Arming the country for cyber attack
Hugh White
13 September 2011
The Age
P. 13

The internet is a dangerous place, but is it a battlefield? Will future wars be fought in cyberspace? Many people think they will, and our government seems to agree, at least up to a point. But a glance at history suggests some of these fears may be exaggerated.

The government is certainly acting as if it takes cyber war seriously. Cyber threats loomed large in the 2009 defence white paper, and in January last year the government opened a big new Cyber Security Operations Centre where 130 people will take command of Australia's cyber skirmishes. Then in July it announced a white paper specifically on cyber security, preceded by a public discussion paper, which is expected soon.

Much of this effort is sensibly aimed at cyber crime and other familiar ills of the internet age. But a lot of the hype that envelops cyber security is driven by the spectre of cyber warfare. How serious is this?

Of course the cyber world is already a prime field for intelligence collection but war is another matter. When people talk about war in cyberspace, they often confuse two very different ideas.

The first idea is to extend old-fashioned war — the kind that uses high explosive — into cyberspace by launching virtual attacks on the computer networks that support an adversary's military in order to degrade their ability to fight a conventional war.

This is quite a big deal. Like every other aspect of modern life, military capabilities today depend in myriad ways on potentially vulnerable computer systems, and attacking those systems will often be much more cost-effective than attacking the capabilities themselves with missiles. The US and China seem to be taking this idea very seriously, and cyber attacks would be a big part of any military clash between them in the western Pacific.

But this hybrid cyber war is very different from the pure cyber war that many enthusiasts talk about. They believe battle in cyberspace could not just support, but actually replace, physical conflict.

They argue that advanced countries such as Australia depend heavily on inherently vulnerable computer networks to operate their physical infrastructure, economies and social systems. An adversary that disrupts those networks would bring a country to its knees and force it to surrender in just the way invading armies used to do — but without a shot being fired.

This unsettling vision drives a lot of the anxiety about cyber security, so it's worth examining carefully. A bit of historical perspective helps. This is not the first time new technologies have threatened to overtake conventional war and produce victory without battle. Between the two world wars, many people became convinced that air power would replace armies.

The bomber seemed unstoppable, and air power enthusiasts assumed that no society could withstand a rain of high explosive on its cities for more than a few days. Civilians would not stand it, and governments would be forced to surrender. So, they argued, battles between armies would disappear as wars were decided quickly and decisively by bomber attacks directly on cities and citizens.

Of course it did not work out that way. World War II certainly showed how appallingly lethal the bomber could be. Conventional bombing of cities killed perhaps a million people, mostly in Germany and Japan. But it also showed how extraordinarily tough civilians are. Germany did not stop fighting until the Soviets took Berlin, and Japan until the second nuclear bomb took Nagasaki.

The lesson of this, and later conflicts, is that massive and costly air campaigns are strategically ineffective. You cannot force a country to submit by killing its citizens and pounding its cities to rubble. The air-power enthusiasts were wrong.

And that is the weakness in the idea of pure cyber war. It relies on the assumption that if we lost our air traffic control system, our stock markets, or our national power grid, a country such as Australia would simply fold up and surrender. That shows a deep misunderstanding of the nature of war and the way societies react to it — including Australia. Our experience of bombing is mercifully light, but in the First World War Australia lost 60,000 from a population of only 5 million without folding up. Losing the stock exchange for a few weeks seems trivial in comparison.

History suggests that cyber attacks on civilian systems would not be too hard to defend against. What makes cyber attacks worrying is that they are relatively cheap and easy to mount and very hard and expensive to repel. But that applies to an adversary as much as it does to us.

Cyber war is a perfect example of a conflict in which the best defence is deterrence. No doubt other countries can disrupt our banking system, but no doubt we can do the same to them.

Any potential adversary will be as vulnerable as we are, so the most cost-effective way to make sure we are not attacked is to make it clear that any cyber attack on Australia would provoke a swift and sure cyber retaliation.

This suggests that the best way for the government to protect us against cyber attack is to build robust cyber attack capabilities of our own, and discreetly make sure potential adversaries know about them. Perhaps that is what it is doing.

Hugh White is professor of strategic studies at ANU and a visiting fellow at the Lowy Institute.