PACIFIC ISLANDS
LAW OFFICERS' NETWORK

TALANOA

December 2022: Issue 3

CONTENTS

SEASONS GREETINGS EVERYONE

As we approach the festive season, we reflect back on the past year, the many activities we were all engaged in and forums that we contributed to. 2022 was certainly a packed year for PILON, with continued engagement within the Working Groups, the 41st Annual Meeting held virtually in November, as well as a very successful fourth and final annual Cybercrime Workshop in Nadi, Fiji. Over the year, PILON continued to be present at the forefront of Pacific issues, with the Secretariat attending the Pacific Islands Forum (PIF) FOC-Subcommittee on Regional Security (FSRS) meeting.

We would like to extend a warm thank you to the Executive Committee of PILON, our Chair of PILON and the Chairs and the members of PILON's three Working Groups and Legislative Drafters Committee and our partners, colleagues, friends and families for your continued support. May the spirit of Christmas bring you peace, the gladness of Christmas gives you exceeding joy, and the warmth of Christmas grants you love unending.

PILON CYBERCRIME WORKING GROUP WORKSHOP

NADI, FIJI 29 NOV – 2 DEC 2022

Strengthening Cybercrime Responses in the Pacific

Law and justice officials gathered in Nadi from 29 November to 2 December to discuss strategies to strengthen Pacific responses to cybercrime at the 2022 PILON Cybercrime Workshop.

The Workshop featured presentations from senior officials from across the Pacific and globally including the United States Federal Bureau of Investigations (FBI), the Pacific Islands Forum Secretariat (PIFS), the Pacific Islands Chiefs of Police and the Reserve Bank of Fiji.

The Workshop was held in a hybrid format to allow participants from the around the region to join both in-person and virtually. The Chair of the PILON Cybercrime Working Group,

Attorney General Tonga, Linda Folaumoetu'I, Chair PILON Cybercrime Working Group

the Attorney General of Tonga Mrs Linda Simiki Folaumoetu'i, said:

'I am very pleased that the Cybercrime Working Group is finishing 2022 by hosting a flagship event.'

The Workshop was co-hosted by the Government of the Republic of Fiji and PILON and supported by the Australian Government's Cyber and Critical

L to R: Attorney General Tonga, Attorney General Palau, Director Public Prosecution Sol Is, Attorney General Samoa

Technology Cooperation Program (CCTCP) and the Council of Europe.

It facilitated knowledge sharing, skill building, cooperation between police and prosecutors and regional cooperation with a theme of 'Combatting Cybercrime: Trends and Tools in a Changing World'. It focussed on gendered impacts of online engagement and the most common types of cyber-enabled offences in Pacific communities.

Dr Tobias Feakin

The Opening Ceremony on 29 November 2022 featured keynote addresses by the Fijian Acting Permanent Secretary for Communications, Ms Tupou'tuah Baravilala and Australian Ambassador for Cyber Affairs and Critical Technology, Dr Tobias Feakin. Ms Pirjo-Liisa Heikkila, Head of Political, Trade and Information Section, the Delegation of the European Union for the Pacific, and Ms Ana Elefterescu, Senior Project Officer, Cybercrime Programme Office, Council of Europe, also delivered remarks at the Opening Reception, held that same evening.

Ms Tupou'tuah Baravilala spoke on the Fiji Government's commitment to ensure that people access meaningful connectivity in a secure

L to R: Tupou Baravilala; Su'a Hellene Wallwork AG Samoa; Aiyaz Sayed-Khaiyum AG Fiji; Rachel Olutimayin DPP Solomon Is; Linda Folaumoetu'I AG Tonga; Lauren Murray Snr Legal Officer AG Dept Australia

cyberspace and utilise the vast opportunities that the internet provides. She also spotlighted the need for closer collaboration in our collective fight against cybercrime and highlighted that:

'The shift to online spaces has presented a challenge – the attack surface area has increased. Digital technologies continue to accelerate, and with it, cybersecurity risks continue to become more evident'.

'There have been emerging and evolving threats which are transboundary in nature and which have an impact on international peace and security and thereby, placing cybersecurity as a priority', said Ms Baravilala.

Tupou'tuah Baravilala

She also emphasised the need to ensure that cybersecurity measures are robust and agile, and have stronger protection tools in place so that recovery is swift and business operation disruption is minimised, should an attack succeed. She called for the need to create a culture of cyber hygiene practices amongst our people.

'It requires all of us, proactively synergising our efforts, and implementing cyber security safeguards and measures. Only then, can we turn the tide on these cyber threat actors which are a readiness across the Pacific, everyone needs to collaborate and make the most of existing regional networks such as PILON, the Pacific Cybersecurity Operational Network (PACSON), and the Pacific Transnational Crime Network through collaboration and information-sharing between these networks, threat to peace, security, prosperity and the well-being of our people', said Ms Baravilala.

Erja Askola

Ms Erja Askola, Deputy Head of Delegation of the European Union (EU) to the Pacific spoke of the EU's commitment to continue supporting the work and collaboration with PILON that is required in this challenging but exciting field.

