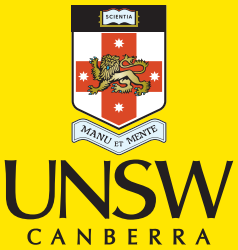

UNSW
CANBERRA

ACCS Briefing Paper #2

Human Capital for Cyber Security: The Australian Case

Greg Austin

November 2017

UNSW AUSTRALIA

Australian Centre for Cyber Security
UNSW Canberra

HUMAN CAPITAL FOR CYBER SECURITY:

THE AUSTRALIAN CASE

ACCS Briefing Paper No. 2

Greg Austin

Australian Centre for Cyber Security
University of New South Wales Canberra
23 November 2017

Introduction

On the 100th anniversary of the Battle of Beersheba, Australia's Minister for Veterans' Affairs, Dan Tehan, joined the Prime Minister, Malcolm Turnbull, in a commemorative visit to Israel. Tehan, who is concurrently Assistant Minister to the PM for Cyber Security, used the opportunity and most of his time in Israel to also lead a delegation from industry, government, and academia to stimulate closer ties between the two countries in the realm of cyber security. To that end, Israel and Australia agreed to a communique, committing them to concrete bilateral measures in the field. There is considerable potential. For this author who participated in the visit, one of the most educational parts of the visit was to learn about Israel's policies for human capital formation for security in cyber space. Israel has both a policy and concrete national level actions to advance its agenda for national cyber security education.

In contrast, as I noted in a recent publication for the Committee for the Economic Development of Australia, many of our government's new commitments to education in its landmark Cyber Security Strategy of 2016 were fairly generalized, lacking granularity and far from concrete.[1] These included an intention to increase numbers for cyber security graduates, women in the profession, and school students "in the know". The first annual review in April 2017 showed little progress on the education objectives, which are after all the foundation for any enduring change in all other areas of policy. In the medium term, we will need the government to provide some metrics on how many graduates in the field, and its various sub-fields, we actually need. We also need to see the baseline statistics for any future growth. In 2017, the government announced very modest funding to two Australian universities to promote cyber security education ($1.9 million over four years) and a more generous funding ($50 million over seven years) for a cooperative research centre (CRC) in protection of national critical infrastructure in cyber space. These are easy measures to announce and fund, but much harder to test and evaluate for their contribution to the national needs. For example, the CRC is primarily a research vehicle. While it will have useful and important flow-on effects in formal university courses, that will be a slow and accidental process.

Australia has some way to travel yet before it graduates to a coherent national cyber security strategy, fully informed by global realities and funded accordingly. Australia does not yet have a national strategy for developing a sovereign cyber security knowledge economy that can sustain the war-fighting needs of the country in cyber space. This discussion paper, containing two brief notes, has been prepared as a background resource for an international workshop on cyber security education at the University of New South Wales Canberra on 27 and 28 November 2017.

---

[1] Greg Austin, "Are Australia's responses to cyber security adequate?", *Australia's Place in the World*, Committee for Economic Development of Australia (CEDA), November 2017, pp. 57-58. This material is used with permission from CEDA.

Contents

PART 1: An Educational Maturity Model for Australia

It would be great if the challenges of cyber security education, digital literacy promotion and workforce development could be easily bounded and managed by a single government agency or peak professional body in the sector. The challenges cannot be so bounded. Security in in the information age and the teaching of it are as unbounded a set problems, and as multi-dimensional, as we can find elsewhere in social policy short of problems like ending poverty. The essential problem is that *laissez-faire* ("permissiveness") is the guiding principle in business, in all non-government scientific research, and in tertiary sector education practices. The United States, which is the most wealthy country in the world and the largest cyber power, has failed to meet the cyber security education needs it has set itself. Even authoritarian governments, such as Russia and China, have been unable to mobilise adequate cyber security education strategies.

For these reasons, a government cyber security education strategy will be most successful where it is directed exclusively at the operational needs of government. It will likely fail if it sets a broader ambition. The government strategy that will have most success in enhancing security in cyber space will be one that aims to provide information technologies that are inherently more secure and much more people-proof than most available today.

