



PACIFIC REGIONAL INFORMATION & COMMUNICATION TECHNOLOGY (ICT) OFFICIALS' MEETING

Nuku'alofa, Tonga, 16 – 17 June 2010

ICT for development, governance and sustainable livelihoods

AGENDA ITEM 3(2): ICT POLICY, LEGISLATION, REGULATORY FRAMEWORKS

Strengthening cybercrime legislation in the Pacific region

Purpose

1. This paper provides an overview of the assessment of the cybercrime legislative frameworks in Pacific Island countries by the Council of Europe (CoE). The CoE paper *Strengthening Cybercrime legislation in the Pacific region* is attached as Annex 1.

Background

2. The Council of Europe (CoE), based in Strasbourg (France), now covers virtually the entire European continent, with its 47 member countries. Founded on 5 May 1949 by 10 countries, the Council of Europe seeks to develop throughout Europe common and democratic principles based on the European Convention on Human Rights and other reference texts on the protection of individuals. More information can be found at the website: www.coe.int.

3. The purpose of the CoE report is to help advance a discussion on the strengthening of cybercrime legislation and other measures against cybercrime in the island states of the Pacific region based on international standards.

4. Given the growing reliance on ICT, countries need to equip themselves among other things with effective cybercrime legislation consistent with international standards. Globally, the standard of reference with regard to cybercrime legislation is the Budapest Convention on Cybercrime (www.coe.int/cybercrime) of the Council of Europe. It allows countries to prepare harmonised legislation aimed at criminalising conduct, providing criminal justice authorities with means to investigate cybercrime and secure volatile evidence and to engage in efficient international cooperation.

5. The fact that non-European countries (Canada, Japan, South Africa and the USA) participated in the drafting of this treaty indicates that it was intended to have a reach beyond Europe from the outset. All four have signed and the USA also ratified this treaty. It is open for accession to third countries. Chile, Costa Rica, the Dominican Republic, Mexico and the Philippines have already been invited to accede. Australia has also expressed a clear interest to accede to this treaty. Equally important is that more than 100 countries worldwide have used this convention as a guideline for domestic legislation.

6. Following discussions between SOPAC/SPC and the participation of a SOPAC representative in the global Octopus Conference on Cybercrime (Strasbourg, France, March 2010), the Council of

Europe prepared this report with suggestions on how the Pacific region could proceed with the strengthening of cybercrime legislation and related measures.

The Budapest Convention on Cybercrime

Criminalizing Conduct

7. In terms of conduct to be criminalised the Convention covers offences against the confidentiality, integrity and availability of computer data and systems and other computer-related offences;

Procedural Law

8. In terms of procedural law measures it includes expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of stored computer data, real-time collection of traffic data, and interception of content data. Such a range of procedural law measures is unusual for an international treaty, but without such measures it would be very difficult to carry out cybercrime investigations and gather electronic evidence, in particular given the volatility of computer data.

Efficient international cooperation

9. The measures for efficient international cooperation include extradition, mutual legal assistance, and spontaneous information (CoE Report pg 7-8).

Accession by third countries

10. Member States of the Council of Europe and other countries that participated in the preparation of the Budapest Convention (Canada, Japan, South Africa, USA) can sign and subsequently ratify this treaty. Other **countries can nevertheless become a party by acceding to it under Article 37**. By the time of accession, however, the necessary domestic legislation should be place so that the acceding country is capable of fully cooperating with other parties.

Commonwealth Model Law

11. Based on the Budapest Convention, in 2002, the Commonwealth Model Law on Computer and Computer-related Crime was adopted in 2002. The text follows very closely the wording of the Budapest Convention. The main differences are that it does not cover computer-related forgery and fraud, nor does it contain provisions for international cooperation. Nevertheless, a country having implemented this Model Law will be largely compliant with the Budapest Convention. In the Pacific Tonga's Computer Crime Act 2003 was based on the Commonwealth Model Law.

Analysing cybercrime legislation in the Pacific region

12. The analysis started with review of article by article of legislation in place against the convention (CoE Report pg 9).

13. Such a review is likely to show that Tonga through the Computer Crimes Act 2003 legislation seems to be largely in line with international standards. Having followed the Commonwealth Model Law the Act of 2003 does not contain specific provisions on forgery and fraud nor on international cooperation. One would need to analyse other laws to verify whether these are covered. The same applies to child pornography.

