The Pacific response to cybercrime:

effective tools and good practices

PILON Cybercrime Workshop

23-25 May 2017, Kingdom of Tonga

PILON Secretariat

ATTORNEY GENERAL'S OFFICE KINGDOM OF TONGA

Australian Government

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

ISBN: 978-1-925593-07-5 (Print)
ISBN: 978-1-925593-08-2 (Online)

Acknowledgement

Illustrations by Jessamy Gee of Think in Colour

The Pacific response to cybercrime: effective tools and good practices

PILON Cybercrime Workshop

23-25 May 2017, Kingdom of Tonga

CONTENTS

In May 2017, the Cybercrime Working Group of the Pacific Islands Law Officers' Network (PILON) and the Council of Europe, together with the Kingdom of Tonga, hosted the first of a series of workshops to provide Pacific Island participants from the law and justice sector with a greater understanding of how to acquire and handle electronic evidence. This is increasingly important to the investigation and prosecution of a range of crime types, including cybercrime.

The role of the PILON Cybercrime Working Group is to improve the capacity of Pacific Island countries to combat cybercrime and:

- strengthen laws to more effectively prevent, detect and deter cybercrime
- build awareness and capacity to prevent, detect and deter cybercrime, and
- foster international cooperation and coordination to address cybercrime.

The workshop was attended by approximately 70 law and justice officials from PILON member countries. This included Attorneys-General and senior policy officials, as well as investigators and prosecutors specialising in the gathering and use of electronic evidence. Australia, the Council of Europe, Tonga, Fiji, the United States, New Zealand and INTERPOL all provided expert presenters and facilitators. Australia and the Council of Europe proudly co-funded the event.

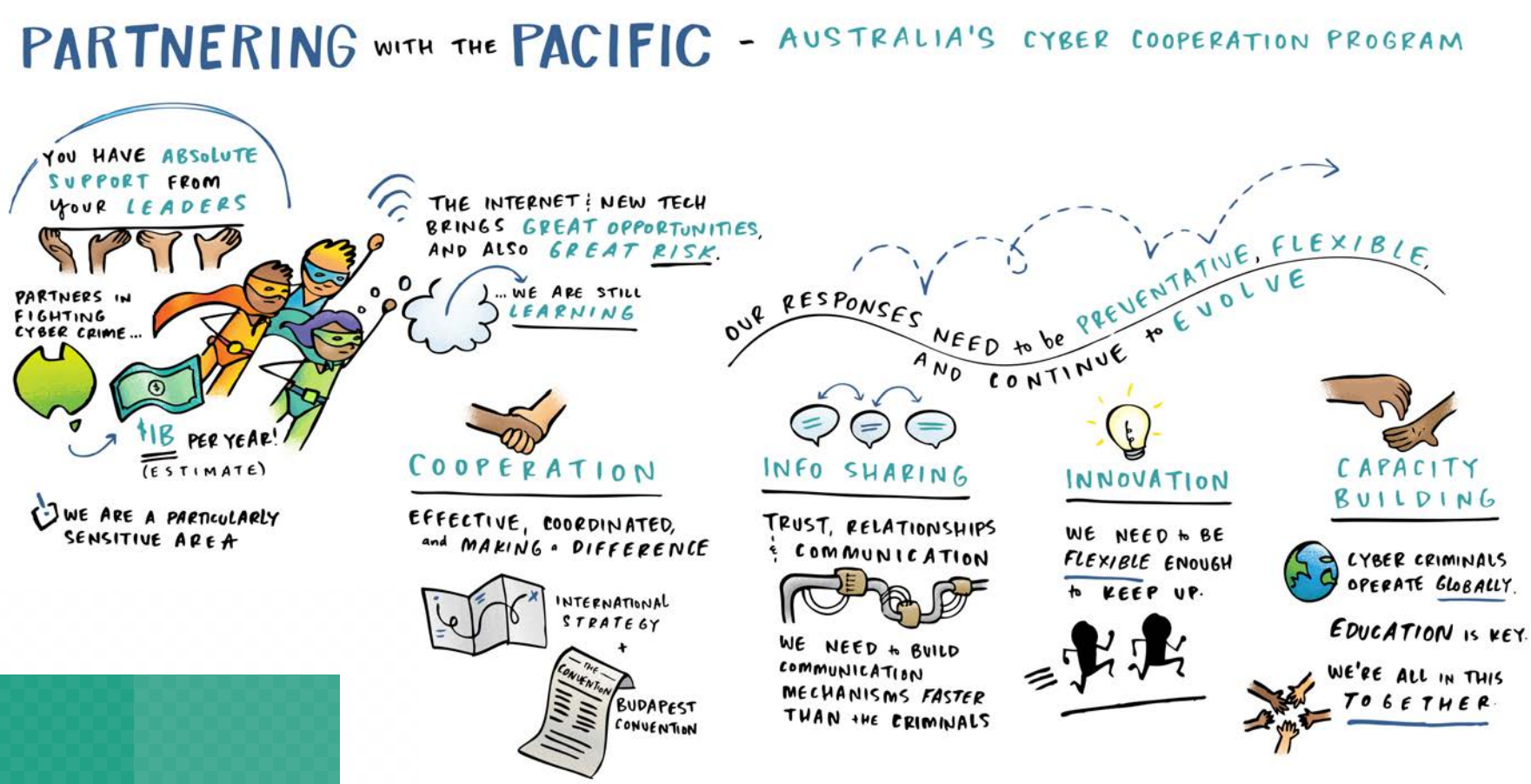
This booklet provides an overview of the discussions.

The workshop helped build a Pacific wide network of policy officials and practitioners able to work together more effectively to combat cybercrime. It also encouraged a number of Pacific countries to follow the Kingdom of Tonga's lead and express an intention to accede to the Council of Europe Convention on Cybercrime (the Budapest Convention). Since the workshop, the Australian Attorney-General's Department has been working with a number of these countries to assist them with this important endeavour.

