Jump TO Article

Jump TO Article

Training and education for cyber security, cyber defence and cyber warfare

An edited version of a presentation to the
2016 Seminar on Military Strategy on 31 May 2016 by

Professor Jill Slay, AM
Director, Australian Centre for Cyber Security
University of New South Wales, Canberra[1]

Australia's response to advanced technologies has been poor in education, and in a range of social management and government functions. Australia's cyber security, cyber defence and cyber war education and training policy is foundational to the establishment, development and enhancement of every other cybersecurity policy. As the threats from advanced technologies rapidly escalate at the global level, Australia will need new mechanisms and agencies to respond, of which an enhanced science, technology, engineering and mathematics approach is a vital one.

Key words: advanced technologies; cyber defence; cybersecurity; cyber warfare; education; training.

Cyber security[2], cyber defence and cyber warfare have moved to the front of our thinking with the release of the 2016 Defence White Paper (Defence 2016). There is a set of strongly held beliefs around the premise that cyber warfare is an area where a small nation such as Australia can generate, if necessary, a disproportionate effect in the global strategic environment. It is postulated that this will be achieved principally by the effects that could be generated by an effective Australian cyber warfare force and the individual capabilities required to generate those effects. It also can be argued that cyber warfare presents the Australian Government with an opportunity to generate a strategic effect which is disproportionate to our relatively modest military, technological, economic and diplomatic power. To the writer's knowledge, however, there is no recognised mechanism by which a mature operating environment for the cyber effects can be established. The Australian Defence Force (ADF) needs to quickly recruit, train and retain its own workforce and develop expertise.

The country's cyber security, cyber defence and cyber war education and training policy is foundational to the establishment, development and enhancement of every other cyber security policy and as guidance for the glaringly obvious national lack of a skilled workforce. Australia needs to make giant steps, of which an enhanced science, technology, engineering and mathematics (STEM) approach is but one – one that will have no strong pay-offs in the next decade at least.

This paper reviews the contexts and problems that have brought us to this current situation and puts forward a curriculum for cyber training that is already in use or being trialled. The new suite of forward-looking Australian government policies, announced since September 2015, will be greatly affected by the presence, or absence, of an effective education and training policy agenda for cyber-security, cyber defence and cyber war and a national implementation plan.

Defining and differentiating Cyber Security, Cyber Defence and Cyber Warfare

First, though, we should define some key terms and I shall draw on Austin and Slay (2016) to do so. The term 'cyber security' covers a multitude of quite diverse considerations (Table 1). Every country, and even actors within one country, will focus on a different combination of these considerations because they will have different organisational priorities and quite distinct economic and security potentials.

Table 1. Policy impact on education, training, research and workforce needs in cyber security, cyber defence and cyber warfare.

Security Need	Putative Policy/Advice Sources	Education, Research and Training implications
Cybersecurity	Australian Signals Directorate Top 4 Strategies (ASD 2013)	Cohort of government and industry staff who are trained in: network security information security incident response digital forensics software development criminology
Warfare	Defence White Paper 2016 (Defence 2016)) Defence White Paper 2009 (Defence 2009)	Cohort of government and industry staff who are trained in: network security information security incident response digital forensics software development reverse engineering cyber effects open-source intelligence law policy
Espionage/ counter-espionage	Defence White Paper 2016 (Defence 2016) Defence White Paper 2009 (Defence 2009) ASIO Report to Parliament 2011/12 (ASIO 2012) ASIO Strategic Plan 2013-16 (ASIO 2013)	Cohort of government and industry staff who are trained in: network security information security incident response digital forensics software development reverse engineering cyber effects open-source Intelligence law policy

[1]E-mail: j.slay@adfa.edu.au

[2]In this paper, "cyber security" connotes the legal, policy and/or national security aspects of cyber; whereas "cybersecurity" connotes the technical issue of securing computers and networks.

