Cyber attacks more widespread than we know
Alan Dupont
The Australian
29 May 2013
P. 10

Allegations by ABC1's Four Corners that Chinese cyber spies have stolen the top-secret blueprints for ASIO's new headquarters heats up what director-general of security David Irvine has labelled a ``cold cyberwar''.

It is an unfortunate irony that the agency responsible for protecting Australia's secrets from foreign espionage has been hacked, illustrating the vulnerability of all Australians to cyber intrusions by spies, criminals, terrorists and politically motivated hactivists.

In less than a decade, cyber attacks have moved from the arcane world of computer geeks to become the No 1 concern of national security communities globally, including Australia.

Earlier this year, in the first national security strategy, the Gillard government designated cyber security as one of three priority areas.

But if ASIO cannot protect its secrets, how can far less resourced businesses and individuals?

An essential first step is greater public disclosure of the seriousness of the problem, led by government, which alone has the knowledge and resources to facilitate an informed debate. If we don't understand the problem, we won't find solutions. Silence is not the answer.

This does not mean resiling from the convention that governments don't comment on security breaches. There are good reasons for not being drawn into commentary, not least of which is not disclosing our cyber capabilities and vulnerabilities.

There also may be uncertainty about who is responsible -- the attribution problem -- as well as concerns about the political fallout in naming an attacker without proof.

If the source of the ASIO attack is a server located in China, does this necessarily mean that the attack was sanctioned by the Chinese government?

However, none of these concerns should preclude the government from getting on to the front foot about cyber security; it could take a lesson from the US. Three years ago, President Barack Obama went public with US concerns about cyber threats, authorising an article for the journal Foreign Affairs by Deputy Secretary of Defence Bill Lynn that set out the unprecedented scale of the threat.

In the face of overwhelming evidence that foreign states have siphoned off vast amounts of US intellectual property, as well as sensitive defence and intelligence information, Washington has revealed details of successful cyber penetrations to raise public awareness and warn perpetrators that future attacks will no longer be cost free.

Recently it has gone further, warning Beijing that if the cyber attacks emanating from China continue, there will be serious repercussions. The Gillard government has been unnecessarily coy about Australia's cyber vulnerabilities, which proportionately are not far removed from US experience and much of the Western world.

On the positive side, there have been some admirable initiatives in establishing more effective mechanisms for co-ordinating government cyber responses, while Irvine has been allowed to speak to the press about the threat.

But Julia Gillard needs to give a speech that fleshes out the motherhood pronouncements in the national security strategy. She also should release the long-promised cyber security white paper. Its non-release contradicts the government's assertion that cyber security is a top national security

priority.

If there is proof of Chinese government complicity in the ASIO theft, we ought to make clear to China the adverse implications for the bilateral relationship.

Finally, what to do about the ASIO building? It is unacceptable to live with the fact another country has detailed knowledge of the wiring, fit and location of computer and communication servers because it would be much more difficult to prevent further penetrations of the whole linked, national security community.

Completely, or partially, stripping the building would be extremely expensive -- but far less so than allowing ASIO to occupy a compromised building.

Alan Dupont is professor of international security at the University of NSW and a non-resident fellow at the Lowy Institute.