CYBER SECURITY AND LEGISLATION IN THE PACIFIC

A H Angelo*

This comment gives a brief overview of cybersecurity law in the countries of the South Pacific, considers the main model laws and legislative examples available to Pacific countries as they seek to deal with cybersecurity matters, and then reflects on a proper approach to dealing with the needs of Pacific countries. Particular reference is made to the Council of Europe Convention on Cybercrime of 2001[1] *(the European Convention) as a legislative precedent. By way of conclusion, a Pacific model law is proposed which takes cognisance of the limitations in national infrastructures but which would still be consistent with international cybersecurity laws.*

Cet article permet de dresser un tableau des règles de droit interne et des conventions internationales applicables en matière de cybersécurité dans les principaux pays de la zone Pacifique. Sont également précisées quelles pourraient être les autres solutions envisageables susceptibles d'assurer dans ce domaine, une protection des petits Etats insulaires du Pacifique. Dans ce contexte, les règles édictées par la Convention sur la cybercriminalité du Conseil de l'Europe de 2001 servent de fil conducteur à la réflexion de l'auteur qui propose ce qui pourrait former le cadre d'une future convention internationale adaptée aux besoins spécifiques de ces petits en matière de cybercriminalité et de cybersécurité.

I INTRODUCTION[2]

Cybersecurity[3] in the Pacific islands is a problem. At the time of the ITU Cybersecurity Forum in Brisbane in 2008, international news coverage was telling of the intentional severing of a fibre optic cable in one country and a DOS attack in another. One was a domestic incident and

* Professor, Faculty of Law, Victoria University of Wellington, New Zealand. This is an edited version of a paper first presented at the ITU Cybersecurity Forum in Brisbane 2008.

1 Council of Europe Convention on Cybercrime (23 November 2001) ETS 185 (available at www.coe.int).

2 This paper has been adapted from an "Overview of Cyber Legislation in the Pacific Islands" conference paper presented at the ITU Regional Cybersecurity Forum for Asia-Pacific *Cybersecurity and Small Islands Developing States* (Brisbane, 2008) available at www.itu.int.

3 The terms "cybersecurity" and "cybercrime" are used interchangeably throughout this paper.

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.

Cybersecurity presents problems that need to be addressed and addressed at the earliest possible date. It needs to be dealt with because of issues relating to state security. Action is needed also to make way for future and foreseeable developments in the area of globalisation as it effects the movement of goods and persons. Increasingly these movements are subject to the international exchange of information by cyber communication. Before a country will be able to participate, for instance, in Single Window developments,[4] that country will need to be able to guarantee cybersecurity.

II 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 on the general criminal law relating to damage to property. Some countries also have provisions in legislation relating to civil aviation and broadcasting which could be called in aid. Australia, Kiribati, Tonga and New Zealand do have some specific legislation. The detail of the provisions varies but the important thing is that each of these countries has taken steps to address cybersecurity.

A Australia

In Australia the main legislative provisions can be found in the Cybercrime Act 2001 and the Security Legislation Amendment (Terrorism) Act 2002. The Cybercrime Act is based on the Computer Misuse Act 1990 (UK),[5] and also covers the matters in the European Convention but shows no evidence of direct influence from that Convention. The Cybercrime Act is an omnibus Act which has no substantive provisions but which amends a number of other statutes: the Australian Security Intelligence Organisation Act 1979; the Crimes Act 1914; the Criminal Code Act 1995; the Education Services for Overseas Students Act 2000; the Telecommunication (Interception) Act 1997; and the Customs Act 1901. Most importantly the Cybercrime Act inserts a new Part 10.7 into the Schedule of the Criminal Code Act 1995.

---

4 "Single Window" is a cross-borders trade facilitation measure that utilises a single standard form for traders/transporters to satisfy all import, export, and transit regulations. The concept is dependent on the establishment of a clear and consistent system and ready and secure communication.

