Jump TO Article

Jump TO Article

Cyber warfare and its implications for Australia

An edited version of a presentation to the 2016 Seminar on Military Strategy by

Clive Lines
Deputy Director, Australian Signals Directorate
and Co-ordinator, Australian Cyber Security Centre

Cyber security is a top national security priority for Australia as cyber intrusions are a persistent threat. Herein, Mr Lines differentiates between cyber war/cyber attack and low-level cyber activity; explains their likelihood and effect; and outlines Australia's response.

Key words: cyber war; cyber security; cyber intrusions; information networks; national security.

Cyber security is a top national security priority for Australia. This is because cyber intrusions on government, critical infrastructure and other information networks present a real and persistent threat to Australia's national security and interests.

Definition of Cyber War and Cyber Attack

There is no globally agreed definition of cyber attack, nor is there a globally agreed position on how existing principles of international law might apply. Different organisations and governments have come up with their own interpretations of what constitutes an act of cyber war.

In Australia, we define cyber attack as a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident in them, with the effect, in cyberspace or the physical world, of seriously compromising national security, stability or prosperity.

Establishing a clear national definition means that the response to an incident is proportionate. The Australian definition aims to provide clarity and consistency, as the term 'cyber attack' is often used inconsistently. A proportionate response means that the appropriate time and resources are dedicated to a cyber security incident response. Each incident can be evaluated on a case by case basis.

This definition was developed in 2011 to support the announcement that the provisions of the ANZUS Treaty[1] will allow Australia and the United States to consult in the event of a cyber attack on either party. The definition is also consistent with the Tallinn Manual – currently the foremost authoritative interpretation of existing international law for security issues in cyberspace (International Group of Experts 2013). By this definition, Australia has not yet been subjected to any activities that could be considered a cyber attack.

Low-level cyber activity – which includes website defacement, spear-phishing, social media hijacking, cybercrime, and the theft of personal data – is often described as 'cyber attacks' by the media, academia and industry. But this use of 'cyber attack' to encompass low-level activity complicates a mature appreciation of the cyber security risk and vulnerability, and removes it as a meaningful threshold for policy makers to develop responses.

Importantly, Australia is not the only country thinking like this. In 2014, the definition of cyber attack was also a topic discussed at the NATO[2] Summit in Wales. NATO agreed that cyber attacks could reach a threshold that not only threatens transatlantic prosperity and security, but could even be "as harmful to modern societies as a conventional attack" and thus merit an invocation of the NATO collective defence clause.

Australia has taken a very similar approach. In fact, definitions and thresholds are the easy part – deciding how to respond is much more complicated. For example, allegations that the Chinese hacked Lockheed systems and stole blueprints for the Joint Strike Fighters are widespread. This potentially would produce a tangible strategic loss for the United States and allied nations such as Australia. It demonstrates how adversaries not only seek the information to build a competitor aircraft, but also information to help defend against it. The United States responded by indicting the hacker in question. Such acts were defined as theft rather than an "attack".

But there has been malicious cyber activity that would have fallen under our, and others', definitions of a cyber attack. For the most part, this activity has taken place during periods of heightened tension between states or during actual conflict. People refer to cyber attacks against Georgia, Estonia, and, most recently, Ukraine – where a cyber incident at the national power grid left roughly 700,000 people without power for several hours in the coldest months of winter. And this is what we have always expected to see: cyber attack used as one element of a broader campaign.

We have also seen some states use cyber attack as a means of coercion in peacetime, but admittedly still during periods of heightened tension or dispute. The attack on Sony attributed by the FBI[3] to North Korea is a very good

[1]The 1951 Australia, New Zealand, United States Security Treaty, a collective security agreement which binds Australia and New Zealand and, separately, Australia and the United States, to co-operate on military matters in the Pacific Ocean region.

[2]North Atlantic Treaty Organisation

[3]United States Federal Bureau of Investigation

example of this. North Korea had requested the United States Government intervene with Sony to seek withdrawal of a movie which they regarded as disrespectful. When this did not occur, North Korea used its resources to attack Sony in an attempt to coerce the United States Government. The attack cost Sony millions of dollars in direct remediation costs, resulted in their internal correspondence and intellectual property being published online, the destruction of their data and cost the chief executive officer his job.

Of course, the Stuxnet virus, which was allegedly deployed to sabotage an Iranian nuclear facility, is another example of malicious cyber activity that could have – and for the Iranians, probably did – cross the threshold to cyber attack.

