

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

**WORKSHOP ON CYBER-SECURITY ORGANIZED BY THE
COMMITTEE OF INTELLIGENCE AND SECURITY SERVICES OF AFRICA**

**7-11 NOVEMBER 2015
KHARTOUM, SUDAN**

**STATEMENT BY MR. EL-GHASSIM WANE
DIRECTOR OF THE PEACE AND SECURITY DEPARTMENT OF THE
COMMISSION OF THE AFRICAN UNION**

STATEMENT

Honorable Minister of Information of the Republic of Sudan, Mr. Ahmed Bilal,

Lieutenant-General Engineer Mohamed Atta Al-Muwla Abbas, Director-General of the National Intelligence and Security Services of Sudan,

Mr. Shimeles Semayat, Executive Secretary of the Committee of Intelligence and Security Services of Africa,

Representatives of member services of CISSA,

Representatives of the media,

Ladies and Gentlemen,

It is a great pleasure for me to be here in Khartoum and to make opening remarks on the critical issue of cyber-security. I wish to thank the Sudanese authorities and people for their legendary hospitality and the warm welcome extended to the delegation of the Commission of the African Union. I also wish to thank the Committee of Intelligence and Security Services of Africa for convening this important event.

The collaboration between the Commission of the African Union and the Committee of Intelligence and Security Services of Africa has grown stronger over the past few years. We work together on a range of issues of common concern and in various frameworks, including the Nouakchott and Djibouti Processes for the enhancement of security cooperation in the Sahel region and in East Africa, respectively.

I would like to convey to you the warm greetings of the Chairperson of the Commission of the African Union, Dr. Nkosazana Dlamini-Zuma, and of the Commissioner for Peace and Security, Ambassador Smail Chergui. They wish you successful deliberations and look forward to the recommendations of this workshop, as we strive to promote lasting peace, security and stability on the continent.

Ladies and Gentlemen,

The relevance and timeliness of this workshop cannot be overemphasized. The Internet or, more broadly, the cyberspace has had great impact on all parts of our societies over the last decade or so. It has significantly transformed modern societies and has become an indispensable and empowering tool, affecting all areas of human life and interaction, including education, socio-economic development and broader social change. Cyberspace has allowed

entrepreneurs and activists to realize significant change that they could not have otherwise achieved in the prevailing political, economic and social environment.

However, like any technology, the cyberspace has been abused and exploited to facilitate all sorts of destructive and criminal activities.

There is a wide range of criminal activities that are carried out in the cyberspace. These include financial crimes such as bank fraud and identity theft, terrorism, trade in illicit goods, as well as human trafficking and child exploitation. The cyberspace has also been exploited to commit acts of a racist and xenophobic nature.

Thus the issue of cybercrime is critical to any discourse on the cyberspace and how to maximize its benefits.

Ladies and Gentlemen,

Africa is home to some of the world's most rapidly growing economies. The Internet and mobile technology has been an important tool in this growth. According to the International Telecommunications Union, more than 16% of the African population is now using the Internet. Globally, business to consumer e-commerce sales is worth over a trillion dollars, and although it is dominated by developed economies, the share of the Middle East and Africa is expected to rise from 1.6 per cent to 2.3 per cent by 2016. This percentage is clearly very low, but the trends indicate that there is a huge potential for growth on the Continent that can work in different ways, both positive and negative.

Indeed, this increased technological exposure is not without risks and challenges, particularly when network and information security is very weak, as is the case on our Continent. Symantec Corporation, a leading US-based technology company, reports that cybercrime is increasing at a more rapid rate in Africa than in any other area of the world. Globally, the number of targeted cyber-attacks has increased by 42% in recent years. 31% percent of these attacks, categorized as cyber-espionage, have hit both large and small businesses. The financial loss in Africa in recent years due to cyber-crime and cyber-fraud is in the hundreds of millions of dollars.

Transnational criminal and terrorist groups have exploited the Internet for various ends, including planning and communication, financing, recruitment and inciting violence, propaganda and publicity, threatening States and instilling fear among the general public. The recording and online dissemination of the acts of executions and beheadings are among the most egregious illustrations of the abuse of the Internet by terrorist groups.

Of equal concern is the use of the Internet as a tool for terrorist recruitment. Research shows that vulnerable youth, including in the Diaspora, were recruited to join terrorist groups, such as al-Shabaab in Somalia, through the Internet, where such groups post elaborate messages that appeal to disenfranchised youth. In addition to recruitment, radicalization and incitement to

terrorism through the Internet have also contributed to the commission of terrorist acts by un-affiliated individuals.

Another issue of great concern relates to terrorist training through the Internet and the online dissemination of the know-how in guerilla fighting methods and the making of Improvised Explosive Devices (IEDs), as well as other forms of weapons such as radiological dispersal devices. This allows terrorist groups and operatives, regardless of their capabilities, to develop expertise to further wreak havoc and destruction. In fact, some terrorist groups publish on-line magazines on a regular basis, such as *Inspire*, allegedly published by Al-Qaida in the Arabian Peninsula (AQAP), with the stated objective of enabling Muslims to train for Jihad at home.

As indicated above, the development of Internet can work in different ways. While terrorists can take advantage of the Internet in the pursuit of their criminal activities, this tool can also and should be effectively used to counter terrorism in a number of ways, including the generation of knowledge and collection of information about the functioning, activities and sometimes the targets of terrorist organizations from websites, chat rooms and other Internet communications. As such, the increased Internet use for terrorist purposes provides a corresponding increase in the availability of electronic data, which may be compiled and analyzed for counter-terrorism purposes.