14. The Telecommunications Act 2004 of Kiribati and the Fiji Crimes Decree of 2009 seem to meet only some requirements, although it is possible that these are covered by other laws.

Strategic approaches to cybercrime and cybersecurity

15. In state governed by the rule of law, legislation is to be the basis for criminal justice action against cybercrime. At the same time, legislation is only a starting point for a broader range of measures. Countries and organisations increasingly adopt policies and strategies aimed at enhancing cyber security, that is, to primarily protect information technologies.

16. It would seem that while with the Pacific Regional Digital Strategy a broader framework was adopted, specific strategies on cybersecurity or cybercrime are not yet available.

17. While the Budapest Convention represents the core of the Council of Europe's approach against cybercrime, a number of other instruments and tools have been developed that offer a more comprehensive array of measures regarding cybercrime or Internet governance in a broader sense including:

- a. *Additional treaties*- There are other legally binding treaties that are open for accession to third countries and contain elements related to cybercrime and Internet security.
- b. *Contact points for international cooperation* - Cybercrime is very much transnational crime. Attacks launched by a person in one country or jurisdiction can affect persons in multiple other countries, and even an email communication sent to a person in the same country may generate electronic evidence elsewhere as data may be transmitted through servers in several countries. At the same time electronic evidence is volatile. Thus, urgent measures that are needed to preserve data at the national level are also necessary within the framework of international co-operation.
- c. *Guidelines for the cooperation between law enforcement and Internet service providers*. Both, law enforcement and Internet service providers play a crucial role in building trust in information and communication technologies (ICT) and helping societies around the world make best use of these technologies. As the investigation of cybercrime by law enforcement is often not effective without the cooperation of Internet service providers, it is essential that both cooperate with each other in an efficient manner. The roles of both are different: law enforcement must uphold the law, while service providers are to provide users with the ability to communicate. The question that many countries are faced with is how both can best cooperate with each other to make the Internet safer while at the same time respect their different roles and the fundamental rights of users. **A crucial part of the solution - and in many ways a precondition for cooperation - is clear legislation that defines responsibilities, authorities and limitations.** Full implementation of the Convention on Cybercrime, in particular its procedural law provisions, is essential in this respect.
- d. *Training*. Many crimes involve information technologies in one way or the other. Particular efforts are therefore required to enable law enforcement authorities, judges and prosecutors to investigate, prosecute and adjudicate cybercrime as well as to secure and make use of electronic evidence through training, networking and specialisation.
- e. *Specific measures for the protection of children*. Fostering children's trust and confidence in the Internet coupled with the protection of their dignity, security and privacy is a priority for the Council of Europe. The Internet is a space of freedom to express and communicate, to search for information and to learn, to work and to play. Access to the Internet thus offers great potential for children to exercise and enjoy their rights and values through the Internet.

- f. *Protection of children.* At the same time, threats such as cybercrime and the sexual exploitation and abuse of children through information and communication technologies pose particular challenges. The Council of Europe is addressing these by setting common standards and policies, by supporting educational, preventive and other measures to empower children, by promoting criminal justice action and by strengthening multi-stakeholder and international cooperation. These measures may also be of interest to countries of the Pacific region.

Recommendations

18. *The officials of ICT are invited to:*
- a) note the Council of Europe report;
 - b) acknowledge the importance of having legislation and appropriate measures to combat cybercrime;
 - c) acknowledge the need to protect children from abuse using ICT; and
 - d) call on SPC to approach Council of Europe, ITU and other development partners to formulate a Pacific strategy for combating cybercrime.

2 June 2010
Suva, Fiji

Annex 1

Project on Cybercrime

www.coe.int/cybercrime



COUNCIL CONSEIL
OF EUROPE DE L'EUROPE

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version 26 May 2010

**Strengthening Cybercrime legislation
in island States of the Pacific region:
Suggestions**

Contact:

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and
Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

Disclaimer:

This technical report does not necessarily reflect official positions of the Council of Europe or of the donors funding this project or of the Parties to the instruments referred to in this document

