COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

Internet Governance Forum 2017 – BPF on Cybersecurity
CTO Contribution to Questionnaire

1. *How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?*

   ICTs and Technology play a key role in education, sustainable cities, clean energy, resilient infrastructure, promoting sustainable industrialisation, fostering innovation and in many more SDGs. For technology to effectively deliver its developmental impact, safety, security and resilience are critical within cyberspace.

   Cybersecurity is key component in realizing and maintaining the general ICT security objectives of availability, confidentiality and integrity. The CTO is of the view that an effective Cybersecurity Strategy is essential for each country to engage fully in the increasingly cyber-dependant trade and commerce. Robust cybersecurity frameworks enable individuals, companies and nations to realise the full potentials of the cyberspace, without fear or reservation, promoting cross-border delivery of services and free flow of labour in a multi-lateral trading system.

2. *How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?*

   Cybersecurity frameworks enhance a country's preparedness to respond to the challenges of cyberspace. For instance measures to strengthen and protect critical information infrastructure can support economic development and attract international business. Poor cybersecurity hinders growth and trust in ICTs as it leads to lack of confidence in online systems and services, thus discouraging investment and usage A lack of cyber hygiene increases vulnerability to cyber attacks and reduces the ability to effectively respond to and recover from cyber incidents which in turn promotes a lack of trust in the digital economy.

3. *Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:*

   - *Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services*
   - *Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments*
   - *Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended*
   - *Confidentiality and availability of sensitive information, in particular in medical and health services*
   - *Online abuse and gender-based violence*
   - *Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Point (IXP) communities*

- *Vulnerabilities in the technologies supporting industrial control systems*
- *Use of information collected for a particular purpose, being repurposed for other, inappropriate purposes. For instance, theft of information from smart meters, smart grids and Internet of Things devices for competitive reasons, or the de-anonymization of improperly anonymized citizen data*
- *The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis*
- *Unauthorized access to devices that take an increasing role in people's daily lives*
- *Other: describe a cybersecurity issue critical to developing the SDGs in ways not listed above relevant to your stakeholder community (100 words or less) –*

  How do small and medium enterprises (SMEs) secure themselves from cyber attacks and also promote confidence and trust in their online services?

  CTO is of the view that this is an important issue as SMEs contribute to 60% of total employment and up to 40% of national income (GDP) in emerging economies. CTO has been promoting the adoption of smaller cyberstandards such as Cyber Essentials, as existing standards such as ISO 27001 have been found to be too onerous for smaller organisations. Such cyberstandards can help organisations protect themselves against common cyber attacks and thereby facilitate secure online transactions within the growing digital economy. Moreover a common standard will promote cross border trade.

4. *Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected ways. Stakeholders are managing complexity. This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely we may adopt security requirements or measures that prevent the development, deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?*

   Responsibility for cybersecurity must be a collective one. A culture of cybersecurity is one which should be encouraged and promoted across all sectors. This can help ensure that there is consideration for security and privacy in the development of new applications and technologies which can be safely utilised for the benefit of all.

   Cognisant of the unique nature of Cyberspace and of the importance of maintaining it as a place that fosters interactions, innovation and entrepreneurship, the CTO, in 2014, embarked on a project to develop the Commonwealth Cybergovernance Model that draws on the shared values and principles of the Commonwealth as encompassed in the Commonwealth Charter. These principles are used as a guide when developing national cybersecurity strategies.

   The fourth principle of the *Commonwealth Cybergovernance Model*[1] states:

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

"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.

5. *What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?*

One critical cybersecurity issue which would benefit from a multi-stakeholder approach is that of jurisdiction/cross border information sharing. Cybersecurity is a transnational issue and there is a need for greater dialogue, understanding and cooperation on this jurisdictional matters as challenges exist in relation to legal cooperation, the digital economy, cybercrime and many more related issues. The fact that criminal investigations may require access to information about users or digital evidence which is stored outside of the requesting country, or that content or acts which may be legal in one country and illegal in another are just two cases which demonstrate the need greater discussion on facilitating cross-border cooperation.

The Internet & Jurisdiction Policy Network is one stakeholder which can be invited to address this issue as its work focuses on the tension between the cross-border Internet and national jurisdictions.