Another way through which the Internet can serve as a counter-terrorism tool is the on-line dissemination by Governments and civil society of sensitization and education materials that aim to provide a counter-narrative to extremist ideology and to delegitimize violence and terrorism as a means to effect political change.

The Internet has not been exploited for financial gain and terrorism only. There are other issues that require the urgent attention of the African Union and member States. More and more African children and adolescents are now exposed to online threats and vulnerabilities, endangering their safety. While research and data on the online child abuse material is limited, incidents of recruitment into prostitution rings, child-pornography, trafficking and other forms of exploitation by domestic and international elements have however been reported in several African countries. Regrettably, in many of our member States, laws and enforcement capacities have not been developed to prevent and prosecute such crimes.

It is important to indicate that sometimes States themselves, both developed and developing, have been involved in the abuse of the cyberspace. Some have used it to hack into other States' data systems, while others have been accused of resorting to it to restrict fundamental freedoms of their citizens and of opposition elements.

Ladies and Gentlemen,

Various challenges face member States in dealing with cybercrime. The borderless nature of this problem further exposes member States to new forms of on-line criminality that they are poorly equipped, both technically and financially, to detect, to investigate and to respond to.

Generally, there is limited awareness of the technological and informational threats and risks, which contributes to the low level of security measures implemented by the public and private sector alike to address them. At the individual level, many users rely on pirated software and operating systems that expose them to countless virus and malware risks that could facilitate identity theft and credit card fraud.

Legislation to respond to cyber-crime is also poorly developed and implemented. Various forms of cyber-crime still don't have corresponding laws. This in addition to the limited capacities of law enforcement agencies and the criminal justice as a whole in investigating and prosecuting cybercrime. It is important to point out that cyber-crime and other crimes facilitated by information and communication technology require substantive technological know-how and resources, as well as international cooperation due to the multiple jurisdictions that are usually involved in dealing with such crimes.

Poor coordination and harmonization of policies among the various stakeholders undercut efforts to prevent and respond to cyber-crime. Cyber-security requires a whole-of-government, action-oriented, well-coordinated and well-resourced approach. Such an approach must include the relevant agencies responsible for information and telecommunication, law enforcement, social affairs, the financial sector, and the private sector.

Ladies and Gentlemen,

As we gather here, we should acknowledge the progress that has been made in addressing cyber-crime within the framework of the rule of law. Various regional instruments have been developed, including by the East African Community, the Economic Community of West African States, the Common Market for Eastern and Southern Africa and the Southern African Development Community.

More recently, the African Union June 2014 Malabo Summit adopted a Convention on Cyber Security and Personal Data Protection. The Convention addresses a wide range of online activities, including electronic commerce, data protection, cyber-security and cybercrime. Regarding cybercrime, it requires African States to adopt laws that criminalize attacks on computer systems and computerized data breaches. The Convention also addresses offences such as the dissemination of child pornography.

Furthermore, the Convention emphasizes the need to enhance international cooperation and requires States to harmonize cybercrime legislation and regulations. It recognizes the critical importance of capacity building in the fight against cybercrime. In this respect, the Convention requires State parties to establish appropriate institutions to combat cybercrime and to offer training to the relevant national agencies.

Let me however stress that, prior to the adoption of the Convention, the African Union had taken steps to address the threat posed by cyber-crime and the exploitation of the Internet by terrorists. These steps are part of the overall African Union counter-terrorism framework, which addresses different manifestations of the problem of terrorism, including on-line recruitment, radicalization, planning and execution of terrorist acts, as well as financing.

I wish to mention that, in July 2011, the African Union Summit adopted a Model Law on Counter-Terrorism to assist member States adjust and strengthen their national legislations, with a view to meeting their obligations under the relevant African and international instruments. The Model Law contains guiding provisions to enable law enforcement agencies obtain electronic evidence from Internet and telecommunications service providers and to intercept or conduct surveillance using the due legal process.

I would like to underline that from the perspective of the African Union Commission cyber security is also an issue to be addressed in relation to the AU headquarters and our various field missions.

Ladies and Gentlemen,

In concluding, I would like to emphasize that cyber-security is an issue that requires effective and action-oriented measures that are implemented through a coordinated, comprehensive and cooperative manner at the national and regional levels. Despite the challenges at hand, the African Union believes that there are opportunities that we must capitalize on. This meeting is an important first step towards addressing this issue collaboratively among the members of the African security and intelligence community.

In so doing, we should be mindful of the fact that cyber-security measures may have an impact on the enjoyment of a range of human rights, including the rights to freedom of speech, freedom of association, privacy and a fair trial. For the African Union, effective cyber-security measures and the protection of human rights should be complementary and mutually reinforcing objectives, which must be pursued together. Thus, responses and strategies to the threat posed by unlawful and criminal use of the Internet must meet the highest standards in terms of respect for human rights and the rule of law, including the African Charter on Human and Peoples' Rights and the African Charter on Democracy, Elections and Governance.

The African Union Commission commends the Committee of Intelligence and Security Services of Africa and the National Intelligence and Security Services of Sudan for this timely workshop. We look forward to the outcome of this workshop and to working with CISSA in the follow up phase.

I wish you fruitful deliberations and thank you for your kind attention.