Contents

1	Introduction	4
2	Cybercrime legislation: international standards and good practices	6
2.1	The Budapest Convention on Cybercrime	6
2.1.1	Criminalising conduct	6
2.1.2	Procedural law tools for investigation	7
2.1.3	Measures for efficient international cooperation	2
2.1.4	Accession by third countries	2
2.2	State of implementation and examples of good practice	8
2.2.1	State of implementation	8
2.2.2	Examples of good practice	8
2.2.2.1	Country profiles	8
2.2.2.2	Romania	8
2.2.2.3	Commonwealth Model Law	9
2.2.2.4	Barbados Computer Misuse Act 2005-4	9
3	Analysing cybercrime legislation in the Pacific region	2
4	Cybercrime legislation in Context: Strategic approaches to cybercrime and cybersecurity	11
4.1	Strategic approaches on cybercrime and cybersecurity	11
4.2	Other Council of Europe instruments and tools on cybercrime	11
4.2.1	Additional treaties	11
4.2.2	Contact points for international cooperation	12
4.2.3	Guidelines for the cooperation between law enforcement and Internet service providers	12
4.2.4	Training	13
4.2.5	Specific measures for the protection of children	3
5	The way ahead: suggestions	15
Appendix:	Provisions of the Budapest Convention on Cybercrime, explanatory report & examples of implementation – Working Document	

1 INTRODUCTION

Societies around the world rely increasingly on information and communication technologies (ICT). This is also the case for the island states of the Pacific region.¹

The dependence on such technologies makes societies vulnerable to threats such as cybercrime, that is, offences against as well as offences committed by means of computer data and systems.² States governed by the rule of law have the positive obligation to protect their citizens and ensure their security.³ With regard to cybercrime this means that States need to criminalise specific conduct and equip their criminal justice authorities with the means to enforce the law and to protect the rights of their citizens.⁴

A large number of attacks occur at any moment, and an attack launched in one country may have global repercussions. For example:

- The “I love you” worm that was triggered ten years ago (May 2000) in the Philippines and created several billion US dollars in damage around the world.⁵ At that time, the writing of malware was not criminalised in the Philippines and the two authors of the code had to be released.
- In April/May 2007, following a dispute about a Russian war memorial, Estonia faced a series of distributed denial of service attacks that paralysed the information infrastructure of the country. Given that Estonia relies on ICT possibly more than any other country, the impact was very serious.⁶
- In August 2008, the Russian/Georgian military conflict was accompanied by coordinated attacks against the information infrastructure of Georgia. Waves of distributed denial of service attacks (BOTNET attacks) paralysed government and news websites in Georgia.⁷ Legislation in place did not allow Georgia to take criminal justice action or to engage in international cooperation.⁸

These examples show that states need to put measures in place to protect the rights of their citizens and control threats against their own societies but also threats emanating from their territories against other countries and regions. These measures include criminal law and criminal justice action.

1 For the purposes of this report these include: Cook Islands, Fiji, Kiribati, Marshall Islands, Federate States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu.

² The Budapest Convention on Cybercrime of the Council of Europe provides a typology of cybercrime. www.coe.int/cybercrime.

³ Council of Europe/Rapporteur Group on Legal Co-operation (2008): The Council of Europe and the Rule of Law - An overview (document GR-J(2008)11 of 16 September 2008). With reference to the case law of the European Court of Human Rights the report notes: “A state based on the rule of law has the duty to employ the necessary measures to uphold the law on its territory and to ensure the security of all as well as the enjoyment of human rights (*Lelièvre*, 8.11.2007, § 104). As one element of a state subject to the rule of law, prosecuting authorities must show the necessary diligence in the implementation of criminal law in order to prevent and repress crime and protect the citizens (*Saygili*, 8.1.2008, § 35).”

⁴ A specific example: In December 2008, the European Court of Human Rights of the Council of Europe ruled in a case involving the malicious misrepresentation of a 12-year old boy. An unknown person had published intimate details of the boy as well as offers of sexual services on a dating site. The Internet Service Provider refused to provide information on the identity of the person who had posted the information because at that time, there were no legal provisions in place allowing an ISP to disclose subscriber information. The European Court of Human Rights found a violation of Article 8 (Right to Private Life) of the European Convention on Human Rights. The Court underlined that the Government had failed in its positive obligation to protect the private life by failing to put criminal law measures in place that would allow effective investigation and prosecution. (*K.U. v. Finland* (application no. 2872/02) of 2 December 2008).

