Engagement between the PSC and the AU Commission on International Law (AUCIL) on international law and cyberspace

Engagement between the PSC and the AU Commission on International Law (AUCIL) on international law and cyberspaceDate | 9 November 2022

Tomorrow (9 November), the African Union Peace and Security Council (PSC) will convene its 1120th session to engage with the AU Commission on International Law (AUCIL) and discuss the issue of international law and cyberspace.

Permanent Representative of Namibia to the AU and Chairperson of the PSC for the month of November, Emilia Ndinealo Mkusa, is expected to make opening remarks, followed by a statement from AU Commissioner for Political Affairs, Peace and Security (PAPS), Bankole Adeoye. Guy Fleury Ntwari, the AU Legal Counsel, will make a presentation touching on the role of international law in the advancement of peace and security and the importance of the role of the AU in shaping international law rules governing peace and security in cyberspace. The PSC also expects presentations on the thematic focus of the session from Hajer Gueldich, Chairperson of AUCIL, and Mohamed Helal, Special Rapporteur on Cyberspace and International Law and a member of the AUCIL.

Tomorrow's session, during which the PSC will interact for the first time with the AUCIL in relation to its mandate, is expected to provide an opportunity for the PSC and the AUCIL to harness their respective mandate for the articulation of an

African position on the formulation of international law rules governing cyberspace with a particular focus on the making of international law rules and peace and security in the cyberspace. The AUCIL is an 11 members independent advisory organ established in 2009 in line with article 5(2) of the AU Constitutive Act. As envisaged under article 4 of AUCIL Statute, the Commission is envisaged to undertake activities related to codification and progressive development of international law in Africa, with particular attention to the laws of the AU; propose draft framework agreements and model regulations; assist in the revision of existing treaties and identify areas in which new treaties are required; conduct studies on legal matters of interest to the AU and its Member States; encourage the teaching, study, publication and dissemination of literature on international law, specifically the laws of the AU.

The nature of the mandate of the AUCIL is such that it can also advise the AU and contribute to the crafting of African positions on the development of international law rules for the governing of global matters that affect peace and security in Africa. Tomorrow's session falls within this category of the mandate and work of the AUCIL.

The technological advance particularly in information and communication technologies (ICT) is a double-edged sword, offering both benefits and risks. Despite the enormous benefits that ICTs continue to produce in the social, economic, political spheres, State and non-state actors are increasingly using the cyberspace to carry out cyber-attacks on critical national infrastructure and democratic institutions, steal and launder money, illegally transfer funds, propagate hate speech, and incite violence. A worrying trend has been also emerging in the continent with the increasing use of the cyber space by terrorist groups who often exploit the platform for radicalization, lure recruits into their ranks, mobilize fundings and logistics, as well as

train individuals, incite and stage violent attacks. Furthermore, it has been used to influence domestic political outcomes that would destabilize governments of another state.

The PSC has addressed itself to the issue of cyber security and the need for addressing the deficit in the rules regulating cyberspace in earlier sessions. In this context, PSC's 627th session of September 2016 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'. In the absence of regulation, the cyberspace therefore poses a serious risk to the national, regional, and international peace and stability. The 627th session recognized 'a safe and secure cyber space' as 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'. Furthermore, Council, in the same session, stressed the importance of 'regional and global frameworks for promoting security and stability in the cyberspace'.

The AU has taken steps in developing framework to govern the cyber space at a continental level with the adoption of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), but such kind of tailor-made frameworks for regulating cyberspace at a global level are still missing. Yet, efforts are underway to clarify and develop a normative architecture for cyberspace. Such effort of developing normative architecture is happening within the UN with the establishment of two working groups with the mandate to study how international law applies to states' operations in cyberspace. The two groups are: UN Group of Governmental Experts (UN GGE) and an Open-Ended Working Group (OEWG). While the GGE is comprised of approximately 25 states, the OEWG is envisaged to be more inclusive, accepting participation of any interested state. Round of talks under

these separate and independent processes indeed reveal consensus on variety of norms of general behavior in cyberspace including the applicability of international law in cyberspace, but the issue of how international law applies in this space remains contested. Some countries are of the view that there is no need for new rules regulating cyber activities. Others favor agreed non-binding norms that complement existing international law, while others have questioned whether existing international law as it stands is capable of regulating states' cyber interactions hence call for the development of new rules.