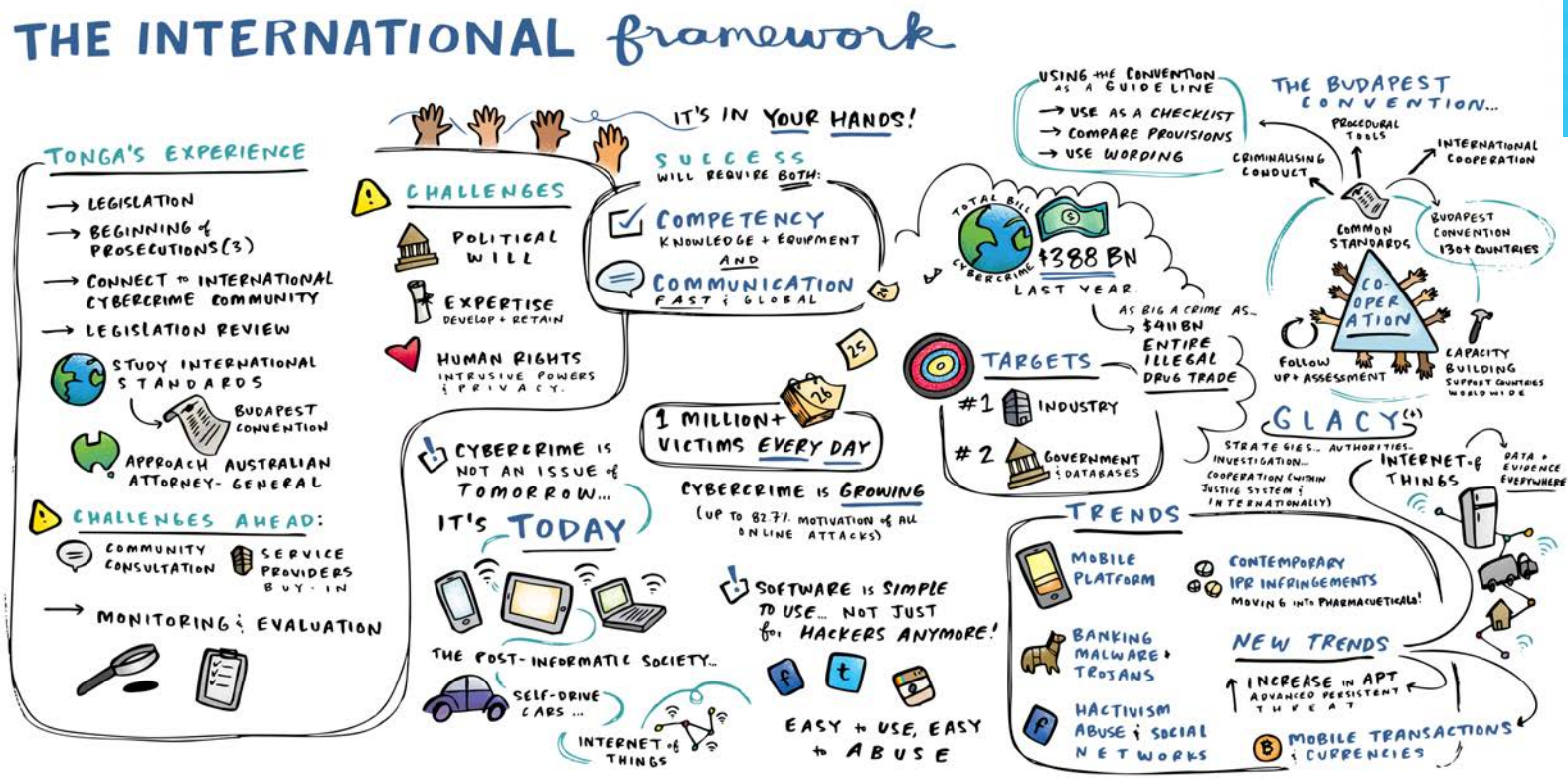
With the support of the Australian Cyber Cooperation Program and key international partners, PILON has agreed to host an annual cybercrime workshop involving police, prosecutors and legal policy officers from PILON member countries, until 2020.

We look forward to your future participation.

Following a gracious welcome by our hosts, Tonga, His Excellency Dr Tobias Feakin, Australia's Ambassador for Cyber Affairs, provided an overview of Australia's Cyber Cooperation Program. He noted the great opportunities for growth and social connectivity that the internet brings, as well the complexities and risks. Australia's Cyber Cooperation Program is designed to strengthen Australia's partnership with the Indo-Pacific, in order to assist the Pacific to build capacity and mechanisms to combat all types of cybercrime.



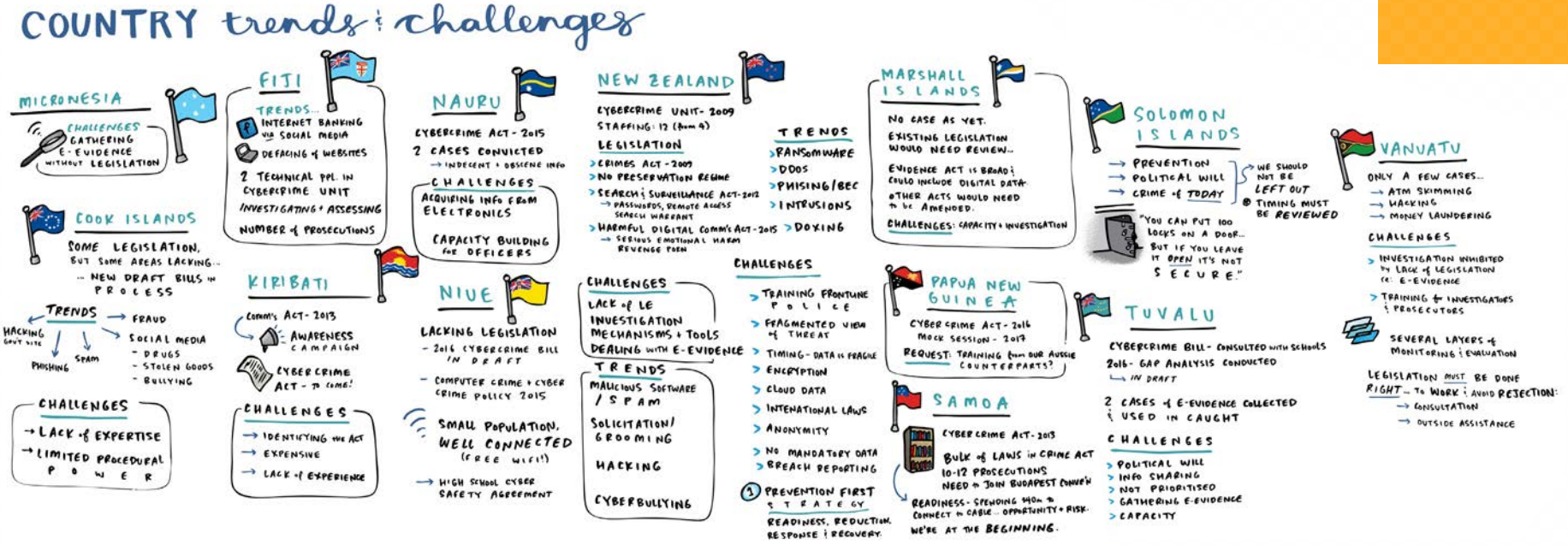
DAY 1 INTERNATIONAL LEGAL FRAMEWORK AND REGIONAL TRENDS



Mr 'Aminiasi Kefu, Acting Attorney General and Director of Public Prosecutions, Kingdom of Tonga, and Chair of the PILON Cybercrime Working Group, and Mr Branko Stamenkovic, Expert, Council of Europe, provided an overview of the Budapest Convention and Tonga's experiences developing legislation to implement it.

The Budapest Convention is the only international convention of its type allowing members to effectively investigate cybercrime over international borders. It sets out the key cybercrime offences countries need to put in place, as well as the procedural and international cooperation provisions to enable the effective collection and sharing of electronic evidence. Tonga was the first Pacific Island country to accede to the Convention, in May 2017. The PILON Cybercrime Working Group encourages PILON member countries to consider acceding to the Budapest Convention to support the enactment of harmonised legislative provisions to facilitate regional and international cooperation in combatting cybercrime across borders.

Federal Agent Matthew Sprague, Australian Federal Police, spoke about current trends in the region involving cyber-enabled transnational crime, and the steps countries can take to mitigate this.



Pacific Island delegations had the opportunity to reflect on and share with one another the key cybercrime trends they currently face. They also spoke about the challenges in handling electronic evidence during investigations and prosecutions, to inform future discussions of workshop participants.

Mr Branko Stamenkovic and Ms Catherine Smith, both Council of Europe Experts, provided the workshop with an introduction to the unique nature of electronic evidence, and an overview of the procedural mechanisms members need to put in place to collect evidence in compliance with the Budapest Convention. This includes putting in place a regime to quickly share subscriber data, preserve and produce traffic and content data—including in real time—and mechanisms to search and seize data.