⁵ <http://en.wikipedia.org/wiki/ILOVEYOU>

⁶ http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

⁷ <http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>

⁸ Georgia has since cooperated with the Council of Europe and the European Union in a joint project. By May 2010 draft laws had been prepared. Once adopted they will allow Georgia to ratify the Budapest Convention. ee http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_en.asp

It seems that most island states of the Pacific region are currently not sufficiently equipped to protect their societies against cybercrime through criminal law nor that they are in a position to engage in efficient international cooperation in this respect.

Globally, the standard of reference with regard to cybercrime legislation is the Budapest Convention on Cybercrime (www.coe.int/cybercrime) of the Council of Europe. It allows countries to prepare harmonised legislation aimed at criminalising conduct, providing criminal justice authorities with means to investigate cybercrime and secure volatile evidence and to engage in efficient international cooperation. It has been signed or ratified by most European countries but also by Canada, Japan, South Africa and the USA. It is open for accession to third countries. Chile, Costa Rica, the Dominican Republic, Mexico and the Philippines have already been invited to accede. Australia has also expressed a clear interest to accede to this treaty. Equally important is that more than 100 countries worldwide have used this convention as a guideline for domestic legislation.

The present report is not aimed at providing a complete analysis of legislation in place⁹ or in preparation nor of other measures against cybercrime.

The purpose of this report is to help advance a discussion on the strengthening of cybercrime legislation in the island states of the Pacific region based on international standards, that is, the Budapest Convention.

The key suggestion is to carry out a detailed analysis of legislation in force or planned using the Budapest Convention as a benchmark and taking into account the experience of other countries. A regional workshop on cybercrime legislation with experts from Pacific countries responsible for legislation may help identify strengths and weaknesses and result in proposals for specific solutions.¹⁰

⁹ For legislation in the Pacific region: <http://www.paclii.org/>
To search databases on legislation: http://www.paclii.org/cgi-bin/sinosrch.cgi?method=all&meta=%2Fpaclii&mask_path=&mask_world=&query=computer&results=50&submit=Search&rank=on&callback=off&legisopt=&view=relevance&max=

¹⁰ Similar workshops have been organised by the Council of Europe with the Organisation of American States and the US Department of Justice in Trinidad and Tobago for the Caribbean region and in Colombia for countries of Latin America in 2008; and with ASEAN and the European Commission for ASEAN countries in Malaysia in 2008 and in the Philippines in 2010. In addition, a range of bi-lateral workshop have been held in different countries around the world.

2 CYBERCRIME LEGISLATION: INTERNATIONAL STANDARDS AND GOOD PRACTICES

In a state governed by the rule of law, criminal justice action must be based on law.¹¹ With regard to cybercrime this means that:

- conduct related to the attacks against computer systems and data and to attacks committed via computer systems and data need to be defined as criminal offences
- law enforcement are provided with procedural law powers to investigate cybercrime and secure volatile electronic evidence in an efficient measures
- countries are able to engage in international police and judicial cooperation in an efficient manner.

2.1 The Budapest Convention on Cybercrime¹²

The main international standard of reference in this respect is the Budapest Convention on Cybercrime.¹³ This treaty was developed by the Council of Europe (currently 47 member States).¹⁴ The fact that non-European countries (Canada, Japan, South Africa and the USA) participated in the drafting of this treaty indicates that it was intended to have a reach beyond Europe from the outset. All four have signed and the USA also ratified this treaty.

2.1.1 Criminalising conduct

In terms of conduct to be criminalised the Convention covers:

- Offences against the confidentiality, integrity and availability of computer data and systems
 - Article 2 – Illegal access
 - Article 3 – Illegal interception
 - Article 4 – Data interference
 - Article 5 – System interference
 - Article 6 – Misuse of devices
- Computer-related offences
 - Article 7 – Computer-related forgery
 - Article 8 – Computer-related fraud
- Content-related offences¹⁵
 - Article 9 – Child pornography
- Offences related to infringements of copyright and related rights
 - Article 10 - Offences related to infringements of copyright and related rights

¹¹ For an overview of the concept of the rule of laws as followed by the Council of Europe see: [https://wcd.coe.int/ViewDoc.jsp?Ref=CM\(2008\)170&Language=lanEnglish&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75](https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2008)170&Language=lanEnglish&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75)

¹² www.coe.int/cybercrime

¹³ www.coe.int/cybercrime

¹⁴ www.coe.int

¹⁵ With regard to content-related offences, an additional Protocol covers acts of racism and xenophobia committed through computer systems (CETS 189). See www.coe.int/cybercrime.

