Mitigating the threat of Cyber Security to Peace and Security in Africa

Automatic Heading TextDate | 19 May, 2019

Tomorrow (20 May), the African Union (AU) Peace and Security Council (PSC) is scheduled to hold a session on cyber security as one of the emerging threats to peace and security in Africa. The Committee of Intelligence and Security Services of Africa (CISSA) and the International Telecommunication Union (ITU) are expected to brief the Council. The Directorate of Information and Communication and the Department of Infrastructure and Energy of the African Union Commission (AUC) may also deliver statements.

The main objective of the session is to highlight the threats associated with the expanding use by government agencies, businesses, individuals and other sectors of society of information and communication technologies (ICT). The growth of ICT has enhanced interconnectedness, e-commerce, efficient delivery of services and information sharing. However, this development was also accompanied by the threat of cybercrime which has brought about a number of private and public security challenges. The increased use of ICT by state and non-state actors for undertaking a wide range of economic, social and private activities has heightened cyber risks and vulnerabilities. As a result, government agencies, businesses, individuals, financial institutions and critical facilities operating on the basis of ICT continue to be exposed to cyber crimes and attacks. These threats also pose great risk to national, regional and international peace and security.

Thus while acknowledging the critical importance of ICT, the session will also look into the challenges of how weak

networks and information security systems and lack of effective regulation and preparedness have exposed the countries of the continent to cyber security threats.

Although cyber crime is a global concern, African countries like many parts of the developing world, remain particularly vulnerable. Despite the growth of the ICT sector in Africa and increasing dependence of various sectors of African economies and increasing number of people, the readiness and possession of the required technology and know-how for addressing cyber security threats remains weak. There is no adequate awareness and appreciation of the scope and forms of vulnerabilities and the nature, manifestations and sophistication of cyber crimes. Additionally, many countries in Africa do not possess specific cyber legislation and this has made the countries vulnerable to cybercriminals.

Moreover, even already existing cyber laws are not strictly implemented and enforced and there is a general lack of awareness about cyber security measures which all have created the space for cyber crime in the continent. With limited resources most African countries would struggle to effectively tackle cyber crime.

Tomorrow’s session envisages to examine the state of the current legal regime for dealing with cyber security at the regional level and articulate mechanisms and actions through which the nature of this emerging threat is adequately identified and it can effectively be addressed. At the continental level the AU has adopted the African Convention on Cyber Security and Personal Data Protection in 2014 at the 23rd AU Summit. The Convention is a broad framework that offers clear guidelines and principles on the management of electronic transactions, on safety systems of personal data and measures to promote cyber security. However, the Convention has not yet entered into force. To date only thirteen countries have signed and four have ratified. As a way of enhancing the digital governance structure the session

may call for renewed commitments in ratifying and implementing the provision of the continental legal instrument. The Convention itself tasked the AUC Chairperson to establish a monitoring mechanism that encourages the implementation of cyber security measures, collects and shares information, offers advice to member states and regularly report to the decision making organs of the AU on the implementation of the Convention. The Council may also follow up on the steps taken by the AUC as per the responsibilities articulated in the Convention.

In 2018 the Executive Council endorsed the decision of the Specialized Technical Committee (STC) on Communication and ICT to establish an Africa Cyber Security Collaboration and Coordination committee. The committee which is also known as the AU Cyber Security Expert Group (AUCSEG) has the central role of advising and providing guidance to decision makers on cyber security policies and strategies. The AUCSEG is also expected to facilitate information sharing and cooperation among AU member states. The session may review if steps have been taken to the operationalization of AUCSEG and other related activities.

Despite the steps taken at the continental level, the level of readiness do not match the multifaceted threat of cybercrime. One of the characteristic features of the cyber space is that individuals and groups with expertise in ICT can use it for organizing, mobilizing, or perpetrating criminal acts ranging from identity theft to using malware for attacking businesses and government agencies. Apart from how the internet has been used by groups such as Al Shabaab and Boko Haram for recruiting and mobilizing funds, the cyber space has become a site for circulating false information and inciting division and violence. In this context, the 812th session of the PSC stressed ‘the need to counter the use of ICT technologies by terrorist groups, whether in their fundraising, narrative promotion, and recruitment of others to commit terrorist

acts’.

As part of the efforts towards mitigating cyber threats, the PSC may recall its previous 627th session which put forward concrete measures to respond to the challenge. It urged member states to develop national cyber security legislations and to create national and regional computer emergency response teams (CERT) and/or computer security incident response teams (CSIRT).It also supported the creation of a special unit within the Peace and Security Department (PSD), which will be exclusively dedicated to the efforts of prevention and mitigating cybercrime at continental level in close partnership with member states. PSC members may inquire on the progress of such initiatives.

The 749th meeting, held on 27 January 2018, at the level of Heads of State and Government, on the theme: “Towards a Comprehensive Approach to Combating the Transnational Threat of Terrorism in Africa” has similarly welcomed and recalled the need to organize an African Dialogue aiming at combating terrorism online and securing cyberspace. Given that cyber security concerns are broader than national boundaries it is necessary to put in place such kinds of robust and collective defensive cyber mechanisms. It is held that such a dialogue affords an opportunity for facilitating coordination among national and regional CERTs may also play a critical role in creating a continent wide security system. African Dialogue may also serve as a key tool to raise awareness on the threats associated with the use of ICT and on mitigation mechanisms. The PSC may thus wish to request an update on this initiative.

While it is clear from the foregoing that various AU bodies have been seized with the issue of cyber security and they proposed initiatives, their engagement and initiatives lack a common organizing strategy. Beyond and above reviewing the status of the various initiatives, it would be of interest to PSC members to review whether the different initiatives are complementary and the steps required for having a common

strategy that ties them all together towards a set of shared objectives leading to a cyber governance and security architecture, anchored on partnership with other regions and international organizations. Also of interest to member states is to identify how to leverage the role of Regional Economic Communities/Regional Mechanisms and AU's partnerships with the UN and the EU. Additionally, in the light of the legal measures adopted by the EU on data protection, the PSC may review the effectiveness of the personal data protection provisions of the 2014 AU Convention and the implications, if any, of the EU's General Data Protection Regulation (GDPR).

The expected outcome of the session is a press statement. Previous Executive Council, STC and PSC decisions have already laid out the relevant steps in setting up continental mechanisms and this particular session may provide more guidance on their operationalization and coordination. PSC may wish to offer guidance on ways to spearhead the accelerated ratification of the 2014 Convention on Cyber Security, and more particularly follow up on the work of AUCSEG and its harmonization with the specialized unit within PSD and other relevant AUC departments and organs. Given that cyber security systems require specialized expertise and resources as well as partnerships, the PSC may also put forward recommendations on ways to enhance the capacity of member states and the role of the AU in leveraging their efforts and its partnerships with African and international actors for collective action.