The U.S. National Initiative for Cyber Security Education (NICE) makes it plain that the three objectives identified above (cyber security education, digital literacy promotion and workforce development) are very different enterprises. To pursue national education needs declared as foundational in the 2016 Cyber Security Strategy, the Australian government needs to explicitly do the same as NICE has done. It will need to assign separate organisations primary responsibility for each objective. Each task is so massive it cannot possibly be coordinated by a small staff of cyber advisers in the Department of Prime Minister and Cabinet.

For example, the Commonwealth Education and Training Department should take responsibility for the first goal (cyber security education), the Department of Communications and Arts should take responsibility for digital literacy, and the Department of Industry, Innovation and Science should take responsibility for work force development. Each will need to work with a large and diverse body of stakeholders to deliver target outcomes. To achieve such target outcomes, it will need to set them against an agreed framework of benchmarks and baselines.

For ease of reference, the three objectives can be referred to as the "cyber security formation triad". "Formation" is a term that has fallen out of common use in this sense, but it is the only available English word that cuts across the three distinct goals. Most importantly, it can be seen in academic literature on cyber security education because in this field, informal education and post-tertiary training are such important parts of learning. Another key concept that is often used is that of "knowledge, skills and abilities" or KSA.

In a 2011 article, several researchers in the field of cyber security education captured the dilemma facing governments around the world in the title of their article: "The Ephemeral Legion: Producing an Expert Cyber Security Work Force from Thin Air" (Locasto et al 2011). Within, they highlighted constraints associated with various programs in the United States, such as an Academic

Centres of Excellence network. The authors made a series of complementary recommendations to try to promote more rapid development of education in the field. One of their recommendations concerned the need to massively expand investment in related educational technologies and research into those educational technologies. And this was in the leading cyber power and the wealthiest country in the world. It raises the question for Australia of its preparedness to expand investment in technologies relevant to cyber security education and research into the educational uses of such technology.

Yet other researchers note fundamental weaknesses even in the very conceptualisation of cyber security education. Schneider (2013) suggested that change is needed on all fronts in how universities develop curricula in this field and deliver them. Conklin et al (2014) have warned against any vision of cyber security education that is monochromatic: "The development of a single foundational curriculum that can meet all major requirements is not a possibility for a field as diverse as information security. Information security is a field that has both breadth and complexity."

These considerations in respect of tertiary level programs, sit alongside a myriad of other fundamental curriculum type issues that any country faces in reorienting its educational and vocational training system to adjust to the threats of the cyber age. Some of these are spelled out in ACCS Discussion Paper #4 by Adam Henry.[2]

This short briefing note sets out ten public policy dilemmas, beyond curriculum content issues, which need to be addressed by Australia in 2017 in framing initial leap-frog strategies, new funding levels and execution plans for enhanced cyber security formation.

Dilemma #1: Evidence-Based Policy

In spite of Herculean efforts by a small handful of researchers in the field of cyber security education in Australia (fewer than ten and closer to five), and related efforts by professional peak bodies, such as the Australian Computer Society and the Australian Information Security Association, or the Australian Information Industry Association, we can safely say that there is no sustained, longitudinal or comprehensive research in Australia on the state of the country's cyber security education, development of its digital literacy, or its workforce development. If the country's stakeholders are serious about the challenges, one first step might be to fund a research stream in one or more research or policy institutions that can deliver this on a standing basis. That would not be a low-cost or low complexity exercise. Furthermore, there is large amount of high quality research work on this subject available internationally that needs to be surfaced in public debate and policy formulation in Australia.

[2] Adam Henry, "Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry Requirements", ACCS Discussion Paper #4, University of New South Wales Canberra, 2017. https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdf..

The few Australian scholars working in the field of cyber security education research have not had the luxury of being able to specialize in it, and some of the leading figures of the past decade have left their full-time research roles in academia.

