA, ETHIOPIA

PSC/PR/COMM.1196 (2024)

COMMUNIQUÉ

SILENCING THE GUNS IN AFRICA
www.peaceau.org

COMMUNIQUÉ

Adopted by the Peace and Security Council (PSC) of the African Union (AU) at its 1196th meeting held on 29th January 2024, considering the Draft Common African Position on the Application of International Law to the Use of Information and Communication Technologies in the Cyberspace.

The Peace and Security Council,

Recalling the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) entered into force on 8 June 2023, the Digital Transformation Strategy for Africa (2020-2030) and the outcomes of the 4th Ordinary Session of the African Union Specialized Technical Committee on Transport, Transcontinental and Interregional Infrastructure, and Energy (STC-TTIIE) held on 12-15 September 2023 in Zanzibar, United Republic of Tanzania;

Further recalling previous decisions and pronouncements on Cyber Security in Africa and related themes, particularly Communiqué [PSC/PR/COMM.1171 (2023)] adopted at its 1171st meeting held on 24 August 2023, Communiqué [PSC/PR/COMM.1148 (2023)] adopted at its 1148th meeting held on 13 April 2023, and Communiqué [PSC/PR/COMM.1120 (2022)] adopted at its 1120th meeting held on 9 November 2022;

Cognisant of the deliberations and outcomes of the United Nations (UN) Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security and the UN Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security;

Noting the opening statement by H.E. Ambassador Amma A. Twum-Amoah, Permanent Representative of the Republic of Ghana to the African Union and Chairperson of the PSC for the month of January 2024, and the presentation of the report by Mr. Kwasi Asante, Minister Plenipotentiary and Deputy Head of Mission of the Republic of Ghana and Chairperson of the PSC Committee of Experts for the month of January 2024, which reviewed the draft Common African Position on the Application of International Law in Cyberspace;

Reaffirming the AU's commitment to deal with the multifaceted challenges confronting the Continent and its peoples in an ever-changing world;

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

1. ***Expresses its deep concern*** over the increasing global cyber threats and attacks, including in the context of armed conflicts, which constitute a serious threat to national, regional, and international peace and security and, in this respect, ***strongly condemns*** malicious cyber operations and cyber-attacks, particularly the recent large-scale attack on the Information Technology (IT) Infrastructure of the AU Commission;

2. ***Affirms*** that international law applies in cyberspace; ***underscores*** that Member States are required to uphold the fundamental rules of international law in cyberspace, including the obligation to respect the territorial sovereignty of States, the prohibition on the threat or use of force, the prohibition on intervention in the internal and external affairs of States, the peaceful settlement of disputes, and the applicable rules of international humanitarian law and international human rights law; and ***further underscores*** that States are under an obligation to combat malicious and criminal conducts in cyberspace by non-State actors;

3. ***Further affirms*** that compliance with international law is essential to keeping cyberspace open, secure, stable, accessible, and peaceful and ensuring that cyberspace continues to contribute to social development, economic growth, poverty eradication, and sustainable development;

4. ***Adopts*** the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace and ***decides*** to refer it to the 37th Ordinary Session of the Assembly of the Union scheduled to take place on 17-18 February 2024 for consideration and endorsement;

5. ***Applauds*** Professor Dr. Mohamed Helal, member of the African Union Commission of International Law (AUCIL) and Special Rapporteur on the Application of International Law in Cyberspace, the Working Group of Experts and the PSC Committee of Experts, the members of AUCIL, and the African scholars of international law who participated in the Working Group of Experts for their efforts in developing the Draft Common African Position on the Application of International Law to the Use of Information and Communication Technologies in the Cyberspace, pursuant to PSC Communique [PSC/PR/COMM.1171 (2023)];

6. ***Commends*** the Chairpersons of the Expert-Level Working Group, Mr. Kwasi Asante, Minister Plenipotentiary and Deputy Head of Mission of Ghana, and Mr. Michael Wamai, Counsellor in the Permanent Mission of Uganda to the AU, for their sterling efforts in steering the review of the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace;

7. ***Encourages*** Member States to consider issuing national position statements on the application of international law in cyberspace, in line with the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace and ***further encourages*** Member States to actively participate in regional and international multilateral forums on the governance of cyberspace, including at the UN;

8. ***Underscores*** the importance of capacity-building and cooperation, including between Member States and partners, international organizations, and the private sector, to further promote development of national capacities in the area of cyberspace and to protect critical infrastructure, including critical information infrastructure; and ***emphasizes*** the imperative of supporting the capacities of developing and least developed Member States at both policy and technical levels in areas such as the development of national cybersecurity and resilience strategies, providing access to relevant technologies, and support to Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs);

9. ***Requests*** the AU Commission and the Special Rapporteur to circulate and promote the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, including at multilateral forums on cyberspace, especially at the UN;

10. ***Further requests*** the AU Commission and the Special Rapporteur to continue to provide technical assistance and capacity-building to Member States on the application of international law in cyberspace; and ***emphasizes*** that developing the rules of international law that apply in cyberspace is a matter of common interest to all States, and that all Member States have equal rights to participate in the articulation of rules of international law that apply to cyberspace;

11. ***Reiterates*** **its** ***encouragement*** to all AU Member States which are yet to sign, ratify and domesticate the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) to do so; and

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

COMMON AFRICAN POSITION

ON THE APPLICATION OF INTERNATIONAL LAW TO THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN CYBERSPACE

I. PREAMBLE

1. Recalling the Constitutive Act of the African Union adopted in 2002, in particular Articles 3 and 4 of the Act and, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) adopted in 2014.

2. Noting that information and communication technologies (ICTs) in cyberspace are an indispensable part of the lives of human beings throughout the world. ICTs are an instrument of human interaction, a vehicle for social development, and an engine of economic growth, poverty eradication, and sustainable development.

3. Further noting that it is in the interest of all States, societies, and present and future generations to develop a global legal architecture that ensures that ICTs are used for peaceful purposes, and that prevents the malicious and criminal use of these technologies, promotes greater cooperation between States, guarantees that cyberspace remains open, secure, stable, accessible, and peaceful, protects basic human rights and fundamental freedoms of individuals and peoples, and advances the common interests of humankind.

