Cyber spying needs concerted action
Alan Dupont
The Australian
16 October 2012
P. 12

While there is nothing new about countries or companies wanting to protect intellectual property for commercial reasons, it has seldom been considered a national security problem.

This is no longer the case as cyber space becomes a battleground between competing states intent on exploiting the vulnerabilities of the internet for economic and strategic gain.

US Defence Secretary Leon Panetta's dramatic warning that the US faces a growing threat of a ``cyber Pearl Harbor'' was triggered by a cascading series of electronic attacks on the US banking system in recent weeks, which underlines the vulnerability of modern economies to cyber espionage and sabotage.

Economic and military vitality are heavily dependent on IP; and its loss to rivals, if sustained and substantial, eventually will translate into a fall in living standards and competitive advantage.

This could be the future for Australia if the unprecedented increase in successful cyber attacks in this country is not reversed. So far this year, more than 5000 cyber ``incidents'' have been reported to the government's computer emergency response team. But these figures are only the tip of the iceberg as most cyber attacks against the private sector go unreported.

In 2009, the then US deputy secretary of defence, Bill Lynn, wrote: ``Every year an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by US businesses, universities and government agencies.''

Proportionally, this is happening in Australia, though neither the government nor business seems ready to admit the seriousness of the problem.

Government is worried about compromising sensitive intelligence methods and sources, offending countries that are complicit in cyber attacks and the admitted difficulty in identifying their precise source -- the so-called attribution problem.

Business is worried about shareholder and stockmarket reaction should the loss of IP and the penetration of company security be made public.

While these are legitimate concerns, we need to get over our coyness before the IP deficit reaches catastrophic proportions.

Sceptics who regard such warnings as exaggerated or ill-informed may like to read last year's report for the US congress on economic and industrial espionage written by the authoritative US government-owned Office of the National Counterintelligence Executive.

It makes for sobering reading. Among its key findings are that cyber space amplifies the significant and growing threat to the US from economic collection and industrial espionage; that Chinese actors are the world's most active and persistent perpetrators of economic espionage; and that the trend towards pooling of information processing and storage will present even greater future problems for the protection and integrity of sensitive information.

While there are no reliable figures for how much electronic pilfering and espionage is costing the US or Australian economies, the figure is almost certainly large and growing rapidly.

More than $1 trillion is spent on cyber defence globally, and leading anti-virus software company Symantec estimates cyber crime costs the world economy $US338 billion ($330bn) annually. This doesn't capture the longer-term erosion of national competitiveness.

The industries most heavily targeted are those focused on information and computer technology, healthcare, pharmaceuticals, agricultural and clean technologies, energy, natural resources, military technologies and advanced materials and manufacturing techniques -- in short, the enabling technologies of the future economy.

Our government is sufficiently concerned to have explicitly warned that a cyber attack on the US or Australia could be a trigger for invoking the ANZUS treaty. But that won't help when business IP is siphoned off by an unknown or opportunist hacker, who may well be an Australian and company insider.

A better approach would be to build community and business awareness through a public information campaign, combined with a commitment to build a public-private partnership around cyber defence.

Good computer housekeeping practices, based on up-to-date firewalls and computer anti-virus programs, could reduce the risk to business and individuals by 80 per cent. It may be necessary for owners of critical infrastructure such as water and power companies to invest in certifiably higher levels of cyber protection to retain their operating licences.

Specialised government agencies would provide a deeper layer of active defence against sophisticated, state-based attacks.

A longer-term solution would involve an alternative to the internet or significant changes in the internet's operating protocols to provide better system security around user identification and authentication.

The government should position Australia as a repository of cyber security expertise and exploit the commercial opportunities for the cyber defence sector. There is no unplug option so we need to learn to better manage the risk.

Alan Dupont is professor of international security at the University of NSW.