Development in Training and Education for Australian Cyber Security: Filling the Gaps

Professor Jill Slay and Professor Greg Austin

UNSW Canberra @ADFA

Abstract - There are several areas in the Australian cybersecurity ambition where key foundations or linking mechanisms are absent. There is a large gap between U.S. 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. 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 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 STEM approach is only one, and one that will have no strong pay-offs in the next decade at least.

1 INTRODUCTION

Australia's response to advanced technologies has been highest in consumer applications, commerce, science, mining and health, moderate in most industrial and defence applications, and poor in education, a range of social management and government functions. The federal government has moved aggressively in the past nine months to redress the country's technological lag with a new ambition to enter the top ten of the most technologically innovative countries in the world. When it comes to addressing threats from advanced technologies, since Australia is a free and open society facing few enemies, and none that are powerful, the country has been even farther behind the pace. Awareness in the broader community and even in

leadership circles of the threats from advanced technology is quite weak. However, 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 in 2016, especially in its innovation strategy, its Defence White Paper, and its Cyber Security Strategy.

There are several areas in the Australian ambition where key foundations or linking mechanisms are absent. There is a large gap between U.S. 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 to Australians. There are unrevealed time / policy trade-offs in the federal government's position.

An example of this concerns Cyber Warfare. There are 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 principally be achieved by the effects that could be generated by an effective Australian cyber warfare force and the individual capabilities required to generate those effects. It can also 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. However, to the writer's knowledge, there is no recognised mechanism by which a mature operating environment for the cyber effects can be established and the ADF needs to quickly recruit, train and retain its own workforce and develop expertise.

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 and as guidance for the glaringly obvious national lack of a skilled workforce. Australia needs to make giant steps, of which an enhanced STEM approach is only one, and 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 examines the current and previous research, education and training policies, plans and practice of our allies (and a potential opponent). The 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 cybersecurity and a national implementation plan. Australia's key allies -- the United States and the United Kingdom – are already at least partially prepared and this paper proposes several recommendations to overcome the country's lagging posture in provision of world class policy research and education relevant to Australia's specific needs.

2 DEFINING AND DIFFERENTIATING -CYBERSECURITY, CYBER DEFENCE AND CYBER WARFARE.

In broad terms, "cyber security" has at least eight "ingredients" or foundation elements, some of which are narrowly technical (but which all involve human input and institutions) and others of which are simultaneously technical but deeply dependent on non-technical inputs. One view of these ingredients is captured in Figure 1 on the next page which describes them as vectors of attack and response. This graphic in Figure 1 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. The Bell Labs concept and our adapted graphic provide a very useful departure point for broadening public understanding of what shapes security in cyber space. 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.

