Inquiry into potential reforms of National Security Legislation

Submission from Michael Angelico

Dear Sir/Madam,

In my submission I will seek to demonstrate three points:

- The proposals as outlined will not significantly increase the level of security for Australians
- The proposals represent a breach of privacy for innocent citizens
- The cost of implementing the proposals will be a drain on both government and corporations

1. Increased Security

The measures outlined in the discussion paper fall roughly into two categories: retaining information for access by intelligence and law enforcement agencies in order to detect criminals, and powers exercisable against criminals once detected.

The measures in the first category, even though more comprehensive than most others, will not prevent anyone with enough understanding of IT from hiding their intentions and protecting any sensitive data from intelligence and law enforcement organizations. Open proxies are widely used to circumvent restrictions based on IP Geolocation in order to download movies and illegal pornography. Any terrorist or organized crime group could easily blend into the crowd.

In order to successfully detect criminal activity it would be necessary to retain, and spend large amounts of time and money processing, vast amounts of data. Criminal organizations could very easily “snowball” intelligence agencies by mixing the traffic which relates to their activities with something unrelated and legal, for example internet TV. The resources necessary to sort through that amount of data is beyond even the world's best funded intelligence organizations.

The proposals as outlined will therefore prove to be of little value in the fight against terrorism and organized crime.

2. Privacy

The powers proposed for ASIO represent a breach of privacy and private property for innocent Australian citizens. The use of third-party computers and communications equipment to prosecute a disruption attack has several implications:

- The internet community blacklists computers from which attacks are detected, which could lead to long outages even after the ASIO operation has been completed
- The owner of the equipment will be denied its use (or partial use) for the duration of the operation, and some additional charges (eg extra bandwidth usage) may be levied on the owner

- The measures necessary to enable such an operation will also make it easier for cyber criminals to carry out illegal activities

3. Cost

The cost of implementing the measures as outlined will be prohibitive. While storage media diminishes in cost on a constant basis, the amount required to store the information proposed would be a major expense. The hard drives would need to be kept in a data centre which would require enterprise-grade maintenance and networking infrastructure. The data centre itself would become a target for criminal activity, and thus would require its own protective security.

Conclusion

The measures outlined in the discussion paper should not be implemented, as they represent a breach of privacy and a significant cost to taxpayers, for little or no security benefit.

Michael Angelico