- Ancillary liability and sanctions
 - Article 11 – Attempt and aiding or abetting
 - Article 12 – Corporate liability

Most cybercrime consists of one or a combination of several elements of such conduct. Therefore, a country incorporating these articles of the Budapest Convention into its domestic legislation will cover most instances of cybercrime.

2.1.2 Procedural law tools for investigation

In terms of procedural law measures it includes:

- Article 16 – Expedited preservation of stored computer data
- Article 17 – Expedited preservation and partial disclosure of traffic data
- Article 18 – Production order
- Article 19 – Search and seizure of stored computer data
- Article 20 – Real-time collection of traffic data
- Article 21 – Interception of content data

Such a range of procedural law measures is unusual for an international treaty, but without such measures it would be very difficult to carry out cybercrime investigations and gather electronic evidence, in particular given the volatility of computer data.

Two points should be emphasised here:

- Article 14 gives these procedural law measures a very broad scope. They not only apply to the specific offences referred to in articles 2-11 of the Convention, but to “other criminal offences committed by means of a computer system” and the “collection of evidence in electronic form of a criminal offence”.
- Article 15 provides that conditions and safeguards are to be established under domestic law to ensure adequate protection of human rights and freedoms.

2.1.3 Measures for efficient international cooperation

These include:

- General principles
 - Article 23 – General principles relating to international cooperation
 - Article 24 – Extradition
 - Article 25 – General principles relating to mutual legal assistance
 - Article 26 – Spontaneous information
 - Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
- Specific provisions
 - Article 29 – Expedited preservation of stored computer data
 - Article 30 – Expedited disclosure of preserved traffic data
 - Article 31 – Mutual assistance regarding accessing of stored computer data

- Article 32 – Trans-border access to stored computer data with consent or where publicly available
- Article 33 – Mutual assistance in the real-time collection of traffic data
- Article 34 – Mutual assistance regarding the interception of content data
- Article 35 – 24/7 Network.

The chapter on international cooperation thus combines classical measures of international police and judicial cooperation with specific provisions for urgent action.

2.1.4 Accession by third countries

Member States of the Council of Europe and other countries that participated in the preparation of the Budapest Convention (Canada, Japan, South Africa, USA) can sign and subsequently ratify this treaty.

Other countries can nevertheless become a party by acceding to it under Article 37. By the time of accession, however, the necessary domestic legislation should be place so that the acceding country is capable of fully cooperating with other parties.

2.2 State of implementation and examples of good practice

2.2.1 State of implementation

By May 2010, the Budapest Convention on Cybercrime had been ratified by 29 countries, including the USA, and signed by a further 17 countries, including Canada, Japan and South Africa. Five countries had been invited to accede according to the procedure under Article 37, namely, Chile, Costa Rica, Dominican Republic, Mexico and the Philippines. Additional request were being processed. Australia also announced its intention to accede.

In addition, a large number of countries was making use of the Convention as a guideline for national legislation. From the Asia/Pacific region these included countries such as Cambodia, India, Indonesia, Malaysia, Pakistan, Sri Lanka, Vietnam and others.

2.2.2 Examples of good practice

2.2.2.1 Country profiles¹⁶

The Council of Europe, under its global Project on Cybercrime, has compiled a number of country profiles to show how countries have implemented the provisions of the Budapest Convention into domestic legislation.

These may be useful for countries of the Pacific region. They may also wish to prepare such country profiles for their own countries in order to facilitate the analysis of legislation in place and the drafting of further laws.

2.2.2.2 Romania

¹⁶ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp

The legislation adopted by Romania in 2004 is a good example of implementation. The text follows the Budapest Convention very closely, and successful investigations and prosecutions are evidence that it works in practice.¹⁷

2.2.2.3 Commonwealth Model Law¹⁸

Based on the Budapest Convention, in 2002, the Commonwealth Model Law on Computer and Computer-related Crime was adopted in 2002. The text follows very closely the wording of the Budapest Convention. The main differences are that it does not cover computer-related forgery and fraud, nor does it contain provisions for international cooperation. Nevertheless, a country having implemented this Model Law will be largely compliant with the Budapest Convention.

