Consideration of the Draft Common African Position on the Application of International Law in the Cyber Space

Consideration of the Draft Common African Position on the Application of International Law in the Cyber Space Date | 28 January 2024

Tomorrow (29 January) the African Union (AU) Peace and Security Council (PSC) will convene its 1196th Session. This session will consider the Draft Common African Position on the Application of International Law in the Cyber Space.

The session is expected to begin with opening remarks by **Amma Adomaa Twum-Am**, the Permanent Representative of Ghana and Chairperson of PSC January, followed by a statement from **Bankole Adeoye**, the AU Commissioner for Political Affairs, Peace and Security (PAPS). **Kawasi Asante,** the Deputy Permanent Representative of Ghana, is also expected to present the Draft Common African Position on the Application of International Law to the Use of Information and Communication Technologies in the Cyber Space.

The last time the PSC held a session to review the progress made towards developing the Common African Position (CAP) on the application of international law in cyberspace was during its 1171st session on 24 August 2023. During this session, the Council acknowledged the draft statement by the AUCIL regarding the Application of International Law to the Use of ICTs in Cyberspace and decided to establish an expert-level working group. The working group, consisting of the PSC

Committee of Experts and interested AU Member States, was given the responsibility to review the Draft African Statement endorsed by the 22nd Ordinary Session of the AUCIL and presented to the 1171st session of the PSC.

The process started at the 1120th Session where the PSC acknowledged the relevance of international law to cyberspace and entrusted the AUCIL, in collaboration with the AU Commission, to conduct consultations with relevant stakeholders on the application of international law to cyberspace. Subsequently, at the 1148th session, the PSC called upon the AUCIL to promptly finalize and submit a draft statement of the Common African Position on the Application of International Law to Cyberspace.

In response to the AU Commission's request during the 1120th session for technical support in Member States' development of their national positions and a Common African Position, in 2023, the AUCIL has organized three 'capacity building' and consultation sessions. These sessions sought to provide Member States with the essential knowledge and skills to actively contribute to the formulation of the CAP. Additionally, the sessions also provided an opportunity for consultations with Member States and African Experts, regarding the draft Statement. Experts representing AU Member States in the UN General Assembly First Committee, which is responsible for multilateral processes and the Sixth Committee, which is responsible for legal affairs, were also involved in these consultations.

Following the establishment of the Working Group of Experts as per the decision of the 1171st Session, the Group met in Tunisia from 29 November – 1 December 2023 and virtually on 9 January 2024. During these meetings, the draft CAP was presented and considered by the working group of experts.

Along with the increasing strategic significance of cyberspace in all areas of life and the growing use of cyber for orchestrating attacks and criminal acts, governance of cyberspace has become a pressing global issue. In this regard, the UN General Assembly took action in 2020 by adopting resolution 75/240, establishing a five-year open-ended working group dedicated to the security aspects of information and communications technologies (ICTs) from 2021 to 2025. This working group has actively encouraged the submission of national positions regarding the application of international law to ICTs. Consequently, several states have submitted their position papers on this matter and discussion forums have been convened.

This issue of safety of the cyberspace is of particular significance for Africa given the level of vulnerability of the continent. A recent manifestation of Africa's vulnerability is the major cyber-attack that inflicted damage to the AU infrastructure in April last year. As one recent study established 'the widespread use of technology, combined with insufficient cybersecurity measures, inadequate legislation in the field of information security, and a low level of public awareness concerning information security, creates favourable conditions for cybercriminals.' Yet, perhaps more than the issue of immediate concerns of cybersecurity, for countries in Africa vulnerabilities that arise from the monopolization of digital platforms by some big corporations carry bigger challenges to their political and cultural as well as socio-economic identity and wellbeing.

"Yet, perhaps more than the issue of immediate concerns of cybersecurity, for countries in Africa vulnerabilities that arise from the monopolization of digital platforms by some big corporations carry bigger challenges to their political and cultural as well as socio-economic identity and wellbeing. "

It is in this context that the question of the role and application of international law in governing cyberspace

acquires particular significance. In this regard, the development of the AU common position on the application of international law can also help articulate formulations that resonate with the particular vulnerabilities and needs of Africa as far as international law's application to and role in governance of the cyberspace is concerned.

Apart from these immediate issues of security, other broader and more strategic issues pertaining to the cyber domain that are of paramount importance include non-intervention, use of force, due diligence, state responsibility, international humanitarian law and international human rights law. These issues are particularly of increasing strategic importance for Africa considering the dominance of the sector by big businesses domiciling mostly in old and new global powers. Reports from the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace, mandated by the General Assembly, have reached a consensus in acknowledging the applicability of the entire UN Charter, particularly regarding sovereignty, dispute resolution through peaceful means and non-intervention.

