

STATEMENT BY THE REPRESENTATIVE OF SOUTH AFRICA ON THE PROBLEM OF CYBERCRIME, 18 JANUARY 2011

Mr Chairman,

We would like to take this opportunity to congratulate you on your appointment as the Chair of this Committee. We also wish to thank the UNODC for the preparations of the documents for this meeting. Our delegation is pleased that this issue is addressed in this fora and wish to assure you of South Africa's full support on the task in dealing with the topics under discussion.

It is not a secret that Information Technology has changed the lives of people in many different ways. It has served humankind in more ways than one and has presented numerous opportunities for better information sharing. We need IT to communicate and empower the societies and to share information. There are however, increasing challenges that come with the advancement of information technology. These challenges include amongst others, abuse of vulnerable groups, sexual exploitation, phishing, hacking, spamming, etc. These crimes have no boundaries, they cross borders - hence the need to have international control measures and cooperation among States in order to prevent and combat these challenges.

Closer collaboration and cooperation amongst various countries must be encouraged. Exchange of useful information on the specific forms of cybercrime, sharing of best practices as well as technical assistance in the implementation thereof amongst Member States can assist in the prevention and combating of these crimes.

South Africa, like all other countries, is not spared from the onslaught of cybercrime. The combating of cybercrime is one of the strategic objectives of our Government. Although cybercrime in South Africa is mostly bank related, it provides a medium to conduct an array of crimes, which include the unlawful access to information, laundering of funds and exchanging, publishing and trade in illegal material. Various methods are used to commit cybercrime including key loggers and internet related fraud bank account information and passwords are sometimes acquired by means of key loggers on computers and ATM devices to commit fraud.

According to the South African Police Service Annual Report of 2009/10, 2533 new cases relating to internet fraud were reported to the police in comparison to 1426 cases reported in the previous financial year.

South Africa has specific legislation to address cybercrime, namely the Electronic Communications and Transactions Act No 25 of 2002 which came into operation on 30 August 2002. The Act contains specific provisions pertaining to unauthorised access to, interception of or interference with data and also provides for computer related extortion, fraud and forgery. In addition to this legislation, South Africa has legislation such as the Films and Publications Act No 65 of 1996 to address internet service providers that know that their services are being used for the hosting or distribution of child pornography and fail to take reasonable steps to prevent access to child pornography or to report it to the police.

In addition to the above, South Africa has enacted the Regulation of Interception of Communications and Provision of Communication-related Information Act No 70 of 2002 to provide for the interception of direct communications as well as indirect communications such as data, text or visual images. This Act also acknowledges assistance to competent authorities outside of South Africa in accordance with international cooperation practice.

To address cybercrime and cybersecurity threats, South Africa published a draft cybersecurity policy on 19 February 2010 aimed at creating institutional capacity to respond to this challenge. This draft policy is currently under discussion in Government and inputs are being made to it. It is envisaged that this policy will promote the development of measures to anticipate and confront emerging cyberthreats, coordinate South Africa's responses, build partnerships amongst stakeholders both locally and internationally, monitor cyber incidents, develop a culture of awareness of cyberthreats and develop requisite skills as well as research and development capacity.

Although South Africa has developed a number of national Acts on this issue, a challenge is a lack coordination in the various Departments administer various Acts that can be used to combat cybercrime. There is therefore a need for coordination and harmonisation of legislation. Further challenges experienced relate to the capacity to investigate cybercrime

and to analyse the forensic evidence generated by cybercrime. As a result the investigators sometimes have to wait for a long period before an analysis is finalised. Capacity building is therefore of utmost importance in this area.

The newly established Directorate for Priority Crime Investigation of the South African Police Service has created a dedicated and skilled capacity to investigate incidents of cybercrime. This Division is already interacting with relevant Departments and the private sector to ensure the effective cooperation in this regard.

On the issue of the scope of the study, South Africa would wish to make the following comments and observations:

1. The definition of cybercrime: There must be a universal definition on cybercrime. Is cybercrime a category of offences or is it broader i.e. where a computer is used to only store information?
2. The role of internet service providers: they have a responsibility as the host in combating and preventing of cybercrime.
3. Response by private sector is very important but how are we ensuring that all inputs are obtained in the process? Do we only involve government partners or do we speak to other stakeholders too?

South Africa remains committed to assist from its side to ensure enhanced national, regional and international action against cybercrime. Our delegation acknowledges the participation of and the important role the private sector and civil society play in combating this phenomenon. In this regard, South Africa welcomes the participation of the private sector, international organizations and NGOs in this meeting.

Thank you Mr Chair.