2.2.2.4 Barbados Computer Misuse Act 2005-4¹⁹

Barbados is a good example of a country that developed domestic legislation based on the Commonwealth Model Law. This is clearly reflected in the Computer Misuse Act of 2005.

It seems that from the Pacific region, Tonga has also made use of the Commonwealth Model Law when preparing the Computer Crimes Act 2003.

3 ANALYSING CYBERCRIME LEGISLATION IN THE PACIFIC REGION

An analysis of the legislation could start with a review article by article of legislation in place against the provisions of the Budapest Convention.

Such a review is likely to show that Tonga through the Computer Crimes Act 2003 legislation seems to be largely in line with international standards. Having followed the Commonwealth Model Law the Act of 2003 does not contain specific provisions on forgery and fraud nor on international cooperation. One would need to analyse other laws to verify whether these are covered. The same applies to child pornography. Given that this Act has been in force for several years, case law and practical experience would certainly provide insights into the effectiveness of the Act. Furthermore, the nature of sanctions would need to be looked into. For example, systems interference – which could involve a major denial of service attack against critical infrastructure – the penalty is “a fine not exceeding \$ 5,000 or imprisonment for a period not exceeding 1 year of both” (Section 6).

The Telecommunications Act 2004 of Kiribati and the Fiji Crimes Decree of 2009 seem to meet only some requirements, although it is possible that these are covered by other laws.

Budapest Convention	Tonga (Computer Crimes Act 2003)	Kiribati (Telecommunications Act 2004)	Fiji (Crimes Decree 2009)
Use of terms/ Definitions			

¹⁷ See country profile Romania with legislation in the appendix:

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Romania%20_April%202008_.pdf

¹⁸ http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

¹⁹ http://www.oas.org/juridico/spanish/cyb_bbs.htm

Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”	Section 2	Section 64(1)	
Substantive criminal law			
Article 2 – Illegal access	Section 4	Section 65	Section 340 and Section 341
Article 3 – Illegal interception	Section 7	Section 68	
Article 4 – Data interference	Section 5	Section 66	Section 340, Section 343 and 344
Article 5 – System interference	Section 6		Section 340, Section 342, Section 344
Article 6 – Misuse of devices	Section 8	Section 66	Section 345 and Section 346
Article 7 – Computer-related forgery			
Article 8 – Computer-related fraud			
Article 9 – Offences related to child pornography		Section 70	
Article 10 – Offences related to infringements of copyright and related rights			
Article 11 – Attempt and aiding or abetting			
Article 12 – Corporate liability			
Article 13 – Sanctions and measures			
Procedural law			
Article 14 – Scope of procedural provisions			
Article 15 – Conditions and safeguards			
Article 16 – Expedited preservation of stored computer data	Section 13 Section 17 (regarding Article 16(3))		
Article 17 – Expedited preservation and partial disclosure of traffic data	Section 13 with Section 12		
Article 18 – Production order	Section 11		
Article 19 – Search and seizure of stored computer data	Section 9 and Section 10		
Article 20 – Real-time collection of traffic data	Section 15 Section 17 (regarding Article 20(3))		
Article 21 – Interception of content data	Section 14 Section 17 (regarding Article 21(3))		
Jurisdiction			
Article 22 – Jurisdiction	Section 3		
International co-operation			
Article 24 – Extradition			
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			
Article 28 – Confidentiality and limitation on use			
Article 29 – Expedited preservation of stored computer data			
Article 30 – Expedited disclosure of preserved traffic data			
Article 31 – Mutual assistance regarding accessing of stored computer data			
Article 32 – Trans-border access to stored computer data with consent or where publicly available			
Article 33 – Mutual assistance in the real-time collection of traffic data			
Article 34 – Mutual assistance regarding the interception of content data			
Article 35 – 24/7 Network			

4 CYBERCRIME LEGISLATION IN CONTEXT: STRATEGIC APPROACHES TO CYBERCRIME AND CYBERSECURITY

4.1 Strategic approaches on cybercrime and cybersecurity

In state governed by the rule of law, legislation is to be the basis for criminal justice action against cybercrime. At the same time, legislation is only a starting point for a broader range of measures.

