Commonwealth

Last Updated: November 2020

Member States

POLICY

Strategy Documents

Commonwealth Approach for Developing National Cybersecurity Strategies

Commonwealth Telecommunications Organisation (CTO)

- Developed by the CTO in 2014 to serve as a guide for countries to develop their individual National Cybersecurity Strategies, provide practical advice and propose actions that can be adapted by countries to suit their individual circumstances; revised in 2015
- Incorporates the Commonwealth Cybergovernance Model adopted in 2014; embraces the Principles of Commonwealth Cybergovernance and draws on published Cybersecurity strategies and good practice from a range of countries
- 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
- Identifies elements of the approach to design of national cybersecurity strategies: risk-based, outcome-focused, prioritised, practicable, globally relevant
- Provides detailed outline guide to national cybersecurity strategies' components:
    1. Introduction / background
    2. Guiding principles
    3. Strategic goals and vision
    4. Objectives and priorities – using a risk-based approach
    5. Stakeholders
    6. Governance and management structure
    7. Implementation

Source Source 2

2015 (revised)

Other Documents

Commonwealth Cyber Declaration

Commonwealth Heads of Government

- Adopted at the Commonwealth Heads of Government Meeting on 16-20 April 2018 in London, UK
- Reflects the commitment of the 53 Commonwealth Heads of Governments:
    - Recognising the potential for a free, open, inclusive and secure cyberspace to promote economic growth for all communities and to act as an enabler for realisation of the Sustainable Development Goals across the Commonwealth: *commit to a cyberspace that supports economic and social development and rights online*
    - Recognising the need for individual and collective action to tackle cybercrime and protect critical national infrastructure: to *build the foundations of an effective national cyber security response*
    - Recognising the importance of international cooperation in tackling cybercrime and promoting stability in cyberspace: *to promote stability in cyberspace through international cooperation*

Source Source 2

20 April 2018

Report of the Commonwealth Working Group of Experts on Cybercrime

The Commonwealth Working Group of Experts on Cybercrime; the Commonwealth Secretariat

- Developed in 2012-2014 by the Commonwealth Working Group of Experts on Cybercrime pursuant to the mandate the Commonwealth Law Ministers' Meeting held in Sydney on 11-14 July 2011
- Delivered at the Meeting of Commonwealth Law Ministers and Senior Officials in Gaborone, Botswana on 5–8 May 2014
- 1st part:
    - finds that the implications of cybercrime in member countries depend on numerous factors, and identifies the general implications of these factors
    - notes that cybercrime is a global concern, as the nature of the internet means that an offender in one jurisdiction can target any other jurisdiction

Commonwealth

Last Updated: November 2020

- considers the nature of cybercrime and the challenges it poses to member countries
- 2nd part:
  - identifies and recommends the most effective means of international cooperation and enforcement to tackle cybercrime
  - encourages adoption of the Council of Europe Convention on Cybercrime by the Commonwealth countries
  - recommends that Commonwealth countries should consider becoming party to and participating in regional conventions and initiatives on cybercrime, in order to ensure further coordinated action
  - recommends adoption of the Commonwealth Model Law on Cyber Crime by member countries
- 3rd part:
  - considers cybercrime training in more detail
  - proposes a strategic model for training, a training model for the Commonwealth, and practical recommendations for use when conducting cybercrime training

Source

5–8 May 2014 (delivered)

Communications

Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity

International Telecommunication Union (ITU), the World Bank, Commonwealth Secretariat, Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), and others

