SPEAKING NOTES AT THE OPENING SESSION OF THE Octopus Conference on Cooperation Against Cybercrime

Strasbourg, France, 6th June, 2012

The Botswana Experience with cybercrime legislation and other measures

By Dr Athaliah L. Molokomme, Attorney General

Distinguished guests, ladies and gentlemen

Let me begin by thanking our hosts, the Council of Europe in particular, Alexander Seger, his Cybercrime Convention Committee and Data Protection and Cybercrime Division for their unwavering commitment to fighting the scourge of cybercrime through international cooperation.

For it is only through working together at regional and international levels that we can succeed in our endeavours, in view of the unique challenges presented by cybercrime. Thank you also for the excellent communication, arrangements and facilities that have been put at our disposal, that I am sure will allow us to participate effectively in this conference.

It is also a pleasure to add my own voice at this opening session to the concerns that we all share about cybercrime, as well as share the response of my country, Botswana, to this challenge. Most importantly, we hope to learn from the experiences of other countries, and find out how we can best contribute to the international response in this regard.

For those of you who do not know Botswana, it is a country that is located in the middle of Southern Africa, sharing borders with its better known neighbours South Africa, Zimbabwe, Zambia and Namibia. This location presents both opportunities and challenges, and we have always endeavoured to embrace the opportunities and tackle the challenges as best we can. Botswana has witnessed a dramatic development path since independence in 1966.

Allow me to share a few general statistics with you by way of example.

- In 1966, adult literacy was estimated at 10%, rose steadily to 34% in 1981, 72% in the year 2000 and currently stands at 87%;

- Primary school enrolment stood at less than 25% at independence. By 1991 it had shot up to 90%;

- Secondary school enrolment, which was less than 10% in 1966, went up to 70% for junior secondary and 60% for senior secondary respectively by 2001;

- In 1966, there were three secondary schools and now we have more than 300;

- The 8 kms of tarred road we inherited at independence have now been multiplied ten thousand times, and we now have 18,000 kms of tarred roads criss-crossing our vast country;

- From a couple of basic mission hospitals in 1966, today 90% of our people are within 15km of a modern health facility;

- On the economic side, Botswana's per capita income rose from U$80 to U$3,000 per anum during the first three decades since independence;

- At the time of independence, Botswana's total revenues were P10 million. In 1990, they were P1 billion; just 15 years later they were P15 billion. An extraordinary increase of P1 billion per annum over the past 15 years.

This is attributable to a number of factors, especially the visionary role of our traditional and modern leaders in guiding our nation to see itself as a single, united entity and its people as having a common destiny. Our traditional *kgotla* system of consultation and delegated responsibility provided a conducive environment for the introduction and development of a modern democracy.

Botswana is a constitutional state based on the rule of law and the principle of separation of powers. Accountability certainty and transparency in decision making are the basic tenets on which our government operates. Under this dispensation, we have had no less than nine free and fair elections and witnessed three peaceful transfers of presidential power.

It is against this background that our concern about rising crime generally, and the new threat posed by cybercrime should be understood. The investments that we have made would have been in vain, and our development gains could be reversed within a very short period of time by the actions of a handful of criminals who abuse the benefits offered by cyberspace for their own selfish ends.

This is why in 2006, the Botswana Cabinet approved the drafting of a Cybercrime Bill for Botswana, which became law the following year in 2007. I should note, however, that a lot of skepticism existed at the time, about the importance and relevance of drafting such a law in the context of a developing country such as ours.

This was especially because at that time, a significant portion of the population did not have access to the internet and basic IT services. Cybercrime legislation was considered to be even less relevant, particularly to those living in rural areas, where rudimentary amenities existed and even the basic infrastructure which was needed to support such services were not in existence.

Furthermore, it was felt by many that we had other more pressing challenges that needed our attention, resources and time, more than issues which did not seem to affect the day-to-day lives of ordinary citizens, such as cybercrime.

Be that as it may, the Botswana Government recognized that it was important to make legislative provision earlier rather than later when cybercrime could have become a bigger problem. We also recognized that without such legislation, Botswana could be viewed by national and international criminal elements as a "soft target". We therefore decided to address the growing international problem of cybercrime, and Botswana's Cybercrime and Computer Related Crimes Act was passed by Parliament in 2007.

