GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Australian Government

PILON Secretariat

Version 16 May 2017

Act 3.2.3 Pacific Islands Law Officers' Network Cybercrime Workshop

23-25 May 2017, Nuku'alofa, KINGDOM OF TONGA

Hosted by the Attorney General's Office of the Kingdom of Tonga holding the Chairmanship of the PILON (Pacific Islands Law Officers' Network) Cybercrime Working Group

in cooperation with the GLACY+ project (Global Action on Cybercrime Extended) of the Council of Europe, PILON and the Australian Government

Outline

Background and justification

The Pacific region is an attractive target and base for malicious cyber actors, with increasing internet connectivity and limited legislative and operational capacity for Pacific island law enforcement agencies to respond. Similarly, electronic evidence is becoming increasingly important to the investigation and prosecution of a range of crime types beyond the context of cybercrime, which is presenting significant challenges to Pacific criminal justice systems.

As part of the Council of Europe's extended GLACY+ project, Tonga is set to become a regional hub and share its experience with the neighboring Pacific islands that are equally vulnerable to cybercrimes and face the same capacity and capability issues. Tonga also chairs the PILON Cybercrime Working Group, whose objective is to strengthen the regional response to cybercrime, with an emphasis on the development and implementation of best practice legislation in line with the Council of Europe Convention on Cybercrime.

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

During the assessments of GLACY+ countries conducted during the inception phase of the project, one of the recommendations regarding Tonga was to consider the organization of a regional workshop in the context of PILON and its Cybercrime Working Group, to facilitate the exchange of experiences between prosecutors and other law officers from the Pacific region on matters related to cybercrime and electronic evidence.

This conference is organised within the Tongan Chairmanship of the PILON Cybercrime Working Group. It is supported by the GLACY+ project of the Council of Europe and the European Union and by the Australian Government, through its Cyber Cooperation Program.

Expected outcome

Carried out under Objective 3, Result 2 of the GLACY+ project, "Organise regional and international meetings in view of sharing good practices and promote harmonisation of legislation as well as rule of law and human rights safeguards", the activity is expected to provide participants from the criminal justice sector with a greater understanding on how to acquire and handle electronic evidence, which is increasingly important to the investigation and prosecution of a wide range of types of crime beyond the context of cybercrime.

By the end of this three-day workshop, the participating countries will have acquired a better knowledge on:

- The international legal framework on cybercrime;
- Challenges and trends on this topic in the Pacific region;
- The legal issues surrounding the investigation and collection of evidence in criminal cases involving technological and electronic means;
- Formal and informal law enforcement cooperation mechanisms, including the 24/7 Network;
- Perspectives from service providers on this topic;
- Mutual Legal Assistance requests;
- Analysis of electronic evidence;
- The distinct roles of CERTs and law enforcement in incident management;
- How national cybersecurity strategies help deter cybercrime;
- Resources available in the Pacific region to draw on.

Participants

Participants will be criminal justice and law enforcement professionals coming from the 15 Pacific island countries that, together with Australia and New Zealand, are members of PILON (the Cook Islands, the Federated States of Micronesia, Fiji, Kiribati, Nauru, Niue, Palau, Papua New Guinea, the Pitcairn Islands, the Republic of the Marshall Islands, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu).

The workshop shall last three days and can accommodate up to 50 participants, being 3 from each of the 15 Pacific island countries that are members of PILON and an additional number from Tonga in its capacity of hosting country, as well as invited speakers and experts from Australia, New Zealand, USA and Europe.

Administrative arrangements and location

The workshop will take place at the Tanoa International Dateline Hotel in Nuku'alofa, Tonga.

Contacts

At the Council of Europe:

Manuel ALMEIDA PEREIRA
Project Manager
Cybercrime Programme Office of
the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 78 32
Email: manuel.pereira@coe.int

Ana ELEFTERESCU
Project Officer
Cybercrime Programme Office
of the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 7836
Email: ana.elefterescu@coe.int

In the Kingdom of Tonga:

Leotrina MACOMBER
Crown Counsel
Attorney General's Office
Nuku'alofa, Kingdom of Tonga
Email: lmacomber@crownlaw.gov.to

At PILON:

Sasae WALTER
Secretariat Coordinator
PILON Secretariat
Apia, Samoa
Tel: +685 23589
Email: Coordinator@pilonsec.org

Agenda

Day 1—International legal framework and regional trends Tuesday, 23 May	
08:30	**Arrival and registration**
09:00	**Opening ceremony** *Separate program to be provided*
09:30	**Group photo and morning tea**
10:00	**1. Workshop overview and introduction of participants** *'Aminiasi Kefu, Director of Public Prosecutions and acting Attorney General, Kingdom of Tonga*
10:30	**2. Partnering with the Pacific: Australia's Cyber Cooperation Program** *Australia's Cyber Ambassador Dr Tobias Feakin*
11:00	**3. The international framework for cybercrime laws** *Branko Stamenkovic, Council of Europe* *'Aminiasi Kefu, Director of Public Prosecutions and acting Attorney General, Kingdom of Tonga* Overview of basic cybercrime offences, procedural powers and international cooperation modelled in the Budapest Convention, including Tonga's experiences developing legislation to implement the Convention
12:00	**Lunch**
13:00	**4. Cyber-enabled transnational crime within the Pacific region** *Federal Agent Matthew Sprague, Australian Federal Police* Overview of trends in the region involving cyber-enabled transnational crime, with 15 minutes for Q&A

