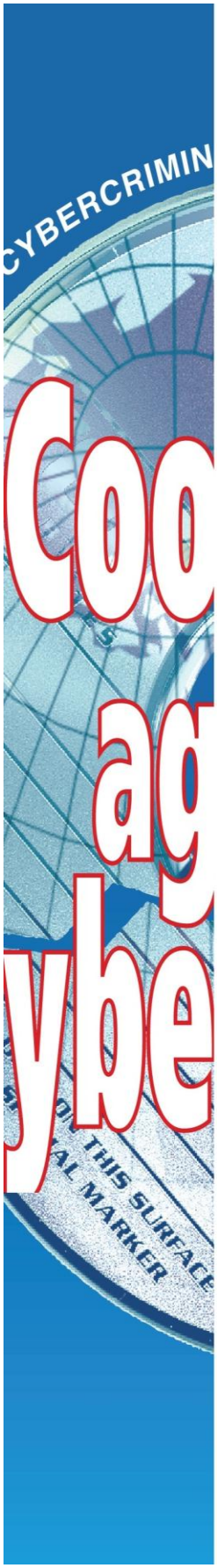

Global Project on Cybercrime

The cybercrime legislation of Commonwealth States:

Use of the Budapest Convention and Commonwealth Model Law

Council of Europe contribution to the Commonwealth Working Group on Cybercrime

Data Protection and Cybercrime Division

Strasbourg, 27 February 2013

www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Project funded by Estonia, Japan, Monaco, Romania, United Kingdom, Microsoft and the Council of Europe

Contact

For further information please contact:

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France

Tel +33-3-8841-2103
Fax +33-3-9021-5650
Email: cristina.schulman@coe.int

Disclaimer

Contents

1 Background

1.1 Commonwealth[1] Secretariat Mandate on Cybercrime

At the meeting of Commonwealth Law Ministers held in July 2011 in Sydney, Australia, Ministers recognised the significant threat posed by cybercrime to national security and law enforcement in all countries of the Commonwealth and mandated the Secretariat to establish "*a multidisciplinary working group of experts to:*

- *review the practical implications of cybercrime in the Commonwealth*
- *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*
- *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*"

At the meeting in Perth, Australia (October 2011), Commonwealth Heads of Government reiterated their commitment to improve national security by improving **legislation and capacity in tackling cyber crime and other cyber space security threats**.

The Commonwealth Working Group on Cybercrime meets to explore and outline strategies on the following core elements of the mandate:

- Explore the practical implications of addressing cybercrime in the Commonwealth
- Identify the most effective means of international cooperation and enforcement to combat cybercrime taking into account the work of other international organisations
- Identify best practice and educational materials for training of criminal justice officials
- Identify suitable training programmes for investigators, prosecutors and judicial officers.

The Working Group is expected to produce a draft report including recommendations for the consideration of the Meeting of Senior Officials scheduled to be held in October 2013, with a view to submitting a final report to the Meeting of Commonwealth Law Ministers in 2014.

The meeting of the Working Group on Cybercrime held in London on 27 February 2012 resulted in the conclusion that the Commonwealth Secretariat must ensure the following:

- that its work does not duplicate, but complements the work of other agencies e.g. UN entities (ITU, UNODC), the Council of Europe, Commonwealth Internet Governance Forum etc.
- that it recognises the utility and importance of international cooperation, including through the Council of Europe Convention on Cybercrime
- that it collaborates to assist Commonwealth member states with capacity building
- that it focuses on best practices to deal with transnational aspects of cybercrime.

[1] More than two billion people in 54 countries across six continents from Antigua and Barbuda to Zambia are part of the Commonwealth.

The Working Group agreed to focus on the following issues:

1. […] Commonwealth Secretariat to conduct a survey by distributing a questionnaire in Commonwealth member states to **assess the implementation of the Commonwealth Model Law on Computer and Computer Related Crime** (Commonwealth Model Law), and so far as relevant the provisions of the London Scheme on Extradition and the recent revisions to the Scheme Relating to Mutual Assistance in Criminal Matters in the Commonwealth (Harare Scheme) as agreed by the Commonwealth Law Ministers at their meeting in Sydney in July 2011

2. conduct a needs assessment at national level based on minimum standards and **set criteria to identify and prioritise areas in which member countries require assistance**

3. mentoring and capacity building for law enforcement officials, legal experts, prosecutors and judicial officers to be delivered in a collaborative manner and to include the **conduct of comprehensive training** based on a collective menu of materials drawn up with relevant stakeholders

4. the development of a **repository or manual of national legislation and best practice** to assist member countries in implementing effective cybercrime laws and developing skills and expertise to address cybercrime

5. the provision of **technical assistance by the Commonwealth Secretariat and specialized agencies, in collaboration with Commonwealth member states, in developing national legal frameworks** in line with the Commonwealth Model Law on Computer and Computer Related Crime as well as the Harare Scheme, the London Scheme on Extradition and other good cross-national practices.

1.2 Purpose of the report

The Council of Europe participates in the Working Group and prepared the present report at the request of the Working Group.

This report provides information on legal measures against cybercrime taken in some Commonwealth countries and underlines where use has been made of the Budapest Convention on Cybercrime and/or the Commonwealth Model Law in drafting national legislation, as well as where an interest in becoming a Party to the Convention has been expressed. It is to help the Working Group identify good practices and give an initial idea of the need for further legal reforms in Commonwealth countries.

The standards of reference used for the purpose of this report are the relevant substantive and procedural law provisions of the Budapest Convention and the Commonwealth Model Law.[2]

Based on information gathered by the Council of Europe, Section 2 (Overview) provides a brief assessment of the implementation of the Budapest Convention and Model law as the minimum standards to be considered by states. (It is possible that other laws may be of relevance in these states but were not available for this assessment).

[2] Even though the mandate of the Working Group includes an assessment of the London Scheme on Extradition and the recent revisions to the Scheme Relating Mutual Assistance in Criminal Matters in the Commonwealth (Harare Scheme) these were not considered in the present report.

Although it can be challenging to identify the sources that might have been considered by states when drafting cybercrime legislation, some definitions, types of conduct, titles of offences and wordings used can indicate sources of inspiration e.g. the Cybercrime Convention, Commonwealth Model Law or the legislation of third countries.

For instance, inclusion of the definition of "*computer data storage medium*", the wordings "*including the Internet*" and "*or any other function"* in the definition of "*computer system*", the mental element "*without lawful excuse or justification*" or "*intentionally or recklessly*", the wordings in the provisions criminalising "*illegal interception of data*", "*interfering with data*", "*interfering with computer system*", "*illegal devices*" and "*child pornography*"; and the absence of computer-related offences (fraud and forgery), could indicate as source the Commonwealth Model Law. With regard to procedural law, the provision of definitions for the terms "*thing*" and "*seize*", the setting of the period for preservation at 7 days, and the wordings used in some provisions, may also indicate the use of the Model Law[3].

The report did not take into consideration the differences that do exist between the Convention and the Commonwealth Model Law. However, when providing legal advice to countries it will be necessary to take into account the differences between the two documents, namely:

- The Budapest Convention is the only binding international instrument on this issue and it is open to any country to become a Party. It serves as a guideline for developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties[4]
- Parties participate in the work of the Cybercrime Convention Committee (T-CY) that deals with the implementation of the Convention and considers further developments of the Convention
- The Convention makes it explicit that Parties should incorporate into their laws the possibility that information contained in digital or other electronic forms can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted[5].

- The Commonwealth Model Law provides language for the implementation of the Convention in the Commonwealth
- The Commonwealth Model Law does not include provisions on computer-related offences (forgery and fraud), nor provisions on international cooperation
- Based on the experience in the application of the Convention, the duration for preservation of computer data provided for by the Commonwealth Model Law (7 days with the possibility of extension) might be too short, in particular for the execution of an MLA request[6]
- The Model Law includes provisions on the admissibility of electronic evidence.

The present report does not offer a thorough analysis and so is not sufficient to provide specific advice on reforms needed in any given state. Such efforts would require a dialog with the relevant authorities, and a more detailed analysis of the legal framework in each country. This would include analysis of the application of the law in practice, for example of problems related to electronic evidence and its admissibility in court etc., in order to be able to identify gaps and make recommendations.

[3] For more information see Appendix 2- Comparative table

[4] Some of the issues raised by Singapore in the paper submitted to the Working Group (preserving/obtaining digital evidence from other jurisdictions; obtaining expeditious responses to requests for MLA; problems associated with extradition) can be resolved by acceding to the Cybercrime Convention.

[5] Explanatory Report 141

[6] For more information on these issues, see the work carried out the Cybercrime Convention Committee http://www.coe.int/t/DGHL/STANDARDSETTING/T-CY/default_en.asp

In any case, it is widely recognised that once legislation has been adopted, significant work is needed to enforce the legislation and ensure the capability of developing countries to investigate and prosecute cybercrime. These issues are to be dealt by the Working Group under a separate report.

1.3 Sources of information

1.3.1 Documents submitted to the Cybercrime Working Group

The Working Group considered documents submitted by Australia, Singapore, Canada and South Africa.

1.3.2 Council of Europe activities carried out under different projects (www.coe.int/cybercrime)[7]

Since 2006, the Council of Europe carried out or contributed to more than 400 activities worldwide under its Global Project on Cybercrime. Examples include the following:

1.3.2.1 Cybercrime legislation for Pacific countries in Nuku'alofa, Tonga (27-29 April 2011)

In June 2010, the meeting of Pacific Ministers for information and communication technologies adopted the "Tonga Declaration" which, among other things, called for "*developing appropriate policy, legislative and regulatory frameworks and strategies to combat cyber crime and promote Internet safety and security, including child online protection*". Ministers instructed their officials to cooperate with the Secretariat of the Pacific Communities (SPC), the Council of Europe and other organizations in this respect.

The Australian Attorney-General's Department (AGD), the Secretariat of the Pacific Community (SPC) and the Council of Europe, therefore, agreed to cooperate in the follow up to the Tonga Declaration and to jointly organise a regional workshop on cybercrime legislation for Pacific countries to be held in Nuku'alofa, Tonga (27-29 April 2011).

Some 70 representatives from the following (mostly Commonwealth) countries participated in the event: Cook Islands, Federated States of Micronesia, Fiji, Kiribati, Marshall Islands, Nauru, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu.

The objective of the workshop was to support the strengthening of cybercrime legislation in the Island States of the Pacific region in line with international standards, in particular the Budapest Convention on Cybercrime.[8]

1.3.2.2 Cooperation against cybercrime in South Asia – International workshop (Colombo, Sri Lanka, 5-6 April 2011)

Building on earlier, country-specific workshops in India, Pakistan and Sri Lanka since 2008, the Information Communication Technology Agency (ICTA) of Sri Lanka, together with the Council of Europe (within the framework of the Global Project on Cybercrime), held a regional event for countries

[7] See Final/Progress Reports of the Council of Europe Global Project on Cybercrime (phase I, II)
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-d-final%20report1i%20final%20_15%20june%2009_.pdf
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_adm_finalreport_V12_9apr12.pdf

[8] see www.coe.int/cybercrime

of South Asia (Bangladesh, India, Maldives, Pakistan and Sri Lanka). The meeting took place in Colombo, Sri Lanka, on 5 and 6 April 2011.

The aim was to enhance the capacity of countries of South Asia to cooperate internationally against cybercrime and more specifically:

- To assess the cybercrime legislation of participating countries in view of their compatibility with international standards (a prerequisite for international cooperation).
- To share experience and promote international police and judicial cooperation, including accession to agreements such as the Budapest Convention on Cybercrime.
- To promote interagency and public-private cooperation at domestic levels.

More than 100 participants engaged in an open and constructive exchange of experience and developed proposals for a further strengthening of legislation, and interagency, public-private and international cooperation.

2 Budapest Convention/Commonwealth Model Law: Overview of implementation[9]

Country	Substantive Law Provisions	Procedural Law Provisions
	Article 1 – Definitions Article 2 - Illegal Access Article 3 - Illegal interception Article 4 - Data interference Article 5 - System interference Article 6 - Misuse of device Article 7 - Computer - related forgery Article 8 - Computer - related fraud Article 9 - Child pornography offence	Article 16 - Expedited preservation of stored computer data Article 17 - Expedited preservation and disclosure of traffic data Article 18 - Production order Article 19 - Search and seizure Article 20 - Collection in real-time of traffic data Article 21 - Interception of content data
Antigua and Barbuda	*Legislation in place (unclear about computer-related offences)*	*Legislation in place*
Australia	*Legislation in place (new legislation was adopted implementing the Budapest Convention)*	
The Bahamas	*Partial legislation in place*	*Insufficient investigative powers*
Bangladesh	*Partial legislation in place*	*Insufficient investigative powers*
Barbados	*Legislation in place*	*Legislation largely in place (unclear about real-time collection of traffic data and interception of content data)*
Belize	*No information available*	
Botswana	*Legislation in place*	*Legislation largely in place (unclear about interception of content data)*
Brunei Darussalam	*Legislation in place*	*Partial legislation in place*
Cameroon	*Legislation in place*	*Partial legislation in place*
Canada	*Legislation in place (draft Bill in the Parliament to introduce amendments)*	
Cyprus	*Legislation in place*	*Insufficient information*
Dominica	*No information available*	
Fiji	*Insufficient legislation in place*	*Insufficient legislation in place*
The Gambia	*No information available*	
Ghana	*The legal framework is to be reviewed with the support of CCI*	
Grenada	*No information available*	
Guyana	*No information available*	
India	*Legislation in place* *(Specific regulations are to be adopted; implementation of Article 6 to be considered)*	
Jamaica	*Partial legislation in place*	*Partial legislation in place*
Kenya	*Partial legislation in place*	*Insufficient legislation in place*
Kiribati	*Partial legislation in place*	*Insufficient legislation in place*
Lesotho	*No information available*	
Malawi	*No information available*	

[9] Explanation:

- Legislation in place - to a large extent these provisions have been implemented in domestic legislation
- Partial legislation in place – some provisions are missing or unclear provisions
- Insufficient legislation/insufficient investigative powers – major gaps are indentified
- No legislation in place – the legal framework is lacking provisions to deal with these types of crimes

Country	Substantive Law Provisions Article 1 – Definitions Article 2 - Illegal Access Article 3 - Illegal interception Article 4 - Data interference Article 5 - System interference Article 6 - Misuse of device Article 7 - Computer - related forgery Article 8 - Computer - related fraud Article 9 - Child pornography offence	Procedural Law Provisions Article 16 - Expedited preservation of stored computer data Article 17 - Expedited preservation and disclosure of traffic data Article 18 - Production order Article 19 - Search and seizure Article 20 - Collection in real-time of traffic data Article 21 - Interception of content data
Malaysia	*Legislation in place*	*Legislation largely in place*
Maldives	*The legal framework is to be reviewed with the support of the Council of Europe and CCI*	
Malta	*Legislation in place*	*Information to be completed*
Mauritius	*Legislation in place*	*Legislation in place*
Mozambique	*No information available*	
Namibia	*Draft Bill (Sep 2010) includes substantive law provisions*	*Draft Bill (Sep 2010) does not include specific procedural law provisions*
Nauru*	*No legislation in place*	
New Zealand	*Legislation in place (review under consideration in view of acceding to the Cybercrime Convention)*	
Nigeria	*Draft law (following the Budapest Convention) is under consideration*	
Pakistan	*Draft law (following the Budapest Convention) is under consideration*	
Papua New Guinea	*No legislation in place*	
Rwanda	*No information available*	
St Kitts and Nevis*	*No information available*	
St Lucia	*No information available*	
Saint Vincent and the Grenadines	*Legislation in place*	*Legislation in place*
Samoa	*Partial legislation in place*	*Insufficient investigative measures*
Seychelles	*No information available*	
Sierra Leone	*No information available*	
Singapore	*Legislation in place*	*Legislation largely in place (more information would be needed to assess possible gaps)*
Solomon Islands	*No legislation in place*	
South Africa	*Partial legislation in place*	*Insufficient investigative measures*
Sri Lanka	*Legislation in place*	*Legislation largely in place*
Swaziland	*No information available*	
Tanzania	*No legislation in place*	
Tonga	*Legislation in place*	*Legislation largely in place*
Trinidad and Tobago	*Legal framework under review*	
Tuvalu*	*No legislation in place*	
Uganda	*Legislation largely in place (not clear about computer-related forgery)*	*Legislation largely in place*
United Kingdom	*Legislation in place*	*Legislation in place*
Vanuatu	*No legislation in place*	
Zambia	*Partial legislation in place*	*Partial legislation in place*

3 Commonwealth countries and the Cybercrime Convention: preliminary conclusions

3.1 The value of the Budapest Convention

The Budapest Convention has reinforced a process of legislative reform worldwide[10]. In particular, there has been significant progress since 2006[11]. The Convention has served as a guideline, and many countries, including from the Commonwealth, have used it when preparing domestic legislation.