The daunting dimensions of the research problem around just one leg of the triad, that of workforce development, has been illustrated in a report by NICE on best practices in that one area (NICE 2012). The report notes that there are three essential layers in studying the research foundations needed for workforce development: process, strategy and infrastructure. Within each of these three layers, there are identifiable best practices just for the research needed to underpin evidence-based policy. One important approach is to undertake risk assessments around each new education plan based on analysis of suddenly emerging gaps between new needs and existing supply. Another best practice is to use research to identify how "rapid fluctuation" in work force supply of cyber security KSA affect downstream risks in infrastructure, financial stability and the physical environment. According to the NICE report, work force planning needs to be supported by a Human Resources Information System on the cyber security work force (Australia does not have one). Best practice would see this system being used for "easy drill-down into data to understand the impact of organizational changes on cybersecurity workload and better manage fluctuations in need". The approach would depend on "maintaining relevant [analytical] tools, which assist in the cybersecurity workforce planning effort". The report also identified that investing in enabling technology for cyber security work force analysis had proven to be a key differentiator in terms of available infrastructures.

In comparison with the ideal research environment for evidence-based policy on work force development as advocated by the NICE report, the current status of the research environment at the national level in Australia would have to be assessed as highly underdeveloped.

In practical terms, the best policy measure Australia could take is to mandate the immediate establishment under the auspices of the new Cyber Growth Centre of a research team whose only mission is to lay the ground work for the continuous study of the rapid development of the cyber security work force in Australia. This team might ideally be a networked (Australia-wide) team, but there would need to be a core research team newly appointed in a single university with recognized strengths in several essential fields: the multi-disciplinary aspects of cyber security, education policy, labor economics and the innovation economy. Australia has no such researchers at present working full-time on these issues. The first priority would be to establish a Human Resources Information System on the cyber security work force.

Dilemma #2: Education Policy Choice Points beyond the Multiple Curricula

A "curriculum" for post-secondary cyber security education (in universities and TAFEs) (not including cyber security literacy) will have hundreds of sub-components depending on the purpose and level of the various educational offerings. This is addressed in the Henry research project at ACCS referred to above. An overview is available in Slay (2016) and Austin and Slay (2016). In essence, there is not one curriculum but many with diverse curricula.

The curriculum-related issues are only a small slice of the policy dilemmas in "cyber security formation" faced by governments and industry stakeholders. Other very problematic choice points

include how much money to invest in transformation of the education system or public information systems for cyber security? Or indeed, should these be transformed or simply incrementally altered? How many new students should be graduated through revamped programs: double the current number of graduates or four time the current number? Should the spending and number ambitions be focused on vocational training, undergraduate education or graduate education? What institutions are best able to deliver new educational outcomes at the pace and on the scale needed?

Are entirely new educational institutions, such as a National Cyber Security College, needed? Israel's Cyber Security and Information Warfare College, which appears to be a private sector initiative, is an interesting model.

An even thornier problem is that of drawing the line between government intervention, free market principles, and free society principles, particularly in respect of university choices about curricula, degree structures and student places.

And then, once all of the choices are made by universities and other delivery institutions, how can a single government escape its own cyber immaturity at the national level. If a country has immature cyber security cultures that permeate business and government, not to mention the wider community and even educational institutions. If a nation has only a small cohort of educators in the discipline, it will inevitably stall in any effort to bring about a significant increase in indigenous cyber security workforce numbers who are better trained than the existing workforce. What level of investment must Australia make in new cyber security educational and teaching roles? To achieve double the number of graduates in cyber security, the investment may be needed more in technologies or teaching support than new teaching posts, since many existing courses are under-subscribed.

Dilemma #3: Measuring Maturity in Education Systems for Cyber Security

Thus, just as the concept of cyber security maturity is widely accepted internationally, we also need a concept of and models for maturity in cyber security education and training (=formation).

There are two basic approaches that spring to mind. One is to create a baseline, matching existing knowledge sets to numbers enrolled and to see maturity in reaching new levels on these types of indicators. But this approach will come up against the very large number of sub-fields and specialisations, not to mention skill levels. Moreover, in most countries, such data is not readily available and most governments will never be able to afford to collect it.

The other immediately obvious approach is to compare existing and planned sets of skills and numbers relative to the types of threats a country faces. If we take the case of Australia, we know that the government, businesses and educational institutions see the current maturity level of cyber security education as inadequate relative to the types of threats. What we don't know is whether these actors view the maturity level as almost satisfactory or desperately weak. From the various surveys available in Australia and related research, one could make a case for an interpretation that the level of maturity in the country's cyber security education, especially in terms of throughput of potential workers, is–relative to the scale and scope of threats–weak to very weak.