In broad terms, 'cyber security' has at least eight 'ingredients' or foundation elements, some of which are narrowly technical (but involve human input and institutions); and others of which are simultaneously technical and deeply dependent on non-technical inputs. One view of these ingredients is captured in Figure 1, which describes them as vectors of attack and response. This graphic is adapted from an approach developed by engineers in Bell Labs to address problems of protection of information and information systems at the enterprise level and to protect enterprise connectivity (Gupta and Buthmann 2007). The Bell Labs concept and our adapted graphic provide a very useful departure point for broadening public understanding of what shapes security in cyberspace. At the same time, even this approach does not do justice to wider institutional, political, legal and social aspects of the problem set. At the national level, all strategy and planning for cyber security depend on the institutional, political, legal and social environment as much as they do on engineering, systems management, or capability-based approaches, such as those implicit in the Bell Labs concept, which was developed almost a decade ago.

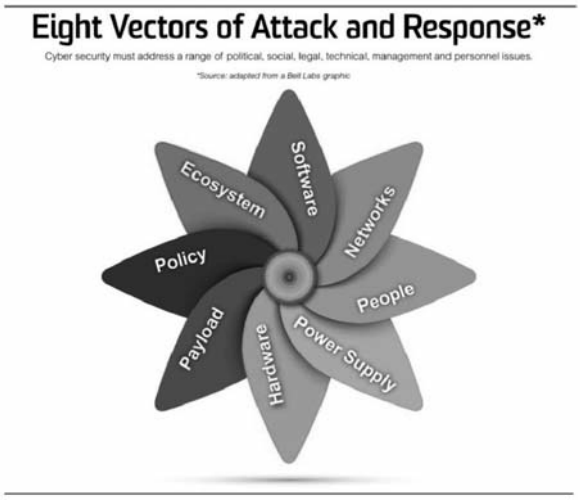

Figure 1. A cyber security model showing eight vectors of attack and response – cyber security must address a range of political, social, legal, technical management and personnel issues [Source: adapted from Gupta and Buthmann (2007)]

In defining terminology, it is important to refer a little to the significance of cyber defence and cyber warfare. Here we use cyber defence simply to mean defending a complex socio-technical system (a company, a country, a government) from attack via people, processes or tools. It is implicit that this system has already been secured and a baseline for security set.

Cyber warfare is a relatively new concept. The cyber domain has evolved rapidly as technological advances in communications and information technologies have not only generated an information advantage for western militaries, but also created vulnerabilities that can be exploited by adversaries seeking to achieve an asymmetric effect and especially contextualized within kinetic warfare. It is clear from both international academic literature and doctrine that most of the material written about cyber warfare tends to be conceptual and without practical outcomes that can be implemented in a governmental or military application. That said, in a technical sense at least, cyber warfare focuses on creating cyber effects to destabilise a secure socio-technical system (a military platform and its people).

Australia's Evolving Cyber Security Policy

There is little evidence that there is a generally held academic model, or body of knowledge, that applies to the cybersecurity profession and, beyond that, to cyber defence or cyber war. In fact, it can be claimed that the term 'cyber security' or 'cybersecurity' is relatively undefined and thus the 'cyber' part of the word is claimed by many who use it to described 'computing' in general and the 'security' part is claimed, especially by vendors, as a descriptor for an ever-growing and complex set of systems and tools which are promised to keep the user safe.

Our understanding of cybersecurity, particularly within academia, does not appear to have been driven by, or to have developed in parallel with, cyber security policy, so I will now identify some highlights of policy evolution in Australia since 2001 before looking at their education, research and training implications.

Cyber security as a national security issue was identified first in the Defence White Paper of 2000 (Defence 2000), where the new challenge was recognised and Defence's role established. The Howard government in 2001 launched an E-Security Initiative, which formed collaboration between federal government agencies; and the Trusted Information Sharing Network, representing major sector groups that were identified as critical infrastructure for the purposes of national security (Parliament 2013).

The Rudd Government reviewed Australia's e-security policies, programmes and capabilities in 2008. This eventuated in new mechanisms for information exchange, but did not meet all its implementation goals at the time. The 2009 Defence White Paper (Defence 2009) discussed emerging threats of cyber warfare; and, later in 2009, the Cyber Security Strategy (Attorney-General 2009) was released, leading to the formation of the Cyber Security Operations Centre (CSOC), to 'provide greater situational awareness', and CERT Australia (the computer emergency response team) which 'provides information and advice on cyber security to the Australian community'. The Australian Security Intelligence Organisation (ASIO) Report to Parliament 2011–12 (ASIO 2012) focused on espionage and state and non-state actors and their role in targeting Australian interests through cyber espionage.