The Budapest Convention requires that all procedural powers contain safeguards to protect the minimum human rights of affected individuals. This helps to and ensure that coercive powers to collect, use, store and share electronic evidence are not abused, which would otherwise put freedom of expression and the right to privacy at risk.

CYBERCRIME
IS HERE

BUDAPEST
CONVENTION
IS AN AVAILABLE
MECHANISM

SUCCESS NEEDS
→ LEGISLATION
→ LAW ENFORCEMENT
→ FRAMEWORK

LEGISLATION
NEED to BE
INTERNATIONALLY
HARMONISED

THERE's A
NEED for
TRAINING
→ CONSISTENT
& REGULAR

E-EVIDENCE
IS CRUCIAL
→ GOOD FORENSIC
PEOPLE

PROCEDURAL
POWERS
MUST BE BALANCED
W- HUMAN RIGHTS
& SAFEGUARDED

DAY ONE
takeaways

During the workshop, participants examined two common cybercrime scenarios to determine, in practical terms, the kinds of evidence needed to investigate and successfully prosecute each matter.

Breaking into groups, participants spoke with:

- Federal Agent Matthew Sprague, Australian Federal Police, and Detective Senior Sergeant Greg Dalziel, New Zealand Police, about law enforcement powers to seize or similarly secure electronic evidence—including preservation requests, production orders, interception powers and chain of evidence requirements

- Ms Patricia Aloi, Principal Federal Prosecutor, Australian Commonwealth Director of Public Prosecutions, and Mr Timothy Flowers, Senior Counsel, United States Department of Justice, about evidential requirements of various cybercrime offences and more broadly, the admissibility of electronic evidence and presentation at trial, including chain of evidence requirements.


PRESERVING and SEIZING ELECTRONIC EVIDENCE
CASE STUDY #1: ELECTRONIC DISSEMINATION of ILLICIT MATERIAL
14 YR OLD GIRL
SEND ME A VID :)
NO...
UNDER YOUR LEGISLATION... HAS an OFFENSE OCCURRED?
ONLINE BULLYING?
INDECENT ASSAULT?
EXPLOITATION of CHILDREN?
CHILD ABUSE?
BLACK MAIL?
PORNO-GRAPHY?
CREATION?
POSSESSION?
GROOMING?
TYPES of THREAT?
YOU NEED to UNDERSTAND the TECHNOLOGY, YOU CAN'T INVESTIGATE...
GET AN ACCOUNT & PLAY
SCREENSHOTS?
FILENAMES?
WHAT ACTIONS DO YOU TAKE?
SEARCH WARRANT
PRODUCTION ORDER
META DATA
- NAME
- PHONE NUMBER
- IPs
VICTIM'S PHONE
TELCOS
OFFENDER'S PHONE #
BE FAST
ESPECIALLY WITH INTERNATIONAL DATA REQUES
ORDER to COMPELL for PASSWORDS?
(IE HEADED-TOY & BUILD RAPPORT FIRST)
BE SMART.
OFFENDER'S ADDRESS
COLLECT DATA IMMEDIATELY
WHO DO ITEMS BELONG TO? WHO HAS ACCESS? HAS the WIFI BEEN HACKED?
THE TRADITIONAL METHODS of POLICING DO NOT CHANGE for ELECTRONIC EVIDENCE
WHEN YOU MOVE an ELECTRONIC FILE, YOU CHANGE IT...
KEEP IN ONE PLACE WHERE POSSIBLE
WHEN YOU ARRIVE...
TURN AIRPLANE MODE ON RIGHT
SECURE ALL ELECTRONIC ITEMS IMMEDIATELY
REMOTE WIPING is POSSIBLE
BREAKING IT DOWN...
COMPLANENT / VICTIM
ASSESS-EVERY STAGE
WITNESSES
SCENE(S)
EXHIBITS
INGREDIENTS of OFFENSE
POWERS
OFFENDER
CASE STUDY #2: CYBER-ENABLED FINANCIAL CRIME
ATM
FOREIGN NATIONAL
ATM SKIMMER
ATM SKIMMING
800 CARDHOLDERS in SWEDEN
VISITED COUNTRY 3 TIMES IN 12 MONTHS
HAS an OFFENSE OCCURRED?
CAN YOU PROVE INTENT?
IS POSSESSION ENOUGH?
EVIDENCE
WHAT DATA CAN YOU OBTAIN from SKIMMER & SIM CARD?
CAMERA
MEMORY CHIP
PHONE
TELCO PRODUCTION ORDER
WHAT DOES the ENTRY CARD SAY?
PRESERVATION
FORENSIC CAPABILITIES
PHOTOS
BEST AVAILABLE to YOU AT the TIME!
PASSWORDS
BE LOOKING: PASSWORD MANAGER? WRITTEN?
ENCRYPTION
STAY UP to DATE WITH TECH
INTERNATIONAL JURISDICTION
CAN BE a LONG PROCESS to be ADMISSABLE.
LAW ENFORCEMENT RELATIONSHIPS + CONTACTS are KEY

SCENARIO 1
ELECTRONIC DISSEMINATION OF ILLICIT MATERIAL

A 14 year old girl has been chatting on Facebook to someone she believes to be a 15 year old boy. Over the course of their online friendship, the girl has taken nude images of herself using her phone and sent them to the boy through Facebook's Messenger feature. He has also sent nude images to her, which she believes are of him. He recently asked her to send him a video of herself, nude. When she refused, he threatened to post the photos she had provided him on her Facebook profile page. He has sent her threatening text messages via a mobile phone, as well as numerous Facebook messages. She has told her parents, who have now reported it to police.

The exploitation of children has been inadvertently facilitated and enhanced by the availability of the internet, where predators can easily pose as children to establish relationships with and gain the trust of children. This can be for a range of illicit purposes, including soliciting child pornography material or grooming children to engage in sexual activity with others.

These offences are increasingly becoming more sophisticated through the use of networks to distribute material, the protection of material by encryption, and on-line access to the material. Cases can involve hundreds of thousands of depraved and disturbing images of children, and the scale and seriousness of this industry poses challenges for investigation and prosecution.

QUESTIONS FOR CONSIDERATION

Have any offences been committed? If so, what are they?

What actions do you take to seize or obtain any relevant evidence to investigate?

How do you preserve that evidence?

Do you need to obtain evidence from a foreign jurisdiction to assist? Why?

Would the evidence be admissible?

How do you obtain evidence in admissible form from foreign jurisdictions, eg obtaining content and non-content data from a foreign service provider?

How do you verify the identity and location of the 15 year old boy?

What do you do if the 15 year old boy turns out to be located in the same country as the victim?

What do you do if the 15 year old boy turns out to be a 35 year old man?

Would you have discovered this activity if the girl's parents had not told you?

SCENARIO 2 CYBER ENABLED FINANCIAL CRIME

QUESTIONS FOR CONSIDERATION

Have any offences been committed? If so, what are they?

What actions do you take to seize or obtain any relevant evidence to investigate?

How do you preserve that evidence?

What do you do if the devices seized as evidence (laptops, mobile phones) are password protected?

Do you need to obtain evidence from a foreign jurisdiction to assist? Why?

Would the evidence be admissible?

How do you obtain evidence in admissible form from foreign jurisdictions, eg obtaining content and non-content data from a foreign service provider?

The National Bank has reported a number of fraudulent credit card transactions occurring overseas, affecting over 800 local cardholders over the last eight weeks. A number of ATM skimming devices have subsequently been identified in the capital city.