This assessment is quickly borne out by reference to a more detailed analysis of existing educational and training offerings relative to national needs. If we make the mistake of seeing these needs in aggregate terms (that is a "cyber security workforce"), then that argument might be challenged. On the other hand, if we take the essential step of breaking down the needs even into top tier sub-components, such as countering cyber crime, fighting cyber war, protecting critical infrastructure, providing online safety for children and the elderly, countering fake news, and ensuring privacy, we can quickly see that there are NO university degrees in the country, and little training activity in professional settings, that prepare students for these sub-disciplines with any depth (except perhaps for specialised training in the country's leading security intelligence agencies).

Even within each of these sub-fields, there are unique problem sets of cyber security which need specialized education and training.

Everything mentioned above is true of technical aspects of cyber security education and training such as: software, hardware, wireless, mobile, payload or network considerations. When we include issues of human computer interaction, personnel security, systems management, enterprise compliance, identity and privileges management, legislation, or the many additional policy elements of the country's information security ecosystem, the level of maturity of the education and training in cyber security is even lower than that of the technical aspects.

Dilemma #4: Resilience and Dependency–The Missing Link in Education and Training

There is yet another level of complexity. There is no university in Australia that prepares graduates for the problem-solving associated with complex questions of system resilience at the national level in cyber space, even though resilience is the main practical goal of all cyber security practice. Since 2009, the U.S. Department of Homeland Security has identified the assurance of resilience as an integral component of cyber security practice (DHS 2009). By way of example, one of the ten principles of cyber security and resilience advocated by DHS is management of external cyber dependencies. There is almost zero specialisation on this topic (cyber resilience and dependency) in Australian educational institutions, a characteristic shared with the tertiary sector in most countries and even in the United States. The main focal points for work on this subject, at least in the English-speaking world, are the Idaho National Laboratory (INL) and the Argonne Laboratory.

Dilemma #5: Immigration and Off-shore Work Forces

If we shift to the question of the balance to be struck between producing a work force through provision of education and training to home-grown students, versus sponsored immigration of foreign nationals already having the knowledge and skills, the picture becomes somewhat more complex. Several questions arise.

How does Australia assess the skills gaps appropriate to the immigration pathways? At present, there is a general provision identifying workers with skills in information and communications technology as a category for special treatment. This does not really reflect the occupational diversity outlined above. The ANZ Standard Classification of Occupational Codes at least lists

ICT Security Specialist as one of 15 occupations, alongside ICT Sales Assistant, ICT Business Manager, and ICT Systems Test Engineer.

In a 2014 submission, the Australian Information Industry Association made a suggestion to review 457 visas, highlighting seven points requiring fresh policy scrutiny:

1. Compliance
2. Regulatory requirements
3. Intra-company transfers
4. English language skills requirements
5. Training benchmarks
6. Market salary rates
7. Labour market testing

While it is broadly accepted by most parties in Australia that there is a need for immigration by ICT security specialists, several points stand out for the AIIA submission. The first is that it reports "the absence of specific data to demonstrate non-compliance by the ICT industry" of the various tests imposed by the 457 visa process. There has been no public domain analysis conducted by anyone of the information security work force brought to Australia under the 457 program, much less a study of how the structure of that work force relates to the evolution of Australia's capabilities and throughput (graduation rates) for cyber security education and training. There has been no study available in the public domain of comparative salary levels for peer appointments of Australians (citizens or permanent residents) and immigrants. It is of some note that the AIIA submission suggests that Australian workers can be more expensive than non-Australian in peer posts because of accumulated annual wage rises of the Australians who stay in the same job for a number of years.

Most importantly, especially for large enterprises who have advocated the need for intra-company transfers to Australia, there is no strong sense in public debates of why some or many posts/roles cannot be adjusted to be executed remotely (online) from outside Australia.

