Cyber Security – Impact on Peace and Security in Africa

Cyber Security – Impact on Peace and Security in AfricaDate | 13 April 2023

Tomorrow (13 April), the African Union (AU) Peace and Security Council (PSC) is expected to convene its 1148th session to discuss the impacts of cyber threats to peace and security in Africa.

The session opens remarks by Abdelhamid Elgharbi, Permanent Representative of Tunisia and Chairperson of the PSC for the month of April followed by a statement of AU Commissioner for Political Affairs, Peace and Security (PAPS), Bankole Adeoye. The AU Mechanism for Police Cooperation (AFRIPOL); the Committee of Intelligence and Security Services of Africa (CISSA); the AU Department of Infrastructure and Energy; AU Office of the Legal Counsel and the United Nations (UN) International Telecommunication Union (ITU) are also expected to participate in the session.

It was at its 850th session that the PSC, recognising the growing relevance of cyberspace in Africa and the importance of ensuring the safety and security of this space, decided to commit an annual meeting on cyber security. Although this decision hasn't been regularly implemented, the PSC has dedicated various sessions to the theme, including the 1097th session which last addressed concerns related to cyber security in Africa. Among other critical points, the 1097th session drew attention to the need for enactment of necessary legislations and regulations at national, regional and continental levels to govern issues related to cyberspace. Tomorrow's session serves to follow up on efforts being deployed to mainstream cybersecurity in all peace and security

mechanisms of the AU, Regional Economic Community and Regional Mechanisms (RECs/RMs) and member states.

This session is coming against the background of the major cyberattack against the AU cyber infrastructure. Early in March, the AU was forced to suspend various operations following a massive cyberattack on its data centre, compromising various IT assets and user devices. This attack has led to not only the disruption of the ordinary functioning of the AU but also the loss of data. As a clear illustration of the susceptibility of African infrastructure to cyberattacks and the enormous costs that such attacks occasion, it would be of interest for members of the PSC to seek information on the source of the attack, the scale of damage caused and the measures required for rebuilding and instituting protective measures to address the vulnerabilities in the AU system that were exploited for orchestrating the attack.

There is also anecdotal data that the extent of threats to the cyberspace in Africa is increasing. This is mostly on account of the weak cyber security arrangements. According to the International Criminal Police Organization (INTERPOL)'s 2021 Africa Cyber Threat Assessment Report, over 90 percent of companies in Africa operate without the necessary cyber security protocols. Many African institutions and businesses have also come under cyberattack over recent years and continue to be susceptible to the perpetration of various cybercrimes.

The impacts of this are multifaceted. One of the many negative consequences of unprotected cyberspaces is that they result in considerable financial loss as well as data theft, including those related to intellectual property and protected business information. At a larger scale, such form of cyber threats manifest in the form of infrastructural sabotage affecting critical social and economic activities, including trade and commerce. Reports have indicated that in recent years, such

form of sabotages have particularly been escalating in the continent, specifically targeting national banks and maritime infrastructures. Ultimately, this will have an adverse impact on Africa's endeavours to advance economic development. As emphasised by the PSC at its 850th session, a secure cyberspace is a necessary precondition for 'reaping the dividends of the digital transformation of Africa and the world and for promoting economic development throughout the Continent'.

Another and perhaps more grave consequence of weak cyber security practices in government and non-governmental institutions in Africa is the fertile ground it creates for anti-peace activities ranging from espionage, to organised crimes and the use of digital space for incitement of violence. With little to no measures put in place to secure the cyberspace, anti-peace entities including terrorist organisations will have ease not only in accessing sensitive data and classified government information, but also in diverting finances to fund their activities, plan their attacks as well as recruit and train others to join their network. It also opens the space and creates the opportunity for the spread of misinformation and incitement of violence, particularly in settings characterised by polarised political tension and dissent. Terrorist groups' usage of cybercriminals to raise funds through cryptocurrencies and exploration of the dark web by human trafficking networks to lure in travellers through fake tour agency accounts are also among the cyber threats in Africa identified by AFRIPOL.

