

ITU Regional Cybersecurity Forum for Asia-Pacific¹

Session 8: Cybersecurity and Small Islands Developing States

Brisbane 16-18 July 2008

Notes for presentation

Overview of Cyber Legislation in the Pacific Islands

Professor A. H. Angelo

Introduction

Cybersecurity is a problem. In the last few weeks alone in the Pacific Islands there has been international news coverage of the intentional severing of a fibre optic cable in one country and a DOS attack in another. One was a domestic incident and undoubtedly covered, if not by specific laws, by generic domestic law, and able to be prevented and prosecuted. The other, the DOS attack, was externally generated and therefore a much more difficult, if not impossible, matter to deal with. Happily there are now many legal tools available to address the issues of cybersecurity and there is an international environment receptive to the idea of cooperation on matters of cybersecurity.

It is the purpose of this comment to give a brief overview of cybersecurity law in the countries of the South Pacific, to consider the main model laws and legislative examples available to Pacific countries as they seek to deal with cybersecurity matters, and then to reflect on a proper approach to dealing with the needs of Pacific countries.

Cybersecurity presents problems for the world and obviously the small countries of the Pacific. It is a problem that needs to be addressed and addressed at the earliest possible date. It needs to be dealt with because of the general issues relating to state security; action is needed also to make way for the future and foreseeable developments in the area of globalisation as it effects the movement of goods and persons. Increasingly these movements are subject to international exchange of information by cyber communication. Before a country will be able to participate, for instance, in any single window development of the

¹ For more information on the ITU Regional Cybersecurity Forum for Asia-Pacific see the forum website at www.itu.int/ITU-D/cyb/events/2008/brisbane/

World Customs Organisation, it will be necessary for that country to be able to guarantee cybersecurity.

The Pacific Situation

The countries of the South Pacific have very little legislation specific to cybersecurity. Most countries would rely, if the issue were to arise in court, on their general criminal laws and particularly those relating to damage to property. There are also some provisions in legislation relating to civil aviation and broadcasting which could be called in aid. New Zealand, Australia, Kiribati and Tonga do have some specific legislation. In New Zealand the main rules are those now found in the Crimes Act 1961 sections 248-252; there are also some provisions in the anti-spam legislation. In Australia the main legislative provisions can be found in the Cybercrime Act 2001 and the Security Legislation Amendment (Terrorism) Act 2002. Kiribati provides for cybersecurity under Part VII (especially sections 64-69) of its Telecommunications Act 2004. Tonga has dedicated legislation in its Computer Crimes Act 2003.

The Tongan legislation shows a clear influence of the European Convention on Cybersecurity. Provisions of that Convention are also reflected in the New Zealand statute. The Australian legislation covers the matters of the Convention but shows no evidence of direct influence from the Convention. The law of Kiribati follows a different pattern and reflects to a degree the Australian legislation. The detail of the provisions varies. The important thing is that each of these countries has taken steps to address cybersecurity.

As a general comment it can be stated that for the small Pacific countries it is likely that New Zealand legislation is likely to provide a better example than Australia simply because the New Zealand legislation is geared to the needs of a small non-federal state. Further the manner of presentation – the drafting style – of current New Zealand legislation is more accessible in countries where English is not the first language of administrators.

Available Precedents and Model Laws

There is now much help available for Pacific administrators and legislators in the form of conventions, model laws, foreign precedents, and guidelines. Of particular relevance in this regard are documents emanating from the ITU, European institutions, and the Commonwealth.

The ITU

Most recent, (and perhaps too recent to have yet been fully appreciated), are the ITU documents: in particular the draft ITU Study Group Q.22/1 Report of January 2008, and the draft ITU National Cybersecurity/CIIP Self-Assessment Toolkit of January 2008.

The Toolkit follows closely the line of thinking of the European Convention on Cybersecurity. The survey in Annex 1 identifies the purpose of each of the key elements of the Convention and describes that element and in most cases provides a specific example. The examples greatly aid accessibility to the provisions of the Convention and facilitate the completion in respect of any country of the self-assessment grid which is part of the Annex. The points made in paragraph 1-31 of the survey can be directly aligned with the Convention.

All these ITU documents are of considerable assistance in clarifying the issues and in setting out a clear pattern for developing a country response to cybersecurity needs.