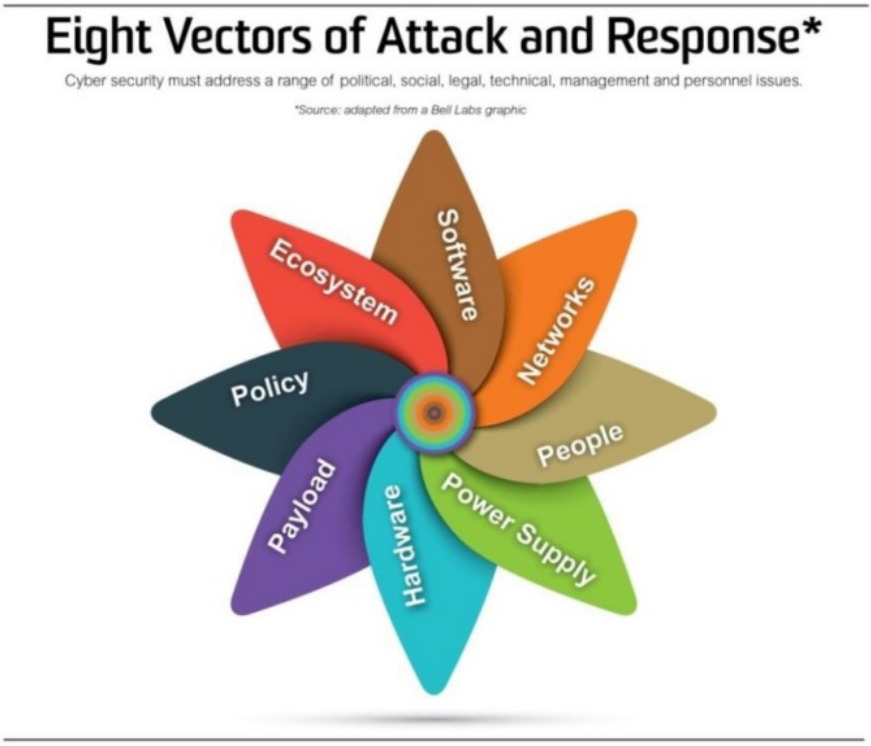

Figure 1 A Cyber Security Model

In defining terminology, it is important to refer a little to the significance of Cyber Defence and Cyber Warfare. Here we use Cyber Defence to simply mean defending a complex socio technical system (a company, a country, a government from attack via people, processes or tools). Implied is the fact that this system has already been secured and a base line 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. While there is much

hype in the media and popular press, it is clear from both international academic literature and doctrine that most of the material written about cyber-warfare tends to be conceptual in nature and without practical outcomes that can be implemented in a governmental or military application.

Newer work that deals with the complexities of defining cyber warfare and then presenting both an academic research agenda and operational definitions has emanated from both the US and UK. Robinson, Jones and Janicke (2015) present an international review of contemporary thought. Their paper, while presented by UK academic and air power experts, is one that does not successfully deal with providing a new definition of cyber warfare but rather one that presents a range of opinions on a very comprehensive range of relevant topics. The greatest problem the paper leaves is the confusion that is often present in media-focused and unclassified literature where the realm of intelligence and cyber 'attack', both commercial espionage and possible attack on Nation States, is not differentiated from the offensive or defensive use of military cyber effects. Both are equally termed 'cyber warfare' and this does not simplify the issue either academically or operationally. While the significance of definition is important, it is clear that 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).

3 THE AUSTRALIAN CYBERSECURITY POLICY LEGACY AND ITS IMPACT ON EDUCATION, TRAINING AND RESEARCH

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 '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 will 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, cybersecurity policy. The following overview details highlights of policy development. The accompanying table then indicates the associated research, training or education needed to either resolve the technical issues indicated in the policy or to develop capacity and capability.

When looking for the antecedents to current policy and practice which can today be aggregated as 'cybersecurity' so as to develop our own understanding of the status quo and the improvements that might be made, we turn to the 44th Parliament Briefing (Parliament 2013) book to realise that cyber security as a national security issues was identified first in the Defence White Paper of 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. It also developed the Trusted Information Sharing Network (TISN) representing major sector groups that were identified as critical infrastructure for the purposes of national security.

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

In April 2013, ASD mandated 'Top 4' Strategies to Mitigate Targeted Cyber Intrusions as part of the revised Protective Security Policy Framework. 'ASD assessed that around 85% 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, AGD, AFP and the Australian Crime Commission.

Also in 2013, the Federal Attorney General's Department introduced a national plan to combat Cybercrime which focused on 'six priority areas for action' including:

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

The Defence White Paper of 2016 (p18) 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'.

The Cyber Security strategy of 2016 indicates that going forward there will be (even though much is yet to be implemented:

- *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 cybercrime.
- *Growth and innovation* including by helping Australian cyber security businesses to grow and prosper, nurturing our home-grown expertise to generate jobs and growth.
- *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.'