13:45	**5. Pacific Islands overview: participant presentations** *Round table: 5 minutes each delegation* Each delegation is invited to comment on their country's current cybercrime trends, as well as challenges in handling electronic evidence during investigations and prosecutions
15:00	**Afternoon tea**
15:30	**6. Introduction to case studies** *Martha Piper, Australian Attorney-General's Department* Overview of proposed case studies, to be discussed throughout the program **Case Study 1—electronic dissemination of illicit material** **Case Study 2—electronic evidence in financial crimes**
16:00	**7. Cyber investigations and criminal procedure** *Branko Stamenkovic, Council of Europe* Introduction to the legal issues surrounding electronic evidence in criminal matters, with 15 minutes for Q&A
17:00	**Close**
Day 2—Gathering electronic evidence for investigations and prosecutions Wednesday, 24 May	
09:00	**8. BREAK-OUT SESSIONS** **a. Preserving and seizing electronic evidence** *Matthew Sprague, Australian Federal Police* *Greg Dalziel, New Zealand Police* Law enforcement powers to seize or similarly secure electronic evidence, including preservation requests, production orders, interception powers and chain of evidence requirements **b. Using electronic evidence in prosecutions** *Patricia Aloi, Australian Commonwealth Director of Public Prosecutions* *Timothy Flowers, United States Department of Justice* Evidential requirements of various cybercrime offences and more broadly, the admissibility of electronic evidence and presentation at trial, including chain of evidence requirements
11:00	**Morning tea**
11:30	**9. Analysing electronic evidence** *Fernando Fernandez, INTERPOL* *Cara Murren, United States Department of Justice* Summarising the outcomes of the break-out sessions, identifying what the investigator and prosecutor can expect from the analysis of digital evidence, and best practice processes for digital forensics laboratories, with 15 minutes for Q&A
12:30	**Lunch**

13:30	**10. International law enforcement cooperation in cyber investigations** *Lili Sun, INTERPOL* *Serupepeli Neiko, Fiji Police* *Kalisi Tohifolau, Tonga Police* International police cooperation initiatives and mechanisms, including the use of INTERPOL policing capabilities in cybercrime investigations, with 15 minutes for Q&A
14:30	**11. Mutual assistance requests** *Timothy Flowers, United States Department of Justice* *Nathan Whiteman, Australian Attorney-General's Department* Procedures for requesting electronic evidence from international partners, with 15 minutes for Q&A
15:30	**Afternoon tea**
16:00	**12. Working with service providers** *Presenters TBC* Perspectives from industry members on partnering with law enforcement in criminal investigations, including obtaining electronic evidence and victim identification
17:00	**Close**
Day 3—Structural responses to cybercrime and cybersecurity Thursday, 25 May	
8:00	**13. Cryptocurrencies and investigation on the Darknet** *Branko Stamenkovic, Council of Europe*
8:45	**14. Review of case studies** *Martha Piper and Nathan Whiteman, Australian Attorney-General's Department* Group discussion reviewing the application of Day 2 sessions to the case studies
9:15	**15. Developing good policy to meet electronic evidence requirements** *Dr Marie Wynter, Australian Attorney-General's Department (Chair)* *Leotrina Macomber, Attorney General's Office of the Kingdom of Tonga (Panellist)* *Patricia Aloi, Australian Commonwealth Director of Public Prosecutions (Panellist)* *Cara Murren, United States Department of Justice (Panellist)* *Catherine Bridges, Australian Department of the Prime Minister and Cabinet (Panellist)* *Catherine Smith, Council of Europe (Panellist)* Panel discussion on developing policy, including legislation, that supports the practicalities of investigating and prosecuting cases involving electronic evidence

10:30	**Morning tea**
11:00	**16. National approaches to cybersecurity** *Catherine Bridges, Australian Department of the Prime Minister and Cabinet* How national cybersecurity strategies help deter cybercrime, and the key components and participants necessary in creating a successful cybersecurity strategy, with 15 minutes for Q&A
12:00	**17. Computer Emergency Response Teams (CERTs)** *Tom O'Brien, CERT Australia* *Tonga CERT* Understanding the distinct roles of CERTs and law enforcement in incident management, with 15 minutes for Q&A
13:00	**Lunch**
13:45	**18. Regional assistance and support** *Catherine Smith, Council of Europe* *Martha Piper, Australian Attorney-General's Department* Resources and initiatives in the region that are available to Pacific Island countries
14:30	**19. Review and closing remarks** *'Aminiasi Kefu, Director of Public Prosecutions and acting Attorney General, Kingdom of Tonga*
15:00	**Close and afternoon tea**