The ongoing debate as to whether traditional principles of sovereignty apply to the borderless nature of the digital realm has raised interesting questions regarding the suitability of well-established notions such as territorial control and state authority in the context of cyberspace. Advocates for maintaining sovereignty in the digital domain emphasize the importance of state responsibility for cyber activities within their borders while opposing viewpoints argue that cyberspace challenges conventional sovereignty concepts by surpassing physical boundaries and involving non-state actors. In this regard, the draft CAP will indicate the clear stance of African states on the applicability of the principle of sovereignty to cyberspace and the protection of persons and objects in the territory of a state against the infliction of cyber threats.

On the other hand, the principle of non-intervention, which is considered a natural extension of the sovereign equality of all states, is a fundamental principle of general international law that is also enshrined in the AU Constitutive Act. This principle encompasses the non-interference in matters within a state's independent decision-making and the use of coercion. In this regard, the draft CAP may clarify the positions of AU member states regarding whether the prohibition of intervention primarily applies between states and does not directly extend to non-state actors, or if it also applies to non-state actors. It cannot be denied that the underlying precepts of the principles of sovereignty and non-intervention linked to the fundamental principle of self-determination of all peoples remain relevant and provide the basis for ensuring that the dominance of certain businesses in controlling digital platforms is not instrumentalized, particularly in the context of rising geopolitical tensions, for manipulation and exercising undue influence on African countries, underscoring the importance of these principles vis-à-vis actions of non-state actors as well. Indeed, the international law rule that imposes an obligation on states to ensure that non-state actors operating within their jurisdiction don't use their territories for engaging in threatening actions against other states can be instructive in this respect. When it comes to coercion, most states hold the position that determining what qualifies as coercion in the cyber context is complex and requires a case-by-case evaluation. Therefore, the draft CAP will likely indicate its stance on the determination of acts of coercion in cyberspace as well.

"It cannot be denied that the underlying precepts of the principles of sovereignty and non-intervention linked to the fundamental principle of self-determination of all peoples remain relevant and provide the basis for ensuring that the dominance of certain businesses in controlling digital platforms is not instrumentalized, particularly in the context

of rising geopolitical tensions, for manipulation and exercising undue influence on African countries, underscoring the importance of these principles vis-à-vis actions of non-state actors as well. "

The draft CAP is also anticipated to incorporate another component, which is the customary international law principle stated in Article 2(4) of the UN Charter and Article 4(f) of the AU Constitutive Act, prohibiting the use or threat of force. This principle is applied with two exceptions: self-defence in the event of an armed attack and the use of force authorized by the UN Security Council under Chapter VII of the UN Charter. Therefore, the determination that is expected to be covered under the draft CAP is whether cyber operations fall under the prohibition of the use of force or not. Furthermore, the draft CAP may provide a position on the interpretation of the right to self-defence as stated in Article 51 of the UN Charter, as it has been a subject of greater disagreement among member states.

Additionally, the draft CAP is expected to cover the topic of a state's obligation of due diligence to ensure that its territory is not used to harm other states. Due diligence is a standard of conduct that requires states to take reasonable measures to prevent their territory from being used for activities that could have significant adverse consequences for other states. The draft CAP may provide a position on how the obligation of due diligence of a state should be determined when it comes to the wrongful use of ICTs located within its territory. It may also indicate its stance on determining a state's knowledge of a wrongful act occurring within its territory.

The draft CAP is expected to comprehensively address the application of general norms of State responsibility to wrongful acts in the cyber context, taking into account the technical challenges in attributing responsibility for cyber operations compared to kinetic operations. It is crucial for

the draft CAP to clarify whether rules for attribution under the law of State responsibility also apply in cyberspace, including the attribution of the acts of non-state actors' conduct to a state. Additionally, the draft CAP may also include the position of states on concerns related to the lack of legal requirements for a state to disclose evidence regarding attribution. Furthermore, the draft CAP will provide guidance on the application of international humanitarian law and international human rights law to cyberspace.

The expected outcome is a communique. The PSC is expected to reiterate the pressing need for a Common African Position on the application of international law in cyberspace. Additionally, the PSC is expected to acknowledge the efforts of the AUCIL in updating AU Member States' representatives and the working group of experts on the latest development of the draft Common African Position in the application of international law to cyberspace. The PSC may endorse the draft Common African Position and recommend presenting it to relevant AU bodies, such as the Specialized Technical Committee (STC) on Justice and Legal Affairs, for wider input. The PSC may further emphasise the importance of Africa's active engagement in the formulation of international legal principles. In this regard, the Council may also encourage member states to increase their engagement in multilateral debates; which will enhance Africa's representation as well as the continent's impact on the development of global standards and frameworks for cyberspace and protection of Africa's interests.