There is also contention over the application of some of the core principles and rules of international law such as sovereignty, intervention, state responsibility, legal response options to malicious cyber activity, as well as the rules governing the use of force (*jus ad bellum*) and international humanitarian law (*jus in bello*) within the context of cyberspace. On sovereignty, one of the controversial issues remains the question of whether cyber operations affecting networks in another state's territory would amount to a violation of state's sovereignty. Regarding intervention, while there could be common understanding that the principle of non-intervention applies to state conduct in cyberspace within the context of the fulfillment of two conditions that the action constitutes coercive interference and falls into the *domaine réservé* of a state. Yet, there is no clarity on the threshold of the coercion element as well as which specific acts falls within the *domaine réservé* of a State. For instance, it is not clear whether cyber operations to manipulate electoral results of another state could constitute as a breach to the international obligation of non-intervention. Again, on the prohibition of use of force, there is unclarity on which specific cyber operations could constitute the use of force (armed attack) against another state and therefore trigger the right to self-defence. On due diligence, while states are under obligation not to allow

knowingly their territory to be used for acts contrary to the rights of other states under international law, there is a need for clarifying how far this obligation applies in the cyberspace. With respect to state responsibility, the main confusion concerns the technical aspect of the application of the attribution standard to cyberspace given the anonymity, interconnectedness, transboundary nature, and the use of proxies in cyberattacks. On legitimate response to cyber attacks, while there seems to be agreement among some states about the availability of at least three options (retorsion, countermeasures, and the plea of necessity), there is unclarity on whether collective countermeasures are permitted, whether there is a duty of prior notification of the response options, and whether states are allowed to take non-cyber-based countermeasures for cyberattacks. The other uncertainty is on the extent of the application of human rights and international humanitarian law (IHL) to cyberspace.

Despite the growing importance of the cyberspace to the life of individuals, communities and societies on the continent and the grave threat that cyber attacks pose to the peace and stability of Africa, the discourse on the making of the international law rules for governing peace and security in the cyberspace is dominated by the global north. In this respect, countries such as Germany, Canada, Sweden, Australia, Estonia, France, the Netherlands, the United Kingdom, and the United States have released their comprehensive positions on the application of international law in cyberspace. There should be similar efforts from the continent of Africa in developing and publishing its views and perspectives on how international law applies to cyberspace so that African voices are taken onboard in the ongoing effort towards developing rules of international law governing cyberspace in general and peace and security in cyberspace in particular. Tomorrow’s PSC engagement with the AUCIL therefore comes within this framework of developing African common position on the issue.

The expected outcome from tomorrow’s engagement is a communique. Among others, Council may express its concern over acts of violence in the cyber security, which constitute serious threats to national, regional, and international peace and security. While highlighting the need to harness the potentially of information and communication technologies for enhancing democratic governance and socio-economic advancement, Council may also reiterate its concern over their increasing use by state and non-state actors of cyberspace for malicious activities, including the spread of misinformation and disinformation, propagation of hate, cyber attacks on critical infrastructure, manipulation of elections, and incite violence. It may encourage all Member States, which have not yet done so, to expedite the signature and ratification of the Malabo Convention. The PSC may welcome the engagement with the AUCIL on the issue of international law and peace and security in the cyberspace. Cognizant of the role that Africa should play in the development of rules of international law in the area of cyberspace, Council may emphasize the importance of having Africa’s common position on the application of international law to cyberspace. In this respect, it may request the Commission, together with the AUCIL, to prepare the common position and submit for its consideration within a specified timeframe. While preparing the common position, Council may direct the Commission to engage Member States with the view to getting their respective national perspectives on the issue of the application of international law in cyberspace and their positions on contested issues.