Weeks after these events, a foreign national has been stopped at immigration attempting to enter the country with what appears to be an ATM skimming device in his luggage, which was picked up in a routine luggage scan. He has visited the country at least three times in the last 12 months, stating the purpose of his visits as tourism. He has in his possession a local sim card and phone, as well as a foreign sim card and phone.

ATM card skimming is a method used by criminals to capture data from the magnetic stripe on the back of an ATM card. Devices used can be very small and are often fastened in close proximity to, or over the top of, the ATM's factory-installed card reader. Some skimming devices look just like a normal card entry slot (as pictured). The skimming device will be accompanied by strategically positioned cameras or other imaging devices to fraudulently capture PIN numbers. Downloaded information can be transmitted wirelessly to other devices. Criminals may loiter nearby to observe customers and remove equipment after machine use. Once captured, the electronic data is put onto a fraudulent card and the captured PIN is used to withdraw money from accounts.

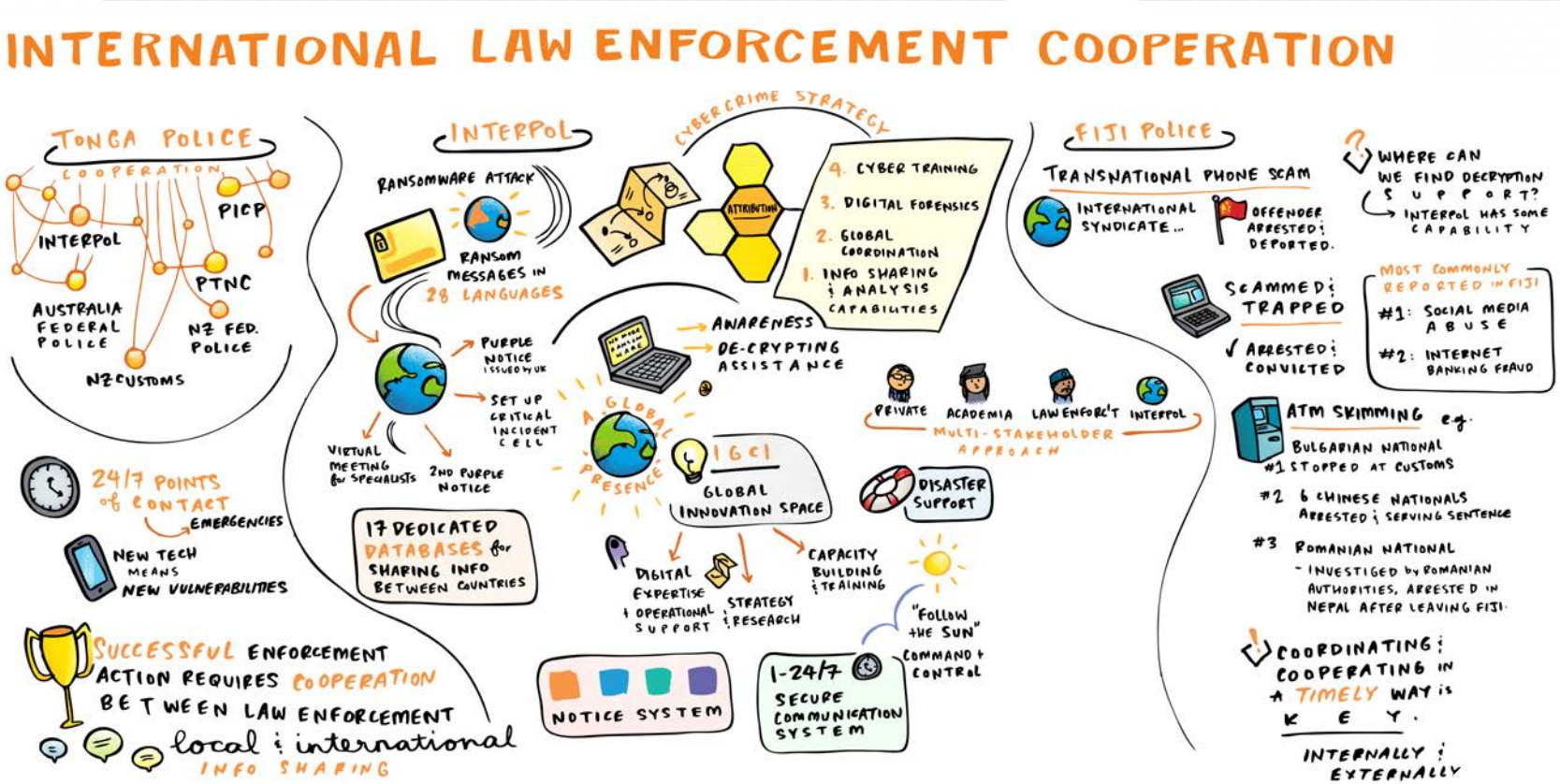
A number of ATM skimming cases have occurred across the Pacific in recent years. The Fiji Financial Intelligence Unit has reported that the last major and carefully orchestrated incident occurred in December 2015 and affected more than 500 credit and debit card holders, and an attempt to conduct ATM skimming in January 2016 was successfully foiled (see http://www.fijitimes.com/story.aspx?id=342290).

