**South Africa's views on scope, objectives and structure (elements) of the envisaged International Convention on Countering the use of Information and Communications Technologies for Criminal Purposes**

The Government of the Republic of South Africa welcomes the invitation to submit views on the scope, objectives and structure (elements) of the envisaged International Convention on the Use of Information and Communications Technologies (ICTs) for Criminal Purposes in accordance with the United Nations General Assembly Resolutions A/RES/74/247 and A/RES/75/282, taking into full consideration existing international instruments at the national, regional and international levels in particular the work and outcome of the open-ended working group on Cybercrime (IEG), amongst others.

South Africa reiterates its commitment to this inclusive process of elaborating an international Convention on the use of ICTs for criminal purposes.

## 1. Objectives

The international system in its current form is not equipped to deal with the growing scourge of cybercrime, thus necessitating that the world unites in formulating a true international instrument that will protect the victims of crimes committed in cyberspace and guarantee maximum protection and legal remedies. South Africa moves from the premise that the UNTOC is not sufficient in addressing cybercrime despite dealing with "new and emerging forms of crime". Similarly, regional instruments such as the Budapest Convention and the AU Convention on Cyber Security and Personal Data have their merits and can be used to elaborate an effective international instrument at the level of the United Nations for equal access and ownership by all Member States.

South Africa submits that the main objectives of the envisaged international convention should be to:

a) Pursue a common criminal policy aimed at the protection of society against cybercrime;
b) Gap-fill national criminal laws that do not comprehensively deal with cybercrime or that do not contemplate the kind of cross-border cooperation required in combating cybercrime;
c) enhance international cooperation against cybercrime;

d) create enforceable mutual legal assistance (MLA) provisions to facilitate and expedite sharing and assistance in cybercrime matters; and
e) have capacity building at its centre.

**2. Scope**

It is submitted that the scope of the Convention should include, among others:

a) **Substantive criminal offences** - The Convention is to include offences to be criminalised and measures to be taken at a national level. The focus should be on criminalising the misuse of ICTs for criminal purposes rather than the technology itself. Criminal offences must be clearly defined and narrowed to avoid legal uncertainty caused by vague provisions resulting in gross violation of human rights and fundamental freedoms.

b) **Procedural Aspects -** The Convention must describe procedural measures to be taken at the national and international levels for the purpose of criminal investigation of the offences committed by means of a computer system and the collection of electronic evidence for litigation purposes, i.e. "expedited preservation of stored computer data" with a view to enabling national competent authorities to order or obtain the expedited preservation of specified stored computer-data in connection with a specific criminal investigation or proceedings. The Convention should describe action to be taken and procedures to be followed for electronic evidence admissibility in a cybercrime investigation.

c) **Enhanced international cooperation** should be a priority in the Convention when considering the extent of cybercrime and its impact on economic development (severe in developing countries). It is the duty of all States to ensure that criminals do not have anywhere to hide hence the general scope of the obligation for States to cooperate needs to be dealt with in **the Convention**. The Convention must clearly indicate that international cooperation is to be provided among all parties **"to the widest extent possible"** to repatriate assets, extradite those who are evading justice and to ensure that citizens of the world benefit from crime free cyberspace. To this end, the establishment of 24/7 points of contacts could be beneficial.

d) **Capacity building and technical assistance** should be prioritised in **the Convention** and should be based on the receiving State's objectives and request. Law enforcement agencies in some countries often do not have sufficient capacity to investigate complex cybercrime cases and should be assisted to build adequate capacity.

e) **Jurisdiction:** The Convention must establish a criteria under which parties are obliged to establish jurisdiction over the criminal offences based upon the principles of territoriality and sovereignty.

f) **Roles and responsibilities** of service providers and the private sector: The Convention should clearly define the respective roles and responsibilities of service providers, especially ISPs in the investigation and combating of cybercrime. There should also be enhanced public-private partnerships in the prevention of cybercrime as a significant proportion of the internet infrastructure is owned and operated by the private sector.

## 3. Structure (Elements)

South Africa proposes the following structure (elements) for the Convention:

1. Foreword – sets out the path to the instrument separate from the preamble;
2. Preamble - outlines the objectives and basic principles underpinning the Convention such as respect of human rights and fundamental freedoms);
3. Definition of terms and concepts;
4. Fundamental Principles underpinning the Convention;
5. Substantive Criminal Offences – clearly defined to avoid ambiguity;
6. Procedural Rules;
7. International Cooperation;
8. Capacity building and Technical Assistance;
9. Implementation Mechanism;
10. Enforcement mechanism