The imperative for a more robust cybersecurity in Africa will only continue to rise as the continent continues to expand its reliance and use of cyber operated technologies not only for socio-economic activities but also for security purposes as the expansion of the use of drones and unmanned aerial vehicles (UAVs) as well as other artificial intelligence (AI) for enhancing military operations shows. As far as the use of such technologies, particularly what are known as autonomous

weapons systems (which Africa is not in possession of), is concerned, Africa has the responsibility for promoting the development and strict enforcement of rules that ensure effective human control over and full responsibility of states for how such technologies are used as the surest means for averting not only breaches of human rights and international humanitarian law rules but also damages that may result from hacking of such technologies.

Africa's internet and telecom market which has experienced a major boost in recent years is only expected to grow significantly in the near future to accommodate the demands of the continent's massive population. While this creates great opportunities to advance Africa's socio-economic and developmental aspirations, it also expands further the nature and extent of cyber threats expected to be experienced. If relevant strategies are not put in place well in advance to avert, manage and effectively respond to these threats, the continent may be facing complex peace and security challenges. According to the 2021 Global Cybersecurity Index, only 29 African countries have introduced cyber security legislation while the remaining majority are yet to adopt relevant rules and regulations to deal with this specific area of concern. This indicates the need for heightened awareness among member states of developments in Africa's cyberspace and their commitment to take solid steps towards securing it, including through the adoption of relevant normative standards to regulate the safe and secure utilisation of cyberspace.

At the continental level, the AU has already adopted key legal instruments and frameworks relevant to the regulation of cyberspace and for ensuring cyber security in Africa, including the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention); the 2020-2030 Digital Transformation Strategy for Africa; the AU Data Policy Framework and the AU Interoperability Framework for Digital ID. In line with the decision of the Executive Council's 32nd

Ordinary Session [EX.CL/Dec.987(XXXII)], the AU has also established the Cyber Security Expert Group (AUCSEG) which is charged with providing advice to the AU Commission on matters related to cyber security. Few member states such as Botswana, Ghana, Lesotho and South Africa have also made commendable strides towards securing the cyberspace through the adoption of Cybercrimes and Cybersecurity Acts. Despite these encouraging developments, the current efforts to respond to cyber threats are largely disproportional to the magnitude of the challenge in Africa.

The expected outcome of tomorrow's session is a Communiqué. The PSC is expected to express grave concern over the recent cyberattack the AU experienced and commend AFRIPOL and other relevant AU organs for committing the necessary efforts to resolve the issue. It may emphasise that with growing digitalisation and socio-economic development come increasing cyber threats and as such, call on member states to mainstream cyber security throughout all of their digital endeavours. The PSC may take note of the increasing significance of the digital space for trade and commerce in Africa and call on all relevant stakeholders including member states and the private sector to protect transactions by investing on cyber security measures. It may stress the importance of establishing the normative framework for cyber security and urge member states to adopt the necessary legislation to regulate cyberspace in a manner compatible with human rights norms guaranteeing fundamental rights and freedoms. It may urge member states to ensure responsible use of emerging technologies in efforts aimed at enhancing military capabilities and to put in place the necessary cyber security measures to avert hacking and diversion of such technologies. It may also highlight the need to ensure implementation of existing continental legal frameworks for the protection of cyberspace including the Malabo Convention. It may further encourage RECs/RMs to contribute to cyber security efforts through enactment of relevant strategies for enhancing regional collaboration in

taking action against cyber threats. The PSC may call on the AU Commission, AFRIPOL, CISSA working with relevant expert bodies to develop guidance for member states, RECs/RMs and AU institutions on identifying vulnerabilities for cyberattacks and instituting effective cybersecurity measures to avoid the kind of attacks the AU experienced recently.