The Budapest Convention on Cybercrime requires states to criminalise conduct such as illegal access, data and system interference, child pornography and other offences in their domestic legislation, and to provide their law enforcement authorities with effective tools to investigate cybercrime and collect electronic evidence.

In this respect, conditions and safeguards regarding investigative powers are to be put in place to ensure due process and protect fundamental rights. Countries should also consider data protection regulations to protect the rights of individuals, to facilitate international law enforcement cooperation and to enable e-commerce and out-sourcing of services. There is a tendency in some model laws promoted in different regions to ignore this crucial element. This creates a serious risk that a government will have difficulty striking the appropriate balance between its obligation to protect people against cybercrime and its obligation to protect the fundamental rights of citizens subjected to a criminal investigation[12].

The United Nations General Assembly[13] recommended that UN member states use existing frameworks, including the Budapest Convention to "ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime".

With the Budapest Convention on Cybercrime an instrument providing guidance is already available and widely used by countries of all regions of the world as a benchmark, as recommended by the UN General Assembly (Resolution A/RES/64/211).

The initiative of negotiating a new treaty is highly controversial, mainly because this would absorb valuable resources, disrupt reforms already underway in many countries, create years of uncertainty and impede the provision of technical assistance. It may lead to more international division and less cooperation and, eventually, the end product may reach a lower standard and be less effective than the Budapest Convention. Technical assistance on legislation and enforcement based on the Budapest Convention will be more valuable more quickly to more countries than the alternatives

Therefore, countries in different regions of the world should make use of the Budapest Convention when reforming their legislation and consider accession to this treaty. International

[10] An Article on "The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web" by Alexander Seger is available at:
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf

[11] In 2006, the Council of Europe launched its Global Project on Cybercrime that assists countries in the implementation of the Budapest Convention.

[12] A report dealing with the implementation of Article 15, which includes the examples of Croatia, the Netherlands and the USA, is available at:
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

[13] UN General Assembly Resolutions A/C.2/64/L.8/Rev.1/20 Nov 2009 and A/RES/64/211/March 2010 on Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical infrastructures.

and bilateral donors should provide technical assistance to countries that require support in the implementation of this agreement.

In 2011, following the meeting of Commonwealth Law Ministers, Attorneys General from Canada, the United States, the United Kingdom, New Zealand and Australia met in Sydney to develop an action plan to address the significant and growing issue of cybercrime. In the Quintet of Attorneys General - Action Plan to Fight Cyber Crime (2011), in connection with the Cybercrime Convention, Attorneys General concluded that all Quintet countries should

> ***"take steps to become parties to the Convention;*** *consider how the Convention can assist Quintet countries to share information and help to solve practical issues; and promote the Convention as the key international instrument for dealing with cybercrime and use the Convention as a basis for delivering capacity building and awareness raising activities".*

3.2 No need for regional approaches

The participants in the workshop on cybercrime legislation for Pacific countries (Nuku'alofa, Tonga, 27-29 April 2011) concluded that:

- *Given the example of Tonga as well as the guidance of the Budapest Convention and the Commonwealth Model Law,* ***participants did not see the need for the preparation of a regional model law.***[14] ***On the contrary, they considered that the preparation of a regional model law would cause unnecessary delays and disrupt the reforms already underway in some of the countries.***

- *To consider the Budapest Convention on Cybercrime (Convention) as providing a guideline for cybercrime legislation in line with international standards, and to further note the existence of the Computer Crimes Act 2003 (Tonga) and related Acts as a good example for the Pacific region of implementation of the Convention's provisions.*

3.3 Capacity building and enforcement of law

Adequate legislation is a prerequisite for fighting cybercrime. Without legislation in place an investigation cannot even start. However, important elements need to complete the legal framework in order for it to be effective (e.g., training for all criminal justice officials to deal with electronic evidence; inter-agency cooperation; cooperation with the private sector; preserving the integrity of electronic data and ensuring its admissibility in court etc.[15]).

Some countries, such as Tonga, Barbados, Botswana, Cameroon and Saint Vincent and the Grenadines have a good level of implementation of international standards - the Cybercrime Convention and the Commonwealth Model Law. However, the need clearly remains for additional support to enforce legislation and strengthen capacities (law enforcement and judicial training; the creation of high-tech crime units and forensic capabilities) to investigate and prosecute cybercrime.

3.4 Commonwealth states make use of the Budapest Convention

The present report shows that Commonwealth states have made use of the Budapest Convention on Cybercrime and/or Commonwealth Model Law as follows:

[14] It would seem that workshop on cybercrime held by the International Telecommunication Union in Vanuatu in March 2011 had proposed such an approach
[15] See Appendix 1: Council of Europe's approach

- 4 Commonwealth countries (Australia, Cyprus, Malta and United Kingdom) are Parties to the Convention and 2 others (Canada and South Africa) have signed the Convention
- Antigua and Barbuda, Barbados, Botswana, Cameroon, Ghana, India, Jamaica, Kenya, Kiribati, Malaysia, Maldives, Mauritius, Namibia, New Zealand, Nigeria, Pakistan, St Vincent and the Grenadines, Samoa, Sri Lanka, Tonga, Trinidad and Tobago, Uganda, and Zambia have made use of the Budapest Convention/Commonwealth Model Law and/or expressed an interest in becoming a Party to the Convention
- At this point, 16 Commonwealth countries (Antigua and Barbuda, Barbados, Botswana, Brunei Darussalam, Cameroon, Ghana, India, Jamaica, Malaysia, Mauritius, New Zealand, Saint Vincent and the Grenadines, Singapore, Sri Lanka, Tonga, Trinidad and Tobago) – based on a preliminary analysis of available information – seem to have legislation (draft or in force) that is largely consistent with the standards of the Budapest Convention. These countries could submit a request for accession. Their accession and the completion of the ratification process by Canada and South Africa could increase the number of Commonwealth countries able to use the Convention as a framework for international cooperation to 22 and the total number of Parties to 56[16]
- Other Commonwealth countries would require minimal improvement to achieve compatibility. The Commonwealth Working Group could recommend targeted assistance for these countries
- Nauru, Papua New Guinea, Solomon Islands, Tuvalu, Vanuatu have no legislation in place. The intention is to prepare a law based on the law of Tonga and the Budapest Convention
- The Bahamas, Bangladesh, Brunei Darussalam, Fiji, Singapore did not use the Convention nor the Commonwealth Model Law
- No information is available for Belize, Dominica, Mozambique, Rwanda, St Kitts and Nevis, St Lucia, Seychelles, Sierra Leone, Swaziland, the Gambia, Grenada, Guyana, Lesotho and Malawi
- The Council of Europe has engaged in cooperation activities with 39 countries out of 54 Commonwealth countries.

3.5 Budapest Convention – framework for harmonised international cooperation against cybercrime

3.5.1 Mutual Legal Assistance in the Commonwealth[17]

There are three informal schemes in which member states can choose to participate and which aim to facilitate the provision of mutual legal assistance between countries.

- The Harare scheme, currently being updated, provides for the giving of assistance by the competent authorities of one country (the requested country) in respect of criminal matters arising in another country (the requesting country).
- The London Scheme for Extradition within the Commonwealth governs the extradition of a person from the Commonwealth country in which the person is found, to another Commonwealth country, in which the person is accused of an offence.
- The Scheme for the Transfer of Convicted Offenders enables a sentenced offender to be transferred from the sentencing country to another country (the administering country) in order to serve the remainder of his sentence.

[16] Eight countries (Argentina, Chile, Costa Rica, Mexico, Morocco, Panama, Philippines and Senegal) requested accession and have been invited to accede to the Budapest Convention

[17] Source: the Commonwealth's website: http://www.thecommonwealth.org/Internal/190714/190928/international_agreement_between_countries/

The Commonwealth Network of Contact Persons has been set up with the aim of providing an initial point of contact in a country for those seeking mutual legal assistance to approach to gain informal advice on how to initiate a formal mutual legal assistance request, and the requirements which must be fulfilled to do so. The Network comprises at least one contact person from each of the jurisdictions of the Commonwealth.

Other informal channels or conventions might be relevant, as they include Commonwealth countries. For instance:

- Hemispheric Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition of the Organization of American States (OAS).[18] This Network has been under development since 2000, when the Third Meeting of the Ministers of Justice or of Ministers or Attorney Generals of the Americas decided to increase and improve the exchange of information among member States of the OAS in the area of mutual assistance in criminal matters.
- Inter-American Convention on Mutual Assistance in Criminal Matters (ratified by Antigua and Barbuda, Bahamas, Canada, Grenada, Guyana, Jamaica and Trinidad and Tobago)
- Inter-American Convention on Extradition (ratified by Antigua and Barbuda and St. Lucia)

Over the years, several multilateral treaties have been drafted that deal with mutual legal assistance. In addition, many states have entered into bilateral treaties on mutual legal assistance.

There is the possibility that, in a given situation, two or more treaties on criminal matters are applicable or, on the contrary, that no international or bilateral agreements are available to engage in cooperation. This renders cooperation against cybercrime, including mutual legal assistance, inefficient and unpredictable.

3.5.2 International cooperation in Chapter III of the Budapest Convention

Cybercrime continues to be on the rise, putting at risk the security of citizens, governments and businesses worldwide that rely on information technologies. Valid concerns are expressed by many countries in this respect and effective international cooperation is vital. At the same time, important progress has been made. Many States have adopted relevant legislation, improved their criminal justice capabilities, begun to engage in more efficient international cooperation and joined agreements such as the Budapest Convention on Cybercrime.

Chapter 3 of the Budapest Convention consists of provisions on international cooperation that include general principles related to extradition, mutual legal assistance, spontaneous information etc., as well as specific measures e.g. expedited preservation of stored computer data, the expedited disclosure of preserved computer data, mutual assistance regarding accessing stored computer data, trans-border access to stored computer data, mutual assistance in the real-time collection of traffic data, mutual assistance regarding interception of content data, 24/7 points of contact.

The Budapest Convention on Cybercrime is thus comprehensive, not only in terms of its substantive law and procedural law but also with regard to international cooperation. It

[18] Members: Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia (Plurinational State of), Brazil, Canada, Chile, Colombia, Costa Rica, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, St Kitts and Nevis, St Lucia, St Vincent and the Grenadines, Suriname, Trinidad and Tobago, United States, Uruguay and Venezuela (Bolivarian Republic of)

combines the traditional mutual assistance regime with urgent measures to allow efficient cooperation, and it follows the principle of subsidiarity; that is, that existing bi- or multilateral agreements may be used first before resorting to the provisions of the Convention on Cybercrime.

3.5.2.1 General principles for international co-operation

Article 23 establishes three principles for international co-operation:

1. International co-operation is to be provided among Parties "to the widest extent possible." This principle requires Parties to provide extensive co-operation to each other, and to minimise impediments to the smooth and rapid flow of information and evidence internationally.

2. Co-operation is to be extended to all criminal offences related to computer systems and data as well as to the collection of evidence in electronic form related to any criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g. a murder) involves electronic evidence, the terms of Chapter III are applicable.

3. Co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws." The latter clause establishes the general principle that the provisions of Chapter III do not supersede the provisions of international agreements on mutual legal assistance and extradition, reciprocal arrangements as between the parties thereto (described in greater detail in the discussion of Article 27 below), or relevant provisions of domestic law pertaining to international co-operation.

3.5.2.2 General principles related to extradition

Principles related to extradition are covered by Article 24, which contains a number of sub-provisions and requires Parties to make the cybercrime offences of the Convention (articles 2-11) extraditable. At the same time, it establishes thresholds so that not every offence is extraditable per se.

Article 24 also refers to other international or bilateral agreements on extradition and stipulates that in cases where an extradition is refused because of the nationality of the offender (many countries do not extradite their own nationals) the principle of "aut dedere aut judicare" (extradite or prosecute) applies.

3.5.2.3 General principles related to mutual legal assistance

Article 25 repeats some of the general principles of Article 23, namely that cooperation is to be provided for to the widest extent possible and that the obligation to co-operate not only refers to cybercrimes as such but also to traditional offences involving electronic evidence. It states that - where such treaties are available - applicable mutual legal assistance treaties, laws and arrangements shall be used for this purpose.

Parties to the Convention furthermore need to establish a national legal basis to carry out the specific measures in articles 29 to 35 of the Convention. Paragraph 3 of this article is aimed at accelerating the process of obtaining a response to a mutual assistance request so that critical information or evidence is not lost. It empowers the Parties to make urgent requests for co-operation through expedited means of communications, rather than through the traditional,

much slower transmission of written, sealed documents through diplomatic pouches or mail delivery systems. Paragraph 3 also requires the requested Party to use expedited means to respond to requests in such circumstances. Each Party is required to have the ability to apply this measure if its mutual assistance treaties, laws or arrangements do not yet provide so.

Paragraph 4 sets forth the principle that mutual assistance is subject to the terms of applicable mutual assistance treaties (MLATs) and domestic laws. These regimes usually provide safeguards for the rights of persons located in a state party in the event of a request for mutual assistance being made to that state. For example, it may be that an intrusive measure, such as search and seizure, will not be executed on behalf of a requesting Party, unless the requested Party's fundamental requirements for such a measure, as applicable in a domestic case, have been satisfied. Parties may also ensure protection of rights of persons in relation to items seized and provided through mutual legal assistance.

Paragraph 5 is essentially a definition of dual criminality for purposes of mutual assistance under this Chapter. Where the requested Party is permitted to require dual criminality as a condition to the providing of assistance, dual criminality shall be deemed to be present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws. This is the case even if its laws place the offence within a different category of offence or use different terminology in denominating the offence.

Countries that are Parties to the Convention are required to have criminalised the conduct defined in Articles 2 to 11 (illegal access, data interference, child pornography etc.) and thus the condition of dual criminality can therefore be considered as having been met.

3.5.2.4 Mutual legal assistance in the absence of applicable international agreements

The previous provisions of the Convention on international co-operation made extensive reference to the use of existing agreements. In fact, European countries agree a large number of such treaties as well as bilateral agreements. However, non-European countries increasingly become Parties to the Convention on Cybercrime and these countries are not necessarily acceding to other treaties on co-operation in criminal matters. In such situations Article 27 provides the basics for mutual legal assistance between countries that have no other legal agreement.

3.5.2.5 Specific provision: expedited preservation of stored computer data

The expedited preservation of stored computer data is necessary at both the national (article 16) and the international level. This is provided for in Article 29 of the Convention.

A Party receiving a request is obliged to act very quickly in order to have data preserved. The condition of dual criminality only applies in exceptional circumstances. It is important to underline that this is only a provisional measure through which data is preserved, mostly at the level of the Internet service provider. The actual disclosure of information is a subsequent step that may require a mutual legal assistance request.