Countries and organisations increasingly adopt policies and strategies aimed at enhancing cyber security, that is, to primarily protect information technologies. Examples are:

- Australia: Cyber Security Strategy 2009²⁰
- United Kingdom Cyber Security Strategy 2009²¹
- Estonia: Cyber Security Strategy 2008²²
- European Union: Stockholm Programme (2009)²³ and EU Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime (2010).²⁴

It would seem that while with the Pacific Regional Digital Strategy (SOPAC)²⁵ a broader framework was adopted, specific strategies on cybersecurity or cybercrime are not yet available.

4.2 Other Council of Europe instruments and tools on cybercrime

While the Budapest Convention represents the core of the Council of Europe's approach against cybercrime, a number of other instruments and tools have been developed that offer a more comprehensive array of measures regarding cybercrime or Internet governance in a broader sense.²⁶

4.2.1 Additional treaties

Additional legally binding treaties that are open for accession to third countries and contain elements related to cybercrime and Internet security include:

- Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data (CETS 108) and additional Protocol (CETS 181)

²⁰ <http://www.ag.gov.au/cybersecurity>

²¹ <http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf>

²² http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

²³ <http://register.consilium.europa.eu/pdf/en/09/st17/st17024.en09.pdf>. The European Union, among other things, calls for global implementation of the Budapest Convention on Cybercrime.

²⁴ <http://www.enisa.europa.eu/media/news-items/council-cyber-crime>

²⁵ <http://www.sopac.org/Digital+Strategy>

²⁶ The overall approach of the Council of Europe regarding Internet governance issues is reflected in the submission of the Secretary General to the Internet Governance Forum in Sharm El Sheikh, Egypt, November 2009 (see [http://www.coe.int/t/information/society/documents/SG_Inf\(2009\)19_en.pdf](http://www.coe.int/t/information/society/documents/SG_Inf(2009)19_en.pdf)). The submission to the 12th United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, April 2010) provides an overview of relevant rule of law standards and practices of the Council of Europe http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/SG%20Inf%20_2010_4%20-%20UN%20Crime%20congress_ENGLISH.pdf

- Additional Protocol to the Convention on Cybercrime concerning the Criminalisation of Acts of Racist and Xenophobic Nature Committed Through Computer Systems (CETS 189)
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)
- Convention for the Prevention of Terrorism (CETS 196)
- Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198)
- (Draft) MEDICRIME Convention on counterfeiting of medical products and similar crimes involving threats to public health (to be opened for signature in autumn 2010).

4.2.2 Contact points for international cooperation

Cybercrime is very much transnational crime. Attacks launched by a person in one country or jurisdiction can affect persons in multiple other countries, and even an email communication sent to a person in the same country may generate electronic evidence elsewhere as data may be transmitted through servers in several countries. At the same time electronic evidence is volatile. Thus, urgent measures that are needed to preserve data at the national level are also necessary within the framework of international co-operation.

Chapter III of the Convention on Cybercrime provides a legal framework for international cooperation with general and specific measures, including the obligation of countries to cooperate to the widest extent possible, urgent measures to preserve data and efficient mutual legal assistance.

An important provision in this respect is Article 35 on the creation of points of contact available 24 hours a day, seven days a week, to facilitate international cooperation:

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

- a the provision of technical advice;
- b the preservation of data pursuant to Articles 29 and 30;
- c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

This Article is very much based on the experience of the G8 Sub-group on High-tech Crime that established a network of such contact points already in 1997. It currently comprises more than 50 members.

4.2.3 Guidelines for the cooperation between law enforcement and Internet service providers²⁷

²⁷ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

Both, law enforcement and Internet service providers play a crucial role in building trust in information and communication technologies (ICT) and helping societies around the world make best use of these technologies. As the investigation of cybercrime by law enforcement is often not effective without the cooperation of Internet service providers, it is essential that both cooperate with each other in an efficient manner. The roles of both are different: law enforcement must uphold the law, while service providers are to provide users with the ability to communicate.

The question that many countries are faced with is how both can best cooperate with each other to make the Internet safer while at the same time respect their different roles and the fundamental rights of users.

A crucial part of the solution - and in many ways a precondition for cooperation - is clear legislation that defines responsibilities, authorities and limitations. Full implementation of the Convention on Cybercrime, in particular its procedural law provisions, is essential in this respect.