4. Reaffirming that international law applies in cyberspace and governs the use of ICTs in cyberspace, and underscoring that States are under an obligation not to engage in internationally wrongful acts such as those outlined in this Common Position and to combat malicious and criminal cyber operations by non-State actors. In this regard, it is necessary, in light of the unique technical characteristics of cyberspace and the distinctive nature of the threats posed by unlawful behavior in this domain, by both States and non-State actors, to further expand dialogue between States, regional organizations, and other relevant stakeholders as appropriate and within their respective roles and responsibilities through transparent, inclusive, and multilateral processes on how international law should further apply in this area.

5. Reiterating their commitment, consistent with their obligations under international law and in accordance with due diligence, to combat malicious and criminal cyber operations by non-State actors and emphasized that non-State actors, particularly those whose conduct is attributable to States, should refrain from engaging in malicious or criminal use of ICTs in the Cyberspace.

6. Emphasizing that the process of further clarifying how international law applies to the use of ICTs in cyberspace and, where necessary, further developing the rules of international law that are applicable in this area is a matter of common interest to all States. All States have an equal right to participate in the articulation of rules of international law that apply in cyberspace and the views of all States have equal weight and value in this process.

7. Noting that the process of articulating rules of international law that apply to the use of ICTs in cyberspace would benefit from the adoption of a United Nations declaration on this subject that would be negotiated with the participation of relevant stakeholders, as appropriate and within their respective roles and responsibilities, including other international and regional organizations.

8. Taking note of the ongoing meetings of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. The African Union encourages its Member States which have not yet done so, to consider signing and ratifying the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention).

9. Commending the efforts undertaken by the United Nations to address issues relating to cybersecurity, especially the World Summit on Information Society hosted in Africa by a Member State of the African Union, Tunisia, and recalling, in this regard, the Tunis Commitment and the Tunis Plan of Action contained in U.N. Document A/60/687.

10. Highlighting that this Common African Position was adopted in the spirit of seeking to contribute to global debates on the application of international law to cyberspace. In this regard, given the continuous and rapid development of technology in this area, this Common African Position should be viewed as a non-exhaustive contribution to ongoing discussions in this field. The positions expressed herein may further evolve in light of technological developments and continuing engagement in discussions with the international community. The Member States of the African Union are also encouraged to issue national statements on the application of international law to the use of information and communication technologies in cyberspace. Moreover, there are aspects of the rules of international law as they apply in cyberspace that are not addressed in this statement, such as the immunities of diplomatic missions and international organizations, the inviolability of official State communications and diplomatic correspondences, the legality of countermeasures, and the restrictions on invoking necessity as a circumstance precluding wrongfulness, on which the African Union reserves its position

11. Reaffirming that the adoption of this Common African Position confirms the commitment expressed by the African Union in the Digital Transformation Strategy for Africa to harness digital technologies and innovation to transform African societies and economies to promote Africa's integration, generate inclusive economic growth, stimulate job creation, bridge the digital divide, and eradicate poverty for the continent's socio-economic development and ensure Africa's ownership of the modern tools of digital management.

II. SOVEREIGNTY IN CYBERSPACE

12. Sovereignty is an attribute of States. By virtue of sovereignty, States enjoy, under international law, territorial sovereignty, and supremacy in their internal and external affairs. States are also under an obligation to uphold principles of international law including the duty not to infringe on the independence of other States or to violate their territorial sovereignty.

13. Territorial sovereignty is a corollary of State sovereignty. By virtue of territorial sovereignty, States are entitled, within the limits established by the applicable rules of international law, to exercise exclusive control over their land territory and its appurtenances, including the airspace and maritime zones that are subject to the sovereignty of the State. The obligation to respect the territorial sovereignty of States is a primary rule that is firmly established in international law, which applies to State conduct in cyberspace. This rule is reflected in several judicial decisions, including the judgment of the International Court of Justice in the *Corfu Channel Case*, which affirmed that "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations," and the judgment of the International Court of Justice in the *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, which affirmed that "[t]he basic legal concept of State sovereignty in customary international law, expressed in, *inter alia*, Article 2 paragraph 1, of the United Nations Charter, extends to the internal waters and territorial sea of every State and to the air space above its territory."

14. By virtue of territorial sovereignty, States are entitled to exercise jurisdiction, including legislative, adjudicative, and enforcement authority, over the components of cyberspace that are located on their territory. The jurisdiction of States also applies extraterritorially to ICTs located on

aircraft and ships flying the State's flag and satellites and other spacecraft in outer space registered by the State.

15. The African Union affirms that international law, as it applies to the use of ICTs in cyberspace, does not permit a State to exercise enforcement authority on the territory of a foreign State in response to unlawful cyber activities that emanate from the territory of that foreign State. This applies even if the exercise of such enforcement authority by a State does not have harmful effects, whether virtual or physical, on the territory of a foreign State.

16. The African Union affirms that by virtue of territorial sovereignty, any unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is unlawful. Therefore, the African Union emphasizes that the obligation to respect the territorial sovereignty of States, as it applies in cyberspace, does not include a *de minimis* threshold of harmful effects below which an unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State would not be unlawful. The African Union further affirms that cyber operations that are attributable to a State against ICT infrastructure located on the territory of a foreign State that causes effects, such as loss or impairment of functionality, on the territory of a third State, may constitute a breach of the territorial sovereignty of that latter State.

17. The African Union underscores that seeking to codify rules of international law that apply in cyberspace that purport to permit States to exercise enforcement authority on the territory of a foreign State or that establish a threshold of harm that reduces the protective scope of the rule of the inviolability of the territorial sovereignty of States poses significant risks from a policy perspective. Given the vast disparities of technical capabilities between States, such rules would, as noted by the International Court of Justice in the *Corfu Channel Case*, "from the nature of things, be reserved for the most powerful States," which could give rise to serious abuses that would undermine the principles of the independence and sovereign equality of States.

18. As a corollary of territorial sovereignty, States shall protect, in accordance with the applicable rules of international law, especially international human rights law and, when applicable, international humanitarian law, natural and legal persons located on their territory against unlawful uses of ICTs in cyberspace that are attributable to foreign States or non-State actors.

19. The obligation to respect the territorial sovereignty of States is a rule that applies in inter-State relations. Accordingly, only an internationally wrongful act that is attributable to a State in accordance with the applicable rules of international law, as outlined in Section 9 herein, could constitute a violation of the territorial sovereignty of a State.