3.5.2.6 Specific provision: expedited disclosure of preserved traffic data

As data often transits several countries, it is often not sufficient to order the preservation of traffic data in one country. Instead, the data must be preserved in all countries or on all servers involved in the chain. Therefore, a service provider must disclose sufficient information so that the path through which a communication was transmitted can be identified and the preservation of further data be ordered. This is provided for in Article 30 of the Convention (which is the equivalent to the partial disclosure provision under Article 17 at the national level).

3.5.2.7 Specific provision: mutual assistance regarding accessing of stored computer data

Article 31 allows a Party to request another Party to access, seize and disclose data stored on a computer system on its territory. This article also provides for expedited responses to requests.

3.5.2.8 Specific provisions: mutual assistance for the interception of data

Two provisions relate to the interception of data, namely Article 33, which covers the real-time collection of traffic data, and Article 34, which is about the interception of content data. Of course, as the interception of content data represents a high level of intrusion, mutual assistance in this respect is restricted and subject to safeguards, other applicable treaties and domestic law.

3.5.2.9 Specific provision: the network of 24/7 points of contact

In order to facilitate urgent action, and in particular the expedited preservation of data in another country, a network of 24/7 points of contact has been established under Article 35 of the Convention. Each Party is required to establish a point of contact for co-operation in urgent cases. This point of contact supplements and does not replace other existing channels of co-operation.

3.5.3 Relevant work on international cooperation carried out by the Cybercrime Convention Committee (T-CY)

The Cybercrime Convention Committee (T-CY), at its 6th plenary session (23-24 November 2011), decided to establish an ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows. During its 8th Plenary (5-6 December 2012) a report was adopted.[19] Furthermore, the Committee decided to extend the Terms of Reference of the Transborder Group to 31 December 2013 with the following tasks:

- Preparation of a Guidance Note on Article 32 of the Budapest Convention, including a consultation with private sector entities. A draft should be prepared for discussion at the 9th Plenary of the T-CY in mid-2013 and a hearing of private sector entities could be held on that occasion. The Guidance Note should then be submitted for adoption to the 10th Plenary before 31 December 2013.
- Submission by June 2013 for approval by the T-CY of a draft Mandate of the Committee of Ministers tasking the T-CY to prepare an Additional Protocol. The Group should at that point provide further elements regarding the possible content and scope of such a Protocol.
- Pending the Mandate by the Committee of Ministers, preparation of a first draft text of a possible Protocol for discussion by the 10th Plenary of the T-CY before 31 December 2013.
- The T-CY decided to invite Japan to provide an expert to join the Transborder Group, and to open up the work of the Group to representatives of other Parties to the Convention who may wish to participate in its meetings. Additional experts may be invited case by case.

The Committee adopted in principle the Assessment Report of articles 16, 17, 29 and 30 of the Budapest Convention (measures on expedited preservation of stored computer data and disclosure of traffic data at domestic and international level).

[19] Available at:
http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

Furthermore, it was decided to assess in 2013 implementation by the Parties of the following provisions on international cooperation:

- Article 31 – Mutual assistance regarding accessing of stored computer data
- Article 23 – General principles relating to international co-operation
- Article 25 – General principles relating to mutual assistance
- Article 26 – Spontaneous information
- Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Commonwealth countries	Party/Signatory/ Country invited to accede to the Budapest Convention	Participated in the CoE capacity building activities	Does state's cybercrime legislation consider the Budapest Convention (BC) and/or Commonwealth Model Law (CML)?
1. Antigua and Barbuda	no	yes	Yes (some provisions are copied)
2. Australia	Invited in 2010 and acceded on 30 November 2012	yes	Yes See also: Quintet of Attorneys General
3. The Bahamas	no	yes	-
4. Bangladesh[20]	no	yes	-
5. Barbados	no	yes	Yes (reproduction of CML complemented with provisions from BC)
6. Belize	no	-	-
7. Botswana	no	yes	Yes (sources used: CML, BC and legislation of Mauritius, South Africa and India)
8. Brunei Darussalam	no	yes	-
9. Cameroon	no	yes	Yes (follows the standards of BC and includes additional provisions)
10. Canada	Signed on 23 Nov 2001	yes	Yes (amendments in the Parliament to ratify the BC) See also: Quintet of Attorneys General
11. Cyprus	Signed on 23 Nov 2001 Ratified on 19 Jan 2005	yes	Yes (Party; substantive law provisions copied from BC)
12. Dominica	no	-	-
13. *Fiji Islands*[21]	no	yes	-
14. The Gambia	no	-	-
15. Ghana	no	yes	Yes (some provisions copied from CML; law to be reviewed with the assistance of CCI)
16. Grenada	no	-	-
17. Guyana	no	-	-
18. India	no	yes	Yes (assistance provided by the CoE; recommendations made were included in the law adopted in 2008

[20] (*) Italics indicates countries which are not currently members of the Commonwealth Foundation
[21] Following the decisions taken by the Commonwealth Ministerial Action Group on 31 July 2009, Fiji Islands was suspended from membership of the Commonwealth on 1 September 2009

19. Jamaica	no	yes	Yes (some provisions seem to be inspired by BC; other legislation might have been used)
20. Kenya	no	yes	Yes (CML, BC and other legislation)
21. Kiribati	no	yes	Yes (CML, BC and other legislation)
22. Lesotho	no	-	-
23. Malawi	no	-	-
24. Malaysia	no	yes	Yes (CML, BC and other legislation)
25. Maldives	no	yes	Yes (requested CoE's assistance on legislation)
26. Malta	Signed on 17 Jan 2002 Ratified on 12 April 2012	yes	Yes (Party; BC)
27. Mauritius	no	yes	Yes (BC and other legislation)
28. Mozambique	no	-	-
29. Namibia	no	-	Yes (some provisions)
30. *Nauru**	no	yes	Intention to prepare law based on law of Tonga and BC
31. New Zealand	no	yes	See: Quintet of Attorneys General
32. Nigeria	no	yes	yes
33. Pakistan	no	yes	Yes
34. Papua New Guinea	no	yes	Intention to prepare law based on law of Tonga and the BC
35. Rwanda	no	-	-
*36. St Kitts and Nevis**	no	-	-
37. St Lucia	no	-	-
38. St Vincent and the Grenadines	no	yes	yes
*39. Samoa**	no	yes	yes
40. Seychelles	no		-
41. Sierra Leone	no		-
*42. Singapore**	no	yes	UK Computer Misuse Act
43. Solomon Islands	no	yes	Intention to prepare law based on law of Tonga and the BC
44. South Africa	Signed on 23 Nov 2001	yes	yes
45. Sri Lanka	no	yes	yes
46. Swaziland	no	-	-
47. Tanzania	no	yes	-
48. Tonga	no	yes	yes
49. Trinidad and Tobago	no	yes	yes
50. *Tuvalu**	no	yes	Intention to prepare law based on law of Tonga and the BC
51. Uganda	no	yes	Yes (some provisions copied from BC and CML;

			comments provided by the CoE during the drafting)
52. United Kingdom	Signed on 23 Nov 2001 Ratified on 25 May 2011	yes	Yes See also: Quintet of Attorneys General
53. *Vanuatu**	no	yes	Intention to prepare law based on law of Tonga and the BC
54. Zambia	no	yes	Yes (some provisions)

4 Country synopses

4.1 Antigua and Barbuda

4.1.1 Relevant legislation

- The draft Computer Misuse Act 2006
- The Forgery Act
- The Evidence (Special Provisions) Act 2009

4.1.2 Definitions

- "computer"; "computer contaminant"; "computer network"; "computer output"; "computer service"; "computer system"; "damage"; "data"; "electronic, acoustic, mechanical or other device"; "function"; "intercept"; "program or computer program".

4.1.3 Substantive law

The draft Computer Misuse Act seems to be inspired by the Convention on Cybercrime (CETS no 185) and includes additional offences e.g. identity theft (Section 14), unauthorised disclosure of access code (Section 8), unauthorised access to computer data.

Offences:

- Unauthorised access to computer program or data
- Unauthorised receiving or giving access to computer program or data
- Unauthorised use or interception of computer service
- Unauthorised obstruction of use or use of computer
- Causing a computer to cease to function
- Denial of service attacks
- Illegal devices
- Unauthorised disclosure of access code

4.1.4 Procedural law

Definitions for procedural law, being Section 23 (Production of data), Section 22 (Record of and access to seized data), Section 24 (Disclosure of stored traffic data), Section 25 (Preservation of data), Section 26 (Interception of electronic communications) and Section 27 (Interception of traffic data) **are copied from the Commonwealth Model Law,** namely from: Definitions for this Part: 14 (Record of and access to seized data), 15 (Production of data), 16 (Disclosure of stored traffic data), 17 (Preservation of data), 18 (Interception of electronic communication) and 19 (Interception of traffic data).

4.1.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

- The definitions of the terms "*computer*", "*computer system*", "*computer network*", "*data*" "*program or computer program*" are clearly inspired from the Convention, its Explanatory Report and the Commonwealth Model Law.
- The conduct criminalised follows the same structure as the above-mentioned documents (illegal access, interception, data interference, system interference etc.).

- The wordings used in some of the offences e.g. Section 7 (unauthorized obstruction of use or use of computer) Section 11 (Causing a computer to cease to function) - seem to consider Section 6 (Interfering with data) or Section 7 (Interfering with computer system) of the Commonwealth Model Law.
- Section 13 (Illegal devices) is copied from the Commonwealth Model Law.
- The omission of provisions on computer-related offences (fraud and forgery) indicates that Commonwealth Model Law was the main guide used in drafting the legislation.
- Section 12 (Child pornography) is copied from the Commonwealth Model Law (Section 10), including definitions of terms "child pornography", "minor" and "publish".
- Procedural law provisions largely inspired from the Commonwealth Model Law (see above).

4.1.6 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 3.

4.1.7 Cooperation with the Council of Europe: Yes

- Global Project on Cybercrime Phase 1

    - OAS/USDOJ regional workshop on legislation in the Caribbean region (13-15 May 2008, Port of Spain, Trinidad and Tobago)

4.2 Australia

4.2.1 Relevant legislation

- Criminal Code Act No 12 of 1995 as amended in 2012
- Crimes Act No 12 of 1914 as amended in 2012
- Mutual Assistance in Criminal Matters Act No. 85 of 1987 as amended in 2012
- Telecommunication (Interception and Access) Act No 114 of 1979 as amended in 2012

4.2.2 Definitions

- "access to data held in a computer", "Commonwealth computer", " data", "data held in a computer", "data storage device", "electronic communication", " unauthorized access", "modification or impairment"

4.2.3 Substantive law

Offences:

- Unauthorised modification of data to cause impairment
- Unauthorised access, modification or impairment with intent to commit a serious offence
- Unauthorised access to, or modification of, restricted data
- Interception of a communication
- Interfering with, or interrupting or obstructing the lawful use of, a Commonwealth computer
- Destroying, erasing or altering data stored in, or inserting data into a computer
- Producing, supplying or obtaining data with intent to commit a computer offence
- Manufacturing etc. a circumvention device for a technological protection measure
- Forgery, using a forged document and possession of forged document
- Fraudulent conduct
- Using a carriage service for child pornography material
- Possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service
- Unauthorised use of copies or information
- Removal or alteration of electronic rights management information
- Distribution to the public etc. of works whose electronic rights management information has been removed or altered
- Commercial-scale infringement prejudicing copyright owner
- Making infringing copy commercially
- Commercial-scale infringement prejudicing copyright owner

4.2.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Australia was invited to accede in 2010 and became Party to the Budapest Convention on 30 November 2012.

On 22 August 2012, the Cybercrime Legislation Amendment Bill 2011 passed the Australian Senate. The Cybercrime Legislation Amendment Bill 2011 amends the Mutual Assistance in Criminal Matters Act 1987, the Criminal Code Act 1995, the Telecommunications (Interception

and Access) Act 1979 and the Telecommunications Act 1997. The Bill was intended to ensure that Australian legislation is consistent with international best practice and to enable domestic agencies to access and share information to facilitate international investigations. It allowed Australia to accede to the Council of Europe Convention on Cybercrime.

The official position expressed by the Attorney General of Australia[22] is that Australia desires to become "*an active member of this Convention simply because the modern ever-changing world demands it*".

In the Quintet of Attorneys General, Australia agreed on the Action Plan that concluded that all Quintet countries should take steps to become parties to the Convention; to promote the Convention as the key international instrument for dealing with cybercrime; and use the Convention as a basis for delivering capacity building and awareness raising activities.

4.2.5 Country profile available: Yes

Country profile updated under the Global Project on Cybercrime Phase 2

4.2.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
  - Participation in AUSCERT cybercrime conference and meetings with Australian authorities (18-21 May 2008, Brisbane, Australia)
- Global Project Phase 2
  - Pacific Islands Workshop on cybercrime legislation (27-29 April 2011, Tonga)
  - Participation in the Octopus Conference in 2011 (high level representation) and in 2012

[22] Speech delivered by Robert McClelland, Attorney General, Australia during the special meeting Budapest Convention - 10th anniversary (Strasbourg, 23 November 2011) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Presentations/default_en.asp

4.3 Bahamas

4.3.1 Relevant legislation

- Computer Misuse Act of 2003
- Penal Code of 1926
- Electronic Communications and Transactions Act of 2003

4.3.2 Definitions

- "computer"; "computer output" or "output"; "computer service"; "damage"; "data"; "electronic, acoustic, mechanical or other device"; "function"; "intercept".

4.3.3 Substantive law

Offences:

- Unauthorized access to computer material
- Access with intent to commit or facilitate commission of offence
- Unauthorised modification of computer material
- Unauthorised use or interception of computer service
- Obstruction of use of a computer
- Publication of obscenity

4.3.4 Procedural law

With the exception of search and seizure, the investigative measures provided by the Computer Misuse Act and the Electronic Communications and the Transactions Act do not seem to provide law enforcement adequate powers to prosecute cybercrime.

Overall, the existing provisions are insufficient and reflect only partially the standards of the Convention on Cybercrime/ Commonwealth Model Law. A legal review could be considered in view of amending the legislation.

4.3.5 Country profile available: Yes

Country profile prepared within the Global Project Phase 3.

4.3.6 Cooperation with the Council of Europe: Yes

- Global Project on Cybercrime Phase 1
    - OAS/USDOJ regional workshop on legislation in the Caribbean region, 13-15 May 2008, Port of Spain, Trinidad and Tobago

4.4 Bangladesh

4.4.1 Relevant legislation

- The Information and Communication Technology Act of 2006

4.4.2 Definitions

- "access", "act", "computer network", "computer resource", "data", "electronic form", "electronic record", "information", "law", "offence", "computer database", "computer virus", "damage"

4.4.3 Substantive law

Penalty for damage to computer, computer system, etc.

- If any person, without permission of the owner or any person who is in charge of a computer, computer system or computer network,
  - accesses or secure access to such computer, computer system or computer networks for the purpose of destroying information or retrieving or collecting information or assists other to do so;
  - downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
  - introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
  - damages or causes to be damaged willingly in any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;
  - disrupts or causes disruption of any computer, computer system or computer network;
  - denies of causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
  - provides any assistance to any person to facilitate access to a computer, computer system or computer network, in contravention of the provisions of this Act, rules or regulations made thereunder;
  - for the purpose of advertisement of goods and services, generates or causes generation of spams or sends unwanted electronic mails without any permission of the originator or subscriber;
  - charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network;

then the above said activities shall be treated as offences of the said person.

- Tampering with computer source code
- Hacking with computer system
- Publishing fake, obscene or defaming information in electronic form
- Failure to surrender licence
- Failure to comply with order
- Failure to comply with order made by the Controller in emergency
- Unauthorized access to protected systems
- Misrepresentation and obscuring information
- Disclosure of confidentiality and privacy
- Publishing false Digital Signature Certificate

- Publishing Digital Signature Certificate for fraudulent purpose etc.
- Using computer for committing an offence

4.4.4 Procedural law

Overall, the existing provisions seem to be insufficient to tackle cybercrime. A legal review could be considered in view of amending the legislation.