5 See Cybercrime Bill 2001 Digest.

Part 10.7 of the Schedule to the Criminal Code Act 1995 deals with three types of computer misuse (unauthorised access, unauthorised modification, and unauthorised impairment), and has four levels of offending. In general unauthorised access as such is not an offence.[6] Section 477.1 deals with computer misuse with intention to commit an offence punishable by imprisonment of 5 years or more. There is no requirement that the misuse be intended for benefit or gain. Sections 477.2 and 477.3 cover modification or impairment of data or electronic communication with the intention to cause that modification or impairment or recklessness as to that result. The maximum penalty for both is imprisonment for 10 years. Section 478.3 addresses possession and control of data. Intention to commit a computer offence is required; recklessness is not enough. Sections 478.1 and 478.2 deal with the lowest level of computer offending: access or modification of restricted data and impairment of computer disk data. A person must intend the access, modification, or impairment and must know that what is done is done without authorisation.[7]

There are a number of special definitions in Part 10.7. There has been criticism that these provisions have been drafted too widely and will encompass some computer-related activity that is not criminal.[8] A clearer distinction could be made between behaviour that is hurtful or destructive and that which is innocent or unintended. This may involve separately defining what is "unauthorised" in relation to access, modification and impairment.[9]

B Kiribati

Kiribati provides for cybersecurity under Part VII (especially sections 64-69) of its Telecommunications Act 2004. The law of Kiribati reflects to a degree the Australian legislation. The three main offences are unauthorised access (section 65), unauthorised modification (section 67), and unauthorised use or interception (section 68). Access is defined separately and unauthorised access includes access beyond the scope of authorisation (section 64(5)).

C Tonga

Tonga has dedicated legislation in its Computer Crimes Act 2003. The Tongan legislation shows clear influence of the Europe Convention. It contains extensive procedural powers (Part III) in line with the cooperative approach of law enforcement envisaged by the European Convention. There are four types of computer offences: illegal access (section 4); interference with data or a computer

---

6 See Criminal Code Act 1995 (Cwlth), ss 477.1, 478.1 compared with Crimes Act 1961 (NZ), s 252.

7 Sections 478.1 and 478.2 appear to require a higher level of intention (knowledge and intent) for a lower penalty (2 years) in comparison to sections 477.2 and 477.3 which require a lower level of intention (knowledge and recklessness) for a higher penalty (10 years).

8 Greg Taylor "The Council of Europe Cybercrime Convention: a civil liberties perspective" (2001) 8 PLPR 69.

9 Sections 476.1 and 476.2.

system (sections 5 and 6); illegal interception (section 7); and illegal devices (section 8). For sections 5, 6 and 8, wilfulness or recklessness are sufficient to establish the offence.

D New Zealand

In New Zealand the main rules are in the Crimes Act 1961 sections 248-252 (Part X); there are also some provisions in the anti-spam legislation.[10] The Crimes Amendment Act 2003 was passed following a lengthy gestation period. In 1998 the Law Commission published a report that found New Zealand legislation required major law reform to deal adequately with criminal misuse of computers.[11] The Report recommended the creation of four new offences in relation to computer misuse: unauthorised interception; unauthorised access; unauthorised use; and unauthorised damage. In 1999, the Crimes Amendment (No 6) Bill was introduced to update the Crimes Act by addressing the legislative inadequacies highlighted in the Law Commission's Report. The Amendment Act was eventually passed and came into force on 1 October 2003.[12]

The Amendment Act introduced into the Crimes Act 1961 a new Part X for crimes involving computers. Part X is widely drafted to keep pace with rapid technological advances. Provisions of the European Convention are reflected in this Part. It covers a range of computer-related criminal activities beyond the more well-known hacking and cracking. There are four main computer-related offences: access for dishonest purpose (s 249); damage or interference (s 250); software for committing crime (s 251); and access without authorisation (s 252). Section 249 covers the use of computers to commit fraud or forgery. The offence is satisfied if the access occurred with the intention and a dishonest purpose but without the need to actually benefit or gain from that access.[13] Section 250 addresses unauthorised access causing damage or interference including denial of service attacks. Intention or recklessness is required. Section 251 targets the programmers and software writers who assist in the commission of computer crime. Section 252 is aimed at hackers who gain unauthorised access to a computer system. The necessary ingredient is either knowledge that access is unauthorised or recklessness.

