COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

Commonwealth Approach to Cybergovernance and Cybersecurity

By the Commonwealth Telecommunications Organisation

Trends in Cyberspace

- Cyberspace provides access to ICT
  - Bridging the digital divide and influencing social-economic activities
- Cyberspace is increasingly becoming a global system
  - Anticipated to grow from 2-4 Billion users by 2020 (mostly from developing countries)
- Cyberspace is open, decentralised and empowering
  - This has fostered innovation, collaboration and rapid development
- Cyberspace success depends on it's infrastructure
  - Infrastructure should be secure, resilient and available to users
- Cyberspace can also be used for criminal activities
  - Cybercrimes, extremisms and other social crimes

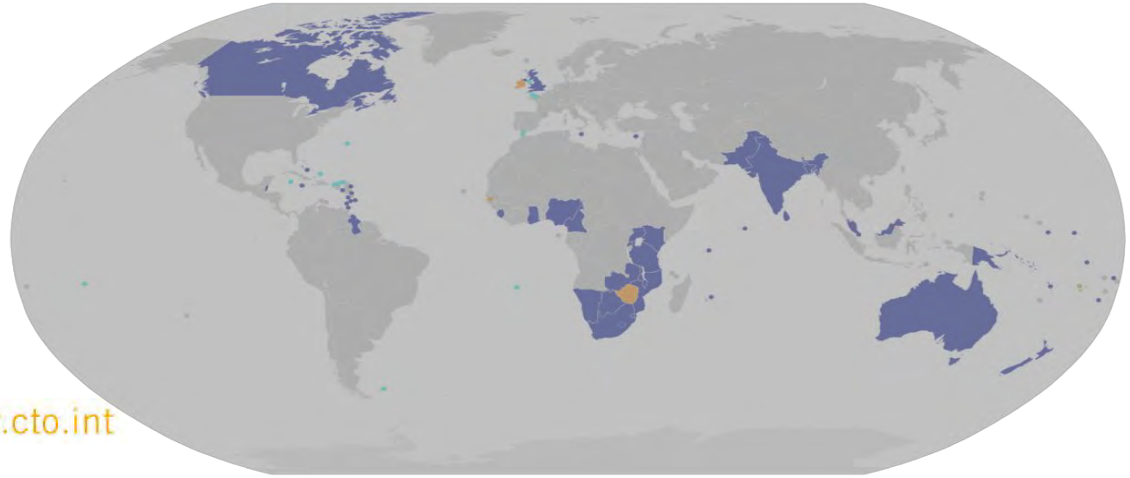
Why a Commonwealth Model for Cybergovernance

- Contrasting views emerging across the world on governing the Cyberspace
- Harmonisation is critical to facilitate the growth and to realise the full potentials of Cyberspace
- Commonwealth family subscribes to the Charter of the Commonwealth (http://thecommonwealth.org/sites/default/files/page/documents/CharteroftheCommonwealth.pdf)
- The values and principles are equally well applicable to Cyberspace
- CTO is the Commonwealth agency mandated in ICTs
- The project was launched at the 53rd council meeting of the CTO in Abuja, Nigeria (9th Oct 2013)
- Wide consultations with stakeholders
- Adopted at the Commonwealth ICT Ministers Forum on 3rd and 4th March 2014 in London

Objectives

The Cybergovernance Model aims to guide Commonwealth members in:-

- Developing policies, legislation and regulations
- Planning and implementing practical technical measures
- Fostering cross-border collaboration
- Building capacity



www.cto.int

CTO
COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Commonwealth Values in Cyberspace

- Based on Commonwealth Charter of March 2013
  - Democracy, human rights and rule of law
- The Charter expressed the commitment of member states to
  - The development of free and democratic societies
  - The promotion of peace and prosperity to improve the lives of all peoples
  - Acknowledging the role of civil society in supporting Commonwealth activities
- Cyberspace today and tomorrow should respect and reflect the Commonwealth Values
  - This has led to defining Commonwealth principles for use of Cyberspace

Commonwealth Principle for use of Cyberspace

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.

Commonwealth Principle for use of Cyberspace

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

- 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 single globally connected space that also serves local interests.

Commonwealth Principle for use of Cyberspace

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.

Commonwealth Principle for use of Cyberspace

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;
- we protect the vulnerable in society in their use of Cyberspace;
- we, individually and collectively, understand the consequences of our actions and our responsibility to cooperate to make the shared environment safe; our obligation is in direct proportion to culpability and capability.