III. DUE DILIGENCE IN CYBERSPACE

20. Due diligence performs an important role in the area of cyberspace. Given the technical challenges relating to establishing attribution for internationally wrongful acts committed through ICTs in cyberspace and the fact that such acts are often committed by non-State actors, due diligence provides an important tool to promote the openness, accessibility, safety, and security of cyberspace.

21. The African Union recognizes that due diligence is an obligation that operates in the context of other primary rules of international law. In this regard, the African Union affirms that by virtue of territorial sovereignty, every State is under an obligation, as stated by the International Court of Justice in the Corfu Channel Case, "not to allow knowingly its territory to be used for acts contrary

to the rights of other states." This principle, which is a corollary of sovereignty is also confirmed by other judicial precedents, including the Pulp Mills Case and the Island of Palmas arbitral decision.

22. The African Union considers that due diligence, as it applies in cyberspace, establishes an obligation of conduct, not an obligation of result. Therefore, due diligence does not require a State to guarantee that its territory or territory under its control or jurisdiction is not used to commit an internationally wrongful act. Rather, due diligence establishes an obligation to take necessary measures that are feasible to the extent of a State's capacity and the means available to it to prevent or halt an internationally wrongful act that a State knows or should have known is undertaken using ICTs in its territory or in territory under its control or jurisdiction.

23. The due diligence obligation to take necessary measures, to the extent of the capacity available to the State, to prevent or halt an internationally wrongful act is triggered only if a State has knowledge that such an act is originating from or transiting through ICTs located on its territory or in territory under its control or jurisdiction. Knowledge, however, is not to be presumed simply by virtue of the fact of territorial sovereignty or control. Indeed, in the Corfu Channel Case, the International Court of Justice stated that "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known." Therefore, whether a State knows or has reason to know that an internationally wrongful act is originating from or transiting through ICTs located on its territory or in territory under its control or jurisdiction is a matter that has to be determined on a case-by-case basis in light of the information available to a State, the technical and institutional capabilities, and financial resources available to that State.

24. Due diligence also reinforces the obligation of States not to permit another State to use ICTs located within its territory or under its jurisdiction or control to commit internationally wrongful acts against another State.

25. The African Union also recognizes the unique challenges faced by developing countries in implementing due diligence measures due to resource constraints, and challenges related to technical expertise. The African Union emphasizes the importance of international cooperation and information sharing, including through Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs), to further enable States to fully uphold the obligation of due diligence. In this regard, the African Union underscores the importance of expanding international cooperation and capacity building as outlined in Section X, and further empowering and enabling the full participation of developing countries in policy making forums related to the governance of cyberspace.

IV. THE PROHIBITION ON INTERVENTION IN THE INTERNAL AND EXTERNAL AFFAIRS OF STATES IN CYBERSPACE

26. The prohibition on intervention in the internal and external affairs of States is a principle of general international law that is also reflected in several multilateral treaties, including the founding instruments of regional organizations, such as the Constitutive Act of the African Union, the Charter of the Organization of American States, the Charter of the Organization of Islamic Cooperation, and the Charter of the Association of Southeast Asian Nations, in addition to other instruments, such as the 1975 Helsinki Final Act, and UN General Assembly resolutions, such as the 1970 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States.

27. The prohibition on intervention is a rule that applies to inter-State relations. Accordingly, only acts that are attributable to a State in accordance with the applicable secondary rules of international law could constitute a violation of the prohibition on intervention.

28. The prohibition on intervention protects against acts that impinge on matters within the domestic jurisdiction of States in relation to which each State is permitted, by the principle of State sovereignty, to decide freely. It is also established that, by virtue of their sovereignty, States have an inalienable right to choose their political, economic, social, and cultural systems, without intervention from any other States.

29. The prohibition on intervention applies to the use of any instrument, including armed, political, economic, or any other means, and instruments of information, that may be used by a State for the purposes of intervening in the internal or external affairs of a foreign State. The prohibition on intervention is especially pertinent in the context of cyberspace given the increasing connectivity between States and societies which provides greater opportunities for malicious actors, including States and non-State actors the acts of which are attributable to States, to misuse ICTs for the purpose of intervening in the internal and external affairs of States. Various codifications of the prohibition on intervention have also affirmed that this rule proscribes both direct intervention by de jure and de facto organs of a State and indirect intervention by persons or groups acting under the direction, instruction, or control of a State. This rule also proscribes the organizing, funding, or the provision of any form assistance to non-State actors engaged in acts of intervention against another State.

30. To constitute a violation of the prohibition on intervention, ICTs in cyberspace must be employed in a manner that amounts to coercion, which the International Court of Justice described, in the *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, as the element that "defines, and indeed forms the very essence of prohibited intervention."

31. The African Union is of the view that coercion, in the context of the prohibition on intervention, should be defined as a policy that is designed to impose restraints on the will of a foreign State. Assessing whether the use by one or more States of ICTs in cyberspace to influence the conduct of a foreign State amounts to coercion is a determination that should be undertaken on a case-by-case basis.

32. While the definition of coercion in this context requires further study and deliberation between States, the African Union is of the view that it is not necessary, in order to constitute coercion, that the conduct of a State must rise to the level of completely depriving a foreign State of its freedom of choice or to compel that State to either act or refrain from acting involuntarily. Coercion may also occur through threats of intervention. Furthermore, there is no requirement that, in order to constitute a violation of the prohibition on intervention, an act of coercion must actually succeed in compelling the State subjected to such acts to change its conduct. An unsuccessful attempt of intervention is unlawful under international law. The African Union stresses that offers or calls to peacefully settle disputes through negotiation, enquiry, mediation, conciliation, good offices, arbitration, and judicial settlement, and diplomatic discussions and communications are presumed not to constitute acts of coercion.

33. The African Union recalls that, by virtue of their territorial sovereignty, all States are under an obligation to exercise due diligence to prevent the use of their territory by other States or by non-State actors to engage in acts that constitute a violation of the prohibition on intervention in the internal or external affairs of States.

V. THE PEACEFUL SETTLEMENT OF DISPUTES IN CYBERSPACE

34. The obligation to settle international disputes by peaceful means is a rule of customary international law that is also codified in international and regional treaties, including the U.N. Charter and the founding instruments of regional organizations, such as the Constitutive Act of the African Union.