4.4.5 Country profile available: Yes

Country profile updated within the Global Project Phase 3.

4.4.6 Cooperation with the Council of Europe: Yes

- Global Project on Cybercrime Phase 2
    - Cooperation against cybercrime in South Asia International workshop (Colombo, Sri Lanka, 5-6 April 2011)

4.5 Barbados

4.5.1 Relevant legislation

- Computer Misuse Act of 2005
- Mutual Assistance in Criminal Matters Act, Cap. 140A of 1993
- Extradition Act, Cap 189 of 1985

4.5.2 Definitions

- "computer system", "computer data", "service provider", "traffic data"

4.5.3 Substantive law

Offences:

- Illegal access
- Illegal interception
- Interfering with data
- Interfering with computer systems
- Illegal devices
- Access with the intention to commit an offence
- Child pornography

4.5.4 Procedural law

The procedural law provisions are partially implemented. It is not clear if there are any correspondent provisions for collection of traffic data and interception of content data. Furthermore, the preservation of computer data is possible only for a period of 14 days, extendable once for a further 14 days. This time limit on preservation may be too short to be effective, particularly if an MLA request is required. Article 16 of the Convention provides for a period of 90 days, which may be renewed.

- Preservation of data for criminal proceedings
- Order for disclosure of data
- Search and seizure

4.5.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Section 3 of the *Computer Misuse Act, 2005* defines the same terms provided by Article 1 of the Cybercrime Convention ("computer system", "computer data", "service provider", "traffic data").

Overall, the Computer Misuse Act is a reproduction of the Commonwealth Model Law. In addition, although the Commonwealth Model Law does not include computer-related offences, the Computer Misuse Act criminalises in Section 9 the use of a computer to commit an offence involving property, fraud or dishonesty. It is therefore also largely in line with the Budapest Convention.

4.5.6 Country profile available: Yes

Country profile updated within Global Project Phase 3.

4.5.7 Cooperation with the Council of Europe: Yes

- Global Project on Cybercrime Phase 1

    - OAS/USDOJ regional workshop on legislation in the Caribbean region, 13-15 May 2008, Port of Spain, Trinidad and Tobago

4.6 Botswana

4.6.1 Relevant legislation

- Chapter 08:06 Cybercrime and Computer Related Crimes of 2007
- Mutual Assistance in Criminal Matters Act of 1990
- Extradition Act 1990

4.6.2 Definitions

- "access", "computer data storage medium", "computer service", "computer or computer system", "data", "electronic", "function", "information and communication service", "information and communication technology", "intercepts", "national emergency organisations", "password", "programme", "property", "service provider", "traffic data", "underlying service".

4.6.3 Substantive law

Offences:
- Unauthorised access to a computer or computer system
- Unauthorised access to computer service
- Unauthorised interference with data
- Unauthorised interference with a computer or computer system
- Unlawful possession of devices or data
- Cyber fraud
- Electronic traffic in pornographic or obscene material

4.6.4 Procedural law

In relation with procedural law - the measures established by the Cybercrime and Commonwealth Model Law - the legislation is complete with some elements to be considered in future amendments (e.g. the duration for preservation of computer data has yet to be determined). A review of the existing legislation with regard to admissibility of electronic evidence is under consideration.

- Preservation order
- Disclosure of preserved data
- Production order
- Access, search and seizure
- Real-time collection of traffic data
- Unlawful disclosure by service provider

4.6.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

A number of definitions - "computer data storage medium", "computer or computer system", "service provider", "traffic data" - are taken from the Commonwealth Model Law.

The wording used in the law seems to be inspired mainly by the Commonwealth Model Law (some articles are copied) and complemented with provisions from the Budapest Convention (e.g. unauthorised interference with data includes acts such as deleting, suppressing or modifying data,

and computer fraud). Additional provisions from other Commonwealth countries such as Mauritius, South Africa and India[23] have been also considered.

The Cybercrime and Computer Related Crimes Act is largely in line with the Commonwealth Model Law and the Budapest Convention although some provisions could be improved in the future. The main problem identified is the overlapping of some provisions, which results in the criminalisation of the same acts under different provisions that carry different penalties.

4.6.6 Country profile available: Yes

The country profile prepared under the Global Project on Cybercrime Phase 2

4.6.7 Cooperation with the Council of Europe: Yes

- Octopus Conference, Cooperation against Cybercrime
  - Participation of Botswana from 2010 to 2012 (Ms Athaliah L. Molokomme, Attorney General of Botswana)
- Global Project (phase 3)
  - Capacity building against cybercrime in Botswana (Gaborone, Botswana, 14 - 15 December 2012)
- CyberCrime@IPA[24]
  - Participation of Botswana in the High-level Conference on Strategic Priorities against Cybercrime (Dubrovnik, Croatia, 13 - 15 February 2013)

[23] This is confirmed by Ms Athaliah L. Molokomme, Attorney General, Botswana in her opening address in the Octopus Conference:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus2012/Interface2012_en.asp

[24] Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp

4.7 Brunei Darussalam

4.7.1 Relevant legislation

- Computer Misuse Act of 2007
- Criminal Code of 2001
- Electronic Transaction Act of 2008
- Undesirable Publications Act

4.7.2 Definitions

- "computer", "computer output", "computer program", "computer services", "data"

4.7.3 Substantive law

The Computer Misuse Act of the State of Brunei Darussalam includes several provisions related to cybercrime.

Offences:

- Illegal access
- Illegal interception
- Unauthorised modification of computer material
- Unauthorised obstruction of use of computer
- Unauthorised disclosure of access code
- Enhanced punishment for offences involving protected computers

4.7.4 Procedural law

The legislation of Brunei Darussalam seems to be inspired by Singapore legislation (itself inspired by the UK Computer Misuse Act).

Overall, the substantive law provisions are in place, whilst the procedural law provisions might require further consideration. Updated information about possible amendments is missing.

4.7.5 Country profile available: Yes

The country profile updated under the Global Project on Cybercrime Phase 3

4.7.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
    - Workshop on legislation for ASEAN countries, 27-28 November 2008, Kuala Lumpur, Malaysia

4.8 Cameroon

4.8.1 Relevant legislation

- Cybersecurity and Cybercrime Law from 2010 (available in French)

4.8.2 Substantive law

The new Law has introduced various offences related to cybercrime covering the conduct required by the Convention to be criminalised. Some offences go beyond the minimum required by the Convention.

4.8.3 Procedural law

The Cybersecurity and Cybercrime Law has introduced specific investigative powers and obliged service providers of electronic communication to cooperate with law enforcement in cybercrime investigations. There is an obligation of data retention for 10 years (Article 25), which is excessive. Provisions on data preservation (as distinct from data retention), maintaining the integrity of seized data, and rendering it inaccessible, are missing.

Safeguards and conditions in applying the law enforcement powers should be considered.

4.8.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The Cybersecurity and Cybercrime Law (2010) follows the standards of the Convention and includes some additional provisions.

4.8.5 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 3.

4.8.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
    - Workshop for Western and Central African countries on cybercrime legislation and investigation (organised by the USODJ), 9-11 July 2008, Cotonou, Benin.
    - Organisation Internationale de la Francophonie: Pan African conference on cybercrime (18-20 November 2008, Abidjan, Ivory Coast)

4.9 Canada[25]

4.9.1 Relevant legislation

- Criminal Code of 1985
- Evidence Act 2010
- Bill C-30, An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts (tabled on 14 February 2012 before the Canadian Parliament)

Since the 1980s, Canada has responded to the challenge of cybercrime with a combination of case law developments and legislation. Where possible, existing criminal offences and investigative powers have been amended to ensure their effectiveness in cybercrime scenarios. For example, although the traditional theft offence, (section 322 of the Criminal Code) is capable of capturing most instances of "cyber" theft, Parliament enacted a specific offence for theft of telecommunications services (section 326 of the Criminal Code). Similarly, in the case of mischief, (section 430 of the Criminal Code) a subsection of the offence was created explicitly to cover "mischief to data" (subsection 430(1.1)). Where necessary, entirely new criminal offences, such as unauthorised use of a computer (section 342.1 of the Criminal Code) and investigative powers, such as production orders (sections 487.012 and 487.013 of the Criminal Code) have been enacted. In some cases changes have not been needed because the courts have decided to apply existing rules to the new environment. For example, fraud, (section 380 of the Criminal Code) is adequately capable of capturing most instances of "cyber" fraud. Similarly, with respect to jurisdiction, Canada has jurisdiction to prosecute a transnational offence if any part of it took place in Canada, including the use of Canadian service providers, websites, or other elements of digital infrastructure located in Canada.

The constant evolution of information technologies and the ways they are exploited by offenders means that new developments must always be monitored. Bill C-30 is a response to identified gaps in the capacity to prevent, investigate and prosecute crime, including cybercrime. The recent tabling of this bill also responds to the need to update federal legislation to provide law enforcement and national security agencies with the tools they need to fight crime in the 21st century both at the national or international levels.

4.9.2 Definitions

- computer password"; "computer program"; "computer service"; "computer system"; "data"; "electro-magnetic, acoustic, mechanical or other device"; "function"; "traffic".

4.9.3 Substantive law

Offences:

- Unauthorized use of a computer
- Interception of communications
- Possession of device to obtain computer service (without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence […]
- Instruments for copying credit card data or forging or falsifying a credit card
- Forgery

[25] Information provided through the replies to the questionnaire sent to the Working Group by Lucie Angers (Canada)

- Fraud
- Child pornography
- Related legislation has also been adopted in areas such as anti-spam, mandatory reporting of child pornography and the protection of personal information.

4.9.4 Procedural law

- Production order
- Information for search warrant
- Warrant of seizure
- Interception of communications

4.9.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Canada, along with the USA, Japan and South Africa, took a leading role in the elaboration of the Budapest Convention from 1998-2001 and signed it on 23 November 2001. Canada supports the Convention and has implemented most of its requirements, but has not yet ratified it pending the enactment of the last remaining requirements for conformity. The legislation is presently before Parliament.

In addition, Canada was one of the member states that participated in the drafting of the Commonwealth Model Law in 2001 and 2002. The Model Law, which is based on the Council of Europe Convention on Cybercrime, was one of the standards that was used in helping Canada to develop Bill C-30. Some elements of the Model Law were also informed by earlier Canadian legislative amendments enacted in the late 1980s. The Model Law as a whole was considered in developing Bill C-30. Canada already had legislation pertaining to procedural powers such as search and seizure and interception of private communications. However, no specific provision existed in relation to the preservation of computer data or the disclosure of traffic data.

Canada believes that Model Laws can be a very useful tool in many areas. The development of such provisions provides a good basis for the discussion of legislative issues without the pressures generated by the negotiation of binding international legal obligations. There is more latitude to include general language and to explore alternative options for different countries and justice systems, while at the same time providing a good basis for the adoption of similar or harmonised legislation in different States.

In the Quintet of Attorneys General, Canada agreed on the Action Plan that concluded that all Quintet countries should take steps to become parties to the Convention, to promote the Convention as the key international instrument for dealing with cybercrime, and use the Convention as a basis for delivering capacity building and awareness raising activities.

4.9.6 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 3.

4.9.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 2
    - Information Security Forum 20th anniversary Annual World Congress, 1-3 November, Vancouver, Canada
    - Digital Crime Consortium, 11-16 October 2010, Montreal, Canada

- Octopus Conference, Cooperation against Cybercrime and/or Cybercrime Convention Committee (T-CY)

    - Participation of Canada in 2007, 2008, 2011 and 2012

4.10 Cyprus

4.10.1 Relevant legislation

- The Cyprus Law No 22 (III) / 2004 ratifying the Convention on Cybercrime
- Law 183(I)/2007 Law on maintenance of telecommunications data for the investigation of serious crime offences

4.10.2 Definitions

- "computer system", "computer data", "service provider", "traffic data"

4.10.3 Substantive law

Offences:

- Illegal access
- Illegal interception
- Data interference
- System interference
- Computer-related forgery
- Computer-related fraud
- Child pornography
- Offences related to infringements of copyright and related rights

The Cyprus Law no 22 (III)/2004, largely covers the provisions of the Budapest Convention with the exception of Article 6 referring to misuse of devices.

4.10.4 Procedural law

Cyprus implemented data retention but not preservation order. Internet Service Providers are obliged to retain data for 6 months.

There is not yet an English translation available of the other procedural law provisions.

4.10.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Cyprus signed the Cybercrime Convention 23 November 2001 and ratified it on 19 January 2005.

Cyprus used the Convention in drafting its legislation. The definitions and substantive law provisions are copied from the Convention on Cybercrime[26].

4.10.6 Country profile available: Partial

Country profile of Cyprus was prepared under the Global Project on Cybercrime Phase 1

4.10.7 Cooperation with the Council of Europe: Yes

- Octopus Conference, Cooperation against Cybercrime
  - Participation of Cyprus from 2007 to 2010

26 http://www.coe.int/t/dqhl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_%20Cyprus_2007_June.pdf

4.11 Fiji

4.11.1 Relevant legislation

- Crimes Decree 2009 (Division 6 on Computer Offences (Ss 336 – 346)
- Criminal Procedure Decree 2009

4.11.2 Definitions

- "data", "data storage device", "electronic communication"

4.11.3 Substantive law

The 2009 Crime Decree introduces offences related to cybercrime. The Crimes Decree 2009 introduced a number of substantive law provisions in Division 6 on Computer Offences (Ss 336 – 346). It came into effect on 1 February 2010.

Offences:

- Serious computer offences
- Unauthorised access to, or modification of, restricted data
- Unauthorized impairment of electronic communication
- Possession or control of data with intent to commit a computer offence
- Producing, supplying or obtaining data with intent to commit a computer offence
- Forgery and related offences
- Traffic in obscene publications

4.11.4 Procedural law

The Crime Procedure Decree of 2009 refers only to traditional powers of investigation. Specific procedural law provisions are missing.

4.11.5 Country profile available: Yes

The country profile of the Fiji Islands was prepared within the Global Project on Cybercrime Phase 2.

4.11.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 2
    - Pacific Islands – Workshop on cybercrime legislation (27-29 April 2011, Tonga)

4.12 Ghana

4.12.1 Relevant legislation

- Electronic Transaction Act of 2008
- A comprehensive review of legislation is planned with the aim of further strengthening current laws.

4.12.2 Substantive law

Although some provisions have been in place since 2008 (see below) it appears that there has not been a single example of successful investigation and prosecution of any of these offences.

Problems related to jurisdiction are encountered when the victims are based overseas.

Offences:

- Criminal negligence
- Access to protected computer
- Obtaining electronic payment medium falsely
- Electronic trafficking
- Possession of electronic counterfeit-making equipment
- General offence of fraudulent electronic fund transfer
- General provision for cyber offences
- Unauthorised access or interception
- Unauthorised interference with electronic record
- Unauthorised access to devices
- Unauthorised circumvention
- Denial of service
- Unlawful access to stored communications
- Unauthorised access to computer programme or electronic record
- Unauthorised modification of computer programme or electronic record
- Unauthorised disclosure of access code
- Offence relating to national interest and security
- Causing a computer to cease to function
- Illegal devices
- Child pornography
- Confiscation of assets
- Order for compensation
- Ownership of programme or electronic record
- Conviction and civil claims

4.12.3 Procedural law

- Powers of law enforcement officers
- Law enforcement officer and third party assistance
- Preservation of evidence
- Contents of electronic communications in electronic storage
- Disclosure of electronic information
- Provider to keep logs and records
- Backup preservation
- Customer challenge

- Inadmissible evidence

4.12.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Although some of the articles are copied from the Commonwealth Model Law (e.g. illegal devices (135) and child pornography (136)) the law seems to be unclear and overlapping provisions may pose serious challenges to competent authorities to apply it in practice.

Ghana made a request for assistance to the Commonwealth Cybercrime Initiative. The Council of Europe is prepared to carry out a review of the cybercrime legislation.