Practical Application of Commonwealth Principles

- Develop a Commonwealth approach to National Cybersecurity Strategies
  - based on the Commonwealth Cybergovernance Principles
  - Drawing on operational National Cybersecurity Sttratgies
  - With the help of partners – ITU, OAS, Microsoft etc
- Inform Commonwealth countries of the prototype and help them develop individual strategies
  - addressing unique local needs and socio-economic priorities

Commonwealth Approach to Developing National Cybersecurity Strategies

http://www.cto.int/priority-areas/cybersecurity/national-cybersecurity-strategies/

www.cto.int

CTO COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Cybersecurity Threat Horizon

Cybersecurity is challenging to understand

- Many of the decision makers including policy makers do not get it
- Organisations don't have adequate expertise and resources
- Outsourcing processes and data is on the rise, increasing risks

Reputation is a new target of Cyber attacks

- User information/organization information is becoming more valuable (e.g. co-orporate espionage)
- Cybercrime as a Service (CaaS) is becoming a reality in the criminal underworld with very sophisticated techniques for launching attacks
- Information leakage (Wiki Leaks, Snowden), people are the weakest link
- Anonymity on social networks
- Hactivism (ethics & business behaviour e.g. Starbucks, Google & Amazon have been victims)

Cybersecurity Threat Horizon

Technology changes faster than the law

- Dependency on cloud services creates further complexity
- Mismatch of what to keep in-house and what to keep in the cloud can be challenging
- Bring Your Own Device (BYOD) is always the 'Elephant in the Room'

Governments & Regulators are only part of the solution

- Organisations are expected to manage their own risks
- Regulators are not keeping up with the pace of technology and demands from operators and service providers

Development of the Strategy

- Need the support of highest levels of Government
- Adopt a multi-stakeholder partnership; public sector, private sector and the civil society
- Draw on the expertise of the international community
- Centralised Mandate - Appoint a lead organisation or institution
- Be realistic and sympathetic to the commercial considerations of the private sector when engaging them
- Add a mechanism to monitor and validate implementation

Key elements of the Prototype Cybersecurity strategy

- Introduction and background
- Guiding principles
- Vision and strategic goals
- Specific objectives
- Stakeholders
- Strategy implementation

Introduction & Background

- Focuses on the broad context
- Sets the importance of Cybersecurity to national development
- Assess current state of Cybersecurity and challenges

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
1. Introduction / background This section provides a succinct background of the country's circumstances and the status of its Cybersecurity	• Explain the importance of Cybersecurity to economic and social development. • Describe the use of Cyberspace and the nature of Cybersecurity challenges to justify the need for the Cybersecurity strategy • Explain the relationship to existing national strategies and initiatives.	Uganda's introduction covers: • The definition of information security • The justification for a strategy • Country analysis of current state of information security framework. • Strategy guiding principles • Vision, mission, strategic objectives Note that this example covers the first three sections in this framework.

www.cto.int

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

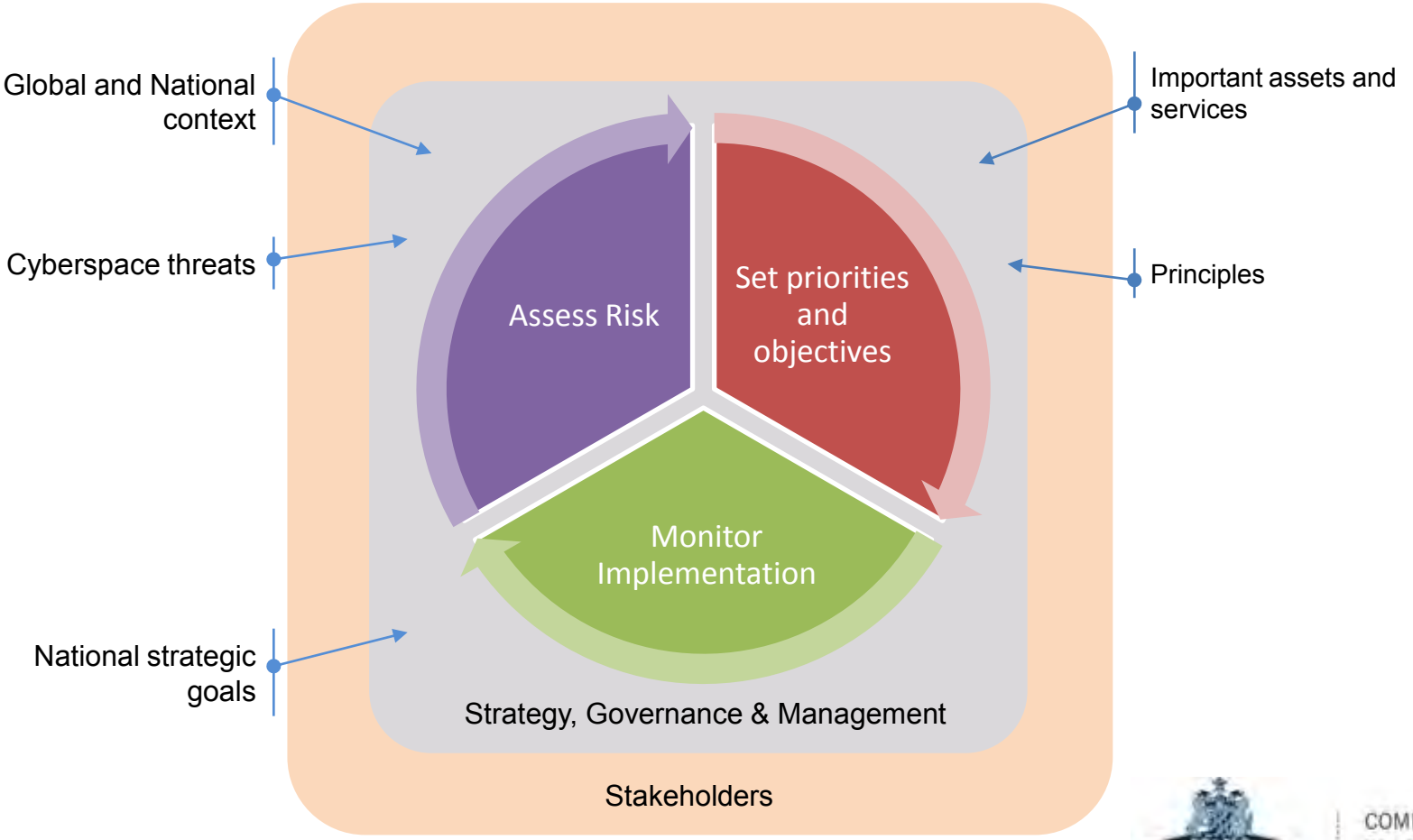
Guiding Principles (1/3)