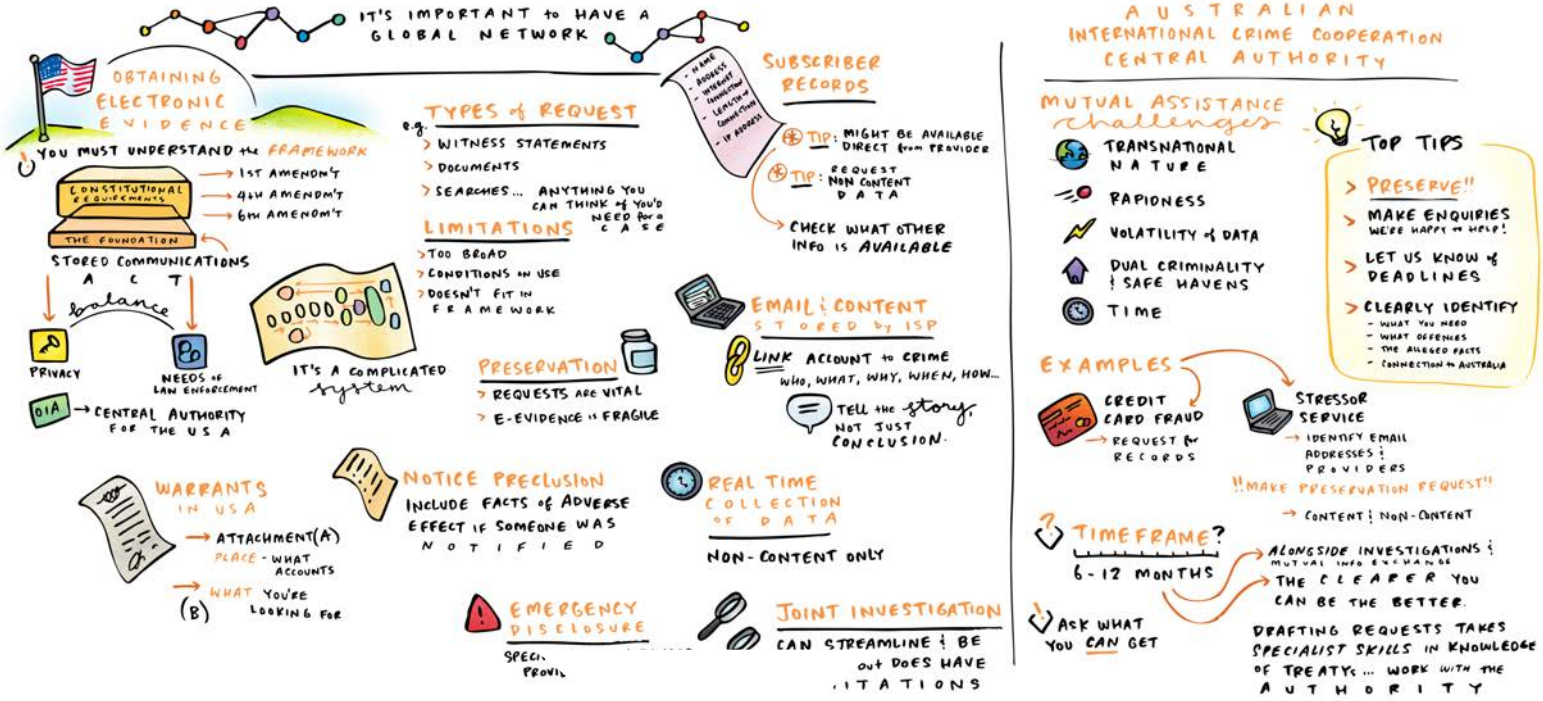
ANALYSING ELECTRONIC EVIDENCE

Following a discussion of the scenarios, Mr Fernando Fernandez, Coordinator Digital Forensic Laboratory from INTERPOL, and Ms Cara Murren, Digital Investigative Analyst from the United States Department of Justice, looked at what the investigator and prosecutor can expect from the analysis of digital evidence and key considerations and processes for digital forensics laboratories.

International law enforcement cooperation is critical in cyber investigations given the borderless nature of cybercrime. Perpetrators, victims and criminal activities can be in different jurisdictions and time zones and be vast geographical distances apart, making it extremely difficult to gather the evidence, identify the perpetrator, and bring them to court. Without international law enforcement cooperation to assist in the initial stages of investigations, cybercrime would go unpunished.

During this session, Ms Lili Sun, Head Digital Investigative Training Unit from INTERPOL, Serupepeli Neiko, Manager Transnational Crimes Unit from Fiji Police, and Inspector Linda Motu'apuaka, Manager Training from Tonga Police, spoke about the international police cooperation initiatives and mechanisms in their respective agencies, including the assistance INTERPOL is able to provide to bolster policing capabilities in cybercrime investigations.





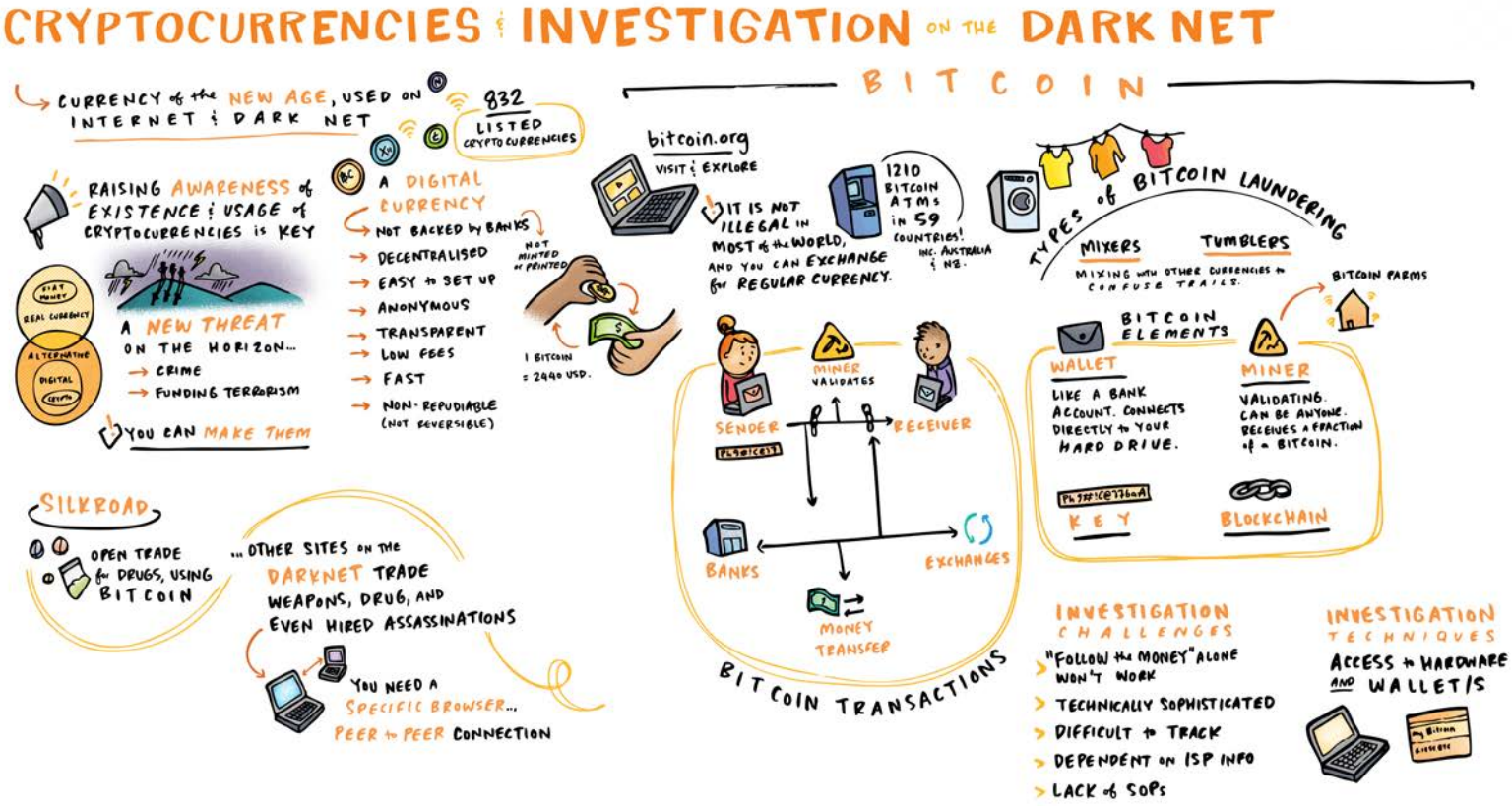
Mr Timothy Flowers, United States Department of Justice, and Mr Nathan Whiteman, Senior Legal Officer, Australian Attorney-General's Department, followed this discussion with a comprehensive session on procedures countries must follow to formally request electronic evidence from international partners to be submitted in court.

The drafting of mutual assistance requests is a specialist skill and requires detailed knowledge of the relevant legal frameworks and procedural requirements. If you need to make a request, make sure you get in touch with the relevant Competent Authority in the country holding the evidence so they can help you navigate the process quickly and efficiently.

WORKING WITH SERVICE PROVIDERS

Day 2 concluded with Ms Catherine Smith, Expert, Council of Europe and Detective Senior Sergeant Greg Dalziel of New Zealand Police sharing their insights on how to work with industry to access electronic evidence, which is critical to a growing number of criminal investigations.