Security Need	Putative Policy / Advice Sources	Education, Research and Training implications
Cybersecurity	ASD Top 4	Cohort of government and industry Staff who are trained in: ▪ Network Security ▪ Information Security ▪ Incident response ▪ Digital Forensics ▪ Software development ▪ Reverse engineering ▪ Cyber effects ▪ OS Intelligence ▪ Criminology
Warfare	Defence White Paper 2016, 2009	
Espionage / Counter-espionage	Defence White Paper 2016, 2009 ASIO Report to Parliament 2011 / 2 ASIO Strategic Plan 2013-16	
Combating theft	National Cyber Crime Strategy 2013	
Combating Harassment, Bullying, Stalking, Grooming (crimes)	National Cyber Crime Strategy 2013	

Security Need	Putative Policy / Advice Sources	Education, Research and Training implications
Reputation Damage		▪ Law ▪ Policy ▪ Human Factors
Data Corruption (crime)		
Critical National Systems	National Critical Infrastructure Plan 2015 Defence White Paper 2016	
Privacy	Cyber Security Strategy 2016	
Combating Data Manipulation and Corruption	National Cyber Crime Strategy 2013	

Table 1 Policy impact on education, training research and workforce needs

Although individual academics and universities have in special circumstances supported Federal and State government 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.

After 2001, and until the present time, there was some (now growing) impact in varying universities in Australia who responded by starting small research groups (usually based in IT) or teaching themes in cybersecurity, digital forensics or critical infrastructure disciplines, largely self-defined, and funded by small contracts with DSTO, small ARC grants, NSST funds from PMC and other small grants from State and Federal government departments. The National Cyber Security Strategy of 2009 detailed, as a strategic priority, cyber education for the nation and 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 in fact been achieved.

The Research Network for Safeguarding Australia was formed around 2005 and did have some focus in cyber or information security spearheaded largely by QUT. There have also been six attempts to get a Co-operative Research Centre in Cybersecurity funded but these have so far failed, possibly through the fact that the technical foci have not always been totally aligned with needs expressed through policy.

The 2017 Australian Academic Centres of Cyber Security Excellence (ACCSE) program has energised academia to take part in Australia's $230 million Cyber Security Strategy. The Government has committed $1.9 million over four years (2016-2017 to 2019 2020) for the establishment of ACCSE in Australian universities to address the nation's critical shortage of skilled cyber security professionals. The centres it is claimed "will help build Australia's capability in cyber security ... increase the number of highly skilled post-graduates ... provide workforce training … provide support for research".

4 ALIGNING CYBERSECURITY FOR ACADEMIA AND CYBERSECURITY FOR INDUSTRY AND NATIONAL SECURITY

There are at least two agendas at play when academics and industry and policy makers come together and consider the issue of cybersecurity. Nationally speaking, Australia needs, and has needed since at least 2001, a cohort of extremely qualified people – qualified from TAFE diploma to PhD level – to plan, design, implement cybersecurity solutions, policies, laws, advice and ethics in a range of domains from engineering, through computer science and network engineering, to law, psychology and political science.

There has been a consistent lack of agreement on the nature of cybersecurity and academics have, and still largely do, focus on the mathematics of verifiable solutions, cryptography, formal methods and machine learning. It has thus largely been the academic publishers, or the US bodies such as the Association for Computing Machinery / Institution of Electrical and Electronic Engineers (ACM / IEEE) or the Association for Information Systems (AIS) who have determined the Australian cybersecurity curriculum since it is the only Computing largely accepted curriculum nowadays that gives.

In fact, Australia is well-known, and at times has been deemed a lead, because of its well-established research, especially pre 2000, in these fields. But, as time and government policy has moved on, these older academics (and there are very few in total in Australia anyway in this discipline) have often chosen to stay in their niche fundable fields and not produce among their students and junior researchers, the new bodies of knowledge needed to respond to modern cybersecurity, cyber defence and cyber warfare challenges. (This is a generalisation and there are notable passionate exceptions too).

