Cyber Security Research Centre

Summary

of

Proposed Submission

to the

Parliamentary Joint Committee on Law Enforcement Inquiry

into

The impact of new and emerging information and communications technology (ICT)

David Irvine
Chair
Cyber Security Research Centre
12 January 2018

Summary of Concept

Our dependence upon the Internet and cyberspace, as a universal vehicle for storing and manipulating information, for conducting business and for direct communications between individuals and entities, has created new vulnerabilities not only in the national security sphere, but also in terms of law and order. The Internet has become a ubiquitous new vector for old threats and old crimes.

Just as Cyberspace has become the Fifth Domain of Warfare, so Cybercrime is becoming one of the most profitable areas of criminal activity, impacting adversely on both individuals and the community as a whole. The global cost of cybercrime is expected to reach over $US 6 trillion in the early 2020s.

Both national security threats and criminal activity exploit the Internet in similar ways. Both need to be countered or managed using similar investigative tools and techniques. Cyber tools facilitate the investigation not only of cybercrime *per se* but of a range of crimes not necessarily committed over the vector of the Internet.

Australia's national capacity to counter threats and criminal activity using cyber investigative tools is relatively weak, uncoordinated and dispersed across a range of agencies in both Commonwealth and State jurisdictions.

This Submission argues that countering cybercrime in Australia will be most effective when investigative support mechanisms are concentrated and coordinated on a national basis, utilising skills and technical capabilities developed in the national security area to strengthen law enforcement activity, and *vice versa*.

It raises for consideration the advantages of a single Commonwealth-led cooperative agency providing expert technical cyber investigative services in support of legal law enforcement and national security investigations carried out by Commonwealth and State agencies. It would support, rather that supplant or duplicate the proper functioning of those agencies under their existing legislative and operational authorization requirements. It would also have a training function, to help develop national cyber resilience across the government, private and individual Internet-user sectors.

Such an agency might fall within the ambit of the Department of Home Affairs, either as a separate entity or associated with the Australian Cyber Security Centre or the Australian Federal Police and Australian Criminal Intelligence Commission, and with a close working relationship with the skills-intensive Australian Signals Directorate. Expert staff would be seconded from appropriate Federal and State authorities.