Australian Government
Department of Foreign Affairs and Trade

DFAT SUBMISSION TO THE PJCLE INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME

06 December 2023

INTRODUCTION

The Department of Foreign Affairs and Trade welcomes the opportunity to make a submission to the Parliamentary Joint Standing Committee on Law Enforcement (PJCLE) inquiry into the capability of law enforcement to respond to cybercrime. The Department notes the terms of reference, namely to inquire into:

- Existing law enforcement capabilities in the detection, investigation and prosecution of cybercrime, including both cyber-dependent crimes and cyber-enabled crimes;
- International, federal and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats;
- Coordination efforts across law enforcement, non-government and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime;
- Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians;
- The opportunities and challenges of the existing legislative framework in supporting law enforcement to investigate and act upon instances of cybercrime;
- Prevention and education approaches and strategies to reduce the prevalence of victimisation through cybercrime; and
- other related matters.

Cyber affairs affect all aspects of international relations and diplomacy –underpinning our national security, the protection and realisation of human rights and freedoms, global economic prosperity, sustainable development, and international stability. DFAT works to increase our international engagement across the full spectrum of cyber affairs, including cybercrime, as the vast majority of cybercrime targeting Australia originates overseas.

Cybercrime is a global threat, and international cooperation is an essential part of Australia's efforts to combat cybercrime. No country can eliminate cybercrime alone – by its very nature, cybercrime is international, with victims, perpetrators and evidence often located across many jurisdictions. International cooperation, collaboration, information sharing and capacity building are vital to any meaningful response to the threat posed by cybercrime.

Our region is only resilient to cybercrime when we tackle this issue collectively. It is in Australia's interest to help our neighbours improve their ability to prevent and respond to cybercrime as doing so will underpin regional economic growth and create a safer environment for Australia and our region to take advantage of the benefits of cyberspace and increased connectivity.

Australia undertakes an array of actions to address the changing cybercrime threat environment internationally, and in our region. We are committed to collaborating with international partners to fight cybercrime, including working together diplomatically and operationally to ensure that cybercriminals have limited opportunities to exploit cyberspace.

DFAT SUBMISSION

Regional Resilience

Domestic capacity and capabilities, along with the ability to effectively cooperate internationally, are central to combating cybercrime. A stronger, more cyber secure Indo-Pacific region will make Australia more resilient to cybercrime, ensuring the people and businesses in our region can take advantage of the digital economy and enjoy the benefits that safer connectivity offers. DFAT continues to work with Indo-Pacific partners on ways to enable greater connectivity and secure access to digital technologies across the region, but this connectivity is not without risk. Greater connectivity increases the threat of cybercrime, and our region is particularly vulnerable to exploitation from this threat.

DFAT provides targeted cyber capacity building and resilience across the region through its Cyber and Critical Tech Cooperation Program (CCTCP). This program ensures that ASEAN and Pacific Island countries can respond to the continued challenges and embrace the opportunities that cyberspace and critical technologies provide. An $81 million investment (from 2016-2025) - through projects in 21 countries – has provided assistance in strengthening cyber capabilities to fight cybercrime; strengthened cyber security; and countered disinformation and misinformation initiatives. DFAT is currently reshaping this program to better prevent cyber incidents, which includes strengthening operational and legal capabilities, and hardening critical ICT systems in the region.

Targeted cyber capacity building projects funded by the CCTCP include (but are not limited to):

- partnership between the Attorney-General's Department that provides direct 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;
- an AFP and Pacific Island countries project - *Cyber Safety Pasifika* - which enhances cyber safety for vulnerable communities in the Pacific. This cyber safety awareness and education program counters cybercrime through: cyber safety awareness and education; development of cybercrime legislation and policy (with support through PILON); and up-skilling of Pacific police in cybercrime investigations;
- a two-week Digital Forensics Workshop (led by the AFP) for the Royal Thai Police focusing on new and emerging cyber technologies, and industry-recognised digital forensic techniques and methodologies. The training enhanced the officers' technical capability to identify, extract, and report on electronic evidence and review electronic data;
- the delivery of bilateral, in-person training courses covering international cyber security, diplomacy, law and norms, data protection, and cybercrime between the ICT for Peace Foundation and Cambodia, Laos and Vietnam;

- supporting the United Nations Office on Drugs and Crime (UNODC) to deliver and exchange with several Pacific Island Countries to strengthen awareness and regional cooperation on ransomware by identifying, collecting, and exchanging ransomware experiences and completing cybercrime training.