Some academics have consistently addressed the issue of Australian information assurance (an earlier focus) or cybersecurity curricula and the issues with aligning learning outcomes with the workforce needs of government and industry. Some options are listed below in Table 2:

Slay (traditional ACS) - requires high level mathematics and scientific background	Hutchinson -postgraduate curriculum that included technical and social science content	Slay - curricula built on the ISC2 certification Body of Knowledge
▪ Historical Background ▪ Societal, Governmental and Legal Imperatives for Information Systems Security and Privacy ▪ Professional Responsibility and Information Systems Security ▪ Computer Security ▪ Access control, Authentication, Integrity, Confidentiality ▪ Security Technologies ▪ Network Security ▪ Trusted Systems and Networks	▪ Database Security ▪ Computer Security ▪ Physical Security ▪ Fundamentals of Cyber-crime ▪ Media and Advertising) ▪ Media and Nation ▪ Media and Social Issues ▪ Ethics, Values and Moral Decision Making ▪ Current Issues in Security	▪ Access Control ▪ Telecommunications and Network Security ▪ Information Security Governance and Risk Management ▪ Software Development Security. ▪ Cryptography ▪ Security Architecture and Design ▪ Operations Security ▪ Legal, Regulations, Investigations and Compliance

Slay (traditional ACS) - requires high level mathematics and scientific background	Hutchinson -postgraduate curriculum that included technical and social science content	Slay - curricula built on the ISC2 certification Body of Knowledge
▪ Concepts of security functionality and enforcement / verification ▪ Verification techniques and software engineering ▪ Security in the Distributed Systems (Client / Server) and Object Oriented Environments ▪ Security and Specific Industry Requirements ▪ Security Management	▪ Advanced Security Risk Management ▪ Advances in Security Technology	▪ Physical (Environmental) Security ▪ Law ▪ Social Science ▪ Socio-political issues (privacy, encryption, surveillance), Activism, Hacktivism, Cyberterrorism and Cyber warfare, Socio-psychological impacts of computing ▪ Fundamentals of Cyber-crime ▪ Ethics, Values and Moral Decision Making ▪ Advanced Security Risk Management

Table 2 Some Suggested Australian curricula

Slay's logic in developing curricula around the ISC2 Body of Knowledge is that this certification has 100,000 holders internationally and has been used as a criterion by the Department of Immigration and Border Protection Sponsored Occupations list. From a research perspective, most Australian research groups have continued to carry out research aligned with that of the small numbers of professors in the field. There is some good work in Cryptography, Network Security, Digital Forensics, Critical Infrastructure Protection, Cyber Norms and Ethics, Criminology, Social Impact – some of these are deliberately aligned with a national agenda but much work is driven by the professor or group and their personal interests. While various PMs have suggested Australia will or needs to have Centres of Excellence in Cyber Security, this has not eventuated so far.

5 COMPARING AUSTRALIA AND SELECTED PEERS

As was indicated above, the US and the UK are both advanced in their approaches to Cybersecurity issues. China has also accelerated its approach to this topic.

US	UK	China
The National Initiative for Cybersecurity Education (NICE) 2009 is a nationally-coordinated effort comprising over 20 Federal departments and agencies, academia, and industry. ▪ to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources ▪ extends beyond the Federal workplace to include private industry, those changing careers, and students in kindergarten through post-graduate school.	Cybersecurity Strategy 2011 Much of this Strategy has been implemented	By the end of 2010, the Ministry of Education granted 64 universities permission to set up InfoSec program. The Ministry of Education InfoSec Higher Education Committee is the prime organisation overseeing InfoSec educational programs. (Chen 2013)