But in all these cases, with actions that we would judge to be within reach of being considered a cyber attack, we have not always seen a state response – noting this does not necessarily have to occur in cyber space. A continued lack of international consensus on proportionate and appropriate responses to cyber attacks makes the threshold for response ambiguous – which in turn raises the risks of miscalculation and possibly encourages some states to continue developing cyber attack capabilities for use as an effective tool.

And this is what we are broadly seeing now: states viewing cyber attacks as a tool for provocation, shaping and coercion; and an increasing number are developing the capability to conduct cyber attacks against targets of their choosing.

What does this mean for cyber warfare in the 21st Century? And what might the effects be on countries like Australia? The thoughts that I wish to put before you are:

- Cyber war will not occur in isolation, but activities through cyber will be employed in conjunction with other forms of coercion throughout a conflict between states.
- The threat to Australia through cyber is real, present and persistent.
- There is much to be done to deal with the threat, but some of our efforts are starting to have an impact.

The Possibility of Cyber War

There are two interesting books on the subject of cyber warfare: Richard Clarke's *Cyber war: the next threat to national security* (Clarke and Knake 2010); and Thomas Rid's *Cyber war will not take place* (Rid 2013). Titles are designed to attract attention and buyers, but each of these titles does sum up the authors' perspectives. Richard Clarke's real purpose is to build awareness of the threat and move policy makers to action. Thomas Rid hopes to reduce the hype surrounding cyber warfare and appeal for sober discussion. I believe both are correct and cyber warfare will be a feature of all interstate conflict – and it is already. But a cyber war, fought in isolation in cyberspace between states, is unlikely given the current levels of both capability and policy maturity.

While cyberspace may be a revolutionary phenomenon, it does not mean our existing knowledge of nation-state behaviour is redundant or irrelevant. Cyberspace has extended the battlefield beyond land, sea, and air. Cyber is best understood as a new, but not entirely separate, component on the spectrum of conflict.

Operations in cyberspace are just one of many options available to nation-states to achieve their strategic ends. And cyber capabilities are likely to be employed in conjunction with kinetic operations as part of an overall military campaign. Countries around the world are attempting to work towards integrating growing cyber capabilities into conventional military planning and operations.

It is highly unlikely for a standalone cyber war to occur, but activities through cyber will be part of future wars. You can anticipate seeing a surge in cyber activity in the lead up to conflict and certainly throughout its opening phases. The aim will be to impact an adversary's command and control and situational awareness, as well as putting pressure on areas outside conventional military reach.

This leads to another point – some people overemphasise the anonymity of the internet and believe attribution will be difficult in the context of cyber warfare. But attribution will – to some level – be quite straightforward: it is the state you are in heightened tension or conflict with. And states sometimes want people to know they are behind certain activities in order for the intended message to be understood.

Another aspect which needs to be considered in cyber warfare is cost. The development and maintenance of an effective cyber warfare capability is very expensive. This is not only due to the particular people and skills required for such a capability, but because cyber attacks designed against particular systems or software vulnerability require a significant amount of integration with intelligence collection, reverse engineering, persistent access, and command and control capabilities.

Not all states will have this degree of capability or the income to support this, but others may acquire such capabilities through purchasing lower-end commercial off-the-shelf equipment from cyber criminals. All of that said, the real and present threat for Australia is espionage and criminal threat through the cyber medium.

The Cyber Threat

Espionage through cyberspace has been practised by state and state-sponsored actors for around a decade. Its purpose, like espionage throughout the ages, is to obtain knowledge of the intent of another state, to accrue a strategic advantage, or to appropriate intellectual property.

In Australia today this threat is real, it is persistent and it has real-life consequences. And it is for this reason that the Australian Cyber Security Centre (ACSC) was established in 2014 to bring together capabilities from various governmental organisations to ensure that we have the best possible response against cyber adversaries.

At the ACSC, we have found that cyber adversaries are aggressive and persistent in their efforts to compromise Australian networks and information. They are constantly improving their tradecraft in an attempt to defeat our network defences and exploit new technologies.

Australia is an innovative country with a globally important resources sector. We are also a regional leader with global interests and important partnerships. But we are also a highly connected nation. All these factors make Australia a target-rich environment for cyber adversaries.

There is a range of cyber adversaries motivated to target Australian networks. These include issue-motivated groups, serious and organised criminals, and foreign state-sponsored adversaries.

Hactivists and individuals causing nuisance, attempting to draw attention to themselves and their causes, while usually less capable and sophisticated, are still able to cause disruption to Australian government and businesses.

Financially motivated criminals who exploit and access systems for financial gain are a substantial threat to Australia. Transnational serious and organised cybercrime syndicates are of most concern, specifically those that develop, share, sell and use sophisticated tools and techniques to access networks and systems impacting Australia's interests.