In April 2013, the Australian Signals Directorate (ASD) mandated its 'Top 4' strategies to mitigate targeted cyber intrusions (ASD 2013) as part of the revised Protective Security Policy Framework. ASD assessed that around 85 per cent of intrusions would be mitigated once the 'Top 4' strategies were implemented. This was closely followed by the formation of the Australian Cyber Security Centre (ACSC) and was built on CSOC and ASD and other cyber security capabilities from ASIO, Attorney-General's Department, Australian Federal Police and the Australian Crime Commission.

Also in 2013, the Attorney-General's Department introduced a national plan to combat cyber-crime

(Attorney-General 2013) which focused on 'six priority areas for action' including:

- educating the community to protect themselves;
- partnering with industry to tackle the shared problem of cyber-crime;
- fostering an intelligence-led approach and information sharing;
- improving the capacity and capability of government agencies;
- improving international engagement on cyber-crime; and
- ensuring an effective criminal justice framework.

The 2016 Defence White Paper notes its cyber focus as: "New and complex non-geographic security threats in cyberspace and space will be an important part of our future security environment. The cyber threat to Australia is growing. Cyber attacks are a real and present threat to the ADF's warfighting ability as well as to other government agencies and other sectors of Australia's economy and critical infrastructure." (Defence 2016: 18)

The 2016 Cyber Security Strategy (Prime Minister and Cabinet 2016) indicates that, going forward, there will be:

- a ***national cyber partnership*** between government, researchers and business, including regular meetings to strengthen leadership and tackle emerging issues;
- ***strong cyber defences*** to better detect, deter and respond to threats and anticipate risks;
- ***global responsibility and influence***, including working with our international partners through our new cyber ambassador and other channels to champion a secure, open and free Internet, while building regional cyber capacity to crack down on cyber criminals and shut safe havens for cyber crime;
- ***growth and innovation*** including by helping Australian cyber security businesses to grow and prosper, nurturing our home-grown expertise to generate jobs and growth; and
- a ***cyber-smart nation*** by creating more Australian cyber security professionals by establishing Academic Centres of Cyber Security Excellence in universities and fostering skills throughout the education system.

Impacts of Cybersecurity Policy on Education and Training

Although individual academics and universities have in special circumstances supported federal and state governments in cybersecurity issues, to the writer's knowledge, Australian university academics were first asked by Prime Minister Howard in 2001, via their vice chancellors, to identify if their research was aligned to the defence of the national information infrastructure and to volunteer to collaborate with government.

From 2001 until now, there has been a minor response in some Australian universities where small research groups were started, usually based in information technology departments; or teaching themes were developed in cybersecurity, digital forensics or critical infrastructure disciplines, largely self-defined, and funded by small contracts with the Defence Science and Technology Organisation, small Australian Research Council grants, National Security Science and Technology funds from the Department of Prime Minister and Cabinet, and other small grants from state and federal government departments.

The 2009 National Cyber Security Strategy detailed, as a strategic priority, cyber education for the nation and stated that the government would seek to "educate and empower all Australians with the information, confidence and practical tools to protect themselves online" (Attorney-General 2009). It is not clear if this has been achieved.

The Research Network for Safeguarding Australia was formed around 2005 and did have some focus in cyber or information security. It was spearheaded largely by the Queensland University of Technology.

There have also been five attempts to get a Co-operative Research Centre for Cybersecurity funded, but these have so far failed, possibly because the technical foci have not always been sufficiently aligned with policy needs. There are at least two agendas at play when academics, industry and policy-makers come together and consider the issue of cybersecurity. One is driven by the needs of academics to publish, win grants and maintain their hold on niche research areas; the other is driven by our need for cyber warriors in industry and Defence.