US	UK	China
KNOWLEDGE		
1. The Department of Homeland Security (DHS) and The National Security Agency (NSA) jointly sponsor the National Centers of Academic Excellence (CAE) program, designating specific 2- and 4-year colleges and universities as CAEs in Cyber Defense (CD). 2. Offers degrees in approx. 20 disciplines 3. Cybersecurity scholarships for service and internships	1. Improve our ability to anticipate the technological, procedural and societal behaviour developments that affect our use of cyberspace. 2. Expand our understanding of the threats and vulnerabilities in cyberspace that affect the UK. 3. By March 2012, conduct research on how to improve educational involvement with cyber security significantly at all levels – including	1. Chinese Information Security curricula focused on learning the technology, while curricula in the United States focused on supporting business with Information Security 2. The faculty teaching Information Security programs had academic backgrounds in Telecommunication Engineering, Computer Science, and Mathematics in China, 3. One of the most overriding drivers of differences between InfoSec

US	UK	China
	higher education and postgraduate level.	programmes in China and the USA is that the influence of the government in China is more pronounced, with the Ministry of Education specifying curriculum causing programs to contain many core courses, especially from technical areas. Subsequently students are limited in their elective choices. Chinese InfoSec programs are regarded as an interdisciplinary and applied science of technology on Mathematics (Cryptography), Telecommunication, and Computer Science (Shen et al., 2007).

US	UK	China
SKILLS		
1. The NICE Workforce Framework is the blueprint to categorize, organize, and describe cybersecurity work. The Workforce Framework was developed in partnership with the National Initiative for Cybersecurity Education (NICE) and Department of Homeland Security (DHS) to provide educators, students, employers, employees, training providers, and policy makers with a systematic and consistent way to organize the way we think and talk	1. Improve levels of professionalism in information assurance and cyber defence across the public and private sector. Establishing a scheme for certifying the competence of information assurance and cyber security professionals by March 2012, and a scheme for certifying specialist training in 2012. Continuing to support the Cyber Security Challenge as a way of bringing new talent into the profession.	Ten most important skills required by industry (Chen 2013) 1. Enterprise-wide Information Security Risk Assessment and Mitigation 2. Enterprise Security Policies Development 3. Security Events and Incidents Detection and Response (Network and Systems)

US	UK	China
about cybersecurity work, and understand what is required of the cybersecurity workforce. 2. 2000 course listed and available to gain skills 3. Free online training	2. Put in place clear leadership of cyber across Government, with a dedicated minister and oversight at the highest levels of Government.	4. Web Application Vulnerability Scanning and Resolving 5. Security System Proposal Development 6. Security Log Management and Monitoring 7. Servers and Systems Operations and Maintenance 8. Antivirus Analysis and Prevention 9. Enterprise Encryption Standards Development and Support Access Control

US	UK	China
CAPABILITY		
1. To further advance the cybersecurity field and create the next generation of able and willing cybersecurity professionals, the government aims to recommend national-level standards for the cybersecurity field through Curriculum Evidence Standards. 2. Provides the Workforce Framework – the blueprint to categorize, organize, and describe cybersecurity work.	1. Support the application of research, working with the Government Office for Science and others to build innovative cyber security solutions, building on our world-leading technical capabilities in support of our national security interests and wider economic prosperity. 2. Manage crucial skills and helping to develop a community of 'ethical	▪ High level of skills cf. to Australia among law enforcement including reverse engineering of malware capability

US	UK	China
	hackers' in the UK to ensure that our networks are robustly protected. 3. Enhance the world-class technical skills of GCHQ.	
RESEARCH		
1. National Industry / Government Centre of excellence 2. NSA has designated some universities as National Centers of Academic Excellence in Information Assurance Research, and Intelligence Community has "Center of	1. Identify Centres of Excellence in cyber research to locate existing strengths and providing focused investment to address gaps. First focused investment by March 2012.	▪ Newly founded Cyber Security Association of China – industry and academia – to protect China's cyber security ▪ Premier requires more collaboration

US	UK	China
Academic Excellence" designated by the Department of Homeland Security.	2. Now has 13 Centres of Excellence and 2 Centres of Excellence in HD Research	

6 POTENTIAL RESEARCH AND EDUCATION MODELS

In summarising the models and frameworks of our allies and a large power, China, in the AP region, we note:

- Each has an implementation plan which allows policy to be translated into action
- Each has input from industry as major sponsors of activity as well as large amounts of government funding
- Each government has supplied and continues to supply strong leadership from the top down

Each of the countries examined here has to some extent a similar model. Government policy is implemented by standardising curriculum, supporting research agendas and regulating it by decree or by the provision of online resources, networks, mentors or both (as can be seen in the US National Centers of Academic Excellence in Information Assurance Research model).