Section 252 does not cover the situation of an authorised person who accesses a computer system beyond the scope of that authorisation.[14] This is a significant exclusion given that most unauthorised access originates from a source with authorised access.[15] The rationale may be that

---

10 Eg Unsolicited Electronic Messages Act 2007, ss 3, 20.

11 Computer Misuse Report 54 (Law Commission, Wellington, 1999)

12 Along with an expanded definition of theft to include intangible property.

13 *Police v Le Roy* (12 October 2006) HC WN CRI-2006-485-000058 Gendall J.

14 Crimes Act 1961, s 252(2).

15 *International Review of Criminal Policy – UN Manual on the Prevention and Control of Computer-Related Crime* www.uncjin.org/Documents/EighthCongress.

access beyond authorisation may be better dealt with as an employment disciplinary matter.[16] To criminalise this type of behaviour by authorised users may be too harsh a reaction to an act that is more unethical rather than illegal. However if there are no clearly established organisational protocols relating to access or no in-built protections regarding ethical conduct in the employment agreement, employers may find themselves in much the same situation as did the courts before 2003 trying to adapt existing rules to deal with computer misuse. Given that most security risks are reputedly internal, a middle ground could be found on the basis of the vicarious liability of employers. Section 252 could be amended to distinguish between unauthorised access during the course of employment (criminal) and unauthorised access arising out of employment (not criminal).

As a general comment, it can be stated that for the small Pacific countries 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.

III AVAILABLE PRECEDENTS AND MODEL LAWS

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

A The ITU

Most recent are the Draft ITU Study Group Q.22/1 Report of January 2008, and the Draft ITU National Cybersecurity/CIIP National Self-Assessment Tool Implementation Matrix of September 2008. The ITU National Cybersecurity/CIIP Self-Assessment Toolkit of January 2008 follows closely the line of thinking of the European Convention. The survey in Annex 1 of the Toolkit identifies the purpose of each of the key elements of that Convention and describes that element and in most cases provides a specific example. The examples greatly aid accessibility to the provisions of the European Convention.

B The European Initiatives

The European Convention 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 April 2009, 46 states had signed the Convention but only 25 had ratified it.[17] Only one state outside of Europe had ratified

16 Eg David Harvey *internet.law.nz* (2ed, LexisNexis, Wellington, 2005) 223.

17 The Convention was most recently ratified by Germany on 9 March 2009 and Serbia on 14 April 2009.

and that is the USA. Of the other 24 countries in which the Convention is in force, France, Italy, the Netherlands, Norway and Germany are the most important. Spain and the UK have signed but not ratified. In the Asia-Pacific region only Japan has signed.

This data raises questions about the nature and role of the European 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 European Convention provides that a state may, when it becomes a party, "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 European 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.

C The Commonwealth

The Commonwealth responded to the European Convention in 2002 by preparing two model laws for the use of Commonwealth countries. Those drafts are the Model Law on Computer and Computer Related Crime and the Model Law on Electronic Evidence.[18] These are succinct, clearly presented, and speak directly to the systems of small Commonwealth Common Law countries.[19] They are probably the best available examples for the countries of the South Pacific: the next best would be the Tongan Computer Crimes Act 2003. All reflect the European Convention.

D The European Convention adapted

The European Convention is very good. It provides minimum standards and those minimum standards can be readily adapted for national legislation. An adaptation of the requirements to a legislative form that could suit most Pacific Island countries is provided in the Appendix to this paper. In terms of the criminal offences, the draft follows the European Convention almost word for word. This close correspondence has the advantage that national courts can, for the interpretation and application of the law, refer to the convention's background and to the practical experience with the European Convention both at the national and regional level. The European Convention has

---

18 The Model Laws are available at www.thecommonwealth.org.

19 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.

within it many options; the draft in the Appendix is a spare 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. The 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 the model law. It is clearly a less polished document than the Commonwealth models but in its use of the European Convention and reliance on existing legal procedures it is very similar.