35. The African Union recalls Article 4(e) on the peaceful resolution of conflicts and Article 4(f) on the prohibition of the use of force or the threat to use force of the Constitutive Act of the African Union, and reaffirms that in accordance with Article 2(3) and Article 33 of the U.N. Charter the obligation to settle international disputes peacefully applies to any dispute that may arise between States relating to acts, omissions, or any disagreement on a point of law or fact, that relates to the use of ICTs in cyberspace, or that relates to the application or interpretation of international law in this field. This obligation is not limited to disputes the continuance of which is likely to endanger the maintenance of international peace and security.

36. In accordance with the U.N. Charter, States are obligated to settle international disputes through peaceful means such as negotiation, enquiry, mediation, conciliation, good offices, arbitration, judicial settlement, resort to regional agencies or arrangements, or any other peaceful means of their own choice.

37. The African Union recognizes the potential of information and communication technologies (ICTs) to enhance the peaceful settlement of disputes and encourages the use of ICTs in the context of dispute settlement. The African Union also supports the development of ICT-based tools and platforms for the peaceful settlement of disputes, such as online mediation platforms and dispute resolution software, and urges states to invest in research and development of ICTs for the peaceful settlement of disputes in cyberspace.

VI. THE PROHIBITION ON THE THREAT OR USE OF FORCE IN CYBERSPACE

38. The prohibition on the threat or use of force is a rule of jus cogens[1] and a fundamental and cardinal rule of general international law that is also a cornerstone of the U.N. Charter. This rule is also enshrined in many treaties and founding instruments of regional organizations, such as the Constitutive act of the African Union, and in bilateral agreements. This rule of international law applies in cyberspace and governs the conduct of States in relation to ICTs in cyberspace.

39. The prohibition on the use of force admits only two exceptions: the use of force in self-defense if an armed attack occurs, and the use of force that is authorized by the UN Security Council acting under Chapter VII of the UN Charter. The African Union affirm that this rule applies to the use of armed force by States. The African Union is of the view that cyber operations would fall within the scope of the prohibition of the use of force when the scale and effects of the operation are comparable to those of a conventional act of violence covered by the prohibition. In particular, a cyber operation, depending on its scale and effect, would amount to use of force if it is expected to cause physical damage, injury, or death, that is comparable to the use of force by an act covered by the prohibition.

40. For example, a cyber operation that destroys, inflicts damage, or permanently disables critical infrastructure or civilian objects within a State, may be considered as amounting to a use of force

[1] The Kingdom of Morocco, expressed a reservation regarding the reference to the concept of "jus cogens. The Kingdom of Morocco holds the view that: In the framework of the progressive development of international law, the prohibition of the use of force could eventually be qualified as a peremptory norm by the competent organs of the United Nations to whom the mandate of codification and progressive development of international law is entrusted.

under international law. Similarly, a cyber operation that targets a military asset by destroying, damaging, or deactivating a missile defense system, could constitute a violation of the prohibition on the use of force. The determination of whether a cyber-operation or a cyber-operation that is executed in combination with the use of non-cyber weapons constitutes a use of force should be undertaken on a case-by-case basis.

41. The African Union underscores that there is a distinction between the gravest forms of the use of force that constitute an armed attack, which entitle the injured State to invoke the right to individual or collective self-defense in accordance with Article 51 of the U.N. Charter, and less grave forms of the use of force. Whether a particular cyber operation constitutes a use of force or amounts to an armed attack should be determined on a case-by-case basis. That determination should be thoroughly substantiated on the basis of an assessment of the scale and effects of the particular cyber operation. Generally, the criterion of scale requires an examination of elements such as the duration of the attack, the nature of the targets attacked, the locations of the targets attacked, and the types of weapons used, while the criterion of effects measures the extent of the damage caused by the attack.

42. The African Union takes note of the views that assert that States have a right to exercise self-defense against imminent threats of the use of force. This is a controversial question on which there is a paucity of judicial precedent and a lack of unanimity among highly qualified publicists. The African Union is of the view that this matter requires further study and deliberation between States taking into consideration both the unique characteristics of cyberspace and cyber-operations and the implications that any rules that may emerge in relation to this question may have for the integrity of the prohibitions on the threat or use of force. In this regard, the Member States of the African Union emphasize that, from a legal perspective, the Article 51 of the U.N. Charter permits States to use force in individual or collective self-defense "if an armed attack occurs" against a U.N. Member State. Furthermore, the African Union underscores that, from a policy perspective, the maintenance of international peace and security favors the continued adoption of a restrictive interpretation of the exceptions to the prohibition on the use of force.

43. The prohibition on the threat or use of force addresses States in their international relations. Therefore, this rule and the exceptions thereto do not apply to the conduct of non-State actors that is not attributable to States. Accordingly, the African Union affirms that the right of self-defense is triggered solely if an armed attack is attributable to a State according to the applicable rules of customary international law of State responsibility.

44. The African Union notes that arming and training non-State actors could amount to a violation of the prohibition on the threat or use of force. This applies to the provision of technical assistance or training to non-State actors that engage in acts amounting to the threat or use of force through ICTs against another State.

45. In this context, the African Union reiterates that, by virtue of their territorial sovereignty, all States are under an obligation to exercise due diligence as reflected in Section III above and to ensure that their territory is not knowingly used to violate the rights of other States through acts that constitute a threat or use of force, whether such acts are undertaken by organs of the State or non-State actors acting under the direction, control, or instruction of the State.

46. Conduct that does not amount to a violation of the prohibition on the threat or use of force may, depending on the circumstances, constitute a breach of other rules of international law, especially the obligation to respect the territorial sovereignty of States and the prohibition on intervention in the internal or external affairs of States.

VII. INTERNATIONAL HUMANITARIAN LAW IN CYBERSPACE

47. The African Union affirms that International Humanitarian Law (IHL) applies in cyberspace. Despite the fact that most rules of IHL emerged before the appearance of cyberspace, IHL applies, concurrently with any other applicable rules of international law, to cyber-operations that may be undertaken in the context of an armed conflict. As noted by the International Court of Justice in its advisory opinion on the *Legality of the Threat or Use of Nuclear Weapons*, by virtue of its "intrinsically humanitarian character," IHL applies to "all forms of warfare and to all kinds of weapons, those of the past, those of the present, and those of the future."