Foreign state-sponsored adversaries, including nation-states, seek economic, foreign policy, defence and security information for strategic advantage. Such adversaries have traditionally possessed the most advanced and sophisticated tools to conduct their activities, sometimes maintaining access to an organisation's network for years at a time to steal the information they require.

At the ACSC we see daily cyber espionage activities targeting our government networks, businesses and individuals for both espionage purposes and criminal commercial gain. If an organisation is connected to the internet, it is vulnerable. The solution is in part about hardware, software and strengthening network infrastructure and security. But it is also about the management of an organisation, its people, culture and resources. Network security is only as strong as the least security-aware individual, so it requires the attention of IT[4] specialists and senior leaders alike.

Australia's Response

One of our challenges has been to help bring an awareness of the cyber threat to ministers, senior officials, business leaders and industry. In April 2016, after extensive consultations, the Prime Minister released the Australian Cyber Security Strategy (Prime Minister and Cabinet 2016) in Sydney, and appointed Alastair MacGibbon as the special advisor on cyber security in the Department of the Prime Minister and Cabinet. He also announced the creation of a new cyber ambassador position at the Department of Foreign Affairs and a junior ministerial position with responsibility for cyber. This demonstrates the importance of cyber security to the Australian Government.

The Prime Minister also announced for the first time that an offensive cyber capability is housed within the Australian Signals Directorate (ASD) to provide another option for government to respond to serious cyber incidents against Australian networks.

The Strategy also called for building a national cyber partnership between government and business, and to enhance Australia's networks and systems so that they are harder to compromise and more resilient to cyber attacks. Strong cyber security is the best way to militate against cyber intrusions; prevention is always better than a cure.

Conclusion

There are few international norms currently agreed to for the conduct of cyber warfare – although it is a rapidly evolving space, particularly around global norms.

Cyber warfare is unlikely in isolation given the current level of capability and policy maturity. It will most likely be present in the lead up to conflict and increasing tensions between states. Actions such as the attack on Sony and the Ukrainian power system provide some insights in how a cyber capability might be used in the lead up to warfare or as part of a broader campaign plan.

The anonymity of cyberspace is useful for espionage purposes or where you want your actions to be deniable, but is not always helpful when states escalate to an attack.

Cyber warfare will clearly be part of the broader military capabilities of many states, but will not necessarily be the great equaliser that some have foreseen. Like all military capabilities, it is likely to be expensive to develop and maintain cyber capability at a sophisticated level.

The Author: Clive Lines is the Co-ordinator of the Australian Cyber Security Centre, and the Deputy Director of the Australian Signals Directorate. He had earlier served as First Assistant Secretary, Information Communications Technology Reform, in the Department of Defence; and as Head of the Defence Imagery and Geospatial Organisation. Prior to the latter appointment, he had served briefly as Director of the Defence Signals Directorate and had earlier served as both the Deputy Director Capability and Deputy Director Intelligence in the Defence Signals Directorate. Mr Lines has also worked in the Defence Intelligence Organisation as Assistant Secretary, Analytical Services. [Photo of Mr Lines: Department of Defence]

The **Australian Signals Directorate** collects foreign signals intelligence and maintains information security for government and the ADF. Both roles have existed since the organisation was established in the aftermath of World War II. Foreign signals intelligence supports a broad range of government policy development and decision-making, and the conduct and planning of ADF operations. On the security side, ASD is responsible for cyber and information security standards for Commonwealth agencies. It is this component of ASD that has been incorporated into the Australian Cyber Security Centre.

The **Australian Cyber Security Centre** was opened in November 2014 bringing together cyber security capabilities from ASD, the Defence Intelligence Organisation, the Australian Security Intelligence Organisation, the Australian Criminal Intelligence Commission (ACIC), the Australian Federal Police (AFP) and the Computer Emergency Response Team Australia. The focus of the centre covers all aspects of cyber security including government, industry and critical infrastructure. The presence of the AFP and ACIC also provides direct links to the law enforcement community. In addition, all agencies bring their international relationships and information exchange to the centre.

References

Clarke, Richard A., and Knake, Robert K. (2010). *Cyber war; the next threat to national security and what to do about it* (Ecco: New York).

International Group of Experts (2013). *Tallinn manual on the international law applicable to cyber warfare* (Cambridge University Press: Cambridge).

Prime Minister and Cabinet, Department of (2016). *Australia's Cyber Security Strategy* (Commonwealth of Australia: Canberra).

Rid, Thomas (2013). *Cyber war will not take place* (Oxford University Press: Oxford).

[4]Information Technology