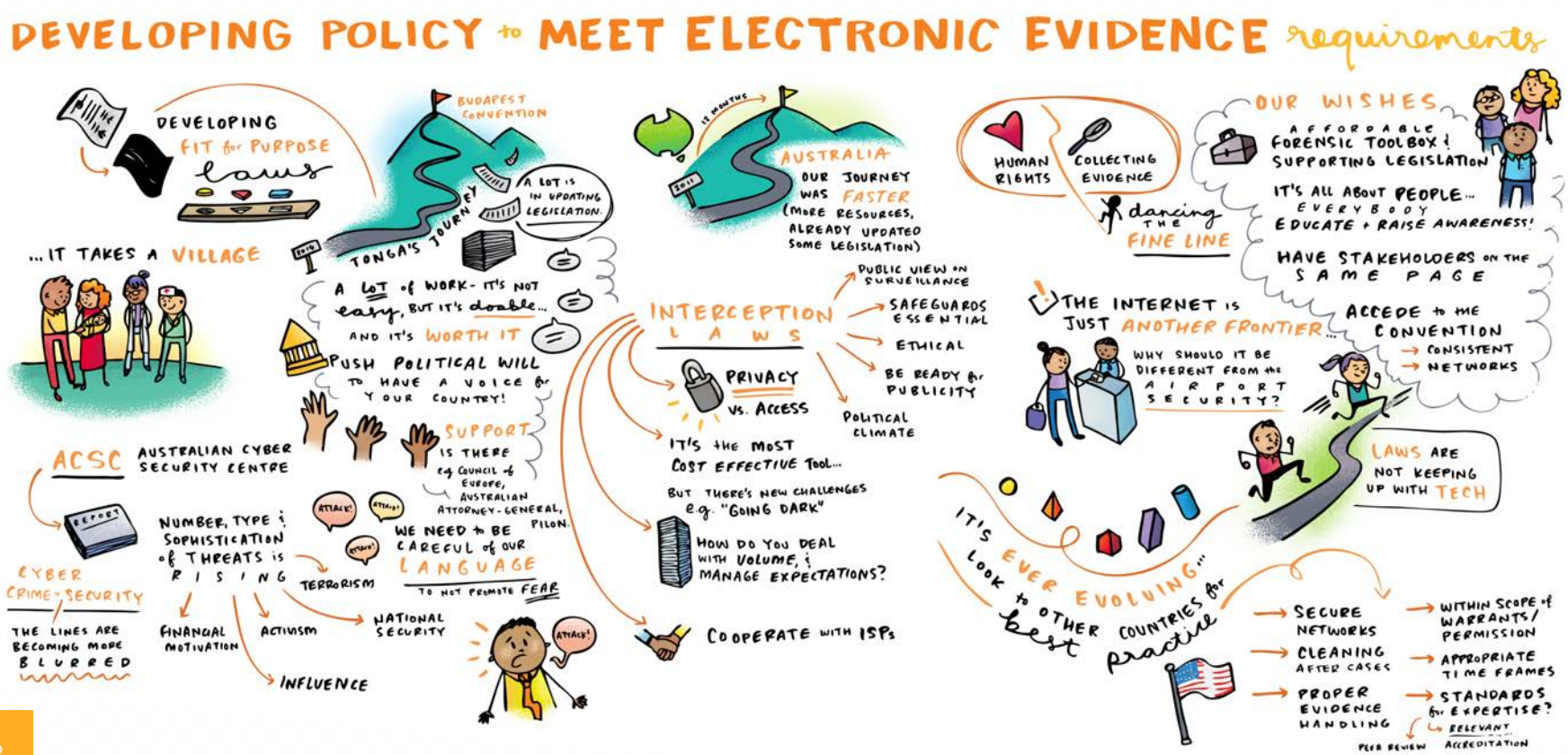
DAY 3 STRUCTURAL RESPONSES TO CYBERCRIME AND CYBERSECURITY



A new and emerging area of transnational crime is the use of cryptocurrencies to conduct transactions on the darknet. During this session, Mr Branko Stamenkovic, Expert, Council of Europe, explained to participants the nature of cryptocurrencies and how they are created and used. Bitcoin is just one of hundreds of different kinds of listed cryptocurrencies available for purchase. Although cryptocurrencies can be used for valid commercial transactions, increasingly they are also linked to illegal activities on the darknet. Countries need to be aware of this emerging threat.

This session examined the policy process behind making laws to gather, use and share electronic evidence, so they are fit for purpose and adapted to the requirements of the country making them. Dr Marie Wynter, Senior Legal Officer, Australian Attorney-General's Department, led a discussion with panelists from the Kingdom of Tonga, Australia, the United States and the Council of Europe to share their experiences in developing and implementing cybercrime and related legislation in their respective jurisdictions.

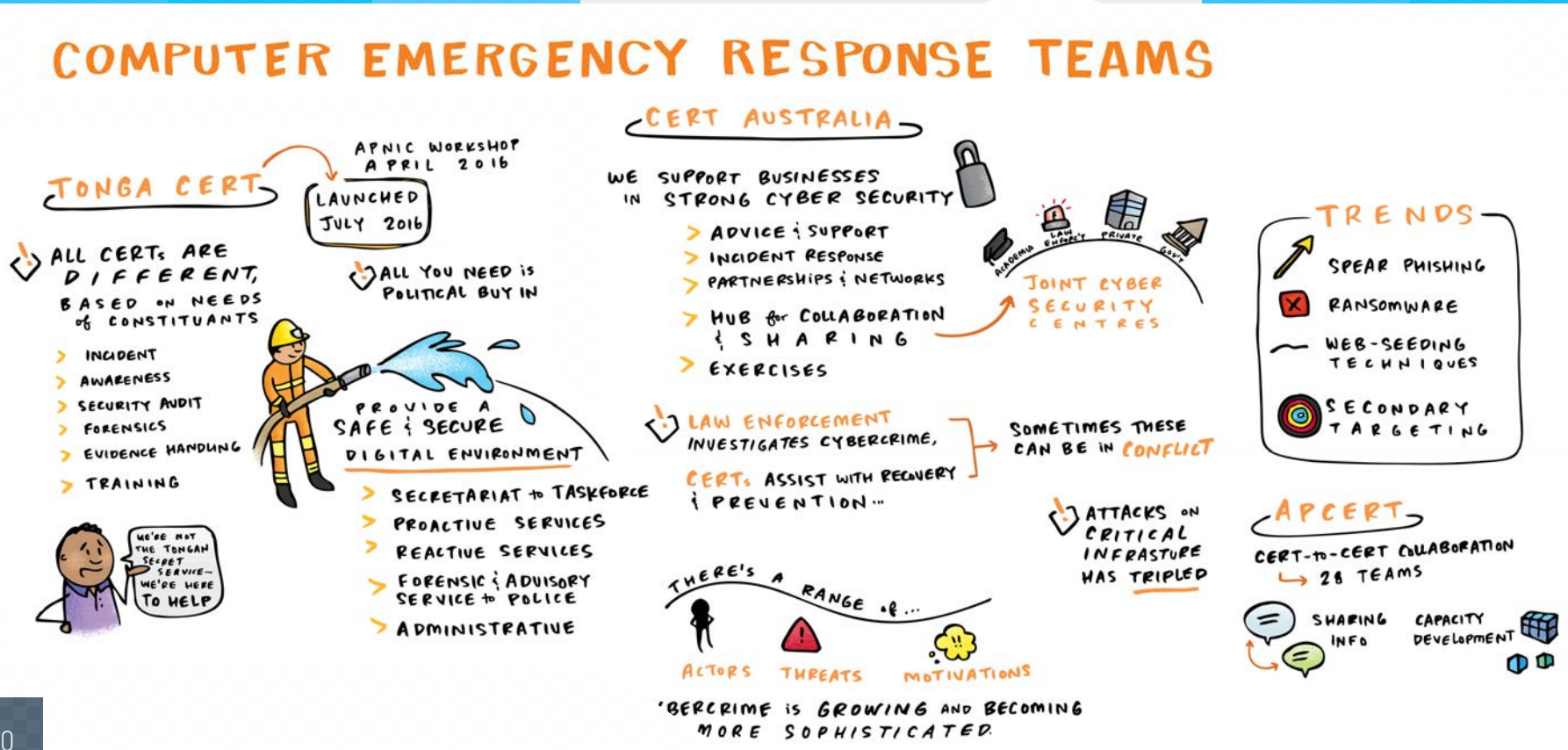
As noted by the panel, translating policy into law is not easy, but it is possible and worth it. Policy is not developed in isolation but needs the support of many to fine tune it to make it workable. Political will is vital, as is buy-in from all sectors involved in implementation. In addition to investigators and prosecutors, this includes telecommunications providers and industry, who hold much of the data, and the community whose information is accessed. Careful balancing of human rights and access arrangements are central to ensuring community acceptance and success. The PILON Cybercrime Working group encourages PILON members to consider acceding to the Budapest Convention, which offers a framework for countries to develop common legislative standards and receive significant implementation support.



