Commonwealth Telecommunications Organisation – Proposal for IGF Open Forum 2017

Title: Facilitating Investment in Cybersecurity as a means of achieving the Sustainable Development Goals

Description: Information and Communication Technology (ICT) now serves as the foundation for the development of every modern and progressive society, allowing for integration into the global information economy. Despite the benefits and opportunities offered by ICTs, cyberspace presents several risks and challenges. Safety, security and resilience are critical for Cyberspace to deliver its potential developmental impact. The CTO is of the view that National Cybersecurity strategies provide the framework to support an all encompassing approach to protect the Cyberspace infrastructure, its content and users. It states national priorities and goals, assigns roles and responsibilities and resources. With robust cybersecurity frameworks in place, countries can better leverage the opportunities offered by ICT for socio economic development. We recognise however that implementation and budget allocation for cybersecurity activities presents a significant challenge for states. This proposed forum will therefore address how countries can allocate resources, especially financial resources for cybersecurity activities, and how such activities can contribute to the UN SDGs such as education, gender equality and innovation. The agenda would entail:

1. Developing and implementing cybersecurity strategies with special attention on financial allocations. Resources to assist in this regard will be shared (the background paper provides more details on strategy development);
2. Discussions from speakers and participants on resource challenges and what can be done to address these. Ideas for financial assistance for strategy implementation will be shared, for instance, feasibility of creating special funds for activities such as training and participation at international events which support overarching goals of coordination and cooperation;
3. Facilitating peer arrangements where less developed countries can be paired with more advanced ones to share ideas and learn best practices based on experience.

Tags: #cybersecurity #cybergovernance #commonwealth #capacitybuilding #cyberfunding #SDGs

Speakers: Shola Taylor; Mark Carvell

Online Moderator: Commonwealth Telecommunications Organisations

Background Paper

Introduction

Information and Communication Technology (ICT) now serves as the foundation for the development of every modern and progressive society, allowing for integration into the global information economy. Despite the benefits and opportunities offered by ICTs, cyberspace presents several risks and challenges. Safety, security and resilience are critical for Cyberspace to deliver its potential developmental impact.

The Commonwealth Telecommunications Organisation (CTO) is the largest and oldest Commonwealth membership organisation committed to using ICTs appropriately and effectively for development (ICT4D). In recent years the CTO has undertaken a substantial volume of research, consultancy and advisory work on behalf of its member governments, donor agencies and the private sector. CTO's research, consultancy and advisory, and capacity building services have become an essential tool for many government ministries, ICT regulatory authorities and ICT implementing agencies. High-profile consultancies and training projects recently undertaken by the CTO have provided a number of public sector entities and governments with advice, plans and guidance on how to meet new challenges, develop requisite skill sets, create institutional frameworks and plan to reap maximum benefits from the ICT revolution. These consultancies, along with its normal work, have called for the CTO to analyse and understand how best to leverage the strengths of ICTs to ensure socio-economic development.

The CTO brings extensive, in-depth experience in strategic planning, institutional design and diagnostics, organisational strategies, regulatory frameworks, strategic planning, e-governance and m-governance, regulatory capacity building, the delivery of research projects that have informed strategic planning processes, policy and regulatory development, and regional harmonization. This has given the CTO a unique understanding of the motivations of all stakeholders that make up the ICT ecosystem, and has allowed the CTO to build a strong understanding of what drives growth and development of ICT sectors.

Commonwealth Approach for Developing National Cybersecurity Strategies

The CTO recognises that an effective Cybersecurity Strategy is critical for each country to engage fully in the increasingly cyber-dependant trade and commerce. It enables individuals, companies and nations to realise the full potentials of the cyberspace,

without fear or reservation. It engages all parties in addressing the challenges and opportunities.

In 2014, the CTO developed a guide entitled "*Commonwealth Approach for Developing National Cybersecurity Strategies*"[1]. The guide was revised in 2015. It is based on the *Commonwealth Cybergovernance Principles* and provides practical advice and proposes actions that can be adapted by countries to suit their individual circumstances.

The initiative to develop the Cybergovernance principles was launched at the 53rd Council meeting of the CTO in Abuja, Nigeria which was followed by a range of consultations with stakeholders. The Commonwealth Cybergovernance Model was adopted by the Commonwealth ICT Ministers at the meeting held in London in March 2014. The Model is a unique Commonwealth approach based on four key principles, each steeped in the Commonwealth values. The principles are as follows:

Principle 1: "We contribute to a safe and an effective global Cyberspace"

- as a partnership between public and private sectors, civil society and users, a collective creation;
- with multi-stakeholder, transparent and collaborative governance promoting continuous development of Cyberspace;
- where investment in the Cyberspace is encouraged and rewarded;
- by providing sufficient neutrality of the network as a provider of information services;
- by offering stability in the provision of reliable and resilient information services;
- by having standardisation to achieve global interoperability;
- by enabling all to participate with equal opportunity of universal access;
- as an open, distributed, interconnected internet;
- providing an environment that is safe for its users, particularly the young and vulnerable;
- made available to users at an affordable price.