Multilateral Engagement

International cooperation is essential to combatting cybercrime. Rapid and substantial shifts in the geopolitical, economic and technological landscape will require close cooperation to mitigate the rising competition for cyber and technology dominance across our region. It is in our interests that cybercrime and other associated threats do not undermine the stability of the governments, economies, and societies in our region. A rules-based cyberspace provides the stability and independence for countries to determine their own digital future and economic development.

To that end, Australia is actively engaged in negotiations for a new United Nations convention to combat cybercrime, which, if agreed, will provide a global standard for cybercrime internationally. Uplifting and harmonising cybercrime legislation, investigation, and cooperation across all 193 UN member states would narrow the operating space of organised cybercrime groups, and help eliminate unintentional safe-havens. Australia's engagement in negotiations prioritises a convention that will be built on existing and proven legal frameworks, such as the Budapest Convention, respect existing international norms and put human rights protections and safeguards at its core, while providing appropriate mechanisms for international cybercrime cooperation.

International crime cooperation is increasingly important to ensure Australian authorities can adequately detect, investigate, and prosecute cybercrime. Australia's law enforcement is closely interwoven with law enforcement agencies in our region on combatting cybercrime, as criminal perpetrators often target Australians from the perceived safety of overseas jurisdictions. In addition to uplifting the cyber resilience of the Pacific, Australia supports partners in the region to upskill their law enforcement capabilities in response to the increasing threat of cybercrime. This operational work is complemented by policy dialogue at the regional level to identify shared challenges and opportunities for collaboration. DFAT works closely through 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.

Deterrence measures

Malicious cyber activity threatens the endless opportunities for economic growth and innovation that cyberspace offers, and the increased scale and severity of malicious cyber activity by both state and non-state actors is of serious concern. Measures to deter malicious cyber activity, including cybercrime, protect both Australia's national interest and the interests of our partners. Effective deterrence helps maintain international stability and promotes continued global economic growth. Public attributions, which call out states that flout international rules, and threaten international stability in cyberspace, are an important component of deterrence measures. DFAT continues to work across government, and with partners regionally and internationally, to ensure deterrence measures, including attributions, are proportionate, always contextual, collaborative, and in Australia's national interest.

Sanctions are an important mechanism to demonstrate Australia's deterrence and response efforts to malicious and significant cyber incidents, including cybercrime. They are not the only tool available, and they will rarely be the first choice. Cyber sanctions are consistent with Australia's commitment to upholding existing international law and the agreed norms of responsible state behaviour in cyberspace. Our framework was designed to work alongside partners with similar frameworks (such as the United Kingdom,

United States, and European Union) so that we can take coordinated action with likeminded partners to amplify the effect of sanctions to deter and respond to malicious cyber actors where appropriate.

Australia's autonomous sanctions framework in relation to significant cyber incidents was established in 2021. Under this framework, the Minister for Foreign Affairs may impose a cyber sanction if satisfied that a person or entity has caused, assisted with causing, or been complicit in, a cyber incident or an attempted cyber incident that is significant or which, had it occurred, would have been significant. Prior to imposing the cyber sanction, the Minister for Foreign Affairs must obtain the agreement in writing of the Attorney-General and consult such other Ministers as the Minister for Foreign Affairs considers appropriate.

The cyber sanctions framework aims to deter cybercrime by:

- disrupting criminal activity where prosecution may, or may not, be a viable option;
- exposing cybercriminals' activities and their identity, placing them at further risk of detection by other law enforcement agencies; and
- imposing costs and consequences on cybercriminals, hackers and threat actors targeting Australia and other countries.

DFAT considers each cyber incident closely and may consider recommending to the Foreign Minister that sanctions be imposed on those who carry out or facilitate a significant cyber incident, including cybercrime, when there is sufficient evidence, and it is in our national interest to do so. Australia's ability to impose sanctions under this framework relies on continued cooperation with law enforcement, the intelligence community, and likeminded partners.

Sanctions will continue to be reserved for the most egregious situations of international concern and will remain one of the strongest ways Australia can signal our objection to conduct that is contrary to international norms and behaviours. They will be considered in conjunction with other foreign policy levers to effect positive change and to deter, and respond to, malicious and significant cyber incidents, including cybercrime.