48. In order to trigger the application of IHL, a situation must amount to an armed conflict. IHL recognizes two categories of armed conflict: international armed conflicts, in which the parties are States that are engaged in hostilities using armed force, and non-international armed conflicts, in which the parties are State armed forces engaged in hostilities against organized armed groups or a situation in which armed groups are engaged in hostilities amongst each other on the territory of a State.

49. In an international armed conflict, the application of IHL commences whenever armed force is used between States regardless of the intensity of such activities. The application of IHL to an international armed conflict is unaffected by either the absence of a formal declaration of war or by the assessment of the legality, under the applicable rules of the U.N. Charter, of the use of force by the belligerent States. On the other hand, The African Union is mindful of the possibility that cyberoperations as in itself may trigger a non-international armed conflict. The application of IHL commences in a non-international armed conflict when the intensity of the conflict amounts to protracted armed violence, which means that it is above the level of violence associated with internal disturbances, such as riots, isolated, and sporadic violence, and in situations where the armed groups engaged in hostilities reach a certain degree of organization.

50. The African Union reaffirms their commitment to the cardinal principles of IHL that govern all means and methods of warfare and reiterate that such principles apply to the use of ICTs in cyberspace as a means of warfare and afford protection to civilian ICTs during armed conflicts. In particular, the African Union recalls the principle that "the right of belligerents to adopt means of injuring the enemy is not unlimited" and the principle that belligerents are under an obligation to limit the suffering, injury, and destruction caused by an armed conflict.

51. On the basis of these general principles, the African Union underscores the importance of the principle of distinction, which prohibits attacks that are directed at civilians or civilian objects, including ICTs, whether such attacks are undertaken using kinetic or cyber means. The African Union also emphasizes the importance of the principle of proportionality, which prohibits attacks that are expected to cause incidental civilian harm that would be excessive to what is necessary to achieve a definite military advantage.

52. The African Union emphasizes that certain civilians and civilian objects, including the related ICT infrastructure associated with them, enjoy additional specific protection under the relevant rules of IHL. These objects, which are indispensable to the survival of the civilian population, include hospitals, medical personnel, and facilities as well as humanitarian relief operations. Such objects must be respected and protected at all times and not be interfered with, attacked, destroyed, removed or rendered useless.

VIII. INTERNATIONAL HUMAN RIGHTS LAW IN CYBERSPACE

53. The African Union affirms that international human rights law (IHRL), whether codified in universal or regional conventions to which States are party or embodied in customary international law, applies in cyberspace, and also reaffirms the universality, indivisibility, interdependence, and interrelation of all human rights and fundamental freedoms, including the right to development. Accordingly, States shall respect, protect, and ensure the human rights of individuals and peoples on their territory or under their jurisdiction that relate to the peaceful use of ICTs in cyberspace, including by protecting such individual and collective rights against infringements by third parties and non-State actors.

54. The African Union further affirms that IHRL requires States to protect the freedom of expression online, including the right to seek, receive, and impart information and ideas and to disseminate opinions through ICTs. Any restrictions imposed by States on these rights must be provided by law and must be limited to what is strictly necessary in a democratic society to respect and protect the rights or reputations of others and to protect national security, public order, public health, or morals. The African Union also reaffirms that States shall ensure that ICTs are not misused for the purposes of inciting to violence, hate crimes, terrorism, violent extremism, organized crimes and trafficking in persons, or discrimination on any grounds, including race, ethnicity, color, sex, language, religion, political or any other opinion, national and social origin, fortune, birth or other status. In this regard, the African Union recalls that special regard should be to be paid to persons in vulnerable situations.

55. The African Union is of the view that responsible behavior in relation to the use of ICTs in cyberspace requires States to ensure that their conduct does not infringe on the human rights of individuals or peoples in other States. In particular, certain activities undertaken by States, such as the transnational interception of communications, indiscriminate surveillance and data misuse, may constitute a violation of the right to privacy of individuals who are subjected to such conduct, in addition to potentially violating the territorial sovereignty of States on the territory of which such interception occurs. Despite the existence of international and regional legal frameworks, the African Union expresses concern about the misuse of private data by malicious or criminal actors as well as its misappropriation and commodification by private actors.

56. The African Union affirms that States shall protect individuals and peoples within their territory or in areas under their jurisdiction against violations of human rights that are committed by third parties, especially business enterprises operating in the ICT sector. Moreover, business enterprises that operate in the ICT sector have a responsibility to respect and protect human rights, especially the right to privacy and the freedom of expression, including by exercising due diligence to identify, prevent, mitigate, and account for any adverse human rights impacts of their activities.

57. The African Union emphasizes the importance of keeping cyberspace open, secure, stable, accessible, and peaceful, which is an important element in promoting economic growth, attracting investment opportunities, and advancing sustainable development, especially in developing and least developing States. In this regard, The African Union underscores that, pursuant to the right to development under international law, States shall cooperate in good faith including as outlined in Section X on Capacity-Building and International Cooperation, to support developing countries in their efforts to expand their scientific and technological capacities, including in the area of ICTs, in order to accelerate the realization of the economic, social, and cultural rights of the peoples of those countries.

58. The African Union highlights the importance of bridging the digital divide to ensuring the full enjoyment of human rights. In this regard, States shall contribute to further empowering women and

girls. States shall also further promote the full enjoyment of the benefits of ICTs by persons with disabilities by ensuring that the design, development, and production of ICTs incorporates assistive and adaptive technologies that are accessible to persons with disabilities.

59. The African Union calls for the responsible development and management of digital identity systems in a manner that will respect human rights of all individuals.

60. The African Union encourages States to consider the conclusion of agreements on mutual assistance in the area of combating all forms of cyber-crime, which would further contribute to the protection and full realization of individual human rights.

IX. THE RULES OF ATTRIBUTION OF CONDUCT TO A STATE IN CYBERSPACE

61. Subject to the emergence of specific rules of attribution, the African Union affirms that the customary rules on State responsibility, as reflected in the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts provide the applicable rules of the attribution to States of conduct undertaken through ICTs in cyberspace.

