



Capacity Building

An Enabler of Capacity- Building by Andrea Martin-Swaby, Senior Deputy Director of Public Prosecutions delivered on the 22nd day of August, 2023.



The Report of the OEWG – Final Substantive Report

- ▶ “ The international community’s ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond.

What capacity exists within member states?

1. The capacities within member states differ in respect of their ability to address malicious activities in cyber space;
2. The human resources, policies, legislative structure, policies and institutions also differ among member states;



The Dilemma

Consequences of Insufficient Capacity -

- Where member states lack the capacity to prevent and to respond to malicious activities in cyber space, a vulnerability in the international community may be created;
- Malicious activities in cyberspace are potentially multi-jurisdictional in terms of impact;
- Where a member state lacks capacity to prevent, it becomes a soft target and in some instances a safe space/ conduit through which to perpetrate a malicious act.




Capacity Building – North - South

- ▶ Capacity Building – Developed and Developing Countries

PRACTICAL CONSIDERATIONS -

This form of capacity building is critical in facilitating targeted assistance to developing countries.

- Demand Driven –
- Correspond to national needs and priorities
- Results focused



Methodology – North to South

- ▶ Developing Country to identify critical needs or a specific area of focus which is a priority;

IDENTIFY FOCUS AREA

- ▶ For example creation of National Cyber Security strategy/ implementation of National strategy;
- ▶ Building knowledge base of investigators regarding ransomware investigations;
- ▶ Strengthening National CSIRT



Role of Recipient -

- Properly identify needs and priorities;
- Develop a road map of what will be needed to achieve the desired outcomes eg. Jamaica;
- Present these to the developed country which may be able to offer assistance;



UN Convention on Cybercrime- Capacity Building & Technical Assistance

- ▶ The current treaty being negotiated includes a chapter dedicated to capacity building and technical assistance;
- ▶ This is particularly important for small developing states.



Technical Assistance – Main Areas

TECHNICAL ASSISTANCE -

- Training;
- Mutual exchange of relevant experience & specialized knowledge;

CAPACITY BUILDING-

- Methods used in the detection, prevention, investigation and prosecution of Cybercrimes;
- Legislative development ;
- Collection & sharing of electronic evidence;
- Law enforcement techniques.



Conclusion.