Principle 2: "Our actions in Cyberspace support broader economic and social development"

[1] http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf

- by enabling innovation and sustainable development, creating greater coherence and synergy, through collaboration and the widespread dissemination of knowledge;
- respecting cultural and linguistic diversity without the imposition of beliefs;
- promoting cross-border delivery of services and free flow of labour in a multi-lateral trading system;
- allowing free association and interaction between individuals across borders;
- supporting and enhancing digital literacy;
- providing everyone with information that promotes and protects their rights and is relevant to their interests, for example to support transparent and accountable government;
- enabling and promoting multi-stakeholder partnerships;
- facilitating pan-Commonwealth consultations and international linkages in a globally connected space that also serves local interests.

Principle 3: "We act individually and collectively to tackle cybercrime"

- nations, organisations and society work together to foster respect for the law;
- to develop relevant and proportionate laws to tackle Cybercrime effectively;
- to protect our critical national and shared infrastructures;
- meeting internationally-recognised standards and good practice to deliver security;
- with effective government structures working collaboratively within and between states;
- with governments, relevant international organisations and the private sector working closely to prevent and respond to incidents.

Principle 4: "We each exercise our rights and meet our responsibilities in Cyberspace"

- we defend in Cyberspace the values of human rights, freedom of expression and privacy as stated in our Charter of the Commonwealth;
- individuals, organisations and nations are empowered through their access to knowledge; users benefit from the fruits of their labours; intellectual property is protected accordingly;

- users can benefit from the commercial value of their own information; accordingly, responsibility and liability for information lies with those who create it;
- responsible behaviour demands users all meet minimum Cyberhygiene requirements.

Bearing in mind these principles, the approach document offers guidance to countries in the development, deployment and revision of their national Cybersecurity strategies, emphasising the need for each country to take into account its culture, its national priorities, the risks it faces and the impact of its strategy both regionally and globally. It shows key aspects of what should be contained within a national strategy and how these can be captured, while also maintaining that the strategy should reflect the conscious and continuous balance of the achievement of security goals, while respecting privacy and protection of civil liberties.

The document also recognises that some actions called for by the strategy will be delivered under the direct control of government agencies but those agencies are quite likely to lack the necessary skills and resources. Therefore, a key part of the strategy's design should consider, where necessary, including the allocation and development of those resources in order to respond to the strategy. Some actions will fall on the private sector and it is important that expectations are realistic and sympathetic to their commercial environment, to avoid perverse outcomes that may result when market forces respond to government intervention. A collaborative multi-stakeholder approach is vital to avoid such damaging outcomes.

Key performance indicators are also a crucial component of Strategies as they ensure the objectives of the national Cybersecurity strategy are being achieved, and that appropriate mechanisms are put in place to monitor and validate its implementation. Effective monitoring and evaluation relies on the careful choice of key performance indicators (KPI) that ideally complement the key risks to national level outcomes identified earlier. In this way, the measure of performance is tied to the desired outcome, not to the consumption of resource.

Assistance provided by the CTO

The guide was created as a tool to assist countries and has led to the CTO providing assistance to Member States such as Fiji, Botswana, Cameroon, Uganda, Malawi, Tanzania and Mozambique, to develop and adopt National Cybersecurity Strategies.

National strategy development assistance to countries are usually provided through consultancy services, in some cases in partnership with local or other international consultants. CTO recommends a risk-based approach, framed by principles that reflect the country's culture and the Commonwealth Cybergovernance Principles. Design and delivery of the strategy should include a wide range of stakeholders from across the public and private sectors, across academia and drawn from civil society. CTO also works with the stakeholders involved to create log frames which set out the timeframes, responsible parties and costs involved for each activity within a strategy.

The CTO works with all relevant stakeholders within each country to understand the local context, including what already exists and areas where there are gaps. CTO has partnered with the University of Oxford's Oxford Martin School which has developed a Cybersecurity Capacity Maturity Model (CMM). This CMM is used for conducting stakeholder consultations. It examines the maturity of a nation across five unique and key dimensions namely: Policy and Strategy; Culture and Society; Education, Training and Skills; Legal and Regulatory Frameworks; and Standards, Organisations, and Technologies. The CMM has been conducted by the CTO in a number of countries including Rwanda, Uganda, Tanzania, Mozambique and Malawi.

To complement national strategy development and/or implementation, the CTO has also been delivering workshops to various countries on Critical Information Infrastructure Protection (CIIP) and Cyber Standards. CIIP is a key component of any strategy and the assistance provided by the CTO usually targets stakeholders from all relevant sectors to explain basic concepts and to identify critical sectors within each country. Similarly, as it relates to cyber standards, it is the belief that a certification scheme which evaluates entities individually will extend the Commonwealth approach to Cybersecurity to an operational level and build trust across borders. The CTO recognises that small and medium enterprises do not have the necessary resources to implement large standards such as ISO27001. In this regard, training is offered in partnership with Information Assurance for SME (IASME) consortium in the UK to raise awareness on Cyber Essentials and to conduct accessor training for entities to become certified. These activities would lead to greater confidence in virtual networks and structures by national and international parties and held drive investment in electronic commerce.

These are but a few initiatives which are currently being undertaken by the CTO in its approach to Cybersecurity across the Commonwealth. We believe that greater support for implementation is required for states as investing in activities which promote the safety, resilience, and availability of ICT infrastructure through the creation of

educational programs to train citizens, research and innovation, data protection frameworks and other related activities.

In support of our Strategic Goals 2016-2020, the CTO remains committed to working with all its members to build capacity, strengthen Cybersecurity and enhance coordination and platforms like the IGF can assist in facilitating discussions to achieve this work.