Starting from the 2013 EU Cybersecurity strategy (reviewed in 2017) the EU has developed a

coherent and holistic international cyber policy and has supported countries in increasing their cyber resilience and ability to tackle cybercrime, through capacity building programmes funded and implemented together with partners. The 2020 Cybersecurity Strategy enables the EU to step up leadership on international norms and standards in cyberspace, and to strengthen cooperation with partners around the world to promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.

To support countries across the globe in fighting cybercrime, the EU has partnered with the Council

Nick Wilson, Malachi Boinar, Titimaea Nemaia, Angelo Chan Mow

of Europe through the GLACY+ joint project which focuses on developing and aligning agreement on cybercrime and sets common legislative standards that foster greater international cooperation and

focuses on developing the capacities of criminal justice authorities worldwide to implement such norms.

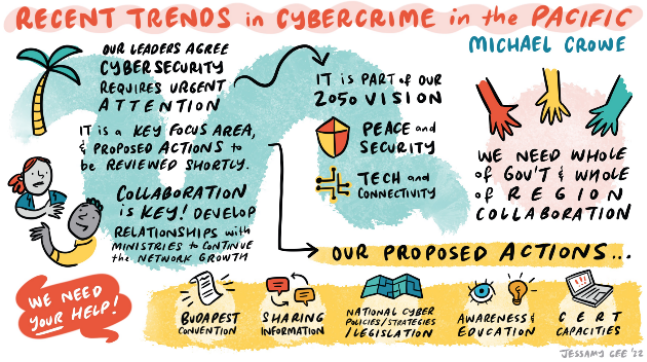
Ana Elefterescu

Ana Elefterescu, Senior Project Officer, Cybercrime Programme Office, Council of Europe shared with delegates the COE Octopus

Community, which is a platform for information sharing and cooperation on cybercrime and electronic evidence.

The COE shared some training materials and resources and webinars that can be accessed by prosecutors and legal professionals. She also shared some online tools – Country Wiki profiles on cybercrime legislation and policies, training materials and many more to bring together experts, counterparts, academics and professionals in the cybercrime field.

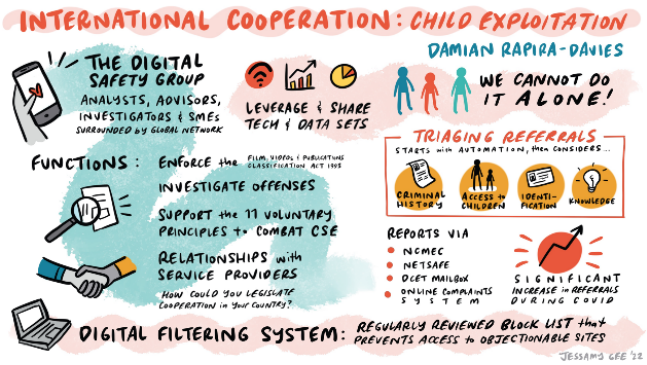
SUMMARY OF TOPICS AND PRESENTATIONS



Day 1 provided a 'Stocktake of Global Trends in Cybercrime'. The Pacific experience of global trends was illuminated by Session 2 presenters, Michael Crowe, Regional Security Advisor, PIFS, Titimaea Nemaia, Pacific Transnational Crime Coordination Centre (PTCCC), Samoa Police, and Wei Xian Tee, Council of Europe. Each presented on Recent Trends in Cybercrime and Cyber-Enabled Crime in the Pacific, which assisted with contextualizing emerging threats that were subsequently discussed throughout the rest of the Workshop.

The second part of the session emphasised the importance of regional cooperation on cybersecurity, particularly when countering child exploitation. Presenters Phil McEvoy, National Centre Bureau, Interpol, Australia, Dean Chappel, Assistant Legal Attaché, FBI, and Damian Rapira-Davies, Lead Operational Advisor, Digital Safety, New Zealand (NZ) identified challenges and resources involved in combatting this often-borderless crime type.

In the final session of the day, Dr Jeffery Garae, Chair, Pacific Cybersecurity Operational Network, Chief Superintendent Kalisi Tohifolau, Tonga Police, and Enoka Feterika, Pacific Islands Chiefs of Police Secretariat, Cyber Safety Pasifika, shared their knowledge on cybersecurity and cyber expertise, discussing how legal and police professionals can work effectively with cybersecurity experts to investigate and prosecute cybercrime offences. Several participants stated that they found the diversity of both police, prosecutor and other subject matter experts in the audience helped them develop insights into cybercrime challenges and opportunities for more effective collaboration across the entire justice system.

