

**Your Excellency the President of the Republic of Cote d'Ivoire**  
**Honourable Minister of Post and Telecommunications in Liberia**  
**Honourable Minister of ICT in Cote d'Ivoire**  
**Honourable President of the Organizational Committee**

**Distinguished Delegates**  
**Ladies and Gentlemen**

I would like to thank the Government and the people of the Republic of Cote d'Ivoire for hosting this very important conference and for their hospitality.

**Your Excellencies**  
**Ladies and Gentlemen**

The global community adopted eight Millennium Development Goals to guide and measure the development efforts globally. Apparently those goals applied and needed mostly in our beloved continent Africa and our ability to achieve those goals, is driven by not only the urgency of the concerns, but also the realization that we have within our reach the know-how and the tools to make the goals reality. One such set of tools is Information and Communication Technologies and its cyberspace. ICTs have transformed our world, and in the process, our belief in how we can address its challenges.

ICT crosses all sectors, bringing increased efficiency and new opportunities to areas from small enterprise development and international trade, to education and healthcare and even entertainment. It has also allows us to share experiences across borderless world so that we learn collectively and build on each others' advances. In the African Union Commission we have an ICT component in almost every programme and plan, ARAPKE is entirely for ICT, African S&T CPA, the 2<sup>nd</sup> Decade of Education and the African Youth Charter all has a very important component on ICT.

**Your Excellencies**  
**Ladies and Gentlemen**

In 1995 the Internet was in its infancy, email was the killer application and the World Wide Web looked like it had potential. Now the Internet touches our lives in many ways, some of which are less desirable than others. The Internet was never intended to introduce new forms of crime or to make illegal material more readily available, but this is a reality that we must all accept.

An exploited vulnerability could range from the annoying to the catastrophic. Botnets, spam, phishing, malware, spyware, viruses and other attacks make up more-than-\$100 billion global market for cyber-crime. The threats are real. Hackers are becoming more sophisticated and focused in their efforts.

Cybercriminals are exploiting vulnerabilities and loopholes in national and regional legislation as they shift their operations to countries where appropriate and enforceable laws are not yet in place, and can, with almost total impunity, even launch attacks on victims in countries which do have laws in place.

We are now more and more vulnerable than ever. In fact, while a cyber attack definitely would not, be considered a weapon of mass destruction, still it can be thought of as a weapon of mass disruption. One person with relatively little training, inexpensive equipment, and access to the Internet has the potential to disable an entire ICT network or infrastructure. The financial and other related costs to such attacks are enormous.

**Your Excellencies  
Ladies and Gentlemen**

We in Africa should identify priority areas at all levels be it national, regional or continual to secure the cyberspace. Those areas should include; cybersecurity laws, legislations and response system; cyberspace threat and vulnerability reduction program; cybersecurity awareness and training program and International cybersecurity cooperation plan.

International cooperation in particular is very essential because there are no boundaries in cyberspace. The vulnerabilities of the Information Age transcend national borders. Our information and communications infrastructures are converging into a seamless global network. This means that, as we transmit proprietary business data, sensitive personal information, and protected intellectual property back and forth between our countries, it is critical that we work together to coordinate and implement cyber security strategies and policies.

**Your Excellencies  
Ladies and Gentlemen**

Governments can not do much by their own, the required solution should be inclusive and involve all stakeholders, because so many of our information systems and networks either owned or operated by the private sector. Accordingly, the basis of our cybersecurity is an effective partnership with private sector and also the academia.

While governments can create the appropriate environment for commercial activity, still the private sector and academia are in best position to identify threats and vulnerabilities, articulate the need for security and protection of assets, and share ideas and best practices for the development of cybersecurity technologies, policies, and programs jointly with the governments. The private sector has an important role in translating government initiatives into concrete joint activity at the business-to-business and people-to-people levels as proposed also by the ITU Global Cybersecurity Agenda for the implementation of Tunis commitment and Tunis Agenda emerged from the second phase of WSIS.

**Your Excellencies**

## **Ladies and Gentlemen**

Many countries have adopted or are working on legislation to combat cybercrime and other misuses of ICTs. These laws are drawn up to be enforceable in well defined geographical boundaries that are either national or regional. But these legal frameworks are not really inter-operable and have its limitations because of the complexities in managing numerous bilateral agreements, and the undesirable effects of trust cascades.

Governments are grappling at the international level to iron out cybersecurity arrangements. Negotiating in intergovernmental organizations and stakeholders are crafting rules to cover a span of strategic issues for the networked world, including cybercrime, taxation, travel, money transfers, and also the environment. One important sample of such International Instruments is the Convention on Cybercrime – an initiative by the Council of Europe.

## **Your Excellencies**

### **Ladies and Gentlemen**

As the Internet has become integral to the basic functioning of all sectors and societies, so has cybersecurity become central to general security. However, the players involved in ensuring a secure cyberspace may have different interests: One government's preferred order is anathema to another, and a business must strive to profit its own shareholders rather than the public at large.

In this early stage of design, there is a window of opportunity for the Africans to affect the global assumptions upon which the cybersecurity framework is based.

## **Your Excellencies**

### **Ladies and Gentlemen**

Cyberspace reflects the beauty and genius of the open societies that created the online world and allowed it to flourish. Our task to secure this has no simple solution and unforeseeable end.

Protecting cyberspace without changing its spirit of openness will challenge us all. We have to balance the temptation to sacrifice the best of cyberspace in the name of precaution and security.

I thank you and wish you a fruitful deliberation