NATIONAL APPROACHES to CYBER SECURITY

Ms Catherine Bridges, International Office of Cyber Security Adviser, Australian Department of the Prime Minister and Cabinet, led a discussion on how national cybersecurity strategies help deter cybercrime, and the key components and participants necessary to create a successful cybersecurity strategy.

Mr Tom O'Brien, Senior Adviser, CERT Australia, and Mr Siosaia Vaipuna, Director, Tonga CERT, followed this with an explanation of the distinct roles of CERTs and law enforcement in incident management.



The workshop concluded with countries reflecting on what they had learnt from the past few days, what they needed to work on, and how they might tackle cybercrime in the future.

IN SUMMARY...

HARMONISE

- LEGISLATION
- SKILL LEVEL
- FRAMEWORK

PARTNERSHIP

LOCALLY & INTERNATIONALLY

COMMITMENT

FROM POLITICAL WILL to FRONTLINE STAFF

PILON CYBERCRIME WORKSHOP AGENDA

23-25 May 2017, Kingdom of Tonga

THE PACIFIC RESPONSE TO CYBERCRIME: EFFECTIVE TOOLS AND GOOD PRACTICES

Providing participants from the law and justice sector with a greater understanding of how to acquire and handle electronic evidence, which is increasingly important to the investigation and prosecution of a range of crime types, including cybercrime.

Day 1	International Legal Framework and Regional Trends **Tuesday, 23 May**	
8.30	**Arrival and Registration**	
9.00	**Opening Ceremony**	
9.30	**GROUP PHOTO AND MORNING TEA**	
10.00	**Workshop Overview**	'Aminiasi Kefu, Acting Attorney General and Director of Public Prosecutions, Kingdom of Tonga
10.30	**Partnering with the Pacific: Australia's Cyber Cooperation Program**	Dr Tobias Feakin, Australia's Ambassador for Cyber Affairs
11.00	**The International framework for Cybercrime Laws**	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 *Branko Stamenkovic, Expert, Council of Europe* *'Aminiasi Kefu, Acting Attorney General and Director of Public Prosecutions, Kingdom of Tonga*
12.00	**LUNCH**	
1.00	**Cyber-enabled Transnational Crime within the Pacific region**	Overview of trends in the region involving cyber-enabled transnational crime, with 15 minutes for Q&A *Matthew Sprague, Australian Federal Police*
1.45	**Pacific Islands Overview: Participant Presentations**	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 *Round table: 5 minutes each delegation*
3.00	**AFTERNOON TEA**	
3.30	**Introduction to Case Studies**	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** *Martha Piper, Australian Attorney-General's Department*
4.00	**Cyber Investigations and Criminal Procedure**	Introduction to the legal issues surrounding electronic evidence in criminal matters, with 15 minutes for Q&A *Branko Stamenkovic and Catherine Smith, Council of Europe Experts*
	CLOSE	

Day 2	Gathering Electronic Evidence for Investigations and Prosecutions **Wednesday, 24 May**	
9.00	**BREAK-OUT SESSIONS**	
	a. Preserving and Seizing Electronic Evidence	Law enforcement powers to seize or similarly secure electronic evidence, including preservation requests, production orders, interception powers and chain of evidence requirements *Matthew Sprague, Australian Federal Police* *Greg Dalziel, New Zealand Police*
	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	**Analysing Electronic Evidence**	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 *Fernando Fernandez, INTERPOL* *Cara Murren, United States Department of Justice*
12.30	**LUNCH**	
1.30	**International Law Enforcement Cooperation in Cyber Investigations**	International police cooperation initiatives and mechanisms, including the use of INTERPOL policing capabilities in cybercrime investigations, with 15 minutes for Q&A *Lili Sun, INTERPOL* *Serupepeli Neiko, Fiji Police* *Linda Motu'apuaka, Tonga Police*
2.30	**Mutual Assistance Requests**	Procedures for requesting electronic evidence from international partners, with 15 minutes for Q&A *Timothy Flowers, United States Department of Justice* *Nathan Whiteman, Australian Attorney-General's Department*
3.30	**AFTERNOON TEA**	
4.00	**Working with Service Providers**	Panel discussion on working with industry to access electronic evidence in criminal investigations *Catherine Smith, Expert, Council of Europe* *Greg Dalziel, New Zealand Police*
	CLOSE	

Day 3	Structural responses to Cybercrime and Cybersecurity **Thursday, 25 May**	
8.00	**Cryptocurrencies and Investigation on the Darknet**	*Branko Stamenkovic, Expert, Council of Europe*
8.45	**Sentencing the Cyber Criminal**	*Patricia Aloi, Australian Commonwealth Director of Public Prosecutions*
9.15	**Developing Good Policy to meet Electronic Evidence Requirements**	Panel discussion on developing policy, including legislation, that supports the practicalities of investigating and prosecuting cases involving electronic evidence *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, Expert, Council of Europe (Panellist)*
10.30	**MORNING TEA**	
11.00	**National approaches to cybersecurity**	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 *Catherine Bridges, Australian Department of the Prime Minister and Cabinet*
12.00	**Computer Emergency Response Teams (CERTs)**	Understanding the distinct roles of CERTs and law enforcement in incident management, with 15 minutes for Q&A *Tom O'Brien, Australia CERT* *Siosaia Vaipuna, Tonga CERT*
1.00	**LUNCH**	
1.45	**Regional Assistance and Support**	Resources and initiatives in the region that are available to Pacific Island countries *Catherine Smith, Expert, Council of Europe* *Martha Piper, Australian Attorney-General's Department*
2.30	**Review and Closing Remarks**	*'Aminiasi Kefu, Director of Public Prosecutions and acting Attorney General, Kingdom of Tonga*
3.00	**CLOSE AND AFTERNOON TEA**	