The European Initiatives

The European Convention on Cybersecurity remains an impressive model and provides a starting point for domestic legislation on cybersecurity and also offers a strong basis for international cooperation for those interested in effectively addressing cybersecurity issues. As at July 2008 45 states had signed the Convention but only 23 had ratified it. Only one state outside of Europe has ratified and that is the USA. Of the other 22 countries in which the Convention is in force, France, Italy, the Netherlands, and Norway are the most important. Interestingly, Germany, Spain, and the UK have signed but not yet ratified. Only one country in the Asia-Pacific region has signed – that is Japan.

This data raises questions about the nature and role of the Convention, but clearly the participation of the USA is of great importance not only for the operation of the Convention but also for countries in the Pacific. Article 38 of the Convention provides that a state may, when it becomes party to the Convention, “specify the territory or territories to which this Convention shall apply”. At the time of ratification France made no express statement about its territories. This is a matter of special interest to the Pacific – if the Convention were to apply in French Polynesia, New Caledonia, and Wallis and Futuna, Pacific coverage by the Convention would immediately be significant.

From Europe there are other useful documents and models notably the Directive on Privacy and Electronic Communications of July 2002, the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks on information systems, the Communication (COM(2006) 688 final) on Fighting Spam, Spyware, and Malicious Software, and the Communication (COM(2007) 267 final) Towards a General Policy on the Fight against Cyber Crime.

The European Convention on Cybersecurity is very good. It provides minimum standards and those minimum standards can be readily adapted for national legislation. A rough and ready adaptation of the Convention requirements to a legislative form that could suit most Pacific Island countries is attached to this paper. It is a quickly prepared Act based on the European Convention. In terms of the criminal offences, it follows the Convention almost word for word. This has the real advantage that national courts can, for the interpretation and application of the law, refer to the background to the Convention and to the European experience with the Convention both at the national and regional level. The document is very much an early draft whose purpose is to indicate how in a simple manner the Convention could be adapted to Pacific country circumstances. The Convention offers within itself many options. The appended draft is a bare version and has adopted the Convention approach of least sophistication. In terms of enforcement procedures and international cooperation, the draft proposes reliance on existing court procedures and an alignment with already existing extradition and mutual assistance laws. It is clearly a less polished document than the Commonwealth models but in its use of the Convention and reliance on existing legal procedures it is very similar.

The Commonwealth

The Commonwealth responded to the Convention on Cybercrime of the Council of Europe in 2002 by preparing two model laws for the use of Commonwealth countries. Those drafts are the Computer and Computer Related Crimes Act and the Electronic Evidence Act. These are succinct, clearly presented, and speak directly to the systems of small Commonwealth common law countries. They are probably the best available examples for the countries of the South Pacific: the next best would be the Tongan Act. All reflect the Convention of the Council of Europe.

Specific legislation of European countries such as the Regulation of Investigatory Powers Act 2000 of the UK (which covers 106 pages of text) are clearly inappropriate to the Pacific situation.

Pacific Needs

The EC Communication of 2006 identifies three factors critical to success in relation to the cybersecurity matters which it addressed:

- A strong commitment by central government to fight on-line malpractices
- Clear organisational responsibility for enforcement activities
- Adequate resources for the enforcement authority.

The ITU Study Group Q.22/1 Report identifies the goal for cybersecurity in complementary terms. At page 9 it is stated

Developing and implementing national cybersecurity plan requires a comprehensive strategy that includes an initial broad review of the adequacy of current national practices and the consideration of all stakeholders... in the process. This means developing a plan, and developing a plan requires an assessment of the present situation. For that assessment the Toolkit is excellent.

The focus in the Pacific Ocean area needs however to be specifically calibrated to the Pacific situation. That is highlighted in the Doha Action Plan in Annex 3 (Asia-Pacific regional initiatives). Paragraph 4 of that Annex states clearly the unique challenges of “isolation, distance and lack of resources”.

Looking at the independent countries of the Pacific it is apparent that a ‘bottom-up’ approach to cybersecurity is desirable. The strategies developed in the international documentation undoubtedly suit most countries of the world. They may not, however, have immediate application to countries which have fewer than 100,000 people or which have weak government structures. Perhaps only three countries of the South Pacific have conditions which approach the paradigm that the documents address. The documents talk of government/industry collaboration – yet there may be no ‘industry’–, they also speak of private sector groups interested in IT, and of R & D. These are not features of the environment in most countries in the South Pacific.

The Q.22/1 Report states in Part III (page 27) that deterring cybercrime can be greatly improved by the proper use of criminal law and procedures. Use of the Toolkit and

completion of its table will disclose the strengths and weaknesses of each national legal system.

