Joint Committee on Law Enforcement

Capability of law enforcement to respond to cybercrime

Attorney-General's Department

Hearing date: 22 October 2024

Hansard page: 38-39

Helen Polley asked the following question:

CHAIR: In relation to the cybercrimes generated from offshore and for law enforcement's capacity to disrupt and arrest, there are obviously democratic countries that are like-minded and so there are good working relationships. Do have any views on whether there need to be additional powers for law enforcement to operate in those countries to do the arrests themselves?
Mr Reeve: I think it is a challenge working with countries that are not cooperative. It's genuinely a case where a multifaceted response is required. Australia is a party, for example, to the Budapest Convention on Cybercrime, which brings together many dozens of countries to cooperate on cross-border investigations into cybercrime. We've been a leading party in the negotiation of the recently concluded UN Convention on Cybercrime, which I'm sure Ms Daley Whitworth can speak to quite authoritatively, which is the first global convention on cybercrime and the first global crime convention in many years. Both of those efforts are about uplifting standards across many countries to have a common language, a common form of engagement, common approaches to investigating and prosecuting cybercrime across as many countries to maximise the ability of law enforcement to work seamlessly and collaboratively across international borders to combat cybercrime. There are also important bilateral efforts. For example, the US has implemented its CLOUD Act for lawful access to information held by US technology companies. Australia has negotiated an agreement with the United States for direct law enforcement access to all of those major tech companies—Google, Facebook, Meta et cetera—which is in the process of being operationalised as we speak. In terms of engagement with those countries that are not cooperative, that do not share a common commitment to combating cybercrime or common commitments to human rights and basic standards, that is a genuine challenge for law enforcement in those contexts. That is a space where we do rely on the sanctions framework, for example, to impose penalties, impose costs on cyber criminals operating from jurisdictions where it is challenging for law enforcement to follow them. I'm sure that Ms Daley Whitworth can speak more on that if required. We also have the SLAID framework as well, which provides powers for the Australian Federal Police to take disruption action online and overseas as well. Ideally, the Federal Police will cooperate with the local law enforcement agencies. That isn't always possible, and so it's important they have those tools.
CHAIR: I'm sure you'll go back and have a look at the evidence that was given this morning in relation to that piece of legislation and the fact that it needs to go further.
Mr Reeve: Certainly.
CHAIR: If you would like to take that on notice, have a look at it and provide any evidence to the committee, we would appreciate that.
Mr Reeve: I'm very happy to do that.

The response to the question is as follows:

The *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act) amended the *Surveillance Devices Act 2004* and *Crimes Act 1914* and associated legislation to introduce three new warrants to enable the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to collect intelligence, conduct investigations, disrupt and prosecute serious criminal online activity. The SLAID Act is intended to complement other, existing frameworks, including:

- international crime cooperation (such as mutual legal assistance or law enforcement cooperation);

- the significant cyber incidents sanctions regime in the *Autonomous Sanctions Act 2011*, administered by the Department of Foreign Affairs and Trade; and

- the Australian Signals Directorate's statutory function under the *Intelligence Services Act 2001* of preventing and disrupting, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia.

Data disruption warrants, introduced by the SLAID Act, enable the AFP and the ACIC to modify data for the purposes of frustrating the commission of serious offences, including where the data is located overseas. Where the location of data is known or can be reasonably determined, an agency must obtain the consent of the relevant foreign government before undertaking actions within the domestic jurisdiction of that state.

In July 2024, the Independent National Security Legislation Monitor Act commenced a statutory review of the operation, effectiveness and implications of the amendments made by the SLAID Act (the Review). The Review will examine the legislative and operational framework in which these warrants are situated, including the use and outcomes achieved by the warrants and whether they are effective in enabling the AFP and the ACIC combat serious and organised crime online in the current and evolving operational and technological environment—including the effectiveness of the data disruption warrant framework. The Review will be delivered with sufficient time to allow the Australian Government to consider any recommendations before the SLAID Act powers sunset in September 2026.

Joint Committee on Law Enforcement

Capability of law enforcement to respond to cybercrime

Attorney-General's Department

Hearing date: 22 October 2024

Hansard page: 39-40

Helen Polley asked the following question:

CHAIR: There was evidence given to us that, in relation to the working relationship between law enforcement and other private industries that deal with cybersecurity, there could be greater collaboration. As it was explained to us, the exercise is that the AFP can pay someone to service their vehicles and to have the sort of expertise, but because cybercrime changes all the time there should be more collaboration. Of course, there's a lot of collaboration already with the private sector. We know that they're involved in the PJC3 unit but that they can't always just provide that as a matter of being good corporate citizens and being happy to do that. There comes a point where perhaps there should be greater collaboration through contracts to provide that expertise. Does either department have a view on that?
Mr Reeve: I will probably take it on notice in terms of the AFP's engagement with industry.

The response to the question is as follows:

The department supports the efforts of Australian Federal Police (AFP) to engage and collaborate with industry to combat cybercrime. The AFP continues to develop and maintain strong relationships with industry, including through the AFP-led Joint Policing Cybercrime Coordination Centre (JPC3), to:

- better inform the AFP's understanding of the cyber ecosystem and support information-sharing with industry;
- leverage industry efforts to support prevention, mitigation and education activities;
- access leading-edge capabilities, tradecraft, knowledge and services through the provision of training and arrangements for incident response, support, and recovery; and
- work closely with, but separate to, industry partners when investigating cyberattacks.

Specific questions on engagement between law enforcement and private industry should be directed to the AFP.