- Based on Commonwealth Cybergovernance principles
- Balance security goals & privacy/protection of civil liberties
- Risk-based (threats, vulnerabilities, and consequences)
- Outcome-focused (rather than the means to achieve it)
- Prioritised (graduated approach focusing on critical issues)
- Practicable (optimise for the largest possible group)
- Globally relevant (harmonised with international standards)

CTO
COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Guiding Principles (2/3)

- Risk-based (threats, vulnerabilities, and consequences)



www.cto.int

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Guiding Principles (3/3)

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
2. Guiding principles This section identifies the guiding principles for addressing Cybersecurity within which the strategy is designed and delivered.	• Build from the principles of the Commonwealth Cybergovernance model. • Include any relevant national principles. • Describe the delivery principles that guide the design of the objectives goals, vision and objectives.	In addition to the Commonwealth Cybergovernance principles and national principles the following delivery principles are recommended: Risk-based. Assess risk by identifying threats, vulnerabilities, and consequences, then manage the risk through mitigations, controls, costs, and similar measures. Outcome-focused. Focus on the desired end state rather than prescribing the means to achieve it, and measure progress towards that end state. Prioritised. Adopt a graduated approach and focus on what is critical, recognising that the impact of disruption or failure is not uniform among assets or sectors. Practicable. Optimise for adoption by the largest possible group of critical assets and realistic implementation across the broadest range of critical sectors. Globally relevant. Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.

Visions & Strategic Goals

- Promote economic development
- Provide national leadership
- Tackle cybercrime
- Strengthen the critical infrastructure
- Raise and maintain awareness
- Achieve shared responsibility
- Defend the value of Human Rights
- Develop national and international partnerships

Visions & Strategic Goals

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
3. Strategic goals and vision This section defines what success looks like in broad summary terms and reflects the country's priorities.	• Make a clear statement of the country's commitment to protecting the use of its Cyberspace • Emphasise the breadth of the use of Cyberspace: covering social and economic activity • Include text that can be quoted as part of the communication with wider stakeholders, e.g. a vision statement.	**Australia**'s vision: "The maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy" Three pillars of the **Australian** strategy: • All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online; • Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers; • The Australian Government ensures its information and communications technologies are secure and resilient." Four pillars of the **UK** strategy: • Tackle cybercrime and be one of the most secure places in the world to do business in cyberspace; • To be more resilient to cyber attacks and better able to protect our interests in cyberspace; • To have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies; • To have the cross-cutting knowledge, skills and capability it needs to underpin all our Cybersecurity objectives.

