



## **Pacific Regional Workshop on Cybercrime Legislation**

Fa'onelua Convention Centre, Nuku'alofa, Tonga, 27-29 April 2011

### **OUTCOMES**

1. The Australian Government Attorney-General's Department (AGD), the Council of Europe (COE) and the Secretariat of the Pacific Community (SPC) co-hosted the Pacific Regional Workshop on Cybercrime Legislation at the Fa'onelua Convention Centre in Nuku'alofa, Tonga from 27 to 29 April 2011.
2. The workshop was opened by Lord Tu'ivakano, the Honourable Prime Minister of Tonga and Minister responsible for Communications. The workshop participants deeply appreciated the presence of the Prime Minister at the opening and his leadership role in supporting the use of information and communication technology (ICT) as a tool for development for Tonga.
3. Seventy delegates attended the workshop, representing the following countries: Australia, Cook Islands, Federated States of Micronesia, Fiji, Kiribati, Marshall Islands, Nauru, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu. Representatives of COE, SPC and the Pacific Islands Forum Secretariat (PIFS) also attended the workshop.
4. The workshop was convened in response to the Tonga Declaration made by Pacific ICT Ministers at the Pacific Regional ICT Ministers meeting held in Tonga on 18 June 2010.
5. The participants recalled that the ministers further directed their officials to work with SPC, COE, and the International Telecommunication Union (ITU) and development partners to develop appropriate policy, legislative and regulatory frameworks and strategies to combat cyber crime and promote Internet safety and security, including child online protection. The participants also noted that at the same meeting, the ministers also endorsed the *Framework for Action on ICT for Development in the Pacific* (FAIDP). One of the key priorities of FAIDP is to strengthen legislative frameworks of Pacific Island countries and territories (PICTs) in support of ICT development.
6. This report summarises the outcomes of discussions at the Workshop. Documents relating to the meeting are available on SPC's website.

### **Appreciation**

7. The participants thanked the Government of Tonga for hosting the workshop in Nuku'alofa and appreciated the support from AGD, COE and SPC.

### **Outcomes agreed at the Workshop**

8. Following on from discussions held over the three days of the Workshop, delegates agreed to support the following outcomes:
  - (i) To note the significant impact of cybercrime in the Pacific region, in particular as a threat to security and economic development in the region;

- (ii) To note that the *Framework for Action on ICT for Development in the Pacific* has set a target for 14 Pacific Island countries to have cybercrime legislation in place by 2015;
- (iii) To consider the Budapest Convention on Cybercrime (Convention) as providing a guideline for cybercrime legislation in line with international standards, and to further note the existence of the Computer Crimes Act 2003 (Tonga) and related Acts as a good example for the Pacific region of implementation of the Convention's provisions;
- (iv) To agree that there is a need to strengthen, and where possible, harmonise domestic legislation to enable law enforcement authorities to effectively combat cyber crime and collect electronic evidence. This legislation should, where possible, seek to criminalise:
  - a. Illegal access to computer data and/or computer systems;
  - b. Illegal interception of computer data
  - c. Interference with computer data and/or systems
  - d. Misuse of devices used to commit further cybercrime offences
  - e. Computer-related forgery and fraud
  - f. Activity relating to the production, distribution and possession of child pornography, and
  - g. Offences relating to copyright infringement; and

should seek to adopt the procedural obligations contained in the Convention relating to investigations involving the preservation of electronic evidence, and mutual assistance and international cooperation;
- (v) To support efforts to improve cooperation between countries and between law enforcement agencies and internet service providers in combating cybercrime. Substantive and procedural legislation harmonised with international standards is a prerequisite for efficient international as well as public-private cooperation. Countries may want to give consideration to the possibility of future accession to the Budapest Convention as a framework for international cooperation;
- (vi) To recognise that there are capacity building issues, including training and specialised institution building for policy officers, legislative drafters, judicial officers and law enforcement agencies, that should be dealt with as a matter of priority;
- (vii) To note countries' individual outcomes from the Workshop (at Attachment A) and note that support is available from donors to help Pacific Island countries implement these outcomes; and
- (viii) To request that this document be tabled for discussion at the Forum Regional Security Committee meeting in June 2011 and be circulated to PICs.