- Facilitated by the ITU and developed by 12 partners from Intergovernmental and International Organisations, private sector, as well as academia and civil society and included the following organisations
- Purpose: to guide national leaders and policy-makers in the development of a National Cybersecurity Strategy, and in thinking strategically about cybersecurity, cyber-preparedness and resilience
- Scope and structure:
  - Section 2 – Introduction: provides an overview of the subject of the Guide with related definitions
  - Section 3 – Strategy development lifecycle: details the steps in the development of a Strategy and its management during its full lifecycle
  - Section 4 – Overarching principles for a Strategy: outlines the cross-cutting, fundamental considerations to be considered during the development of a Strategy
  - Section 5 – Focus areas and good practices: identifies the key elements and topics that should be considered during the development of a Strategy; and
  - Section 6 – Supporting reference materials: provides further pointers to relevant literature that stakeholders can review as part of their drafting effort
- First and foremost targeted at policy-makers responsible for developing a National Cybersecurity Strategy

Source Source 2

2018 (published)

Commonwealth Cybergovernance Model

Commonwealth ICT Ministers

- Follows the Abuja Declaration of Proposed Commonwealth Cybergovernance Model of 9 October 2013 and subsequent consultations
- Adopted by the Commonwealth ICT Ministers on 3 - 4 March 2014 in London, UK
- Outlines implications for cyberspace of each element of the Commonwealth Charter
- Offers set of principles intended to guide Commonwealth members to plan and implement practical actions in policy development, regulation and legislation, cross-border collaboration, capacity building, technical measures and other operational activities:
  - Principle 1: we contribute to a safe and an effective global Cyberspace
  - Principle 2: our actions in Cyberspace support broader economic and social development
  - Principle 3: we act individually and collectively to tackle Cybercrime
  - Principle 4: we each exercise our rights and meet our responsibilities in Cyberspace

Source Source 2

3-4 March 2014

Abuja Declaration on the Proposed Commonwealth Cybergovernance Model

Commonwealth Telecommunications Organisation (CTO)

- Adopted by the ICT Ministers of the Commonwealthj States and the CTO Council at the 53rd Council meeting of the CTO on 9-10 October 2013 in Abuja, Nigeria

Commonwealth

Last Updated: November 2020

- Calls to developing a unique Commonwealth approach to govern the Cyberspace which can be subscribed to by Commonwealth countries and open for adoption by non-Commonwealth countries
- Mandates the CTO to take the lead in developing the Commonwealth Cybergovernance Model, by taking into account the views, priorities and concerns of all Commonwealth countries, liaising closely with other stakeholders whose inputs are necessary to reflect the multistakeholder nature of the Cyberspace
- Identifies the objectives that the Commonwealth Cybergovernance Model may seek:
    1. Foster innovation, freedom and understanding
    2. Promote contributions to economic development
    3. Facilitate social interactions
    4. Recognise legitimate economic, cultural and security concerns of members
    5. Promote multistakeholder partnerships
    6. Facilitate Pan-Commonwealth consultations and international linkages

Source Source 2

9-10 October 2013 (adopted)

STRUCTURE

Specialized Agencies

Commonwealth Telecommunications Organisation (CTO)

- Created in August 1901 as the Pacific Cable Board
- Has 4 main purposes:
    - To support the development and use of ICTs within the Commonwealth and beyond
    - To promote the provision and use of ICTs to meet the needs of members, to support development in Member countries, and to ensure the inclusion of marginalised people
    - To promote effective cooperation and partnership amongst its members and other organisations; and
    - To develop and implement activities to promote the above three objectives
- Offers services to members in four main areas: Capacity Development, Research, Technical Support, Consultancy and Advisory Services and Events and Conferences
- Strategic Plan 2016-2020 is structured around 6 strategic goals, including:
    - Strategic Goal 4: Promote a culture of cybersecurity and effective cyber governance through the establishment of cybersecurity frameworks, standards and guidelines
- Has carried out a project to develop the Commonwealth Cybergovernance Model, and proceeded to develop a Commonwealth Approach for Developing National Cybersecurity Strategies based on the Commonwealth Cybergovernance Model
- In 2010-2017 organized the annual Commonwealth Cybersecurity Forum, aimed at building capacity and facilitating partnerships
- Current and future plans on Cybersecurity include work with the member countries, member institutions and partner organisations to convert the Cybergovernance Model into practical actions and to implement National Cybersecurity Strategies

