OFFICIAL

Australian Government
Department of Foreign Affairs and Trade

DFAT SUPPLEMENTARY SUBMISSION TO THE PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME

10 SEPTEMBER 2025

INTRODUCTION

The Department of Foreign Affairs and Trade (DFAT) welcomes the opportunity to provide a supplementary submission to the re-referred Parliamentary Joint Standing Committee on Law Enforcement (Committee)'s inquiry into the capability of law enforcement to respond to cybercrime. DFAT provided a submission to the Committee's inquiry on 6 December 2023 (December submission) (attached) and testimony at the public hearing before the Committee on 22 October 2024. This submission supplements the earlier submission and evidence provided.

DFAT SUBMISSION

Regional Resilience

DFAT's December submission referenced its Cyber and Critical Tech Cooperation Program (CCTCP) which supported the delivery of targeted cyber capacity building and resilience across the Indo-Pacific. With an investment of $81 million since 2016, CCTCP has delivered projects in 21 countries, providing assistance in strengthening cyber capabilities to fight cybercrime; strengthening cyber security; and countering disinformation and misinformation.

CCTCP has now been succeeded by the Southeast Asia and Pacific Cyber Program (SEA-PAC Cyber) which supports: enhancing cyber security and critical technology capabilities; strengthening cyber incident preparedness and response; and supporting the development of national and regional cyber policies, norms, standards, laws and regulations to reflect an open, free and secure cyber ecosystem. SEA-PAC Cyber supports both Southeast Asian and Pacific Island countries to detect, deter and respond to current and emerging cyber threats, and embrace the opportunities that cyberspace and critical technologies provide.

SEA-PAC Cyber-funded capacity building projects targeting cybercrime undertaken in 2024-25 include (but are not limited to) support to the following agencies and organisations:

Australian Federal Police

- *Cybercrime Leaders Working Group* dialogue in Philippines, which brought together key interlocutors and experts from Southeast Asian police and law enforcement agencies with responsibility for countering and investigating the borderless nature of cybercrime. The workshop reinforced the urgent need for a unified law enforcement response across the region to combat the growing scale and complexity of cybercrime;

- *Cyber Safety Pasifika*, aimed at enhancing the cyber safety of vulnerable communities in the Pacific. The program counters cybercrime through: cyber safety awareness and education; development of cybercrime legislation and policy; and up-skilling of Pacific police in cybercrime investigations;

- covert online investigative training programs, incorporating undercover cyber investigation techniques, delivered in Thailand in 2025 to the Royal Thai Police and the Department of Special Investigations; specifically to those officers involved in cybercrime operations, both locally and on a transnational scale;

- provision of advanced cryptocurrency tracing tools, expert-led training, and operational collaboration frameworks to Mekong law enforcement agencies' cyber investigation teams, with long-term impacts including dismantling cybercrime networks, reducing illicit financial flows, and enhancing international cooperation on financial crime investigations;

Attorney-General's Department

- support to several Pacific Island countries in drafting cybercrime legislative reforms, including developing necessary instruments to implement legislation and delivering training webinars to Pacific Island's Law Officer's Network (PILON) members on topical cybercrime issues;

UN Office on Drugs and Crime (UNODC)

- supporting UNODC and Vietnam to deliver a successful, well attended signing ceremony for the United Nations Convention against Cybercrime in Hanoi in October 2025, including by funding Pacific delegates' attendance at the signing ceremony, and by supporting capacity building for countries to ratify the Convention through a legislative gap analysis for Southeast Asian and Pacific countries in relation to the Convention; and

- delivery of cybercrime training and the exchange of ransomware experiences between several Pacific Island Countries, to strengthen awareness of, and regional cooperation on ransomware.

Multilateral Engagement

In its December submission and testimony, DFAT highlighted Australia's active engagement in the negotiation of the new United Nations Convention against Cybercrime (the Convention). The Convention introduces both cyber-dependent and cyber-enabled criminal offences and is the first UN endorsed global cybercrime convention that will serve to uplift and harmonise cybercrime legislation, investigation and cooperation across all UN member states.

The Convention was adopted by consensus by the UN General Assembly in December 2024. Vietnam will host the formal signing ceremony in Hanoi on 24-25 October 2025. Becoming a party to the Convention is a decision for Government. The Convention provides a consensus framework for what activity should be criminalised across all UN member states, thereby narrowing the operating space of organised cybercrime groups and helping eliminate unintentional safe havens. Should Australia become a party to the Convention, it would provide the AFP with a framework to cooperate and collaborate with a broader set of countries to investigate cybercrimes, such as online child abuse and exploitation, than it is able to under existing international agreements.

DFAT continues to work closely through other regional mechanisms such as the ASEAN Senior Officials Meeting on Transnational Crime, the Pacific Islands Law Officers Network and the ASEAN-Australia Cyber Policy Dialogue, to strengthen and enhance cooperation on cybercrime as a mutual, shared priority.