In relation to the Budapest Convention, the Ministry of Communications noted that the government has worked on ensuring that the appropriate domestic legislation is in place, and aligned with international standards and best practise, prior to analysing the potential benefits of acceding to the Convention.

4.12.5 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 3.

4.12.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
  - Workshop for Western and Central African countries on cybercrime legislation and investigation (organised by the USODJ), 9-11 July 2008, Cotonou, Benin
  - Pan-African Conference, November 2008, Yamoussoukro, Ivory Coast
- Global Project Phase 2
  - 1st West African Internet Fraud Summit 1, 2-3 February2010, Abuja, Nigeria

4.13 India

4.13.1 Relevant legislation

- The Information Telecommunication Act of 2000, amended in 2008 (ITA)

On 22 December 2008, the Parliament of India adopted the Information Technology Act Amendment Bill 2008, which was subsequently signed by the President of India on 5 February 2009. The Government needs to adopt specific regulations to allow for the implementation of the Act

4.13.2 Definitions

- "access", "communication device", "computer", "computer network", "computer resource", "computer system", "data", "intermediary", "originator", "traffic data", "computer contaminant", "computer database", "computer virus", "damage", "computer source code"

4.13.3 Substantive law

Offences:

- Illegal access (including downloads, copies or extracts of any data, computer data base or information)
- Cyber terrorism
- Unauthorized interception
- Damage to computer, computer system, etc
- Breach of confidentiality and privacy
- Cheating by personation by using computer resource
- Publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

4.13.4 Procedural law

- Through the ITA the Indian Evidence Act also applies to electronic records
- Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security
- Preservation and retention of information by intermediaries
- Power to authorize, to monitor and to collect traffic data or information through any computer resource for cyber security.

4.13.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

In 2007/2008 the Council of Europe provided advice to India on the amendments to the Information Technology Act (IRA). Most of the proposals made were reflected in the ITA amendments adopted by the Parliament in December 2008 (shortly after the Mumbai attacks). This brought the overall legal framework in line with the Budapest Convention on Cybercrime. The ITA gives the Ministry of Communications and IT the power to issue secondary regulations. In April 2011, these included personal data protection rules ("Reasonable Security Practices and Procedures and Sensitive Personal Data Rules").

The Council of Europe and India are maintaining a dialogue regarding the possibility of India's accession to the Budapest Convention.

4.13.6 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 2.

4.13.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
  - National Conference on Cybercrime (in cooperation with ASSOCHAM), (September, 2007, New Delhi, India
- Global Project Phase 2
  - Workshop on international cooperation and law enforcement/service provider cooperation, March 26, 2009, New Delhi, India
  - 4th ASSOCHAM International Conference on Cyber and Network Security, April 1, 2011, New Delhi, India
- Global Project Phase 3
  - National conference on cybersecurity, co-organised by the Council of Europe and the Associated Chambers of Commerce and Industries (ASSOCHAM) (10 May 2012, New Delhi, India)
  - Round table on accession to the Budapest Convention (11 May 2012 , New Delhi India)
- Octopus Conference, Cooperation against Cybercrime
  - Participation of India from 2007 to 2010 and in 2012

4.14 Jamaica

4.14.1 Relevant legislation

- Cybercrimes Act 2010
- Forgery Act
- Sexual Offences Act
- Obscene Publication Act

4.14.2 Definitions

- "computer", "computer service", "damage", "data", "electronic", "electronic communication system", "function", "output", "program" or "computer program"

4.14.3 Substantive law

The Cybercrimes Act adopted in 2010 covers offences against the confidentiality, integrity and availability of computer data and systems in a manner closely resembling the Convention.

- Unauthorised access to computer program or data
- Access with intent to commit or facilitate commission of offence
- Unauthorised interception of computer function or service
- Unauthorised obstruction of operation of computer
- Unlawfully making available devices or data for commission of offence
- Offences relating to protected computers

4.14.4 Procedural law

- Preservation of data
- Search and seizure warrants
- Production orders

4.14.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Although elements of the definitions (e.g. computer, data), the structure of the Act, the type of offences and the investigative measures introduced through the Cybercrimes Act 2010 closely follow the Convention on Cybercrime, the language used could also be inspired by other legislation.

4.14.6 Country profile available: No

The country profile of Jamaica is under preparation under the Global Project on Cybercrime Phase 3.

4.14.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
    - OAS/USDOJ regional workshop on legislation in the Caribbean region, 13-15 May 2008, Port of Spain, Trinidad and Tobago

4.15 Kenya

4.15.1 Relevant legislation

- Information and Communication Act enacted in 2009
- Criminal Procedure Code of 2009

4.15.2 Definitions

- "access", "computer", "computer service", "data", "dominant telecommunications service provider", "electronic", "electronic form", "information and communication technologies", "intercept", "modification", "password", "possession", "programme", "telecommunication service", "telecommunication system"

4.15.3 Substantive law

Offences:

- Unauthorized access to computer data
- Unauthorized access to and interception of computer service
- Unauthorized modification of computer material
- Damaging or denying access to computer system
- Unauthorized disclosure of password
- Unlawful possession of devices and data
- Electronic fraud
- Tampering with computer source documents
- Publishing obscene information in electronic form

4.15.4 Procedural law

The Criminal Procedure Code provides traditional powers for search and seizure of tangible objects.

4.15.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The type of the conduct criminalised, and the wording used in 83Y (Damaging or denying access to computer systems) and 84A (Unlawful possession of devices and data) could indicate that the legislator considered the Commonwealth Model Law. 84N is a provision on electronic fraud, indicating as source the Budapest Convention . Other legislation may also have been an inspiration. Overall, practical efficiency of the law should be reviewed.

4.15.6 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 3.

4.15.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
    - Workshop on cybercrime legislation and investigation, November 2008, Nairobi, Kenya

4.16 Kiribati

4.16.1 Relevant legislation

- Telecommunication Act 2004

4.16.2 Definitions

- "computer service", "data", "function", "intercept", "program"

4.16.3 Substantive law

The Telecommunications Act 2004 includes a section on computer misuse that covers some substantive law provisions.

Offences:

- Unauthorised access to computer material
- Unauthorised use or interception of computer service
- Unauthorised modification of computer material
- Unauthorised access for commission of offences
- Distribution and exhibition of obscene matter

4.16.4 Procedural law

The Act does not provide modern powers of investigation.

- Search warrant

4.16.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Some of the definitions of the terms ("data"; "program") and the type of conduct criminalised indicate as source the Cybercrime Convention and/or the Commonwealth Model Law, as well as other possible legislation. Amendments to the existing legislation or the preparation of a specific act may be considered.

The legislation was discussed in the Workshop on cybercrime legislation (27-29 April 2011, Tonga) in view of implementing the Convention.

4.16.6 Country profile available: Yes

Country profile prepared under the Global Project on Cybercrime Phase 3

4.16.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 2
  - Pacific Islands – Workshop on cybercrime legislation (27-29 April 2011, Tonga)

4.17 Malaysia

4.17.1 Relevant legislation

- Computer Crime Act 18 June 1997, which entered into force on 1 June 2000
- Communication and Multimedia Act of 1998, with amendments of 2006
- Criminal Law Act 574 with amendments of 2006
- Criminal Procedure Code Act 593 with amendments of 2006
- Evidence Act 1950 with amendments of 2006

4.17.2 Definitions

- "computer", "computer network", "computer output" or "output", "data", "communications"

4.17.3 Substantive law

Offences:

Malaysia adopted cybercrime legislation at an early stage.

- Illegal access to program or data
- Interception and disclosure of communications prohibited
- Unauthorised modification of the contents of any computer
- Damage to network facilities
- Fraud and related activity in connection with access devices etc.
- Unauthorized access with intent to commit or facilitate commission of further offence
- Improper use of network facilities or network service etc.

4.17.4 Procedural law

- General duty of the licensees (limited to telecommunications sector service providers)
- Specific provisions in relation with the handling and producing of evidence
- Powers of search, seizure and arrest
- Power to intercept communications (includes both traffic and content data)

4.17.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Malaysia has cooperated with the Council of Europe in several activities. A detailed analysis of the national legislation has been carried out to verify its compatibility with the Convention on Cybercrime and recommend accession.

Some of the definitions of the terms used in the law ("data", "program") and the type of conduct criminalised could indicate that the Cybercrime Convention and/or Commonwealth Model Law might have been considered in its drafting, as well as other legislation.

4.17.6 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 2.

4.17.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
    - Round table on cybercrime legislation, 9 April 2008, Kuala Lumpur
    - Workshop on legislation for ASEAN countries, 27-28 November 2008, Kuala Lumpur, Malaysia
- Global Project Phase 2
    - ASEAN/APRIS Workshop on cybercrime legislation and capacity building, 26-28 January 2010, Manila, Philippines
    - Judicial training workshop, 4-8 July 2008, Kuala Lumpur, Malaysia
- Octopus Conference, Cooperation against Cybercrime
    - Participation of Malaysia in 2011 and 2012

4.18 Malta

4.18.1 Relevant legislation

- Criminal Code of Malta

Definitions

- "computer", "computer data", "computer network", "computer output" or "output ", "computer software", "computer supplies", "function", "supporting documentation"

4.18.2 Substantive law

- Unlawful access to, or use of, information

4.18.3 Procedural law

- Search and seizure

4.18.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Malta signed the Convention on 17 January 2002 and ratified it on 12 April 2012. The legislation was amended with a view to implementing the Convention (introducing provisions on, for example, illegal interception, data interference, system interference and misuse of devices); however, more information is needed to complete the legislative profile.

4.18.5 Country profile available: Partial

Country profile is under preparation within the Global Project Phase 3

4.18.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 2

4.19 Mauritius

4.19.1 Relevant legislation

- The Computer Misuse and Cybercrime Act 2003

Definitions

- "access", "computer service", "computer system", "data", "information and communication service", "information and communication technologies", "intercept", "investigatory authority", "modification", "password", "program", "service provider", "subscriber", "subscriber information", "telecommunication", "traffic data"

4.19.2 Substantive law

Offences:

- Unauthorised access to computer data
- Unauthorised access to and interception of computer service
- Unauthorised modification of computer material
- Damaging or denying access to computer system
- Unlawful possession of devices and data

4.19.3 Procedural law

The procedural powers foreseen under the Act are inspired by the Convention. Thus, the powers of preservation of data (Section 11), disclosure of traffic data (Section 12), production order (Section 13) search and seizure (Section 14) and real-time collection of data (Section 15) have been included in the Act.

4.19.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The Convention on Cybercrime was used for guidance in drafting the legislation. This conclusion results from the following provisions of the legislation: the analysis of the terms defined (e.g. "program"; "service provider"; "subscriber"; "subscriber information"; "traffic data"); type of conduct criminalised, the wordings used in some provisions (e.g. unlawful possession of devices and data; electronic fraud), as well as the procedural law measures adopted (e.g. preservation order; disclosure of preserved data; production order; powers of access, search and seizure for the purposes of investigation; and real-time collection of traffic data). This conclusion was confirmed by representatives of authorities from Mauritius.[27]

There are clear indications that the authorities of Mauritius are taking steps to accede to the Budapest Convention.

4.19.5 Country profile available: Yes

Country profile prepared within the Global Project Phase 3

4.19.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 2

[27] Mr Narayan Gangalaramsamy, FBCS, CITP, MSC Computer Security & Forensics, Chief Inspector of Police

- The African Network Information Center (AfriNIC), the Regional Internet Registry (RIR) for Africa: First Afri- Government Working Group (AfGWG Law Enforcement Meeting, 25-26 January 2010, Ebene, Mauritius

- The Council of Europe and the European Union joint regional project (Cybercrime@IPA)[28]

  - A good practice study to help public authorities create or further strengthen specialised cybercrime units was prepared by the Council of Europe together with European Union Cybercrime Task Force and includes experience from Australia and Mauritius.
  - The Council of Europe has prepared a Guide on Electronic Evidence to provide support and guidance in the identification and handling of electronic evidence. The development of the document involved experts from many countries, including Mauritius and Pakistan.

- Octopus Conference, Cooperation against Cybercrime

  - Participation of Mauritius in 2010 and in 2012

[28] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Default_IPA_en.asp

4.20 Namibia

4.20.1 Relevant legislation

- Use of Electronic Transactions and Communication Draft Bill from September 2010
- Criminal Procedure Code of 2004

4.20.2 Definitions

- "access", "addressee", "automated message system", "cache", "data", "data message", "electronic", "electronic record", "electronic communication", "electronic data interchange (EDI)", "electronic signature", "intercept", "intermediary", "information system", "information system services", "originator", "password", "place of business", "secure electronic signature", "service provider", "transaction"

4.20.3 Substantive law

- Unauthorised access
- Unauthorised interception
- Unauthorised interference with data or information systems
- Misuse of services
- Electronic fraud or forgery
- Electronic extortion
- Attempt and aiding and abetting

4.20.4 Procedural law

The draft law includes some general provisions on retention of records and production of documents or information that apply to electronic documents. However, there are no specific investigative measures provided for in the draft. The Criminal Procedure Code currently provides only traditional measures.

4.20.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Some of the definitions (e.g. "data", "information system", "service provider"); types of conduct criminalised; and the wordings of some provisions e.g. misuse of services and electronic fraud indicate the Convention as possible source for drafting the law (indeed the "misuse of services and electronic fraud" is copied from the Convention). Other legislation may also be a source.

4.20.6 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 3.

4.20.7 Cooperation with the Council of Europe: No

4.21 New Zealand

4.21.1 Relevant legislation

- Crimes Act 1961 (Crimes involving computers substituted, on 1 October 2003, by section 15 of the Crimes Amendment Act 2003 (2003 No 39))
- The Films, Videos, and Publications Classification act of 1993
- Summary Proceedings Act 1957

4.21.2 Definitions

- "access", "authorisation", "computer system", "intercept", "interception device", "private communication", " bank note", "false document"

4.21.3 Substantive law

- Accessing computer system for dishonest purpose
- Crimes against personal privacy
- Prohibition on use of interception devices
- Damaging or interfering with computer system
- Making, selling, or distributing or possessing software for committing crime
- Accessing computer system without authorisation
- Forgery

4.21.4 Procedural law

- Search warrants
- Warrant of seizure

4.21.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The information about the cybercrime legislation of New Zealand needs to be completed. Overall, the legislation seems to be largely compatible with the Cybercrime Convention. A detailed analysis and amendments are under consideration in view of acceding to the Convention.

In the Quintet of Attorneys General, New Zealand agreed on the Action Plan that concluded that all Quintet countries should take steps to become parties to the Convention and to promote the Convention as the key international instrument for dealing with cybercrime and use the Convention as a basis for delivering capacity building and awareness raising activities.

4.21.6 Country profile available: Partial

Country profile prepared within the Global Project on Cybercrime Phase 3

4.21.7 Cooperation with the Council of Europe: Yes

4.22 Nigeria

4.22.1 Relevant legislation

- Computer Security and Critical Information Infrastructure Protection Bill 2005, presented before Parliament but failed to enact before the expiration term in 2007
- Cyber Security and Data Protection Agency (Establishment) Bill 2008
- Computer Misuse Bill 2009
- Amendments to Evidence Act 2011
- Cybersecurity Bill of 2011 (draft)

4.22.2 Definitions

- "access", "application", "authorized access", "authorized officer or authorized persons", "computer system", "computer data", "computer network", "computer program", "content data", "critical infrastructure", "damage", "data", "database", "device", "electronic communication", "electronic record", "function", "interception", "law enforcement agencies", "malware", "network", "service provider", "traffic data".

4.22.3 Substantive law

The Council of Europe has supported the process of drafting legal amendments in Nigeria in order to be able to adequately investigate and prosecute cybercrimes.

The inadmissibility of computer and electronic generated evidence in Nigerian courts was a major problem but this was corrected through amendments to the Evidence Act in 2011.