IV 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 identified the goal for cybersecurity in complementary terms. At page 9 it stated:

> Developing and implementing a 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 to do that requires an assessment of the present situation. For that assessment the ITU National Cybersecurity/CIIP Self-Assessment 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 do have elaborate 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 that deterring cybercrime can be greatly improved by the proper use of criminal law and procedures.[20] 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 security 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. In the case of *R v Wilkinson*[21] in New Zealand in 1998, the accused was convicted for false representations he made to a financier in order to access bank funds. Court of Appeal held that the definition of theft under the Crimes Act 1961 was based on the codified Common Law doctrine of things 'capable of being stolen' which excluded intangible items. The appeal against conviction was allowed, however the decision left an uneasy situation where a computer could be dishonestly used to obtain a benefit but not constitute an offence.

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 primary point of reference 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. 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 also speaks of training prosecutors, judges and legislators.[22] In the small Pacific countries training needs to start with the legislators. It is important that they have an understanding of the issues in order to enact the necessary laws. Following that, the local

---

20 Draft ITU Study Group Q.22/1 Report (2008) 27.

21 *R v Wilkinson* [1999] 1 NZLR 403.

22 Q.22/1, 32.

infrastructure can be built up. Only then would it be timely to inform 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 is no specialisation relative to the nature of the crime. Judges at the local level are most likely to be persons indigenous to the country and have relatively little knowledge of ICT issues. At the superior court level many of the judges are expatriate[23] and may bring with them their knowledge of cybercrime.

V CONCLUSION

It is clear, given the ubiquity of electronic communication, that no one country can solve the problems alone. The Pacific Plan has for some years been the focus of regional diplomatic endeavours of the Pacific Islands 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. It has very little to say about telecommunications and nothing about cybersecurity. At the regional level if cybersecurity is to be assured, cybersecurity should find a place as a priority item in the Pacific Plan.

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. On the basis of the documents as 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. Each single step is an important one.

---

23 From Australia, New Zealand, the UK, or the USA.

APPENDIX

The draft law that follows is based on the Council of Europe Convention on Cybercrime. The reference(s) to articles are to the articles of the Convention.

Cybercrime Act

---

1 Name

This is the Cybercrime Act.

2 Objective

The purpose of this Act is to provide better for cybersecurity and the combating of cybercrime and, for that purpose, to foster cooperation with other states and the parties to the Council of Europe Convention on Cybercrime of 23 November 2001.

3 Interpretation [Art 1]

(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;

"Court" means [insert name of court with jurisdiction under this Act]

"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 decisions that have followed the implementation of that 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;

[Art 2]

(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; [Art 3]

(c) intentional damaging, deletion, deterioration, alteration or suppression of computer data without right; [Art 4]

(d) intentional serious hindering, without right, of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. [Art 5]

5 Misuse of devices

(1) It is an offence intentionally and without right – [Art 6]

(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 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 [Art 7]

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 [Art 8]

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 [Art 9]

(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

[Art 10]

(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 [Art 12]

(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 proved 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.

[Art 12(4)]

11 Sanctions and measures [Art 13]

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

12 Processes and orders [Art 14]

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 [Art 20]

The 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 [Art 21]

In relation to serious offences as prescribed by regulations under this Act, the 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 [Art 16(3)]

(1) A service provider shall keep confidential the fact of the execution of any power provided for in this Act and any information relating to it.

(2) A service provider who fails to comply with subsection (1) commits an offence.

16 Jurisdiction [Art 22]

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 [Art 24]

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 [Arts 25/26]

An offence against this Act is a "serious offence" for the purposes of the [insert reference to the legislation on the Proceeds of Crime and the Mutual Assistance in Criminal Matters].

19 Confidentiality and limitation on use [Arts 27/28]

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

[Art 27]

(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 [insert reference to appropriate official] is the designated authority for the purposes of this Act.

21 Full-time network contact [Art 35]

(1) The designated authority is a point of contact available on a twenty-four hour, seven-day-a-week basis, 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

The [insert name of relevant executive authority] may make regulations for the purposes of this Act.