## **RECORD OF THE MEETING**

### **Day One – 27 April 2011**

9. The Workshop was opened by the Prime Minister of Tonga (in his capacity as the ICT Minister of Tonga). Mr Andrew Warnes (AGD), Mr Alexander Seger (COE) and Mr Siaso Sovaleni (SPC) also made welcoming remarks.
10. Five key themes were highlighted in the initial five sessions of the Workshop.

#### *Session One: The Threat of Cybercrime*

11. Mr Seger's presentation outlined cybercrime threats and trends, and key issues to be addressed through cybercrime legislation. Mr Seger's presentation was followed by a discussion on:
  - Attacks against computer data and systems experienced by delegates
  - Offences committed using computers, such as fraud, and
  - Offences committed in the Pacific, which involve electronic evidence.

#### *Session Two: International Standards and National Legislation*

12. Mr Seger provided an outline of the Budapest Convention on Cybercrime (the Convention), and examples of how countries have implemented these obligations into national law. Mr Warnes and Ms Kate Palmer (AGD) provided a presentation on Australia's cybercrime legislation and its involvement with the Convention, in particular its proposed accession to the Convention.

#### *Session Three: Cybercrime Legislation in the Pacific Island States*

13. Delegates provided updates to the Workshop on the current situation regarding domestic cybercrime legislation in the Pacific. In particular, Mr 'Aminiasi Kefu (Solicitor General, Tonga) provided a presentation on Tonga's Computer Offences Act 2003.

#### *Session Four: Cybercrime Definitions in Criminal Law*

14. An outline of definitions used in the Convention, as well as those used in Tonga's *Computer Offences Act 2003*, was provided by Mr Seger. Delegates then discussed equivalent definitions in their jurisdictions.

#### *Session Five: Cybercrime Offences*

15. Mr Seger provided an outline of cybercrime offences contained in the Convention, as well as those used in Tonga's *Computer Offences Act 2003*. Delegates then discussed cybercrime-related offences in their jurisdictions.

### **Day Two – 28 April 2011**

16. Day Two commenced with a discussion amongst delegates of measures required to strengthen definitions and offence provisions in their domestic legislation, in line with the Convention.
17. Procedural laws and international cooperation in relation to cybercrime matters were also discussed.

### *Session Seven: Procedural Laws and Cybercrime*

18. Mr Seger presented on the regulation of search and seizure of computer data, expedited preservation data, production orders, interception of traffic or content data and other investigative procedures and powers.
19. Delegates later discussed (in Session Eight) measures required to strengthen procedural legislation relevant to cybercrime investigation and prosecution in line with the Convention.

### *Session Nine: International Cooperation on Cybercrime Matters*

20. Mr Seger outlined the articles of the Convention relevant to international cooperation in the investigation and prosecution of cybercrime, including mutual legal assistance and the expedited preservation of data. Mr Warnes then provided a presentation on Australia's mutual assistance legislation, as an example of how domestic jurisdictions legislate to facilitate cooperation between law enforcement agencies.

### **Day Three – 29 April 2011**

21. The final day of the workshop commenced with a discussion amongst delegates of measures required to strengthen legislation relevant to facilitating international cooperation on cybercrime matters, in line with the Convention.
22. The remaining sessions of the workshop, briefly outlined below, focused on future actions to be considered by Pacific island countries and development partners.

### *Session Eleven: Cooperation between Law Enforcement Agencies (LEA) and Internet Service Providers (ISP)*

23. Mr Seger's presentation on this issue addressed the need for cooperation between these organisations, COE guidelines on LEA-ISP cooperation and steps that could be taken to strengthen this cooperation. Ms Palmer gave a presentation on Australia's iCODE.
24. Following from the presentation by COE on Procedural Law and Cybercrime, delegates discussed measures required to strengthen procedural legislation relevant to cybercrime investigation and prosecution in line with the Convention on Cybercrime.

### *Session Twelve: Training of Law Enforcement, Judges and Prosecutors and Institution Building*

25. Mr Seger's presentation on this issue addressed:
  - Institutionalising training of law enforcement authorities, judges and prosecutors
  - High-tech crime or other specialised units, and
  - The 2Centre and COE approaches for training agencies and authorities dealing with cybercrime.

### *Session Thirteen: Capacity building against cybercrime*

26. Presentations were provided by ITU and SPC on their capacity building programs. Participants discussed their priorities for capacity building in relation to cybercrime.