A cybersecurity bill was drafted in 2011[29] - ''An act to provide measures for national cybersecurity and for the prevention, detection, response and prosecution of cybercrimes and other related matters''. The Council of Europe provided comments for improvement.

Offences:

- Unlawful access to a computer
- Unlawful interception of communications
- Unauthorized modification of computer program or data
- System interference
- Misuse of devices
- Computer related forgery
- Computer related fraud
- Child pornography and related offences

The Bill criminalises in addition:

- Identity theft and impersonation
- Cybersquatting
- Cyberterrorism

[29] This version was submitted last year by the National Security Adviser (NSA) to the Attorney General (AG). The AG set up a Committee to review the bill. The resulting Bill will be sent the Federal Executive Council (FEC) and upon approval to the National Assembly for commencement of enactment procedures.

- Racist and xenophobic offences
- Offences against critical information infrastructure

4.22.4 Procedural law

- Records retention and protection of data by service providers
- Interception of electronic communications
- Failure of service provider to perform certain duties
- Powers of search and arrest

4.22.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Nigeria expressed on several occasions an interest in acceding to the Budapest Convention. The press release on 19 July 2011 - further to the meeting between Goodluck Jonathan, President of the Federal Republic of Nigeria and David Cameron, Prime Minister of the United Kingdom of Great Britain and Northern Ireland - informed about the intention of Nigeria *'to step up efforts to combat international cyber crime, including by signing the Budapest Convention"*[30].

Nigeria participated in several activities organised by the Council of Europe and received assistance from the Council of Europe in reviewing its legislation.

The Cybersecurity Bill follows the Convention (some definitions and substantive law provisions use almost the same wording) and its Additional Protocol on Racism and Xenophobia (racist and xenophobic offences) closely. The procedural law also includes some investigative measures required by the Convention (e.g. preservation, search and seizure).

Part V (International Co-operation) implements some of the specific measures provided for by the Convention and includes provisions on the 24/7 Network (established under Article 35). Thiswhich confirms the interest of Nigeria in joining the Convention.

4.22.6 Country profile available: Yes

Country profile prepared under the Global Project on Cybercrime Phase 3

4.22.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 2
  - Workshop on the Cybercrime Convention (29-30 July 2009, Abuja, Nigeria)
  - Preparatory Meeting for West African Internet Fraud Summit (2-3 February 2010, Abuja, Nigeria)
  - West Africa Cybercrime Summit (30 November – 2 December 2010, Abuja, Nigeria)

- Octopus Conference, Cooperation against Cybercrime
  - Participation of Nigeria in 2007 and from 2009 to 2012

[30] http://ukinnigeria.fco.gov.uk/en/news/?view=PressR&id=632784582

4.23 Pakistan

4.23.1 Relevant legislation

- Electronic Transaction Ordinance (ETO) 2002
- Criminal Code from 1860
- Prevention of Electronic Crime Ordinance 2009
- Draft Bill - Prevention of Electronic Crimes Act, 2012

4.23.2 Substantive law

The draft Bill was prepared with the assistance from the Council of Europe and with detailed consultation with the Industry IT Association (PASHA) and the ISP Association (ISPAK). The draft was discussed with the Chairman for the Parliamentary Committee. The Committee has asked that the draft be discussed in a smaller consultative group with law enforcement and industry. If this group comes to a consensus the Committee will pass it. If there are outstanding issues the Committee will attempt to resolve them.

4.23.3 Procedural law

The Procedural provisions were to a large extent agreed. The provisions include various investigative powers provided for by the Convention.

4.23.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The Council of Europe made use of Pakistani expertise in several activities. With the help of local experts, it provided assistance to Pakistan in the process of amending the cybercrime legislation in line with the Budapest Convention. The draft law at this stage is largely in line with international standards, in particular the Budapest Convention on Cybercrime and UK Computer Misuse Act.

4.23.5 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 2

4.23.6 Cooperation with the Council of Europe: Yes

- Global project Phase 1
    - Analysis of the Electronic Crime Bill of 2006 provided under the Project, February 2007
- Global Project Phase 2
    - ASEAN/APRIS Workshop on cybercrime legislation and capacity building, 26-28 January 2010, Manila, Philippines
    - Cybercrime training for law enforcement and judges, 23-24 February 2010, Islamabad, Pakistan
    - Legislative advice, October-December 2011, Pakistan
- The Council of Europe and the European Union joint regional project (Cybercrime@IPA)

- The Council of Europe has prepared a Guide on Electronic Evidence to provide support and guidance in the identification and handling of electronic evidence. The development of the document involved experts from many countries, including Mauritius and Pakistan.

- Octopus Conference, Cooperation against Cybercrime

  - Participation of Pakistan in 2007, in 2008 and in 2011

4.24 Papua New Guinea

4.24.1 Relevant legislation

- National Information and Communications Technology Act 2009
- Telecommunication Act 1996
- The Criminal Code Act 1974

4.24.2 Substantive law

Adequate legislation is not in place.

4.24.3 Procedural law

Adequate legislation is not in place.

4.24.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The intention is to prepare a law in the near future based on the law of Tonga and the Budapest Convention (see section 1.3)

4.24.5 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime 2

4.24.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 2
    - Pacific Islands – Workshop on cybercrime legislation, 27-29 April 2011, Tonga

4.25 Saint Vincent and the Grenadines

4.25.1 Relevant legislation

- Electronic Transactions Act (ETA) from 2007

4.25.2 Definitions

- "critical information system", "data", "information system", "access", "electronic data storage medium", "electronic communication", "electronic mail", "service provider", "traffic data"

4.25.3 Substantive law

The ETA contains provisions on protection of critical information systems and liability of service providers.

Offences:

- Illegal access
- Data interference
- Illegal interception
- System interference
- Illegal devices
- Computer-related fraud
- Child pornography

4.25.4 Procedural law

- Preservation of data
- Search and seizure
- Real-time collection of traffic data
- Collection and recording of data interception

4.25.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The Electronic Transactions Act is clearly inspired by the Commonwealth Model Law and the Cybercrime Convention. The definitions of some terms ("data", "service provider"); and the relevant provisions on illegal access, data interference, system interference, illegal interception (which includes electromagnetic emissions), illegal devices, child pornography (which includes the definition of ''child pornography'') and computer related fraud are copied from the Commonwealth Model law and Cybercrime Convention. Similarly, the definitions of "thing" and "seize'', and the investigative tools introduced, show clearly the sources of the law.

4.25.6 Country profile available: No

4.25.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
  - Cybercrime Legislation Drafting Workshop for countries of Latin America and Caribbean, 13-15 May 2008, Port of Spain, Trinidad and Tobago

4.26 Samoa

4.26.1 Relevant legislation

- The Telecommunication Act No 20/2005 lately amended in 2008

4.26.2 Substantive law

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices

4.26.3 Procedural law

- Search premises and seize documents, equipment and other items

4.26.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The mental element (without right), and the wordings used in some provisions (illegal access, illegal interception, data interference, system interference and misuse of devices) show the influence of the Convention in drafting the law.

Overall, the existing legislation covers substantive law provisions (information is unclear about computer-related offences and child pornography). However, the prescribed penalties are mostly fines, and the legislation does not allow for more serious sanctions. Specific procedural law powers are also missing. Thus, the workshop with Pacific Islands identified the need for either a new specific law or amendments to the Crimes Ordinance and the Evidence Act.

4.26.5 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 2.

4.26.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 2
    - Pacific Islands – Workshop on cybercrime legislation, 27-29 April 2011, Tonga

4.27 Singapore

4.27.1 Relevant legislation

- Computer Misuse Act of 1993, revised
- Penal Code of 1871, revised in 2008
- Criminal Procedure Act of 2010

4.27.2 Definitions

- The Computer Misuse Act provides for a number of definitions: "computer", "computer output" or "output", "computer service", "damage", "data", "electro-magnetic, acoustic, mechanical or other device", "function", "intercept", "program or computer program".

4.27.3 Substantive law

The document submitted to the Working Group during the meeting in Geneva (21-22 June 2012) states that the Computer Misuse Act (Cap 50A) was enacted in 1993 and addressed computer crimes. The Act has been amended several times to include emerging offences such as denial of service attacks. The Penal Code was also amended in 2008 to extend the application of traditional offences to the commission of such crimes through computer systems (e.g. forgery).

Offences:

- Unauthorized access to computer material
- Access with intent to commit or facilitate commission of offence
- Unauthorised modification of computer material
- Unauthorised use or interception of computer service
- Unauthorised obstruction of use of computer
- Unauthorised disclosure of access code
- Enhanced punishment for offences involving protected computers
- Sexual exploitation of child or young person

4.27.4 Procedural law

The above-mentioned document stated that the Criminal Procedure Code was amended in 2010 to provide law enforcement with investigative powers in relation to computers for all offences. Prior to the amendments, such powers could only be exercised in relation to offences under the Computer Misuse Act (Cap 50A).

Section 39 provides for the power of an investigator to access a computer that is reasonably suspected to have been used in connection with an arrestable offence. Section 40 empowers the Public Prosecutor to authorise an investigator to access decryption information for the purposes of investigating an arrestable offence.

Section 35 of the Evidence Act (Cap 97), imposes special requirements for establishing the reliability of computer output as a prerequisite for admissibility. However, Parliament has already passed legislation repealing this provision. Once the amendment comes into force in late 2012, digital evidence will be treated the same as any other evidence. Additionally, presumptions have been introduced as to the authenticity of digital evidence in certain circumstances.

4.27.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The documents submitted to the Cybercrime Working Group states[31]: "*Singapore's Computer Misuse Act pre-dates the Commonwealth Model Law on Computer Crime. However, the Act is substantially consistent with the Model Law. In drafting the Act, guidance was sought from the UK Computer Misuse Act*".

4.27.6 Country profile available: Yes

Country profile updated within the Global Project on Cybercrime Phase 3.

4.27.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
  - Workshop on legislation for ASEAN countries, 27-28 November 2008, Kuala Lumpur, Malaysia
- Global Project Phase 2
  - ASEAN/APRIS Workshop on cybercrime legislation and capacity building, 26-28 January 2010, Manila, Philippines
  - Child protection online OECD – APEC symposium, 15 April 2009, Singapore
- Cybercrime Convention Committee (T-CY)
  - Singapore was invited by the Bureau of the Cybercrime Convention Committee to participate in its 8th Plenary Session (5-6 December 2012, Strasbourg France) and to contribute to the discussion on transborder access to data.

[31] The document was prepared by G. Kannan, Senior Director (Technology Crime Unit), Criminal Justice Division, Attorney-General's Chambers, Singapore

4.28 South Africa

4.28.1 Relevant legislation

The documented submitted to the Working Group during the meeting in Geneva (21-22 June 2012) by the Department of Justice and Constitutional Development of South Africa shows that currently RSA does not have any dedicated cybercrime legislation. However, ensuring cybersecurity and combating cybercrime remain key priorities.

A national Cybersecurity Police Framework was was approved on 7 March 2012. It outlines policy positions that are intended to:

- Address national security in threat in cyberspace;
- Combat cyber warfare, cybercrime and other cyber ills;
- Develop, review and update existing substantive and procedural laws
- Build confidence and trust in the secure use of information and communication technologies.

According to the above-mentioned document, various pieces of legislation address aspects of cybersecurity and cybercrime. They overlap in terms of responsibilities and their implementation is not coordinated. Current legislation does not adequately address challenges related to cybercrime and cybersecurity in RSA.

- Electronic Communication and Transactions Act (Act 25 of 2002)
- Criminal Law of 2003
- Criminal Procedure Act of 1977 with 2008 amendments
- Electronic Communications Security Act (Act 68 of 2002)
- Regulation of Interception of Communication and Provision of Communications Related Information Act (Act 70 of 2002)
- State Information Technology Agency Act (Act 88 of 1998)
- Conventional Arms Control Regulations (R7969 of 2004) and Cryptographic regulations (R8418 of 2006)

4.28.2 Substantive law

The Electronic Communications and Transactions Act 2002 (No. 25 of 2002) provides in Chapter I a number of definitions: "data" (electronic representations of information in any form), "information system" (a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet), "information system services", "data message" etc.

Offences:

- Unauthorised access to, interception of or interference with data
- Computer-related extortion, fraud and forgery
- Promotion of sexual offence with child

Article 86 combines a number of offences provided by the Budapest Convention (illegal access, illegal interception, data interference, system interference, misuse of devices, child pornography). In addition, the article criminalises overcoming security measures designed to

protect such data, and interfering with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users.

Although the conduct criminalised considered the requirements of the Budapest Convention the level of implementation and conditions and safeguards in place would require further legal reform.

4.28.3 Procedural law

As indicated in the document submitted to the Commonwealth Cybercrime Working Group (21-22 June 2012), in spite of existing traditional investigative measures such as search, seizure and interception, including within an information system, RSA does not implement the specific powers provided for by the Budapest Convention to enable law enforcement authorities to investigate and prosecute cybercrime.

For the purposes of the Electronic Communications and Transactions Act, any reference in the Criminal Procedure Act 1977 to "premises" and "article" includes an information system as well as data messages.

The law provides for the following powers:

- Power to inspect, search and seize, which includes the power for a "cyber inspector" to enter any premises or access an information system that has a bearing on an investigation; search those premises or that information system; and take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on the investigation; search any data contained in or available to such information system; require the person by whom or on whose behalf the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system to provide him or her with such reasonable technical and other assistance as he or she may require for the purposes of this Chapter
- Obtaining warrant
- Preservation of confidentiality

The investigative powers given to the competent authorities remain insufficient with regard to the needs to conduct a cybercrime investigation.

4.28.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The Republic of South Africa (Signatory) participated in the elaboration of the Convention on Cybercrime (CETS 185) and signed it on 23 November 2001.

- The document submitted to the Commonwealth Cybercrime Working Group (21-22 June 2012) states the following: *"The model law was not utilised in drafting the legislation.* ***It is however viewed as a guiding measure together with the Convention on Cybercrime in developing legislation*** *relating to computer offences*".
- The definitions of the terms "data" (electronic representations of information in any form) and "information system" (a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet) are inspired by the Convention.

- The conduct criminalised follows the same structure as the Budapest Convention (illegal access, illegal interception, data interference, system interference, misuse of devices, child pornography).
- Misuse of devices (paragraph 3) is largely inspired by the Budapest Convention ("a person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence").
- Computer-related forgery (paragraph 2) is inspired by the Convention and uses similar wording for the mental element of the offence ("with the intent that it be considered or acted upon as if it were authentic').
- Criminalisation of computer-related offences (forgery and fraud) demonstrates use of the Convention rather than Commonwealth Model Law.
- The offence of promotion of sexual offence with a child is a poor implementation of Article 9 of the Convention.
- Some of the investigative powers have considered the requirements of the Convention (e.g. make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on the investigation; require the person by whom or on whose behalf the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system to provide him or her with such reasonable technical and other assistance as he or she may require for the purposes of this Chapter).

4.28.5 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 2.

4.28.6 Cooperation with the Council of Europe:

- Global Project Phase 2
    - Meetings to promote the ratification of the Convention on Cybercrime and its Protocol and participation in the Symposium on online security and the safety and welfare of South Africa's citizens
    - 2nd Annual South African Cyber Crime Conference, 29-30 November 2011, Cape Town, South Africa
- Octopus Conference, Cooperation against Cybercrime
    - Participation of South Africa in 2007 and 2008

4.29 Sri Lanka

4.29.1 Relevant legislation

- Computer Crime Act No 24 2007
- Payment Devices Frauds Act 2006
- Code of Criminal Procedure

4.29.2 Definitions

- "computer", "computer data storage medium", "data", "document", "information", "programme", "service provider", "subscriber information", "traffic data"

4.29.3 Substantive law

- Securing unauthorised access to a computer
- Doing any act to secure unauthorised access in order to commit an offence
- Causing a computer to perform a function without lawful authority
- Offences committed against national security etc
- Dealing with data etc., unlawfully obtained
- Illegal interception of data
- Using of illegal devices
- Unauthorised disclosure of information enabling access to a service
- Attempts to commit an offence
- Conspiring to commit an offence
- Compensation to be awarded for loss or damage consequent to an offence

4.29.4 Procedural law

Specific measures for the purpose of cybercrime investigation have been included in the Computer Crime Act:

- Preservation of information
- Powers of search and seizure with warrant
- Police officer to record and afford access to seized data
- Duty to assist investigation
- Confidentiality of information obtained in the course of an investigation

4.29.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The definitions of some terms, the conduct criminalised and the specific procedural laws provided for by the Computer Crime Act show clearly the intention of harmonising the legislation with the relevant international standards, namely the Convention on Cybercrime, the Commonwealth Model Law and other related European standards.