This was a result of the realization that with the advent of emerging, sophisticated technology, there would invariably be those who would be only too willing to exploit such modern advances to further their own criminal pursuits.

In drafting the Bill, desktop research was carried out with other commonwealth countries, and the following Acts were examined: Mauritius' Computer Misuse and Cybercrime Act, South Africa's Electronic Communications and Transactions Act and India's Information Technology Act, amongst others.

In addition, and closer to the subject of this conference, we looked at the Council of Europe's Convention on Cybercrime, as well as the Commonwealth Model Law on Cybercrime and Computer Related Crimes. These were very helpful to us, as they set standards against which we could compare the provisions of our Bill.

It main objectives is to combat cybercrime and computer related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence. We would be happy to share some of the provisions of the Act during the more interactive sessions of the workshops, rather than go into the details during this opening session. For now, I wish to conclude my presentation by sharing some of the lessons we have learnt in the short period of the implementation of the legislation.

It will be obvious that the enactment of the Cybercrime and Computer Related Crimes Act did not instantaneously solve the problem of cybercrime for us in Botswana: The real test arises when it comes to the implementation of such legislation.

Like many of you, we are a small and developing country, hence we have certain common challenges that we all inevitably face. The most serious challenge is the lack of resources and the limited capacity available to train our police officers to investigate such crimes. We also do not have sophisticated technology at our disposal, nor the requisite manpower and expertise to adequately deal with such criminal activities. Our police already have their hands full with the investigation of so-called "traditional" crimes.

At present, we have a very small Police IT Unit, however, we still face the challenges mentioned above due to the lack of training and manpower. I noted from the outcomes of Octopus 2011 that one of the workshops was on capacity building and proposed in its conclusion that, "it is important to address all elements (LEA, Prosecution judiciary, policy makers and the private sector) of combating Cybercrime thereby avoiding "weak links". I agree fully as this is an area of great concern for us. The Police Service, Directorate on Corruption and Economic Crime, Directorate of Public Prosecutions and the Administration of Justice need training on this very critical aspect if we are to avoid "weak links".

We have realized that a piece meal and narrow approach to this issue will not effectively address the problem at hand. As a result we are in the process of seeking assistance from our LEA Prosecutors.

It is hoped that in future, with international support from other jurisdictions and international organisations, a well trained and dedicated unit can be set up within our Police service to investigate such crimes. In relation to cyber fraud and corruption we hope to empower the Directorate on Corruption and Economic Crime to be able to effectively investigate, follow up proceeds and present comprehensive dockets to the Directorate of Public Prosecutions for prosecution. In this regard we would greatly benefit from technical Assistance.

As a country we have taken a resolution to update and bring our law in line with the world's best practices. In that regard, we realized the need for a law relating to admissibility of electronic evidence in our court and currently my department is working on the draft bill which will complete the Criminal Procedure and Evidence Act.

We are in the process of reviewing the Cybercrime and Computer Related Crimes Act, Intellectual Property Act, Telecommunications Law and we would greatly appreciate technical assistance in this area.

In line with this resolve my department has also been instructed to draft new legislation covering the following areas, Data Protection, E-Commerce,

Privacy, and Electronic signatures Act. This assignment is a rather tall order, and we are seeking technical expertise to complement of limited drafting resources. We hope to find partners to assist us to review and update our legislation. This process will help to ensure that Botswana is not a "weak link" or safe haven for cyber criminals.

We have however investigated, prosecuted and secured convictions in five criminal prosecutions for violations of the Act and fines as well as a period of imprisonment have been imposed. This however has been for minor offences. We currently have 10 cases pending in our courts.

Ladies and gentlemen, let me conclude by saying that it is my hope that the proceedings of this conference will produce the outcomes we desire, that is, agreement in principle on a cooperation framework for tackling cybercrime at the international level.

For our part, we look forward to the rich deliberations we know are going to take place, and learning from the experiences of others. We stand ready within our modest resources, to play our part in taking the process further. We welcome the proposal in the background paper that an expert working group be set up to work on ways of cooperation between us in this important area.

I thank you.