Nationally speaking, Australia needs, and has needed since at least 2001, a cohort of extremely qualified people – qualified from Technical and Further Education diploma to PhD level – to plan, design, and implement cybersecurity solutions, policies, laws, advice and ethics in a range of domains from engineering, through computer science and network engineering, to law, psychology, political science and war.

There has been some hesitancy in putting even a tentative curriculum together but the Australian Centre for Cyber Security at the University of New South Wales, Canberra, has now developed, with much input from ADF officers, a curriculum which covers training, education and research issues, including cybersecurity and cyber defence. It is now moving towards including the underpinnings of cyber warfare at several levels. These are offered as a contribution to move forward a pressing issue and provide long-needed knowledge, skills and capability.

Conclusion

Australia's response to advanced technologies has been moderate in most industrial and defence applications; and poor in education, and a range of social management and government functions. As the threats from advanced technologies rapidly escalate at the global level, Australia will need new mechanisms and agencies to respond. The current government has laid a foundation for this response through its innovation strategy, its Defence White Paper, and its Cyber Security Strategy.

There are several areas in the Australian ambition, however, where key foundations or linking mechanisms are absent. There is a large gap between United States assessments of advanced technology threats and the Australian government's public assessments. These gaps have important policy implications, as well as negative impacts on the security and prosperity of Australians.

(Continued on page 31)

Training and education for cyber security… *(Continued from page 26)*

An example of this relates to cyber security, cyber defence and cyber warfare, where there is no recognised mechanism by which a mature and secure operating environment for cyber effects can be established. The ADF needs to quickly recruit, train and retain its own workforce and develop expertise, in an environment of national and international skills shortage.

The country's cyber security, cyber defence and cyber war education and training policy is foundational to the establishment, development and enhancement of every other cybersecurity policy in a civilian or defence context, and as guidance for the glaringly obvious national lack of a skilled workforce. Australia needs to make giant steps, of which an enhanced science, technology, engineering and mathematics approach is a vital one, but one that will have no strong pay-offs in the next decade at least.

The Author: Professor Jill Slay is Director of the Australian Centre for Cyber Security at the University of New South Wales, Canberra. She has an international research reputation in cyber security, including in forensic computing, critical infrastructure protection and cyber terrorism; and has worked in collaboration with many industrial partners. She has supervised 16 PhDs; published one book and more than 120 refereed book chapters, journal articles or research papers; and been awarded some $2.5million in grant funding. She advises industry and government on strategy and policy; and some 30 of her former students are employed in industry and government. She is a Fellow of the International Information Systems Security Certification Consortium; and was made a Member in the General Division of the Order of Australia in 2011.

References

ASD (2014). Top 4 strategies to mitigate targeted cyber intrusions: mandatory requirement explained (Australian Signals Directorate: Canberra).

ASIO (2012). *ASIO Report to Parliament 2011-12* (Australian Security Intelligence Organisation: Canberra).

ASIO (2013). *ASIO Strategic Plan 2013-16* (Australian Security Intelligence Organisation: Canberra).

Attorney-General, Department of (2009). *Cyber Security Strategy* (Commonwealth of Australia: Canberra).

Attorney-General, Department of (2013). *National Plan to Combat Cybercrime* (Commonwealth of Australia: Canberra).

Austin, Greg, and Slay, Jill (2016). *Benchmarking Australia's cybersecurity strategy: a future-looking checklist*. Australian Centre for Cyber Security Briefing Paper No. 1.

Defence, Department of (2000). *Defence 2000: our future defence force – 2000 Defence White Paper* (Commonwealth of Australia: Canberra).

Defence, Department of (2009). *Defending Australia in the Asia-Pacific century: Force 2030 – Defence White Paper 2009* (Commonwealth of Australia: Canberra).

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

Gupta, A., and Buthmann, T. (2007). *The Bell Labs security framework: making the case for end-to-end Wi-Fi security.* Alcatel-Lucent Bell Labs Technology White Paper.

Parliament (2013). Parliament Briefing Book, 44th Parliament: Cyber – accessed on 29 May 2016 at http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber.

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

Robinson, M., Jones, K., and Janicke, H. (2015). Cyber warfare: issues and challenges. *Computers & Security* **49** (March), 70 – 94.