Part III states that the law needs to address cybercrime 'per se', have appropriate procedures and provide for collaboration with other countries. This is clearly a necessary approach. There is too much at stake to have to depend on a general law designed for physical documents and landline telephone communications. Whether an electronic impulse is 'property', whether 'damage' is done by stopping the receipt of a message, or whether data in a computer is a 'document' should be specifically addressed by legislation. As the technology has developed, countries' general criminal law has struggled to deal with these issues.

The first of the requirements mentioned in the European Commission Communication of 2006 was "commitment". Out of that commitment will come dedicated laws. Those laws will in turn identify the responsible organisations. The third step involves the practicalities – are there adequate resources for the monitoring and protecting of cybersecurity? This relates again to government planning, to foresight and to leadership.

If the prescription in the EC Communication of 2006 is relevant to Europe, it is even more relevant in the Pacific. In the Pacific the starting point has to be the national situation; regional specificities must be taken into account. That means the physical vulnerability of the countries, their limited infrastructure, their limited human resources, and typically the government dominance of the IT world. The Q.22/1 Report at page 30 speaks for instance of investigation units "even if they consist of a limited number of investigators". But many countries in the Pacific region may have as few as one person who is trained as an engineer or is appropriately skilled to act as an investigator of a cybersecurity incident.

The Q.22/1 Report at page 32 also speaks of training prosecutors, judges and legislators. The sequence should in the small Pacific countries start with the legislators. It is important to get them to understand the issues and to enact the necessary laws. Following that the local infrastructure can be built up and only then would it be the time for the informing of investigators, prosecutors and judges. With all that in place domestically, international cooperation will proceed more easily. In terms of the prosecutors and investigators, law enforcement tasks generally fall to the police – that is to say there are no specialisation relative to the nature of the crime. Judges at the local level are most likely to be persons

indigenous to the country but at the superior court level many of the judges are expatriate and they bring with them their knowledge of cybercrime, be it from Australia, New Zealand, the UK, or the USA.

It is equally clear, given the ubiquity of electronic communication, that no one country can solve the problems alone. It is interesting to note that the major regional planning document – the Pacific Plan of the Pacific Islands Forum – has very little to say about telecommunications and nothing about cybersecurity. The Pacific Plan has for some years been the focus of regional diplomatic endeavours of the Forum Secretariat and the intention is that it will continue to be so for many years to come. It is seen as a blueprint for future regional activity and as a living document. At the regional level if cybersecurity is to be insured at a national level, cybersecurity should find a place as a priority item in the Pacific Plan.

Conclusion

In the Pacific countries it is important to take the goals and aspirations of the ITU documents and to use them as the basis for mapping the way forward. If the hypothesis is little or no government money for cybersecurity, and one, two, three, four or five people who understand the issues, what then will the planning document look like? On the basis of the document informed by the local circumstances, it will be possible to establish what it is realistic to expect can be done, and thence to understand what cooperation is required and what others must do.

In the absence of regional coordination each country should move ahead as quickly as it can with its anti-spam legislation and with its cybersecurity legislation. Ultimately there will be regional coordination and cooperation as other countries put their policies in place. Every step forward however is an important one.

Attachment
Discussion Draft – Cybercrime Act 2008

1 Short title

This is the Cybercrime Act 2008.

2 Objective

The purpose of this Act is to better provide for cybersecurity and the combating of cybercrime and, for that purpose, to foster cooperation with other states and the parties to the Convention on Cybercrime of the Council of Europe of 2001.

3 Interpretation

(1) In this Act –

"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; "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;

"service provider" means –

- (a) any public or private entity that provides to users of its service ability to communicate by means of a computer system, and
- (b) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

"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.

(2) In interpreting this Act reference shall be made to the preparatory documents relating to the Convention on Cybercrime and to the documents and precedents relating to the implementation of the Convention.

4 Illegal access, interception and interference

The following are offences –

- (a) intentional access to the whole or any part of a computer system without right;

- (b) intentional 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;
- (c) intentional damaging, deletion, deterioration, alteration or suppression of computer data without right;
- (d) intentional serious hindering, without right, of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

5 Misuse of devices

- (1) It is an offence intentionally and without right –
 - (a) to produce, sell, procure for use, import, distribute or otherwise make available
 - (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in section 4(a) to (d);
 - (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 section 4(a) to (d);
 - (b) to possess of an item referred to in subparagraph (a), with intent that it be used for the purpose of committing any of the offences in section 4(a) to (d).
- (2) This section 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 subsection (1) is not for the purpose of committing an offence under section 4(a) to (d), such as for the authorised testing or protection of a computer system.