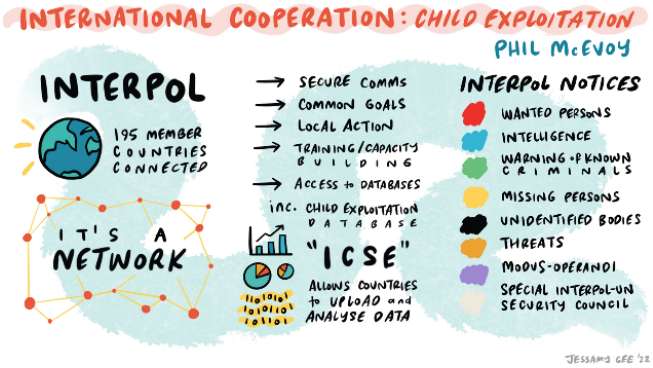


Day 2 focussed on the gendered aspects of cybercrime, with the first session being a Talanoa on the gendered impacts of social media. Speakers Kira Osborne, Office of the eSafety Commissioner, Australia, and Corporal Savenaca Siwatibau, Fiji Police, presented on social media and technology facilitated abuse in the context of broader sociocultural considerations in the Pacific. The speakers focussed on specific harms for women and girls, with opportunity to share legal, operational and other strategies/campaigns which

have succeeded. Some of the topics covered included image-based abuse (sometimes called revenge porn) and the dangers of technology being used to commit stalking.

Session 2 was a discussion of Pacific perspectives on law reform with Andrew Kelesi, Deputy

Director of Public Prosecutions, Solomon Islands, and Josephine Advent Pitmur, Deputy Secretary for Justice Administration, Papua New Guinea (PNG). Andrew discussed his insights on recent cybercrime prosecutions and law reform from a Pacific jurisdiction through a gendered lens, including where electronic evidence or image-based abuse is involved. Josephine provided a comprehensive overview of sorcery-accusation related violence (SARV) within PNG, and in particular spoke on how social beliefs around sorcery are reflected and sometimes amplified in the social media environment.



Session 3 included a panel discussion of strategies for supporting victims of cybercrime with Chief Superintendent Kalisi Tohifolau, Stephanie Dunn and Lavonne Goundar from Fiji Women's Crisis Centre.

They led discussions on building a holistic understanding of victim pathways through legal frameworks regulating cybercrime. Mercy Tamate (PNG Office of the Public Prosecutor) also presented on PNG's use of special measures to support victims throughout the prosecution and trial process. In table groups (and a break-out room for those online), participants worked through an interactive case study on online gender-based abuse. Participants were invited to explore how a victim's experience can be shaped by their access to support at various stages, as well as the role of police and prosecutors in assisting victims to navigate the process.

Day 3 focused on operational tools. In session 1, Siosaia Vaipuna, Global Forum on Cyber Expertise, Nicole Matejic, Principal Advisor, Digital Safety, Te Tari Taiwhenua – Department of Internal Affairs, NZ, and Jope Tarai, PhD Candidate, Australian National University, illuminated the 'changing digital landscape' – specifically, the evolving metaverse and agility required across the whole justice system to respond to novel threats.

In session 2, Michael Callan, CEO, Australian Fraud and Anti-Corruption Academy, Council of Europe, discussed the challenges of extracting evidence from mobile phones and procedural considerations which affect admissibility of digital evidence. Best practice techniques were discussed, as well as viable alternatives in low-resource situations within the Pacific context.

Emma Jaber, Commonwealth Director of Public Prosecutions, Australia, and Michael Callan spoke on how to work effectively with expert witnesses. They identified the types of electronic evidence which may require explanation from a specialist and suggested techniques for presenting this evidence persuasively in court.

For the end of day 3, Corporal Siwatibau and Razim Buksh, Reserve Bank of Fiji, shared their experiences on financial crimes and key issues with electronic evidence in the Pacific in the fourth session. They also shared some best practices for investigating scams, identify theft and common financial crimes.

The final day focused on connecting information from the Workshop. The morning began with Attorney General Folaumoetu'I leading a discussion on the work that the Cybercrime Working Group has done as part of the Zyber 'Fundamentals of Digital Forensics' training course and shared some key learning outcomes from the session. This included a ceremony, presenting certificates to those Zyber participants who had successfully completed the training course in 2022 and feedback from participants.

Ms Elizabeth Watson, Senior Associate, Ashurst, then presented on statutory interpretation, considerations and Standard Operating Procedures for investigation and digital evidence handling.

Dr Tawanda Hondora, Head of Rule of Law Team, Commonwealth Secretariat, elaborated on Elizabeth's presentation – walking participants through a ransomware case study. Participants were involved in making decisions for a fictional country's government who had discovered a ransomware attack, using the procedures and considerations outlined in previous presentations.

For the final session, Attorney General Folaumoetu'I, Ms Tupou K Vainikolo, Crown Prosecutor, Criminal Division, Attorney General's Office, Tonga, and Ms Rachel Olutimayin, Director of Public Prosecutions, Solomon Islands, provided a closer look at the prosecutor's experience of working on trials involving electronic evidence in Pacific jurisdictions. As part of this sharing, the police participants were invited to share their experiences of working with legal colleagues and the common areas of misunderstanding for prosecutors.

The Cybercrime Workshop's agenda included social events, such as a welcome reception and delegate dinner, to support the learnings within sessions and foster networking opportunities between attendees. The Workshop was a resounding success with participants praising the insightful, engaging and practical content provided. PILON once again thanks all that were involved in the fourth annual Cybercrime Workshop.