PARTICIPANTS

NAME	DESIGNATION	COUNTRY
Craig Douglas REFFNER	Assistant Attorney General, Department of Justice, Chief Division of Litigation	Federated States of Micronesia
George E SKILLING	Captain, Department of Justice, Division of National Police, Transnational Crime Unit	Federated States of Micronesia
Radney EDGAR	Information and Communications Technology in the Division of Labour and Immigration	Federated States of Micronesia
Tam RAYNOR	Inspector Prosecution, Nauru Police Force	Nauru
Starsky DAGAGIO	Sergeant Intelligence Unit, Nauru Police Force	Nauru
Kristian AINGIMEA	Prosecutor-Prosecution Division Justice Department	Nauru
Ofisa Pulumauka TAGALOA TUALA	Principal State Prosecutor National Prosecution Office	Samoa
Hermann Paul RETZLAFF	Attorney General, Office of the Attorney General	Samoa
Wisteria Junior Ulupale SAUAGA	Acting Director Samoa Law Reform Commission	Samoa
Nakibwae RATEKI	Kiribati Police Service/OIC Criminal Investigation Division, Betio, Tarawa.	Kiribati
Neiran ARETA	Regulatory Manager/Legal Officer Communications Commission of Kiribati	Kiribati
Ronald TALASASA	Director Public Prosecution Office, Solomon Islands	Solomon Islands
Olivia RATU	Senior Legal Officer, Office of the Director of Public Prosecutions,	Solomon Islands
Rodney WHEATNEY	Acting Director of Police Prosecution	Solomon Islands
Yabaki VOSADRAU	Legal Officer Office of the Attorney-General	Fiji
Lavenia Domo BOGITINI	Legal Officer, Department of Public Prosecutions	Fiji
Serupepeli NEIKO	Manager Transnational Crimes Unit, Fiji Police Force	Fiji
Jenery THOMPSON	Desktop Support Officer Office of the Government Chief Information Officer	Vanuatu
Morris SEULE	Inspector, Vanuatu Police Force Criminal Investigation Department	Vanuatu

NAME	DESIGNATION	COUNTRY
Josaia NAIGULEVU	Public Prosecutor Office of the Public Prosecutor	Vanuatu
Johnathen Saburo KAWAKAMI	Deputy Attorney General	Republic of the Marshall Islands
Eric Trent IBAN	Chief, Civil Division Office of the Attorney General	Republic of the Marshall Islands
Vincent TANI	Captain, Marshall Islands Police Department	Republic of the Marshall Islands
Efren Jagdism JOGIA	Senior Crown Counsel, Tuvalu Attorney General's Office	Tuvalu
Iuni Soloseni PENITUSI	Police Prosecutor, Tuvalu Police Services	Tuvalu
Opetaia SIMATI	Director, Department of Information and Communications Technology	Tuvalu
Alexandrya Tiare HERMAN	Crown Counsel, Te Akinanga o te Ture | Crown Law Office	Cook Islands
Alan Russel RUA	Cook Island Police Service Frontline Department	Cook Islands
Aldric Tutaki RICHARDS	Assistant Crown Counsel, Crown Law Office, Government of Niue	Niue
Narita Janne Freda TUGA	Constable, Community Policing, Niue Police Station	Niue
Josephine Advent PITMUR	Director, Legal Policy, Department of Justice	Papua New Guinea
'Aminiasi KEFU	Acting Attorney General and Director of Public Prosecutions	Kingdom of Tonga
Leotrina MACOMBER	Crown Counsel, Office of the Attorney General	Tonga
'Inoke FINAU	Assistant Crown Counsel, Office of the Attorney General	Tonga
Tupou KAFA	Assistant Crown Counsel, Office of the Attorney General	Tonga
Joycelyn SIKALU	Assistant Crown Counsel, Office of the Attorney General	Tonga
Grace MOTU'APUAKA	Support staff, Office of the Attorney General	Tonga
Pilima MALAFU	Support staff, Office of the Attorney General	Tonga
Siololo TU'ITAVUKI	Support staff, Office of the Attorney General	Tonga
Katalina LEHA	Support staff, Office of the Attorney General	Tonga
Metui VAINIKOLO	IT personnel, Office of the Attorney General	Tonga
Linda MOTU'APUAKA	Tonga Police	Tonga
Lusiena Edna TUKUAFU	Tonga Police	Tonga

NAME	DESIGNATION	COUNTRY
Ofa Rino PASEKA	Trainer, Tonga Police	Tonga
Kalotia MAFUA	Police Constable, Tonga Police	Tonga
Maili LIMONI	Serious Crime, Tonga Police	Tonga
Ane LAULAUPEAALU	Ministry of Justice, Tonga	Tonga
Selosia SATINI	Investigator, Tonga Police	Tonga
Vinise FAHAKI	Police Constable/Investigator, Tonga Police	Tonga
Saimone Fifita TUPOU	Prosecutor, Tonga Police	Tonga
Temaleti VEA	Officer Intelligence Unit, Tonga Police	Tonga
Fielea FAEAMANI	Inspector, Tonga Police	Tonga
Liu FALEMAKA	Engineer MEIDECC	Tonga
Saimone FIFITA	MEIDECC Tonga	Tonga
Taumalago TAPUELUELU	Inspector, Tonga Police	Tonga
Alekesio TONGA	Sergeant, Tonga Police	Tonga
Tevita MAPAPALANGI	Constable, Tonga Police	Tonga
Saia VAIPUNA	Tonga CERT	Tonga
Calvy ADNIMA	MEIDECC Tonga	Tonga
Manase TUIMALA	Sergeant, Tonga Police	Tonga
Selu KAUVAKA	System Analyst, MEIDECC	Tonga
Meli K.	SPA MEIDECC	Tonga
Paula LATAPU	System Analyst, Tonga CERT	Tonga
Cathy AONIMA	MEIDECC	Tonga
Sesilia FAHIUA	Reporter, MEIDECC	Tonga
Kahoa FALEAFA	Information Assistant, MEIDECC	Tonga
Arjun BISEN	Policy Adviser to the Australian Ambassador for Cyber Affairs	Australia
Corrado PAMPALONI	Deputy Head of EU Delegation for the Pacific.	European Union

PRESENTERS

PRESENTERS, SPEAKERS & ORGANISERS
Mr 'Aminiasi Kefu, Acting Attorney General and Director of Public Prosecutions, Kingdom of Tonga
Ms Leotrina Macomber, Crown Counsel, Office of the Attorney General, Kingdom of Tonga
Dr Tobias Feakin, Australian Ambassador for Cyber Affairs, Australian Department of Foreign Affairs and Trade
Mr Branko Stamenkovic, Expert, Council of Europe
Ms Catherine Smith, Expert, Council of Europe
Dr Marie Wynter, International Legal Assistance, Australian Attorney-General's Department
Ms Martha Piper, International Legal Assistance, Australian Attorney-General's Department
Mr Nathan Whiteman, International Law Enforcement Cooperation, Australian Attorney-General's Department
Ms Patricia Aloi, Principal Federal Prosecutor, Australian Commonwealth Director of Public Prosecutions
Ms Catherine Bridges, Australian Department of the Prime Minister and Cabinet
Mr Tom O'Brien, Senior Advisor, Australia CERT
Federal Agent Matthew Sprague, Australian Federal Police
Detective Senior Sergeant Greg Dalziel, New Zealand Police
Mr Timothy Flowers, Senior Counsel, Computer Crime and Intellectual Property Section, United States Department of Justice
Ms Cara Murren, Senior Digital Investigative Analyst, United States Department of Justice
Mr Fernando Fernandez, Head, Digital Forensic Laboratory, INTERPOL
Ms Lili Sun, Head, Training Unit, Digital Investigative Support, Cybercrime Directorate, INTERPOL
Mr Serupepeli Neiko, Manager Transnational Crimes Unit, Fiji Police
Ms Linda Motu'apuaka, Tonga Police
Mr Siosaia Vaipuna, Director, Tonga CERT
Sasae Fualautoalasi-Walter, Coordinator, Pacific Island's Law Office Network

NOTES