

## Australia the victim of 'massive' cyber espionage

Dylan Welch

August 1, 2011



Canberra is seen as the soft underbelly of the Western intelligence club. *Photo: Louise Kennerley*

CYBER espionage is being used against Australia on a "massive scale" and some foreign spies are using Australian government networks to penetrate the cyber defences of allies such as the US, ASIO chief David Irvine has told business leaders.

Mr Irvine's speech is one of the strongest indications yet of the seriousness with which the government is treating the cyber threat.

"Electronic intelligence gathering is now a huge industry," Mr Irvine said. "It is being used against Australia on a massive scale to extract confidential information from governments, the private sector and ordinary individuals."

He hinted that Australia is often targeted by foreign spies as an easy access point into the intelligence holdings of the US and Britain.

Describing the security threat posed by cyber as "pervasive and insidious" he continued: "Worse, our own territory can be used to surreptitiously penetrate the cyber defences of our friends and allies."

Canberra has long been seen as the soft underbelly of the Western intelligence club - the alliance of Australia, Canada, New Zealand, Britain and the US - and foreign nations are known to target Australia in order to steal our allies' intelligence.

With the rise of cyber espionage, foreign states now target Australia's relatively less protected government systems to access secret material held by the US and Britain.

The growth of the cyber threat has risen in parallel with global internet usage, which has soared from about 360 million in 2000 to over 2 billion people last year. Considered to be the greatest content provision system the world has ever seen, the internet has left governments and industry struggling to deal with the myriad of security concerns it has left in its wake.

"From our perspective, I can say that it seems the more rocks we turn over in cyber space, the more we find," Mr Irvine said.

"Internet and increased connectivity has expanded infinitely the opportunities for the covert acquisition of information by state-sponsored and non-state sponsored actors."

There is a general recognition that the fast pace of online development means the advantage currently lies with those who seek to intrude upon, rather than those who try to protect, online systems.

Last week Graham Ingram, the general manager of Australia independent cyber emergency unit AusCERT, told a security conference that Australia was as much as five years behind regarding the issue of cyber security.

Earlier this year it was revealed that foreign spies, likely Chinese, hacked into Parliament House's email system and stole thousands of messages from at least 10 government ministers including the Prime Minister and the ministers for foreign affairs and defence.

Mr Irvine's speech, on July 5, came only days before the US Department of Defence (DoD) released its latest response to the cyber threat, a strategy designed to protect its 7 million computers and other devices.

In doing so, it revealed that "some foreign intelligence organisations have already acquired the capacity to disrupt elements of DoD's information infrastructure".

The US has previously revealed that every year an amount of intellectual property larger than the entire contents of the Library of Congress - some 22 million books - is stolen from US networks run by businesses, universities and government.

Read more: <http://www.smh.com.au/technology/security/australia-the-victim-of-massive-cyber-espionage-20110731-1i6hc.html#ixzz1TpiM2W0g>