Each year the US National Centres of Excellence meet and excellence (among those already designated excellent) is rewarded. This year, 2016, the UK and US Centres of Excellence will meet together to extend their collaboration. In all three countries, required outcomes are established before a partnership is entered into.

7 CONCLUSION AND RECOMMENDATIONS

As was stated above, PM Turnbull has stated that Australia will become '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.'

Australia has already committed itself to Centres of Cyber Security Excellence. It also needs to:

- Establish undergraduate curricula across a range of disciplines in Cyber Security and use reward to ensure that teaching is carried out to some national established standard
- Establish TAFE curricula at Certificate 1-6 since not all jobs are for graduates
- Establish criteria to determine how such Centres of Excellence will be established and how standards will be set high and relevant and how this will be maintained
- Determine a transition plan so that professionals from a range of specified disciplines can be converted into Cyber Security professionals
- Develop mechanism whereby the industries who need to hire cybersecurity professionals can also contribute to training by supply of scholarships or support to colleges and universities; it is hard to see how the public system can generate enough income to support education and training initiatives alone
- Consider how it can generate the 8000 to 10000 cyber security professionals needed in the next few years. Even including increase by migration, there is an international shortage, and the public TAFE and University system would find it hard to produce more than 1000 maximum per year, especially given the lack of qualified academics in the field
    - Consider a National Cyber Security College to get focus and concentrate expertise
    - Consider developing a private system and sector specific initiatives

Government has recently sought assistance from the Australian Computer Society (ACS) to help establish a framework for identifying cyber expertise given its multi-disciplinary nature. The ACS Cyber Security Taskforce was formed to provide recommendations on the development of Australian Professional Standards and Curriculum in Cyber Security. This is to be achieved by:

- Identifying all job roles and occupations aligned with cyber security.

- Identifying national and international best practice for accreditation and certification within cybersecurity
- Establishing a baseline of knowledge and skills criteria which represents the minimum expectations of cyber security technician and professional
- Providing recommendations of professional assessment techniques for determining whether an individual has the cyber security knowledge and skills to fulfil the identified baseline requirements.
- Providing information and recommendations of the relationship and collaboration between ICT and engineering professionals in secure ICT systems.
- Ensuring recommendations are aligned with international best practice and comply with appropriate national and international cyber security professional and technical standards.

Existing frameworks informing consideration of the taskforce are:

- The United States Department of Defense Information Assurance Workforce Improvement Program
- National Institute of Standards and Technology, US Department of Commerce
- National Initiative for Cyber Security Education, Workforce Framework
- US Department of Labor sponsored industry Cybersecurity Competency Model
- ACM Joint Task Force on Cybersecurity Education

It is yet to be seen the impact that this work may have on the Australian National Agenda.

REFERENCE

[1] Chen, H.Y., Maynard, S.B and Ahmad, A., 2013, 'A Comparison of Information Security Curricula in China and the USA', Proceedings of the 11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013, accessed at http://ro.ecu.edu.au/ism/153, May 29th 2016.

[2] Parliament Briefing Book 44th Parliament: Cyber, 2013, accessed at http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber May 29th 2016.

[3] Robinson, M., Jones, K., and Janicke, H., 2015, *Cyber warfare: Issues and challenges, Computers & Security*, Volume 49, March 2015, pp 70–94.

[4] Shen, C., Zhang, H., Feng, D., Cao, Z., & Huang, J. (2007). Survey of information security. Science in China Series F: *Information Sciences*, 50(3), 273-298.