Jump TO Article

Jump TO Article

Strategic significance of cyber and space: seminar summary

Brigadier David Leece, PSM, RFD, ED (Ret'd)
President, Royal United Services Institute, New South Wales[1]

Australia's 2016 Defence White Paper emphasised the threat to government and society posed by warfare in cyberspace and space and enhanced the Defence Force's resourcing for dealing with it. The Institute's 2016 Seminar on Military Strategy examined the strategic significance of cyber and space, assessed the likelihood and effects of warfare in and through these domains, and outlined Australia's response to the threat.

Key words: cyberspace; space; cyber warfare; space warfare; Australia; Defence White Paper; Cyber Security Strategy.

The Royal United Services Institute used its 2016 Seminar on Military Strategy to explain to defence professionals and the general community why cyber and space now play a central role in Australia's defence policy (Defence 2016). We were privileged to hear five experts discuss the strategic significance of cyber and space and how Australia is addressing the issue.

During the seminar, we heard that cyberspace and space are now recognised as domains (equivalent to sea, land and air) in and through which war can be conducted.

Cyber security is a top national security priority for Australia as cyber intrusions are a persistent threat. We must, however, differentiate between cyber war/cyber attack and low-level cyber activity. 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. While cyber intrusions by state and non-state actors on government and commercial enterprises and private persons have become common, cyber attacks have been rare – the Stuxnet worm employed against Iran's nuclear facilities is regarded as the world's first cyber weapon[2].

Global communications are very vulnerable to offensive action by nation-states, but currently are less vulnerable to offensive action by terrorists and criminals. The threat is non-geographic and countering it requires competence in signals intelligence. In Australia, we take a team approach to intelligence gathering, led by the Australian Signals Directorate and co-ordinated by the Australian Cyber Security Centre.

State actors in the offensive cyber field are believed to include China, Russia, North Korea and Iran. Non-state actors include Islamic State and criminals. Much of the offensive action is directed to espionage, to defeat border controls, or to steal state or commercial secrets, including the acquisition of technology or to avoid having to buy or develop it.

Not since World War II has Australia faced a direct threat through a warfighting domain. The use of cyberspace has changed that paradigm. No longer do we need to deploy overseas to face threats; Australia is now facing them at home on a daily basis. The Australian Defence Force (ADF) must enhance its ability to prevent and respond to threats through normalising cyber operations. Among the specific vulnerabilities of the Australian Defence Organisation are its computer networks, the Defence Secure Network and the Defence Restricted Network, especially during periods of high operational tempo. Signals intelligence is generated when outside parties are successful in exploiting these networks.

At the higher level of conflict, there are few international norms currently agreed to for the conduct of cyber warfare. Cyber warfare is unlikely in isolation. It will most likely be present in the lead up to conflict and increasing tensions between states.

In response, Australia now has the ability to disrupt, deny and degrade the computer networks of malicious cyber actors in response to their actions or threatened actions. Indeed, the ADF is well-practised in cyber warfare at the strategic level. It is now developing the capability to engage in cyber warfare at the operational and tactical levels. There are nascent capabilities within the Army and Air Force, and we now have the strategic guidance and funding to further develop these capabilities.

As the threats from advanced technologies rapidly escalate at the global level, though, Australia will need new mechanisms and agencies to respond. The government this year has laid a foundation for this response via its innovation strategy, its Defence White Paper (Defence 2016), and its Cyber Security Strategy (Prime Minister and Cabinet 2016). But there are several areas where key foundations or linking mechanisms are absent. In respect to cybersecurity, cyber defence and cyber warfare, there is no recognised mechanism by which a mature and secure operating environment for cyber effects can be established. Hence, the ADF needs to quickly recruit, train and retain its own workforce, despite a national and international skills shortage in this area.

Given the national lack of a skilled workforce, the country's cybersecurity, cyber defence and cyber war education and training policy is foundational to the establishment, development and enhancement of every other cybersecurity policy. Australia needs to make giant steps in this area, of which an enhanced science,

(Continued on page 31)

[1]David Leece is president of the Institute and editor of *United Service*. These are his personal views. E-mail: office@rusinsw.org.au.

[2]Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon developed during the Bush administration to sabotage Iran's nuclear programme.

Significance of cyber and space…

(Continued from page 7)

technology, engineering and mathematics approach is vital.

Turning now to the space domain, space has not yet been overtly militarised, but China and the United States have demonstrated their ability to shoot down their own satellites and other nation-states are thought to be developing that capability.

At the same time, modern communications and the operating systems of developed and developing nations and their armed forces have become critically dependent on many types of satellites which orbit the earth. These include intelligence satellites, communication satellites, and global positioning system satellites, among many others.

Satellites are vulnerable to anti-satellite weapons systems and to space junk. Coupled with the inherent difficulty of defending space assets against attack, and the uncertainty that clouds attempts to attribute events in space to their causes, such dependence leaves nations, including Australia, uncomfortably vulnerable. Warfare in space has the potential to render large parts of the entire domain unusable for all nations, with significant secondary effects in the other physical domains.

Given that the capability to militarise space is being developed by certain unnamed nation-states, it is a challenge that Australia must now prepare to face. Recognising this vulnerability, Australia is increasing its investment in support of space situational awareness, which underpins assured access to space, and supports the strengthening of international norms regarding the responsible use of space. The principal defence, however, is to have redundancy built into the system – multiple satellites doing the same job.

In conclusion, there currently is an escalatory cycle of militarisation in both cyberspace and space involving several powers including China, Russia, Iran and North Korea, among others. In Australia, we have now laid a firm foundation for our future security in the cyber and space domains – indeed, with our Australian Cyber Security Centre, we are a leader among our allies – but we have some catching up to do to if we are to match the capabilities of potential adversaries. The papers delivered by the five experts follow. I commend them to you.

References

Defence, Department of (2016). *2016 Defence White Paper* (Commonwealth of Australia: Canberra).

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