Sri Lanka is "fully supportive of the approach adopted by the Council of Europe" and dialogue is maintained with the Council of Europe with a view to its possible accession to the Convention[32].

[32] A paper providing the background of the Act on cybercrime legislation – Sri Lankan update by Jayantha Fenrando is available at:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres-SriLanka_Jayantha.pdf

4.29.6 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 2

4.29.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
    - Regional workshop on cybercrime, 5-6 April 2011, Colombo, Sir Lanka
- Octopus Conference, Cooperation against Cybercrime
    - Participation of Sri Lanka from 2008 to 2012

4.30 Tonga

4.30.1 Relevant legislation

- Computer Crimes Act 2003
- Criminal Offences Act 1986, amended in 2007

4.30.2 Definitions

- "computer", "computer data", "computer data storage medium", "computer system", "hinder", seize", "service provider", "traffic data", "protected computer"

4.30.3 Substantive law

The current legislation is largely compliant with the Budapest Convention. Further steps identified include reviewing the jurisdiction provision, increasing the age limit for child pornography, extending the duration of data preservation periods and reviewing the sanctioning regime of the computer crimes act.

Offences:

- Illegal access
- Illegal interception of data
- Interfering with data
- Interfering with computer system
- Illegal devices

4.30.4 Procedural law

The Computer Crimes Act provides investigators with modern tools for investigating cybercrime:

- Preservation of data
- Disclosure of traffic data
- Confidentiality and limitation of liability
- Assisting police
- Search and seizure warrants
- Interception of traffic data
- Interception of electronic communications

4.30.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The definitions of some terms, the conduct criminalised and the specific procedural law provided for by the law show clearly the intention of harmonising the legislation with the Commonwealth Model Law.

4.30.6 Country profile available: Yes

Country Profile prepared under the Global Project on Cybercrime Phase 2.

4.30.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 2
    - Workshop on cybercrime legislation, 27-29 April 2011, Tonga, Pacific Islands
- Octopus Conference, Cooperation against Cybercrime
    - Participation of Tonga in 2011

4.31 Uganda

4.31.1 Relevant legislation

- Computer Misuse Act from 2011

4.31.2 Definitions

- "access"; "application"; "authorised officer"; "computer"; "computer output" or "output"; "computer output" or "output"; "computer service"; "content"; "currency point"; "damage"; "data"; "data message"; "electronic device", "acoustic device", or "other device"; "electronic record"; "function"; "information"; "information system"; "information system services"; "intercept"; "program" or "computer program"; "traffic data"

4.31.3 Substantive law

- Unauthorised access
- Access with intent to commit or facilitate commission of further offence
- Unauthorised modification of computer material
- Unauthorised use or interception of computer service
- Unauthorised obstruction of use of computer
- Unauthorised disclosure of access code
- Unauthorised disclosure of information
- Electronic fraud
- Enhanced punishment for offences involving protected computers.
- Abetments and attempts
- Child pornography
- Cyber harassment
- Offensive communication
- Cyber stalking
- Compensation

Not clear about computer-related forgery

4.31.4 Procedural law

- Preservation order
- Disclosure of preservation order
- Production order
- Search and seizure
- Admissibility and evidential weight of a data message or an electronic record

4.31.5 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

Some of the terms defined (e.g. "data", "program" or "computer program", "traffic data"), type of conduct criminalised and the wordings used in some of the offences indicate as source the Conventions. The new investigative measures introduced by the Act (e.g. preservation order, disclosure of preservation order, production order) are more or less copied form the Convention and the Model Law. Other legislation it seems to have been used in the drafting of the law.

The Council of Europe provided comments on the draft in 2009; however a revised version was not send for additional comments.

4.31.6 Country profile available: Yes

Country profile prepared within the Global Project on Cybercrime Phase 3

4.31.7 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
  - Workshop on cybercrime legislation and investigation (November 2008, Nairobi, Kenya)
- Global Project Phase 2
  - Comments on the Computer Misuse Bill of Uganda, 19 May 2009, Strasbourg

4.32 United Kingdom

4.32.1 Relevant legislation

- The Computer Misuse Act of 1990 (as amended several times)
- Police and Criminal Evidence Act 1984
- Regulation of Investigatory Powers Act 2000
- Acquisition and Disclosure of Communications Data Code of Practice 2007

4.32.2 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The United Kingdom signed the Convention on Cybercrime (CETS no 185) on 23 November 2001 and ratified it on 25 May 2011. The instrument came into force for the UK on 1 September 2011.

4.32.3 Country profile available: No

4.32.4 Cooperation with the Council of Europe: Yes

- Global Project Phase 2
    - SANS European Digital Forensics and Incident Response Summit, 8-9 September 2010, London, UK
    - Meeting on Commonwealth Cybercrime Initiative, 19 May 2011, London, UK
    - Conference on Cyber Space, 1-2 November 2011, London, UK

- Global Project Phase 3
    -
    - In 2012 and 2013 the UK made financial contributions to the Council of Europe for the Global Project on Cybercrime 3 in order to assist countries worldwide in taking measures against cybercrime

- Octopus Conference, Cooperation against Cybercrime/Cybercrime Convention Committee (T-CY)
    - The UK is represented in the Bureau of the Cybercrime Convention Committee
    - Participation of United Kingdom in the Octopus Conference from 2007 to 2012

4.33 Zambia

4.33.1 Relevant legislation

- Electronic Communication and Transactions Act (ECT Act) 21 2009

4.33.2 Substantive law

Offences:

- Unauthorised access to, interception of, or interference with, data
- Computer-related extortion, fraud and forgery
- Prohibition of pornography (the provision does not apply specifically to child pornography)
- Hacking, cracking and viruses
- Denial of service attacks
- Spamming

4.33.3 Procedural law

- Powers of cyber inspectors
- Power to inspect, search and seize
- Warrant to enter
- Prohibition of disclosure of information to authorised persons

4.33.4 Relation with the Budapest Convention on Cybercrime/the Commonwealth Model Law

The type of conduct criminalised and some of the provisions seem to be inspired by the Convention, as well as other legislation.

A review of the gaps and application in practice of the law could be considered in view of further legal reforms.

4.33.5 Country profile available: No

4.33.6 Cooperation with the Council of Europe: Yes

- Global Project Phase 1
    - Workshop on cybercrime legislation and investigation (November 2008, Nairobi, Kenya)

5 Appendices

5.1 Council of Europe's Approach

The Council of Europe helps protect societies worldwide against the threat of cybercrime through the Budapest Convention on Cybercrime, the Cybercrime Convention Committee (T-CY), and capacity building projects, as well as a range of other tools and related instruments.

5.1.1 The Budapest Convention on Cybercrime

The Convention on Cybercrime (or Budapest Convention), signed on 23 November 2001, is regarded as the most complete international standard to date, since it provides a comprehensive and coherent framework providing measures to address the various issues that arise in the successful enforcement of cybercrime law.

The Budapest Convention is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against cybercrime, and as a framework for international cooperation between State Parties to this treaty.

The Convention provides for (i) the criminalisation of conduct – ranging from illegal access and data and systems interference, to computer-related fraud and child pornography; (ii) procedural law tools to make the investigation of cybercrime more effective; and (iii) efficient international cooperation. The treaty is open for accession by any country.

The Convention is supplemented by an Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189).

According to Article 37, any country can accede to the Budapest Convention. By 11 September 2012, the Convention had been ratified by 37 countries (numerous European countries, the USA and Japan), signed by an additional 10 countries (numerous European countries, Canada and South Africa), and eight countries had been invited to accede (Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, the Philippines and Senegal). Many other countries are using the Budapest Convention as a guideline for cybercrime legislation.

- The Convention (ETS 185)

5.1.2 Benefits to becoming a Party to the Budapest Convention

1. The Budapest Convention provides for:

- Substantive criminal law measures, including offences against the confidentiality, integrity and availability of computer data and systems (eg. illegal access, illegal interception, data interference, system interference, misuse of devices), computer-related offences (eg. computer-related forgery, computer-related fraud), content-related offences (child pornography), and infringement of copyright and related rights.

- Procedural law, that is, measures for more effective investigations of cybercrime. These include expedited preservation of stored computer data, partial disclosure of traffic data, production orders, search and seizure of stored computer data, real-time collection of traffic data and interception of content data. The procedural measures are to apply to any offence

committed by means of a computer system, and to the collection of evidence in general. Conditions and safeguards are intended to prevent the abuse of such powers.

- International cooperation, including general principles (related to extradition, mutual legal assistance, spontaneous information etc.), and specific measures (expedited preservation of stored computer data, expedited disclosure of preserved computer data, mutual assistance regarding accessing stored computer data, trans-border access to stored computer data, mutual assistance in the real-time collection of traffic data, mutual assistance regarding interception of content data, and 24/7 points of contact).

The Budapest Convention on Cybercrime is thus comprehensive, not only in terms of its substantive law, but in terms of its procedural law. Furthermore, in international cooperation it combines the traditional mutual assistance regime with urgent measures to allow efficient cooperation, and follows the principle of subsidiarity (that is, that existing bi- or multilateral agreements may be used first before resorting to the provisions of the Convention).

Full implementation of this treaty will:

- Ensure a coherent national approach to legislation on cybercrime
- Facilitate the gathering of electronic evidence
- Facilitate the investigation of cyberlaundering, cyberterrorism and other serious crime
- Ensure the harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries

2. The Convention has the advantage of flexibility. It has been supplemented by an Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189). Further protocols can be added in the future to address emerging challenges should the need arise.

3. The Convention serves as a guideline or model law for the development of national legislation even if a country does not actually become a party to this treaty. Model laws, guidelines and handbooks are based on this treaty. However, actual accession to the Convention on Cybercrime creates additional benefits:

- It serves as a legal basis for international cooperation in cybercrime cases. Parties to the Convention can make full use of the provisions of chapter III on international cooperation, ranging from police to judicial cooperation. These provisions are not limited to cybercrime in the narrow sense, but can support cooperation in tackling all crime involving computer systems or electronic evidence. For this reason the Financial Action Task Force, in their newly consolidated 40 Recommendations, encourage accession to the Budapest Convention to facilitate cooperation against money laundering and the financing of terrorism:
  http://www.fatf-gafi.org/document/50/0,3746,en_32250379_32236920_49653426_1_1_1_1,00.html

- Parties to the Convention participate in the Cybercrime Convention Committee (T-CY). This Committee follows the implementation of the Convention and initiates future work related to the Convention, such as the preparation of additional protocols. This means that countries that have not been involved in the drafting of the original treaty would still be involved in the elaboration of future international cybercrime standards, if they become a party.

4. The Convention also serves as a standard of reference for the European Court of Human Rights.[33]

5. The treaty is a platform facilitating public-private cooperation in cybercrime investigations.

6. The Convention has received strong support from the European Union[34], Interpol, the Asia-Pacific Economic Cooperation, the Organisation of American States[35] and other organisations[36] and initiatives, as well as the private sector.

7. Thus, the Convention on Cybercrime provides a clear and comprehensive solution which has been used by many countries and has proven to function. Some fifty countries covering about one third of current internet users have ratified, signed or been invited to accede to this treaty. In the majority of countries globally, legal and technical experts make extensive use of it.

5.1.3 Technical Assistance

Agreements, tools and good practices to meet the challenge of cybercrime are already available and can be applied by any country. These include in particular the Budapest Convention. However, there are also other instruments on cybercrime and related matters such as organised crime, the exploitation of children, the terrorist use of the internet, financial investigations, money laundering and the protection of personal data. Numerous tools for law enforcement and judicial training, for public/private cooperation and for international cooperation have been developed.

A major capacity building effort to help countries worldwide make use of existing tools, instruments and good practices is the most effective way ahead.

A global approach is required to respond to needs in a pragmatic manner, follow up on expressed commitment by governments, react to incidents, generate or build on momentum in a given country or region, and exploit opportunities to engage in cooperation against cybercrime.

The Octopus Conference 2010 and the United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, April 2010) underlined broad international consensus on the need for technical assistance aimed at strengthening the capacities of States to counter cybercrime.

Geographical scope

- There are projects at national, regional and global levels
- Many countries have been invited to accede or are interested in the Budapest Convention
- Legislation is the best starting point to engage in cooperation
- The Convention and the T-CY are capable of cooperation with regional organisations (AU, ASEAN, APEC, ECOWAS, OAS, SPC and others)
- The Convention is a flexible resource, able to respond to the needs of and opportunities in any country

33 See application no. 2872/02 KU vs Finland at:
http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=2872/02&sessionid=41896292&skin=hudoc-en

34 In the Stockholm Programme for the period 2010-2014 (adopted in December 2009), the European Union states, for example, that "This Convention should become the legal framework of reference for fighting cyber-crime at global level" (section 4.4.4).
http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf

35 See for example the recent Recommendations of Seventh meeting of the Working Group on Cybercrime, Washington DC, 6-7 February 2012
http://www.oas.org/juridico/english/cyber_experts.htm

36 For example, several detailed workshops on cybercrime legislation on the basis of the Budapest Convention have been held with ASEAN member states, the most recent one in Manila, Philippines, on 26-28 January 2010 as a joint activity of the ASEAN Secretariat, the European Union and the Council of Europe.

Experience of the Council of Europe

- **Council of Europe Global Project on Cybercrime (since 2006):** Support given to several hundred activities involving some 120 countries worldwide on harmonisation of legislation, law enforcement and judicial training, public-private cooperation and international cooperation. Annual Octopus conferences on cooperation against cybercrime. So far funded by Estonia, Japan, Monaco, Romania, Microsoft, McAfee and Visa Europe as well as the budget of the Council of Europe. Phase 3 to start in January 2012.

- **EU/CoE joint Project on Cybercrime in Georgia (2009/2010):** Assisted Georgia in adoption of legislation on cybercrime and on the protection of personal data, design of a high-tech crime unit and of training programmes for judges and prosecutors, and in conclusion of a memorandum of understanding between law enforcement and service providers.

- **EU/CoE joint project on cooperation against cybercrime in EU pre-accession countries (2010 – 2013): "CyberCrime@IPA"** covers eight countries/areas in South-eastern Europe (Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo[37]). Launched in November 2010 it focuses on cybercrime policies and strategies, harmonisation of legislation, international cooperation, law enforcement training, financial investigations, law enforcement/service provider cooperation, and assessments of progress made.

- **EU/CoE joint Eastern Partnership regional project (2011-2013): "CyberCrime@EAP"** launched in April 2011 in six countries of Eastern Europe (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) to provide advice and assess measures taken with regard to cybercrime legislation, creation and role of specialised institutions, judicial and law enforcement training, law enforcement/service provider cooperation, financial investigations, international cooperation.