Source Source 2

August 1901 (established)

LEGISLATION

Regulations and Directives

The Commonwealth Model Law on Computer and Computer Related Crime

Office of Civil and Criminal Justice Reform (OCCJR)

- Developed as part of the Commonwealth effort to developed Model Laws and other Legal Tools on Computer and Computer-Related Crime, Electronic Transactions, Broadcasting, and the Protection of Personal Information
- The object: to protect the integrity of computer systems and the confidentiality, integrity and availability of data, prevent abuse of such systems and facilitate the gathering and use of electronic evidence
- Contains 3 parts:
    1. Part I: in section 3 the important definitions of ‘computer data’, ‘computer system’, ‘service provider’ and ‘traffic data’ together with an additional definition of ‘computer data storage medium’; Section 4 deals with the jurisdiction of the enacting state
    2. Part II (sections 5-10): concerned with substantive criminal law and the creation of offences; the Model Law does not cover computer-related forgery or fraud

Commonwealth

Last Updated: November 2020

3. Part III (sections 11 to 21): deals with 'procedural law', contains provisions as to search and seizure warrants, the obligation to assist the police, recording and access to seized data, the production of data, the disclosure of stored traffic data, the preservation of data, the interception of electronic communications and the interception of traffic data, with provisions as to evidence, confidentiality and the limitation of liability together with the necessary definitions

- Final draft was submitted to Commonwealth Law Ministers at their meeting of 18-21 November 2002; as of July 2017, was under consideration for review

Source Source 2

18-21 November 2002 (submitted); under review as of July 2017

COOPERATION

Meetings

Annual Commonwealth Cybersecurity Forum

Commonwealth Telecommunications Organisation (CTO)

- Conducted annually from 2010 to 2011 and from 2013 to 2017 by the Commonwealth Telecommunication Organisation (CTO) with focus on cybersecurity capacity building and facilitating partnerships
- Key topics included: economics of cybersecurity, privacy and data protection, internet governance, protecting critical information infrastructure, cross-border cybersecurity cooperation, cyber standards, cyberspace and extremism
- Conducted Forums:
    1. CTO Cybersecurity Forum 2010: Common Response to a Global Challenge - conducted on 17-18 June 2010 in London, in partnership with the UK Department for Business Innovation and Skills (BIS) and the UK's Office of Cyber Security (OCS)
    2. CTO Cybersecurity Forum 2011 - conducted on 14-15 June 2011 in London, in partnership with the UK Department for Business Innovation and Skills (BIS) and the UK's Office of Cyber Security & Information Assurance(OCSIA) and the Royal United Services Institute
    3. CTO Cybersecurity Forum 2013: Bringing Safety, Resilience and Security into Cyberspace - conducted on 25-26 April 2013 in Yaounde, Cameroon in partnership with the Ministry of Posts and Telecommunications of Cameroon and Cameroon Telecommunications Regulatory Board
    4. CTO Cybersecurity Forum 2014: Developing National Cybersecurity Frameworks - conducted on 5-6 March 2014 in London; sponsored by British Telecommunications PLC, ICANN and Facebook
    5. CTO Cybersecurity Forum 2015 - conducted on 22-24 April 2015 in London, in partnership with British Telecommunications PLC
    6. CTO Cybersecurity Forum 2016 - conducted on 23-24 March 2016 in London, in partnership with British Telecommunications PLC
    7. CTO Cybersecurity Forum 2017: Cybersecurity: From Strategies to Implementation - conducted on 22-24 March 2017 in London, in partnership with British Telecommunications PLC

Source

Annually in 2010-2011 and in 2013-2017

Critical Information Infrastructure Protection (CIIP) Workshops

Commonwealth Telecommunications Organisation (CTO)

