Chinese hackers could shut down Australian power grid, warns former spy boss David Irvine

AFR 9 March 2015

Former Director General of ASIO David Irvine at the AFR Defence and National Security roundtable in Sydney. AFR -

John Kerin

China possesses the weapons in its cyber arsenal to damage Australia's economy by triggering a shutdown of the electricity grid, warns former spy boss David Irvine.

But the former head of the Australian Security Intelligence Organisation says while he doesn't believe Beijing will use its capacity because nations are constrained in peacetime, terrorists and hackers are striving to develop similar capabilities.

Such a blackout of an Australian city during a heatwave would cripple business, cause public transport and traffic chaos, create havoc for emergency services, risk lives of the elderly and the sick and cost hundreds of millions of dollars.

Mr Irvine told a defence round table co-hosted by KPMG and The Australian Financial Review in Sydney government and business were struggling to stay ahead of the growing cyber menace.

"I know China probably has the ability already to turn off our electricity supply," Mr Irvine said.

And he hinted other nations were developing the capacity to target Australia's infrastructure, military planning, communications and weapons networks.

"I can assure you our Chinese friends are very very busy and if they are busy then there are others that are busy too," he said.

But Mr Irvine said he was less worried about the threat from nation States because there are "certain disciplines" restraining them.

"What I am concerned about is the ability of the hacker and the small group to find one of these vulnerabilities that is sitting in our electricity grid, sitting in our petroleum and transport sector, sitting in our bureaus of meteorology without which aircraft can't fly …of sticking some sort of cyber spanner in those works," he said.

Analysts have warned hackers who support murderous organisations like Islamic State/Daish could target vital infrastructure and government IT systems from within Australia rather than heading to the Middle East to fight.

"The warfare of the 21st century is going to be fought over the internet and cyberspace before a shot is fired and it is being fought right now in terms of espionage and in terms of the capacity to sabotage your potential opponents warfighting capabilities," Mr Irvine said.

Mr Irvine urged the government to provide a serious funding boost for intelligence and lead agencies countering emerging threats in the 2015 white paper.

Intelligence sources warn Australia has already experienced a cyber attack that has induced a power blackout either involving a hacker or by a rival nation testing its capabilities.

But the body responsible for ensuring local power grid security, the Australian Energy Market Operator [AEMO] would only say it "adopts a proactive approach to cyber security and has controls and response strategies in place to mitigate potential security risks".

A 2013 report to the US Congress said American power utilities were hit by up to 10,000 cyber attacks a month. Cyber attacks in Australia are estimated to cost at least $1 billion a year.

The head of US Cyber Command, Admiral Michael Rodgers admitted in November China and "one or two" other countries could shut down the US power grid through a cyber attack.

Admiral Rogers said at the time software had been detected in China that could "shut down very segmented, very tailored parts of infrastructure" and it was "only a matter of the when, not the if, that we are going to see something traumatic".

The Defence Round Table panel of experts also included KPMG National Sector Leader Steve Clark, Thales Australia/New Zealand chief executive Chris Jenkins and University of New South Wales professor of International Security Alan Dupont and former Defence Force Chief Admiral Chris Barrie.

The panel broadly urged the Abbott government to put much more emphasis on emerging threats in the white paper which is due for release by August will lay down the Abbott government's 20 year vision for defence.

Professor Dupont said the current approach was "too focussed on the traditional dimensions of warfare"' including army navy and airforce and "not enough on cyber or space" with spending needed to be more evenly spread.

Thales Jenkins said for business "the war has started in the cyber world in terms of theft of intellectual property and financial threats" and while the financial sector was ahead of the curve other sectors were struggling.

The Australian Financial Review