62. The African Union is of the view that, in conformity with the relevant rules of international law, the burden to substantiate a claim that a State has committed an internationally wrongful act through ICTs in cyberspace is on the State making such a claim. The African Union also underscores the importance of cooperation, including between national authorities, such as Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs), to detect, investigate, prevent, and halt internationally wrongful acts undertaken through ICTs in cyberspace.

63. The African Union underscores that responses to internationally wrongful acts committed through ICTs in cyberspace should be in accordance with its obligations under the UN Charter, especially the obligations relating to the peaceful settlement of disputes, and the other applicable rules of international law, including the obligation to respect the territorial sovereignty of States.

X. CAPACITY-BUILDING AND INTERNATIONAL COOPERATION IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES AND CYBERSPACE

64. The African Union emphasizes the importance of international cooperation in facing the global challenges of our times, including in the area of cyberspace. The African Union also recalls that in a digitally interdependent world, international cooperation, including through assistance with technical expertise and capacity-building, is essential for bridging the digital-divide and for ensuring that cyberspace is open, secure, stable, accessible and peaceful.

65. The African Union underscores the importance of cooperation, with partner States, international organizations, and the private sector by developing regional and national institutional capacities through capacity building, technical assistance, and the exchange of technical expertise in area of cyberspace in order to identify and address digital-divides and inequalities, and to improve coordination between technical, policy, legal, and regulatory authorities at the national and international level.

66. The African Union stresses the importance of enhancing capacity-building efforts aimed at enabling States to identify, protect, and collectively safeguard critical national infrastructure, including critical information infrastructure and to cooperatively safeguard critical information infrastructure. The African Union also affirms that special attention is needed to support the capacities of developing states at both the policy and technical levels in areas such as the development of

national cyber security and resilience strategies, providing access to relevant technologies, and support to Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs). The African Union reaffirms that special attention is needed for enhancing international cooperation in further clarifying and developing the rules of international law that apply to cyberspace, in a manner that fully integrates the development dimension in the future elaboration of these rules.

67. The African Union reiterates that capacity-building and technical assistance must respect State sovereignty, and should also be based on mutual trust and recognition of national ownership. The African Union emphasizes that capacity building and all cooperation in this area should respect the integrity and security of national ICT infrastructure, and correspond to nationally identified needs and priorities, and respect and protect the confidentiality of national policies and plans.

XI. CONCLUSION

68. The views expressed in this Common African Position are a non-exhaustive articulation of the views of the African Union regarding some of the salient questions relating to the application of international law in cyberspace. These views are without prejudice to the possible application of other rules of international law that relate to the governance of cyberspace, especially any applicable regional or international instruments relating to combatting cybercrime. These views expressed herein may be the subject of further development and elaboration by the African Union and by the Member States of the African Union acting both individually or collectively, in light of technological developments and the ongoing discussions on these questions.

69. The African Union remains committed to engaging positively and contributing constructively to international, inclusive, and multilateral debates on these matters, with a view to ensuring that cyberspace remains open, safe, peaceful, secure, stable, and accessible, and that ICTs continue to serve as a vehicle for the promotion of regional integration in Africa and upholding the common interests of humankind.

2024-01-29

Communiqué of the 1196th Meeting of the Peace and Security Council held on 29 January 2024 on the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace.

Peace and Security Council

African Union Commission

AFRICAN UNION

الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

Addis Ababa, Ethiopia. P.O. Box: 3243 Tel.: (251-11) 5513 822 Fax: (251-11) 5519 321
Email: situationroom@africa-union.org

PEACE AND SECURITY COUNCIL
1120TH MEETING

9 NOVEMBER 2022
ADDIS ABABA, ETHIOPIA

PSC/PR/COMM.1120.1 (2022)

COMMUNIQUÉ

COMMUNIQUÉ

Adopted by the Peace and Security Council (PSC) of the African Union (AU) at its 1120th meeting, held on 9 November 2022, on the Inaugural Engagement between the Peace and Security Council and the AU Commission on International Law:

The Peace and Security Council,

Recalling the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) and Communiqué [PSC/PR/COMM.1097.1 (2022)], adopted at its 1097th meeting held on 4 August 2022, on Emerging Technologies and New Media: Impact on Democratic Governance, Peace and Security in Africa; Decision [Ext./Assembly/AU/Dec/(XVI)] adopted by the 16th Extraordinary Session of the AU Assembly of Heads of State and Government on Terrorism and Unconstitutional Changes of Government held on 28 May 2022, in Malabo, Equatorial Guinea, as well as all its previous decisions and pronouncements on cyber-security;

Deeply concerned about the malicious use of information and communication technologies and increasing incidents of hostile cyber-activities undertaken by state and non-state actors in times of peace and during armed conflicts, including the targeting of government institutions and public infrastructure; the spread of misinformation and disinformation, subversive activities and interferences with national government processes such as elections, the promotion of ideologies of hate and hate speech;

Mindful of the deliberations and outcomes of the United Nations (UN) Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security and the UN Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security;

Noting the opening statement made by H.E. Ambassador Emilia Ndinelao Mkusa, Permanent Representative of the Republic of Namibia to the Africa Union and Chairperson of the PSC for November 2022, and the statement by Dr. Al Haji Sarjo Bah on behalf of H.E. Ambassador Bankole Adeoye, Commissioner for Political Affairs, Peace and Security; ***also noting*** the statement by Dr. Guy-Fleury Ntwari, the AU Legal Counsel; the statement by Professor Hajer Gueldich, Chairperson of the AU Commission on International Law and the presentation by Professor Dr. Mohamed Helal, member of the African Union Commission on International Law and Special Rapporteur on the Prohibition on Intervention in the Internal and External Affairs of States; and

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

1. ***Welcomes*** the convening of the inaugural engagement with the AU Commission on International Law and ***underscores the importance*** of regularizing the engagements;

2. ***Emphasizes*** that cyberspace and information and communication technologies are essential for promoting peace, security, stability and development in all countries and regions;

3. ***Acknowledges*** the application of international law to cyberspace, and ***stresses*** that the prohibition on the threat or use of force, the prohibition on intervention in the internal or external affairs of states, and the inviolability of the political independence, territorial integrity, and sovereignty of states are foundational rules of international law;

