

**THIRD INTERSESSIONAL CONSULTATION OF THE AD  
HOC COMMITTEE TO ELABORATE A COMPREHENSIVE  
INTERNATIONAL CONVENTION ON COUNTERING  
THE USE OF INFORMATION AND COMMUNICATIONS  
TECHNOLOGIES FOR CRIMINAL PURPOSES**

**Vienna, Austria.**

**Global Vision India Foundation  
Mumbai, India**

Presentation made by

**Dr. Ashok Yende**

**November, 3 - 4 , 2022**

# **CYBER CRIME – GLOBAL CHALLENGE**

- **Cybercrime caused significant harm to developing countries' societies and economies. Serious concern to countries at all levels of developments.**
- **While around 160 countries have enacted cybercrime legislation, with different patterns, varies by region.**
- **The evolving cybercrime landscape and resulting skills gaps are a significant challenge for law enforcement agencies and prosecutors, especially for cross-border enforcement.**
- **Certainly there are challenges in terms of the varying strength of national laws, as well as the capacity of national governments to implement them.**

# CYBERCRIME IS BORDERLESS

- **Lack of consensus among UN member states causing delay, but consensus amongst states & civil society essential.**
- **After years of discussions, the UN General Assembly voted to begin negotiating a Cybercrime Treaty that has potential to restructure policing on a global scale, with serious implications for human rights.**
- **Just as cybercrime is borderless, the impacts of cybercrime on the security of vulnerable groups are inexact.**

# FUNDAMENTAL RIGHTS – HUMAN RIGHTS SHOULD BE ENSURED

- ▶ Human rights are at the core of law and policy decisions of the UN system together with peace, security and development – they are inter-linked and mutually reinforcing.
- ▶ The provisions of the proposed convention ensure that any interference with the right to privacy, including through the collection of metadata, complies with international human rights standards.
- ▶ The provisions, and the proposed treaty should be consistent with international conventions already adopted by UN and ratified by the States.

# SCOPE TO BE EXPANDED

- Convention limited to computer crimes may create more problems than solutions as technology evolves. They call for an expanded scope in the convention which, in addition to the pure cybercrimes, would include a longer list of cyber-enabled crimes like .....
- Use of ICTs for terrorist reasons, the distribution of narcotic drugs, and arms trafficking, in addition to content-related offences such disinformation, coercion to suicide, hate speech, extremism and others.

# PROCESS BE OPEN, INCLUSIVE AND TRANSPARENT

- Legality principle requires criminal law provisions to be publicly accessible, clear, and precise in scope, so that individuals can reasonably ascertain which conduct is prohibited and adjust their behaviour accordingly.
- Vague and imprecise definitions of offenses leave room for arbitrary interpretations and risk infringement of human rights. So clarity is required.
- Civil society should be considered in multilateral negotiations who are rights defenders, especially on issues that are considered the domain of law enforcement, like cybercrime.

Thank you!  
Jim