Specific Objectives

- Provide a national governance framework for securing Cyberspace
- Enhance the nation's preparedness to respond to the challenges of Cyberspace
- Strengthening Cyberspace and national critical infrastructure
- Securing national ICT systems to attract international businesses
- Building a secure, resilient and reliable Cyberspace
- Building relevant national and international partnerships and putting effective political-strategic measures in place to promote Cyber safety
- Developing a culture of Cybersecurity awareness among citizens
- Promoting a culture of "self protection" among businesses and citizens
- Creating a secure Cyber environment for protection of businesses and individuals
- Building skills and capabilities needed to address Cybercrime
- Becoming a world leader in Cybercrime-preparedness and Cybercrime-defence

Specific Objectives

STRATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
4. Risk management (Risk based approach objectives) How the risk management process works, and then setting objectives and priorities This section describes how risk management is performed and provides a top-level analysis. It states specific and tangible targets and assigns relative priorities.	• How risk management is currently performed, for example for national security. • Sources of threat information and of major vulnerabilities. • How granular to make the outcomes and objectives. • How frequently to repeat the risk assessment process.	Source**: Microsoft's guidance**, listed in **appendix 3**: • A clear structure for assessing and managing risk • Understand national threats and major vulnerabilities • Document and review risk acceptance and exceptions • Set clear security priorities consistent with the principles • Make national cyber risk assessment an on-going process

Stakeholders

- Policy makers and other government departments
- Independent agencies (security, emergency & Health/Safety)
- Private sector
- Civil society & Independent Practitioners
- Academia & Research Institutions
- International bodies

www.cto.int

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Strategy Implementation

- Governance and management structure
- Legal and regulatory framework
- Capacity Development
- Awareness and outreach programmes
- Incident response
  - Incentivize commercial competitors to cooperate
  - Create national CERTs
- Stakeholder collaboration
- Research and Development
- Monitoring and evaluation

www.cto.int

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Strategy Implementation

RATEGY COMPONENTS	ASPECTS TO CONSIDER	EXAMPLE TEXT FROM PUBLISHED STRATEGIES AND BEST PRACTICE
6. Implementation This section identifies activities in more detail.	• Define practical actions to be undertaken. • Group actions into categories convenient for their management.	
6.1 Governance and management structure This section describes the establishment of governance and management for the strategy, covering its development and delivery. This must include management of monitoring and improvement.	• Establish a strong leadership role at the highest level to give priority and recognition to the strategy. • Establish suitable multi-stakeholder governance of the strategy to cover all aspects. This should cover all economic sectors, civil society, private and public sectors. • Identify and establish activities required to monitor and validate the strategy's implementation.	"The Specialised Cyber Security Committee will support the National Security Council in performing its functions, particularly in assisting the Prime Minister in directing and coordinating the National Security Policy in the field of cyber security." - **Spain** "The Specialised Situation Committee will be convened to manage crisis situations in the field of cyber security ..." - **Spain** "The Specialised Cyber Security Committee and the Specialised Situation Committee will act in a complementary manner, each in its own area of responsibility but under the same strategic and political direction of the National Security Council chaired by the Prime Minister." - **Spain** Establishment of a Trinidad and Tobago Cyber Security Agency (TTCSA) – **Trinidad and Tobago**

www.cto.int

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Summary of proposals from previous workshops (1)

- Establish a Cybersecurity agency – Central Mandate
- It could be where CERT will be based
- Assistance from the International community to establish a CERT, example ITU
- Enhance stakeholder partnership and collaboration
- Formulate Cybersecurity policies and relevant laws
- Enhance content filtering by ISPs and Operators, where possible provide technical assistance
- Establishment of a digital forensic lab to assist with audit trails and prosecution
- Need to have national register for mobile devices including SIM cards (synchronize the mobile number and MEI number)
- Enhance regional corporation
- Emphasize Cyberspace jurisdiction i.e. using ccTLD
- Formulation and hosting of an ICT conference, similar Digital World Conference

Summary of proposals from previous workshops (2)

- Develop an ICT plan, and specify the objectives and define performance metrics
- Develop R&D in the area of Cybersecurity
- Capacity building in Cybersecurity and Cybercrime
- Develop a framework to introduce Cybersecurity insurance
- Subscriber registration for services needs to be streamlined
- Harmonize the channelling for complaints raised against social networks (such as FB)
- Review the processes for domain registration
- Review the data retention issues by operators and service providers
- Ensure adequate engagement by high-level officials, Ministers, Permanent Secretaries etc

For further information please contact:

Mr Lasantha De Alwis
Director of Operations & Corporate Secretary
Commonwealth Telecommunications
Organisation (CTO)

Email: l.dealwis@cto.int
Tel: +44 (0) 208 600 3814

COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

64 - 66 Glenthorne Road
London W6 0LR
United Kingdom

Tel: +44 (0) 208 600 3800
Fax: +44 (0) 208 600 3819
E-mail: info@cto.int
Website: www.cto.int