4. ***Underlines the urgent need*** for a Common African Position on the application of international law on cyberspace, as well as the need for Africa to actively engage in the process of articulating the rules of international law in this regard;

5. ***Acknowledges*** that basic human rights and fundamental freedoms, especially the principles enshrined in the African Charter on Human and Peoples' Rights, and the fundamental principles of international humanitarian law are also applicable to cyberspace;

6. ***Requests*** the AU Commission on International Law to prepare a draft statement on the Application of International Law to Cyberspace to be submitted to Council for consideration, as well as to circulate to all Member States the background note and questionnaire prepared by the AU Commission on International Law on the application of international law to cyberspace, and ***encourages*** Member States to expeditiously respond to the questionnaire;

7. ***Also requests*** the AU Commission, working in close collaboration with the AU Commission on International Law, to organize consultations with relevant stakeholders, on the application of international law to information and communication technologies and cyberspace and to provide the required technical support to Member States; and

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

AFRICAN UNION

الاتحاد الأفريقي

UMOJA WA AFRICA

UNION AFRICAINE

UNIÃO AFRICANA

UNIÓN AFRICANA

Addis Ababa, Ethiopia. P.O. Box: 3243 Tel.: (251-11) 5513 822 Fax: (251-11) 5519 321
Email: situationroom@africa-union.org

PEACE AND SECURITY COUNCIL
1148TH MEETING

13 APRIL 2023
ADDIS-ABABA, ETHIOPIA

PSC/PR/COMM.1148 (2023)

COMMUNIQUÉ

COMMUNIQUÉ

Adopted by the Peace and Security Council (PSC) of the African Union (AU) at its 1148th meeting held on 13 April 2023, on "Cyber Security: Impact on Peace and Security in Africa".

The Peace and Security Council,

Recalling the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) and Communiqué [PSC/PR/COMM.1120.1.(2022)] adopted at its 1120th meeting held on 9 November 2022 on the Inaugural Engagements between the PSC and the AU Commission on International Law, which affirmed that international law applies to cyberspace and stressed that the prohibition on the threat or use of force, the prohibition on intervention in the internal or external affairs of states, and the inviolability of the political independence, territorial integrity, and sovereignty of states are foundational rules of international law;

Recalling Communiqué [PSC/PR/COMM.1097.1 (2022)], adopted at its 1097th meeting held on 4 August 2022, on Emerging Technologies and New Media: Impact on Democratic Governance, Peace and Security in Africa; Communiqué [PSC/PR./COMM. (DCCCL)], adopted at its 850th held on 20 May 2019; and Press Statement [PSC/PR/BR.(DCXXVII)] adopted at its 627th meeting (Open Session) held on 26 September 2016; as well as Assembly Decision [Ext./Assembly/AU/Dec/(XVI)] adopted by the 16th Extraordinary Session of the AU Assembly of Heads of State and Government on Terrorism and Unconstitutional Changes of Government held on 28 May 2022, in Malabo, Equatorial Guinea, as well as all its previous decisions and pronouncements on cyber-security;

Deeply concerned by the growing threat to peace, security and stability in the Continent emanating from the increasing cyber-attacks, malicious use of information and communication technologies (ICTs) and incidents of unethical and hostile cyber-activities undertaken by both, state and non-state actors, including the targeting of government institutions and public infrastructure; the spread of misinformation and disinformation, subversive activities and interferences with national government processes, as well as the promotion of ideologies of hate and hate speech;

Mindful of the ongoing open-ended deliberations and outcomes of the United Nations (UN) Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security and the UN Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security;

Acknowledging the critical importance of the cyber technologies; information and communication technologies (ICTs) in the promotion of national, regional and continental development; as well as in the promotion of peace, security and stability in Member States;

Noting the opening statement made by H.E. Ambassador Abdelhamid Elgharbi, Permanent Representative of the Republic of Tunisia to the Africa Union and Chairperson of the PSC for April 2023, and the introductory remarks read by Ms. Patience Chiradza, the Director for Governance and Conflict Prevention, on behalf of H.E. Ambassador Bankole Adeoye, Commissioner for Political Affairs, Peace and Security; ***also noting*** the presentations by the representatives of the AU Department of Energy and Infrastructure; the AU Office of the Legal Counsel, the International Telecommunications Union (ITU) and the Committee of Intelligence and Security Services of Africa (CISSA); and

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

1. ***Expresses deep concern*** over the increasing global cyber threats and attacks, which constitute a serious threat to national, regional and international peace and security and, in this respect, ***strongly condemns*** all cyber-attacks, particularly the recent large-scale attack on the AU Commission information technology (IT) infrastructure and ***strongly warns*** the perpetrators that they shall be brought to account for their heinous acts;

2. ***Stresses the need*** for effective internet governance as a matter of urgency and strategic importance and in this regard, ***encourages*** Member States to develop national cybersecurity strategies and to create national and regional computer emergency response teams (CERT) and/or computer security incident response teams (CSIRT);

3. ***Also encourages*** Member States to develop, in collaboration with all stakeholders, national cybersecurity policies and adopt other necessary measures to more effectively secure their cyberspaces;

4. ***Underlines the importance*** of mainstreaming cyber security in all AU activities and; in the same context ***requests*** the AU Commission to expedite the establishment of a Unit within the Political Affairs Peace and Security Department, which will work together with all other stakeholders in monitoring and reporting on cyber-security issues within the Continent, pursuant to Press Statement [PSC/PR/BR.(DCXXVII)] adopted at its 627th meeting (Open Session) held on 26 September 2016;

5. ***Encourages*** Member States to develop robust regulatory frameworks that facilitate the ethical use of ICTs, including the establishment of credible data governance infrastructure and to work together with the private sector, with a view to further strengthen the national cyber security capacities;

6. ***Underscores*** the importance of a Common African Position on cyber security and, in this context, ***requests*** the AU Commission on International Law to expeditiously complete, and submit to the Peace and Security Council, the draft statement of a Common African Position on the Application of International Law to Cyberspace, and ***encourages*** those Member States, which have not yet done so, to urgently complete the questionnaire that was circulated by the AU Commission on International Law on this matter;

7. ***Welcomes*** the capacity-building program that is being organized for the representatives of Member States by the AU Commission on International Law in cooperation with the Government of Canada on the rules of international law applicable to information and communication technologies, and ***encourages*** Member States to participate in the upcoming session of this capacity-building program that will be held at the AU Headquarters during the period June 7-9, 2023;