Discussions in many countries all over the world have shown the need for practical guidelines that can help law enforcement and service providers organise and structure their cooperation.

In 2007, therefore, the Council of Europe - under the Project on Cybercrime - set up a working group with representatives from law enforcement, industry and service provider associations that prepared draft guidelines which were adopted by the global Octopus Interface conference in Strasbourg in April 2008. They:

- include common guidelines for both law enforcement and service providers and specific guidelines for each of them
- are not to substitute legislation or other formal regulations, but rather to supplement and help regulations work in practice
- are based on good practices already available
- are to be adapted to the specific circumstances in each country.

In practical terms, representatives of law enforcement and service providers in a given country may establish a working group with the aim of reaching an understanding or even a formal agreement on how to cooperate with each other. The guidelines could serve as a blueprint or simply as a basis for discussion.

4.2.4 Training²⁸

Many crimes involve information technologies in one way or the other. Particular efforts are therefore required to enable law enforcement authorities, judges and prosecutors to investigate, prosecute and adjudicate cybercrime as well as to secure and make use of electronic evidence through training, networking and specialisation.

Given the very limited opportunities in all regions of the world for judges and prosecutors to be trained, the Council of Europe in 2009 developed a concept paper for the training of judges and prosecutors in cybercrime and electronic evidence matters. It is aimed at helping judicial

²⁸ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/default_en.asp

training institutions develop and integrate such training in regular initial and in-service training. It is to furthermore facilitate networking among judges and prosecutors to enhance their knowledge as well as consistent support to training initiatives by interested partners.

Regarding law enforcement training, the Council of Europe participates in the European Cybercrime Training and Education Group (ECTEG)²⁹ and facilitated the launching of the 2Centre³⁰ initiative of Centres of Excellence for Cybercrime Training. Both, the training approach promoted by ECTEG, including the course materials developed during the past ten years, and the 2Centre initiative may be of interest to the Pacific island States.

4.2.5 Specific measures for the protection of children

Fostering children's trust and confidence in the Internet coupled with the protection of their dignity, security and privacy is a priority for the Council of Europe. The Internet is a space of freedom to express and communicate, to search for information and to learn, to work and to play. Access to the Internet thus offers great potential for children to exercise and enjoy their rights and values through the Internet.

At the same time, threats such as cybercrime and the sexual exploitation and abuse of children through information and communication technologies pose particular challenges. The Council of Europe is addressing these by setting common standards and policies, by supporting educational, preventive and other measures to empower children, by promoting criminal justice action and by strengthening multi-stakeholder and international cooperation.³¹ These may also be of interest to countries of the Pacific region.

²⁹ <http://www.2centre.eu/europolwg>

³⁰ <http://www.2centre.eu/>

³¹ For an overview and links to these measures see:

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Protecting%20children/Default_en.asp

5 THE WAY AHEAD: SUGGESTIONS

As indicated in the introduction, the purpose of this report is point at possible steps that island states of the Pacific could take to strengthen their legislation and take other measures to cope with the challenge of cybercrime. Steps could include:

1. Review of legislation against the provisions of the Budapest Convention on Cybercrime and the Commonwealth Model Law. A regional workshop could be held for experts in criminal law drafting. The appendix to this report could serve as a working document for such a workshop. The workshop could have as its outcome a profile for each country showing provisions already in place as well as gaps that need to be closed.
2. Based on this review, legislative amendments or laws would need to be prepared.
3. In addition to specific provisions on cybercrime, countries may consider additional legislative measures regarding the protection of children, the protection of personal data, the prevention of terrorism and others
4. Countries that have not yet done so, may consider the establishment of high-tech crime units and other specialised police and prosecution services.
5. Countries may establish 24/7 points of contact for urgent international cooperation.
6. Agreements may be concluded between law enforcement and Internet service providers regarding their cooperation in the investigation of cybercrime.
7. A strategy for sustainable law enforcement training may be developed and implemented.
8. Cybercrime and electronic evidence issues could be integrated into the curricula of judicial training institutions for judges and prosecutors.
9. Preventive and educational programmes should be designed for the online protection of children, but also to prevent cybercrime in general.
10. Consider designing broader strategies on cybercrime and/or cybersecurity