6 Computer-related forgery

It is an offence intentionally and without right, to input, alter, delete, or suppress 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 whether or not the data is directly readable and intelligible.

7 Computer-related fraud

It is an offence intentionally and without right, to cause 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.

8 Offences related to child pornography

- (1) When committed intentionally and without right, the following conduct is prohibited –
 - (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) In this section “child pornography” includes 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) In this section “minor” includes all persons under 18 years of age.
- (4) A person who does anything prohibited by subsection (1) commits an offence.

9 Offences related to infringements of copyright and related rights

- (1) A person commits an offence who wilfully, on a commercial scale and by means of a computer system, infringes copyright as protected pursuant to the obligations undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions.
- (2) A person commits an offence who wilfully, on a commercial scale and by means of a computer system infringes copyright as protected pursuant to the obligations undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions.

10 Corporate liability

- (1) Where an offence is committed by –
 - (a) an agent, the person for whom the agent is acting;
 - (b) a body corporate, every person who, at the time of the commission of the offence, was concerned in the management of the body corporate or was purporting to act in that capacity, shall also commit the like offence.
- (2) It is a defence to a charge under this section if it is approved that the offence was committed without the knowledge or consent of the accused and that the accused took all reasonable steps to prevent the commission of the offence.
- (3) Liability under this section is without prejudice to the criminal liability of any natural person who has committed the offence.

11 Sanctions and measures

Any person who commits an offence under this Act is liable on conviction to a fine not exceeding ... and imprisonment for a period not exceeding 10 years.

12 Processes and orders

The processes and orders available in the general law for delivery up, discovery and injunction are, for the purposes of this Act, applicable with equal force to computer systems, computer data, and traffic data as they are to documents and other things.

13 Real-time collection of traffic data

The High Court may, on application of the designated authority, –

- (a) by order permit the designated authority to collect or record through the application of technical means, and
- (b) by order compel a service provider, within its existing technical capability –
 - (i) to collect or record through the application of technical means, 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 transmitted by means of a computer system.

14 Interception of content data

In relation to serious offences as prescribed by regulations under this Act, the High Court may on application of the designated authority –

- (a) by order permit the designated authority to collect or record through the application of technical means, and
- (b) by order compel a service provider, within its existing technical capability –
 - (i) to collect or record through the application of technical means, or
 - (ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications transmitted by means of a computer system.

15 Confidentiality

- (1) A service provider shall keep confidential the fact of the execution of any power provided for in this section and any information relating to it.
- (2) A service provider who fails to comply with subsection (1) commits an offence.

16 Jurisdiction

This Act applies to offences against this Act committed –

- (a) in [country name]; or
- (b) on board a ship flying the flag of [country name]; or
- (c) on board an aircraft registered under the laws of [country name]; or
- (d) by a citizen or permanent resident of [country name], 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.

17 Extradition

Offences against this Act are, for the purposes of the laws of extradition, extraditable offences and subject as such to the general law relating to extradition.

18 General principles relating to mutual assistance

An offence against this Act is a “serious offence” for the purposes of the Proceeds of Crime Act and the Mutual Assistance in Criminal Matters Act.

19 Confidentiality and limitation on use

- (1) When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, this section shall apply.

(2) The requested Party may make the supply of information or material in response to a request dependent on the condition that it is –

(a) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

(b) not used for investigations or proceedings other than those stated in the request.

(3) If the requesting Party cannot comply with a condition referred to in subsection (2), it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

(4) Any Party that supplies information or material subject to a condition referred to in subsection (2) may require the other Party to explain, in relation to that condition, the use made of such information or material.

20 Designated authority

The Commissioner of Police/the Director of Telecommunications is the designated authority for the purposes of this Act.

21 24/7 Network

(1) The designated authority is 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.

(2) The assistance includes facilitating or directly carrying out the following measures –

(a) the provision of technical advice;

(b) the preservation of data;

(c) the collection of evidence;

(d) the provision of legal information; and

(e) the locating of suspects.

22 Regulations

Regulations may be made for the purposes of this Act.

[Restraining injunctions – ~~The High Court may, on the application of any person, grant an injunction restraining a person from engaging in conduct that constitutes or would constitute an offence under this Act.]~~