8. ***Encourages*** civil society organizations, educational institutions, think tanks and the media to also contribute in civic education and public awareness raising on cyber security and the threat posed by cyber attacks to national security and development;

9. ***Underlines the need*** for the Regional Economic Communities and Regional Mechanisms to also actively contribute in the efforts of Member States to combat cyber-attacks and, to this end establish regional cyber security centers;

10. ***Requests the AU Commission*** to establish mechanisms and platforms, such as the regional forums dedicated to address 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;

11. ***Encourages*** Member States to make full use of existing capacities within the Continent, including AFRIPOL and CISSA under the overall coordination of the Political Affairs, Peace and Security Department; in this regard, ***welcomes*** the offer by CISSA to provide training and capacity building to the PSC Committee of Experts on cybersecurity issues;

12. ***Strongly encourages*** all Member States, which have not yet done so, to urgently sign, ratify and fully domesticate the AU Convention on Cybersecurity and Personal Data Protection; and

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

AFRICAN UNION

الاتحاد الأفريقي

UMOJA WA AFRICA

UNION AFRICAINE

UNIÃO AFRICANA

UNIÓN AFRICANA

Addis Ababa, Ethiopia. P.O. Box: 3243 Tel.: (251-11) 5513 822 Fax: (251-11) 5519 321
Email: situationroom@africa-union.org

PEACE AND SECURITY COUNCIL
1171ST MEETING

24 AUGUST 2023
ADDIS-ABABA, ETHIOPIA

PSC/PR/COMM.1171 (2023)

COMMUNIQUÉ

COMMUNIQUÉ

Adopted by the Peace and Security Council (PSC) of the African Union (AU) at its 1171st meeting held on 24 August 2023, on "Updated Briefing on the Development of the Common African Position on Cyber-Security in Africa."

The Peace and Security Council,

Recalling Decision [Ext./Assembly/AU/Dec/(XVI)] adopted by the 16th Extraordinary Session of the AU Assembly of Heads of State and Government on Terrorism and Unconstitutional Changes of Government held on 28 May 2022, in Malabo, Equatorial Guinea and the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention);

Also recalling its previous decisions and pronouncements on Cyber Security in Africa, particularly, Communique [PSC/PR/COMM.1148 (2023)] adopted at its 1148th meeting held on 13 April 2023 on Cyber Security: Impact on Peace and Security in Africa; communique [PSC/PR/COMM.1120.1.(2022)] adopted at its 1120th meeting held on 9 November 2022 on the Inaugural Engagements between the PSC and the AU Commission on International Law (AUCIL); and communique [PSC/PR/COMM.1097.1 (2022)], adopted at its 1097th meeting held on 4 August 2022;

Determined to find a lasting solution to the growing threat to peace, security and stability in the Continent posed by the increasing cyber-attacks, malicious use of information and communication technologies (ICTs) and incidents of unethical and hostile cyber-activities undertaken by both, state and non-state actors, including the targeting of government institutions and public infrastructure; the spread of misinformation and disinformation, subversive activities and interferences with national government processes, as well as the promotion of ideologies of hate and hate speech;

Mindful of the critical importance of cyber technologies and ICTs in the promotion of national, regional and continental development; as well as in the promotion of peace, security and stability in Member States;

Noting the opening statement by H.E. Ambassador Willy Nyamitwe, Permanent Representative of the Republic of Burundi to the Africa Union and Chairperson of the PSC for the month of August 2023; the presentations by Dr. Guy-Fleury Ntwari, the Director of AU Legal Counsel and by Dr. Mohammed Helal, the Special Rapporteur of the AU Commission on International Law; and

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

1. ***Reiterates its deep concern*** over the increasing global cyber threats and attacks, which constitute a serious threat to national, regional and international peace and security and, in this respect, ***strongly condemns*** all cyber-attacks, particularly the recent large-scale attack on the AU Commission information technology (IT) infrastructure;

2. ***Welcomes*** the Draft Statement by the AUCIL on the Application of International Law to the Use of ICTs in Cyberspace prepared by the Special Rapporteur on the Prohibition on Intervention in the Internal and External Affairs of States, which was adopted and endorsed by the 22nd Ordinary Session of the AUCIL in June 2023 and ***requests*** the Special Rapporteur to continue to engage Member States and other key stakeholders, in order to further develop the Draft Statement;

3. ***Commends*** the AUCIL for successfully co-organizing with the Government of Canada, a capacity building training programme on Application of International law on the Cyber-Space for

Member States, the AU Commission and the Regional Economic Communities and Regional Mechanisms (RECs/RMs), in May and in June 2023; and in this regard, ***expresses deep appreciation*** to the Government of Canada for the continued support;

4. ***Also commends*** all Member States which have already developed robust legislative and institutional frameworks on the use of ICTs and the cyber space and ***encourages*** those which have not yet done so to also do the same, and to also develop their own national cyber security strategies;

5. ***Decides*** to establish an expert-level working group, with the participation of the PSC Committee of Experts and other interested AU Member States, with a mandate to review the Draft African Statement adopted and endorsed by the AUCIL, for adoption by the PSC as a Common African Position on the Application of International Law in the Cyber Space; and ***underscores the importance*** of mainstreaming women and the youth, as well as the importance of taking into full consideration the peculiarities of the specific contexts of each Member State;

6. ***Emphasizes*** that the process should be led by the AUCIL through its Special Rapporteur, and supported by other AUCIL members, the AU Commission, and the Working Group of African Experts in order to ensure inclusivity and ownership of the process by all Member States;

7. ***Requests*** the Working Group, once established, to submit the Draft Common African Position on Cyber Security in Africa to the PSC by December 2023, for its consideration before the next Ordinary Session of the AU Assembly to be held in February 2024; in this regard, ***requests*** the AU Commission to establish a timeframe for the Working Group to complete its mandate;

8. ***Once again, encourages*** all Member States, which have not yet done so, to sign and ratify the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention);

9. ***Reiterates the need*** for the Regional Economic Communities and Regional Mechanisms to also actively contribute to the efforts of Member States to combat cyber-attacks and, to this end establish regional cyber security centers; and

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