(See: www.coe.int/cybercrime)

5.1.4 Fields of intervention

Experience suggests that capacity building programmes for cybercrime prevention and criminal justice could address the following:

Cybercrime policies and strategies

- Comprehensive and coherent approaches to cybercrime
- Engagement by decision-makers
- Synergies and links with cybersecurity strategies
- Multi-stakeholder participation
- Contributions by donors and cooperation with partners
- Human rights and rule of law requirements
- Management of implementation, and monitoring and assessment of results and impact

(See: Discussion paper on cybercrime strategies)

[37] All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo

Legislation

- Substantive law measures to criminalise offences against and by means of computers
- Procedural law tools for efficient investigations and use of electronic evidence
- Safeguards and conditions for investigative powers (Article 15 Convention)
- Data protection regulations (in line with Data Protection Convention 108)
- Harmonisation with the Budapest Convention on Cybercrime

(See: www.coe.int/cybercrime)

Cybercrime reporting

- Reporting channels for individuals and for public and private sector organisations
- Triggering law enforcement investigations
- Intelligence for better understanding of scope, threats and trends
- Collation of data to detect patterns of organised criminality

Prevention

- Public awareness/education of users and society in general
- Technical, administrative, procedural measures to protect systems
- Specific measures for users, groups and sectors at risk

Specialised units

- Police-type cybercrime or high-tech crime units
- Prosecution-type cybercrime units
- Computer forensic capabilities
- Specialisation within judiciary
- Interagency cooperation

(See: CoE/EU/EUCTF (2011): Specialised cybercrime units – good practice study)

Law enforcement training

- Sustainable, standardised, replicable, scalable training
- Skills to investigate cybercrime, secure electronic evidence, carry out computer forensic analyses, assist other agencies and contribute to network security
- Skills/competencies required for respective functions and at appropriate level (from first responder to forensic investigators)
- Make use of materials and models already developed
- Cooperation with law enforcement, academia and industry (www.2Centre.eu)

(See: CyberCrime@IPA (2011): Law enforcement training strategy)

Judicial training

- Initial and in-service training for judges and prosecutors on cybercrime and electronic evidence
- Advanced training for a critical number of judges and prosecutors
- Specialisation and technical training of judges and prosecutors
- Enhanced knowledge through networking among judges and prosecutors

(See: Council of Europe/Project on Cybercrime (2009): Judicial training concept)

Public/private cooperation

- Cooperation in cybercrime reporting systems (spam, botnets, child abuse materials)
- Information and intelligence sharing (finance and other sectors)
- Law enforcement/service provider cooperation

(See: Council of Europe/Global Project on Cybercrime (2008): Guidelines for LEA/ISP cooperation)

International cooperation

- Chapter III of Budapest Convention on Cybercrime and accession to this treaty
- Police to police cooperation (direct cooperation, use of Interpol and other channels)
- Judicial cooperation
- 24/7 points of contact

(See: Council of Europe: Resources: international cooperation against cybercrime)

Specific field: Protection of children

- Prevention, protection, prosecution
- Conditions for effective enforcement
- Public private cooperation
- Legislative engagement based on Budapest Convention and Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

(See: www.coe.int/children and EU Safer Internet Programme)

Specific field: Financial investigations and prevention of fraud and money laundering

- Crime reporting systems
- Prevention and public awareness
- Regulation, licensing, supervision
- Risk management and due diligence
- Harmonised legislation
- Specialised units and interagency cooperation
- Public-private cooperation and information exchange
- Training
- International cooperation
- Implementation of Budapest Convention in combination with FATF recommendations or CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198)

(See: Typology Report on Criminal Money on the Internet)

Specific field: Prevention and control of terrorist use of ICT

- Legislation and institution building for the implementation of the Convention on the Prevention of Terrorism in combination with Budapest Convention and other tools
- Rule of law and human rights requirements (Council of Europe guidelines 2002)

(See: www.coe.int/terrorism)

5.2 Convention on Cybercrime/Commonwealth Model Law - Comparative Table

Convention on Cybercrime	Commonwealth Model Law
Chapter I – Use of terms **Article 1 – Definitions** For the purposes of this Convention: a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c) "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.	**Definitions** In this Act, unless the contrary intention appears: "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; "computer data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device; "computer system" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function; "service provider" means: (a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and (b) any other entity that processes or stores computer data on behalf of that entity or those users. "traffic data" means computer data: (a) that relates to a communication by means of a computer system; and (b) is generated by a computer system that is part of the chain of communication; and (c) shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when	**5. Illegal access** A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on

committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**8 Illegal interception of data etc.** A person who, intentionally without lawful excuse or justification, intercepts by technical means: (a) any non-public transmission to, from or within a computer system; or (b) electromagnetic emissions from a computer system that are carrying computer data; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**6 Interfering with data** (1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts: (a) destroys or alters data; or (b) renders data meaningless, useless or ineffective; or (c) obstructs, interrupts or interferes with the lawful use of data; or (d) obstructs, interrupts or interferes with any person in the lawful use of data; or (e) denies access to data to any person entitled to it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both. (2) Subsection (1) applies whether the person's act is of temporary or permanent effect.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be	**7 Interfering with computer system** (1) A person who intentionally or recklessly, without lawful excuse or

necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	justification: (a) hinders or interferes with the functioning of a computer system; or (b) hinders or interferes with a person who is lawfully using or operating a computer system; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both. In subsection (1) "hinder", in relation to a computer system, includes but is not limited to: (a) cutting the electricity supply to a computer system; and (b) causing electromagnetic interference to a computer system; and (c) corrupting a computer system by any means; and (d) inputting, deleting or altering computer data;
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.	**9. Illegal devices** (1) A person commits an offence if the person: (a) intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available: (i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence against section 5, 6, 7 or 8; or (ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8; or (b) has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8. (2) A person found guilty of an offence against this section is liable to a penalty of imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both **[EXPERT GROUP TEXT OF PARAGRAPH (3)** (3) A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6,7 or 8 unless the contrary is proven.]

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	**[ALTERNATE TEXT OF PARAGRAPH 3 PROPOSED BY CANADA** (3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (i) or (ii), a court may infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8, unless the person raises a reasonable doubt as to its purpose.] **NOTE:** S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	No provision
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	No provision
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:	**10.Child pornography** (1) A person who, intentionally, does any of the following acts: (a) publishes child pornography through a computer system; or

a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	(b) produces child pornography for the purpose of its publication through a computer system; or (c) possesses child pornography in a computer system or on a computer data storage medium; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [***period***], or a fine not exceeding [***amount***], or both. **NOTE:** *The laws respecting pornography vary considerably throughout the Commonwealth. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in all member countries. However a country may wish to extend the application of this prohibition to other forms of pornography, as the concept may be defined under domestic law.* **NOTE:***The pecuniary penalty will apply to a corporation but the amount of the fine may be insufficient. If it is desired to provide a greater penalty for corporations, the last few lines of subsection (1) could read:* *"commits an offence punishable, on conviction:* (a) *in the case of an individual, by a fine not exceeding* [**amount**] *or imprisonment for a period not exceeding* [**period**]*; or* (b) *in the case of a corporation, by a fine not exceeding* [**a greater amount**]. (2) It is a defence to a charge of an offence under paragraph (1) (a) or (1)(c) if the person establishes that the child pornography was a bona fide scientific, research, medical or law enforcement purpose. **NOTE:** *Countries may wish to reduce or expand upon the available defences set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defences to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.* (3) In this section: "child pornography" includes material that visually depicts: (a) a minor engaged in sexually explicit conduct; or (b) a person who appears to be a minor engaged in sexually explicit conduct; or (c) realistic images representing a minor engaged in sexually explicit conduct.

	"minor" means a person under the age of [x] years. "publish" includes: (a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; or (b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or (c) print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in paragraph (a).
	PART III PROCEDURAL POWERS **Definitions for this Part** **NOTE:** *As most jurisdictions already have legislative or common law search powers, the purpose of sections 11 and 12 is to illustrate the amendments necessary to existing powers to ensure that such powers include search and seizure in relation to computer systems and computer data. The example given is of necessary amendments to a sample general search warrant provision but similar amendments would need to be made to all search powers, including powers of search on arrest, search without warrant in exigent circumstances, and plain view seizures* *The general search warrant provision is provided for illustration and is not intended as a comprehensive model of general search powers. Some options have been included also where there may be differing standards as between countries. These options are bracketed in bold and italics.* 11. In this Part: "thing" includes: (a) a computer system or part of a computer system; and (b) another computer system, if: (i) computer data from that computer system is available to the first computer system being searched; and (ii) there are reasonable grounds for believing that the computer data sought is stored in the other computer system; and (c) a computer data storage medium "seize" includes: (a) make and retain a copy of computer data, including by using onsite

	equipment; and (b) render inaccessible, or remove, computer data in the accessed computer system; and (c) take a printout of output of computer data.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**17. Preservation of data** (1)If a police officer is satisfied that: (a) data stored in a computer system is reasonably required for the purposes of a criminal investigation; and (b) there is a risk that the data may be destroyed or rendered inaccessible; the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice. (2) The period may be extended beyond 7 days if, on an ex parte application, a [***judge***] [***magistrate***] authorizes an extension for a further specified period of time.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data	**16 Disclosure of stored traffic data** ***Option 1*** If a police officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify:

to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(a) the service providers; and (b) the path through which the communication was transmitted. ***Option 2*** If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify: (a) the service providers; and (b) the path through which the communication was transmitted. **21.Confidentiality and limitation of liability** (1)An Internet service provider who without lawful authority discloses: (a) the fact that an order under section 13, 15, 16, 17, 18 and 19 has been made; or (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both. (2) An Internet service provider is not liable under a civil or criminal law of [enacting country] for the disclosure of any data or other information that he or she discloses under sections 13, 15, 16, 18 or 19.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to	**15. Production of data** If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that: (a) a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; and (b) an Internet service provider in [enacting country] produce information about persons who subscribe to or otherwise use the

Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	service; and (c) [*a person in the territory of [enacting country] who has access to a specified computer system process and compile specified computer data from the system and give it to a specified person.*] **NOTE:** *As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.* **NOTE:** *Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.* **21.Confidentiality and limitation of liability** (1)An Internet service provider who without lawful authority discloses: (a) the fact that an order under section 13, 15, 16, 17, 18 and 19 has been made; or (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both. (2) An Internet service provider is not liable under a civil or criminal law of [enacting country] for the disclosure of any data or other information that he or she discloses under sections 13, 15, 16, 18 or 19.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and	**Definitions for this Part** **NOTE:** As most jurisdictions already have legislative or common law search powers, the purpose of sections 11 and 12 is to illustrate the amendments necessary to existing powers to ensure that such powers include search and seizure in relation to computer systems and computer data. The example given is of necessary amendments to a sample general search

b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	warrant provision but similar amendments would need to be made to all search powers, including powers of search on arrest, search without warrant in exigent circumstances, and plain view seizures The general search warrant provision is provided for illustration and is not intended as a comprehensive model of general search powers. Some options have been included also where there may be differing standards as between countries. These options are bracketed in bold and italics. 11. In this Part: **"thing"** includes: (a) a computer system or part of a computer system; and (b) another computer system, if: (i) computer data from that computer system is available to the first computer system being searched; and (ii) there are reasonable grounds for believing that the computer data sought is stored in the other computer system; and (c) a computer data storage medium "**seize"** includes: (a) make and retain a copy of computer data, including by using onsite equipment; and (b) render inaccessible, or remove, computer data in the accessed computer system; and (c) take a printout of output of computer data. **12 Search and seizure warrants** (1)If a magistrate is satisfied on the basis of [***information on oath***] [***affidavit***] that there are reasonable grounds [***to suspect***] [***to believe***] that there may be in a place a thing or computer data: (a) that may be material as evidence in proving an offence; or (b) that has been acquired by a person as a result of an offence; the magistrate [***may***] [***shall***] issue a warrant authorising a [***law enforcement***] [***police***] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data.

	NOTE: *If the existing search and seizure provisions contain a description of the content of the warrant, either in a section or by a form, it will be necessary to review those provisions to ensure that they also include any necessary reference to computer data.* **13. Assisting Police** 1) A person who is in possession or control of a computer data storage medium or computer system that is the subject of a search under section 12 must permit, and assist if required, the person making the search to: (a) access and use a computer system or computer data storage medium to search any computer data available to or in the system; and (b) obtain and copy that computer data; and (c) use equipment to make copies; and (d) obtain an intelligible output from a computer system in a plain text format that can be read by a person. (2) A person who fails without lawful excuse or justification to permit or assist a person commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both. **NOTE:** *A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self –incrimination* **21.Confidentiality and limitation of liability** (1)An Internet service provider who without lawful authority discloses: (a) the fact that an order under section 13, 15, 16, 17, 18 and 19 has been made; or (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both. (2) An Internet service provider is not liable under a civil or criminal law of [enacting country] for the disclosure of any data or other information that he or she discloses under sections 13, 15, 16, 18 or 19.

	14. Record of and access to seized data (1) If a computer system or computer data has been removed or rendered inaccessible, following a search or a seizure under section 12, the person who made the search must, at the time of the search or as soon as practicable after the search: (a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and (b) give a copy of that list to: (i) the occupier of the premises; or (ii) the person in control of the computer system. (2) Subject to subsection (3), on request, a police officer or another authorized person must: (a) permit a person who had the custody or control of the computer system, or someone acting on their behalf to access and copy computer data on the system; or (b) give the person a copy of the computer data. (3) The police officer or another authorized person may refuse to give access or provide copies if he or she has reasonable grounds for believing that giving the access, or providing the copies: (a) would constitute a criminal offence; or (b) would prejudice: (i) the investigation in connection with which the search was carried out; or (ii) another ongoing investigation; or (iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability:	**19 Interception of traffic data** (1)If a police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request that person to: (a) collect or record traffic data associated with a specified communication

i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	during a specified period; and (b) permit and assist a specified police officer to collect or record that data. (2) If a magistrate is satisfied on the basis of [***information on oath***] [***affidavit***] that there are reasonable grounds [***to suspect***] that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate [***may***] [***shall***] authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. **21.Confidentiality and limitation of liability** (1)An Internet service provider who without lawful authority discloses: (a) the fact that an order under section 13, 15, 16, 17, 18 and 19 has been made; or (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both. (2) An Internet service provider is not liable under a civil or criminal law of [enacting country] for the disclosure of any data or other information that he or she discloses under sections 13, 15, 16, 18 or 19.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure	**18 Interception of electronic communications** (1)If a **[*magistrate*] [*judge*]** is satisfied on the basis of [***information on oath***][***affidavit***] that there are reasonable grounds [to suspect][***to believe***] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [***may***] [***shall***]:(a) order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or (b) authorize a police officer to collect or record that data through application of technical means. **21.Confidentiality and limitation of liability**

the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(1)An Internet service provider who without lawful authority discloses: (a) the fact that an order under section 13, 15, 16, 17, 18 and 19 has been made; or (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [**period**], or a fine not exceeding [**amount**], or both. (2) An Internet service provider is not liable under a civil or criminal law of [enacting country] for the disclosure of any data or other information that he or she discloses under sections 13, 15, 16, 18 or 19.
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Jurisdiction 4**. This Act applies to an act done or an omission made: (a) in the territory of [enacting country]; or (b) on a ship or aircraft registered in [enacting country]; or (c) by a national of [enacting country] outsid e the jurisdiction of any country; or (d) by a national of [enacting country] outside the territory of [enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed. **NOTE:** *The nature of cyber crime is such that it is important to have an extended jurisdictional basis for such offences, as often acts committed in the territory of one jurisdiction may have a substantial impact on other jurisdictions. Some countries can address this issue through case law that interprets "territorial jurisdiction" broadly to include situations where there is a "real and substantial link" to that jurisdiction albeit elements of the offence may have been committed elsewhere. In other countries* *the legislation specifically provides that jurisdiction may be assumed where there is one substantial link to the country, which term is broadly defined. Whichever approach is adopted, it is important that countries consider the question of jurisdiction carefully and adopt provisions that will ensure no safe haven for those who commit cyber crime.*
Explanatory Report […] 141. The Convention makes it explicit that Parties should incorporate into	**20. Evidence** In proceedings for an offence against a law of [enacting country], the fact

their laws the possibility that information contained in digital or other electronic form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted.	that: (a) it is alleged that an offence of interfering with a computer system has been committed; and (b) evidence has been generated from that computer system; does not of itself prevent that evidence from being admitted.