Australian Government

Department of Home Affairs

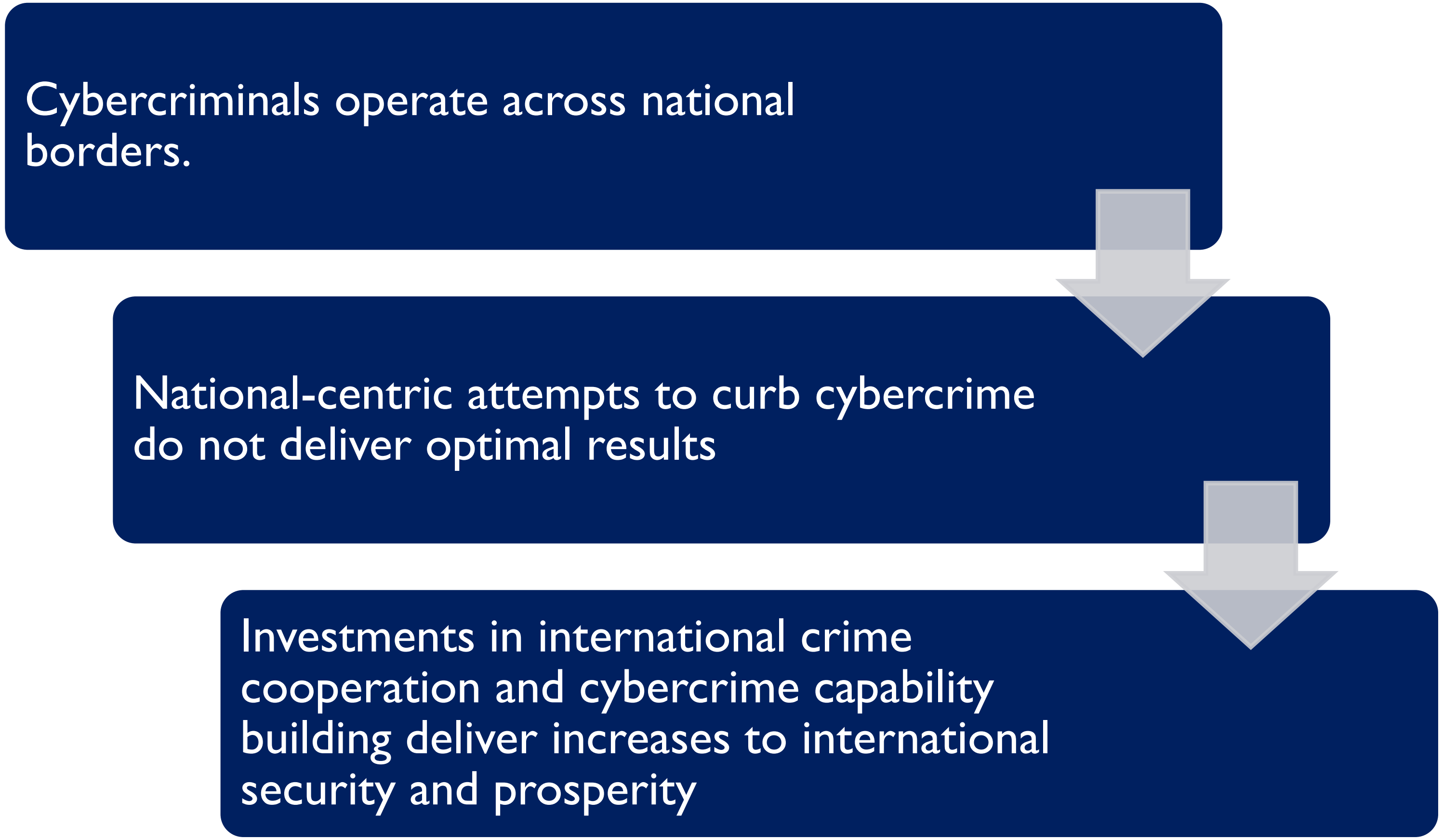
COMBATTING CYBERCRIME

INTERNATIONAL COOPERATION: DELIVERING OPERATIONAL AND LEGISLATIVE RESULTS

Australian Government

Department of Home Affairs

TRANSNATIONAL THREAT, TRANSNATIONAL SOLUTIONS



Cybercriminals operate across national borders.

National-centric attempts to curb cybercrime do not deliver optimal results

Investments in international crime cooperation and cybercrime capability building deliver increases to international security and prosperity

Australian Government

Department of Home Affairs

IM-RAT TAKEDOWN

Imminent Monitor Remote Access Trojan:

- Victim's movement
- Victim's location
- Online/offline activity

- 14,500 buyers across 124 countries. Tens of thousands of victims.
- Collaboration across national and regional law-enforcement agencies, private industry.
- Source-software shut down. Thirteen arrests and 434 devices seized.

Australian Government

Department of Home Affairs

ALIGNING LEGAL FRAMEWORKS AND TECHNICAL CAPABILITIES

Tonga

-

The first Pacific Island country to accede to the Council of Europe Convention on Cybercrime

Cooperation in law reform

Increase in capability across operational areas

Collaboration across government and private service providers

Network of strategically aligned partners

Australian Government
Department of Home Affairs

REGIONAL COOPERATION: BUILDING CAPACITY IN THE PACIFIC

PILON

- Network of key law-enforcement professionals across Pacific Island nations.
- Cybercrime Working Group is developing a cyber handbook covering
  - Mutual legal cooperation
  - Electronic evidence

Cyber Safety Pasifika

- Developing regional awareness of cyber safety.
- Promoting legislative and policy developments.
- Delivering training to cybercrime investigators

CYBER SAFETY PASiFIKA

PILON Cybercrime Workshop Port-Vila, Vanuatu
27–31 May 2019

INTERNATIONAL COOPERATION TO SHARE ELECTRONIC EVIDENCE TO COMBAT CYBERCRIME

SUMMARY OF KEY MESSAGES

Don’t wait to legislate – cybercrime is happening now. Enabling national frameworks and practical capabilities are key to facilitating international cooperation. The IEG should recommend the international community:

- prioritise the **provision of capacity building** and other support to strengthen the capacity of national authorities to respond to cybercrime
- **encourage criminalisation of cybercrime** and crimes committed by electronic means in national laws, in line with contemporary norms
  - important for countries to have **extraterritorial jurisdiction** over cybercrime
  - laws should reference **contemporary norms on cybercrime** including from the Budapest Convention
- enable effective and **admissible handling of electronic evidence**, including where it is destined for or received from a foreign jurisdiction
- put in place **formal and informal mechanisms of international cooperation** (i.e. MLA and police-to-police) for the investigation and prosecution of cybercrimes
- **join multilateral 24/7 contact networks** to enable rapid responses to requests for international cooperation and minimise loss of critical evidence or information
- join and utilise **existing international legal instruments** which provide a basis for international cooperation on cybercrime including UNTOC and the Budapest Convention
- encourage **close cooperation with industry**, particularly around takedown of harmful criminal material

The rapidly evolving cybercrime landscape necessitates ongoing expert and technical exchange on contemporary issues.
The IEG’s work program should be extended beyond 2021.

Thank you