- A series of 6 regional CIIP workshops held by the CTO in 2014-2015 to help States understand the Commonwealth Approach for Developing National Cybersecurity Strategies
- Included stakeholders mainly from relevant government ministries, agencies, departments, private and public sector, academia and civil society group
- The workshop series included:
    1. Southern African Regional Workshop: held in Gaborone, Botswana on 23-24 March 2015
    2. West African Regional Workshop: held in Yaoundé, Cameroon on 24-27 February 2015
    3. East African Regional Workshop: held in Nairobi, Kenya on 20-21 November 2014
    4. Caribbean Regional Workshop: held in Georgetown, Barbados on 17-18 November 2014
    5. Pacific Regional Workshop: held in Port Villa, Vanuatu on 22-26 September 2014
    6. South Asian Regional Workshops: held in Dhaka, Bangladesh on 10-11 September 2014, and in Colombo, Sri Lanka on 25-28 August 2014

Source

August 2014 - March 2015

Activities

Commonwealth

Last Updated: November 2020

Commonwealth Cybercrime Initiative (CCI)

Commonwealth Cybercrime Initiative Consortium (CCI Consortium)

- Launched in 2011 under the auspices of the Commonwealth Connects Programme; unites 35 international organisations, including Interpol, OAS, Council of Europe (CoE), Commonwealth Telecommunications Organisation (CTO) and ITU, contributing to multidisciplinary programmes in Commonwealth countries and constituing the CCI Consortium
- Aims to provide coherent, comprehensive and sustainable assistance to member states to help build the necessary capacity to combat cybercrime
- Modus operandi:
  - Upon a request from a member state, employs a mission team, including at least one technical and one criminal justice expert. The mission team is drawn from the consortium members who are best placed to donate these resources
  - A gap analysis is conducted using the CCI Checklist from which a needs assessment report is produced. The outcomes of this report are agreed with the member state which outlines its priorities and capacities for reform. The CCI Consortium is then asked to make commitments to meet these needs
- Results of the interventions include:
  - The development of partnerships between UK and Ghanaian Universities
  - Reviews and recommendations for reform of Cybercrime Legislation in Ghana, Botswana and Trinidad & Tobago
  - Direct assistance to establish the new Information Commission in Trinidad & Tobago
  - The establishment of networks in East Africa to combat cybercrime
  - Further child online protection and support academic research; and
  - Assisting Botswana with the reform of its Cybercrime Act 2007

Source Source 2

28-30 October 2011 (formally endorsed); ongoing

The Commonwealth Working Group of Experts on Cybercrime

The Commonwealth Secretariat

- Draws from the resolution of the Commonwealth Law Ministers' Meeting held in Sydney on 11-14 July 2011, which mandated the Commonwealth Secretariat to form a multidisciplinary working group of experts to:
  - (i) review the practical implications of cybercrime in the Commonwealth;
  - (ii) identify the most effective means of international co-operation and enforcement, taking into account, amongst others, the Council of Europe Convention on Cybercrime , without duplicating the work of other international bodies; and
  - (iii) collaborate with other international and regional bodies with a view to identifying best practice, educational material and training programmes for investigators, prosecutors and judicial officers.
- Established in January 2012 by the Commonwealth Secretariat to work on the Commonwealth Law Ministers' mandate and present a Report to Law Ministers
- Held 5 meetings:
  - 1st meeting at the Commonwealth Secretariat on 27 February 2012 to discuss its terms of reference and consider how it would take forward its work
  - 2nd meeting in Geneva on 12-13 June 2012
  - 3rd-5th meetings in London on 13 November 2012, 12-13 March 2013, and 16-17 May 2013
- Produced a comprehensive report, divided into three parts, each addressing one part of the Commonwealth Law Ministers' mandate; the report was delivered at the Meeting of Commonwealth Law Ministers and Senior Officials in Gaborone, Botswana on 5–8 May 2014

Source Source 2

January 2012 (established); May 2014 (concluded activities)

External Cooperation

Global Forum on Cyber Expertise, Member

Commonwealth telecommunication Organization (CTO)

- GFCE is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building
- CTO joined GFCE as Member in 2017

Source Source 2

2015 (GFCE established); 2017 (CTO joined as Member)