Dilemma #6: Cost Transfer of Training from the Private Sector to the Public Sector

It is not unreasonable to ask questions about the private sector's long term plan for developing public goods in structured development programs to promote cyber security education and training. It is a common practice in the private sector in many fields to complain of government inactivity or non-performance when there is a shortage of skills in a workforce, rather than take on what may well be the private sector's responsibility. There is no national consensus in Australia on where the division of responsibility lies, except in those professions traditionally regulated by peak bodies such as medicine, law, accountancy and engineering. In the cyber security sector, we need to be alter to the proposition that private businesses are shifting the blame for their own lack of investment in and engagement with universities and other education providers on to an overly sympathetic and overly interventionist government.

Dilemma #7: Online Education and Training: International and Domestic

Apart from certain sovereign defence and security needs, there are almost no education and training needs for the Australian cyber security sector that cannot currently be met, provided the price is right, by non-Australian providers. This includes a diverse list of countries such as the United States, the United Kingdom, France, Israel, India, Russia and China. Much of this education and training can be provided online (albeit outside Australian working hours), and much of it is already being delivered in Australia. A mature cyber security formation policy in Australia would set priorities for where Australia needs to develop its own sovereign education and training capabilities. This could and should include: defence, foreign affairs, security agencies and the police. The highest priority mission sets for the highest level of sovereign capability for education and training include: cyber warfare, cyber espionage, cyber crime and critical infrastructure protection. This is where the Australian government must continue to spend the bulk of its money and planning effort in cyber security formation, but it probably needs a ten-fold increase in funding, specifically, for education and training in the field. We currently have only partial baselines for what the government is spending.

Dilemma #8: Disruptive Technologies

There is a marked difference between developing long-term education strategies for core skills in content-stable subjects (relatively speaking) like languages, physics, chemistry and mathematics, compared with understanding education needs in content-dynamic subjects like contemporary politics, Islamic State terrorism, estimating global warming impacts of current C02 emissions, or cyber security. Opinions will differ about just how dynamic the content of cyber security education will be. It could be noted however that the Idaho National Laboratory sets a two-year time horizon on the likely beneficial outcomes of its research on resilience critical national infrastructure in cyber space. This points us to policy settings that favour practical or on-the-job education strategies rather than those seated in slow-moving institutional frameworks. The primary locus of the best long term cyber security education that takes account of the content-dynamic character of cyber security education needs may well be a new form of "cyber defence workshops" or what some in the United States are developing in the form of continuous cyber labs, where students have 24/7 access to live simulations and actual cyber events.

Dilemma #9: Formal Knowledge and Education versus Self-Taught Informal Knowledge

There may be few fields of modern education where the knowledge skills and abilities (KSA) of practitioners and theorists can be acquired as much by self-taught processes as in cyber security. We would probably all trust many committed hackers without formal education to know what he/she is doing in defence of an IT system more than we would trust a "doctor" lacking formal training to advise on medical interventions in a human being. The emergence of cyber space has been accompanied by a surge in the ability of people to become self-taught. This clearly has dangers as well as benefits. In practical terms, this risk is not handed well by most institutions since few have the ability to certify how much the KSA of individual cyber security operators is derived from formal education (and is therefore testable and hopefully reliable) and how much is derived from self-taught (often "seat of the pants") sources. A national education system for cyber

security must provide a mechanism which understands both the strengths and weakness of the self-taught pathways and how these can be understood and managed.

Dilemma #10: Critical thinking and Personal Resilience as the Core Abilities

Knowledge and skills for cyber security are tough enough challenges for formal cyber security education. What are the unique challenges of formal education for developing graduate attributes for the "A" in KSA: the "abilities"? This concept refers to a student's demonstrated capacity to achieve certain practical outcomes in a measurable or observable way when challenged with a concrete problem or scenario. In cyber security, there are two key aptitudes (not abilities) which need to be developed through formal education. These are critical thinking, and personal resilience. Education for cyber security is more akin to education for other high pressure operational environments, such as surgery or for counter-terrorism operations, than it is akin to education for mathematics or science, which are more passive undertakings and which involve the student mainly as observer or analyst and not as an actor. Assuming that tertiary level studies in cyber security should be expected to meet the "A" requirement in this spirit, modes of "study" do need to be adjusted to include mandatory learning and testing in cyber security operations akin to one year practicums for architecture or medicine degrees.

Recommendations

1. Australian policy makers in government and industry would benefit from articulating separate strategies for each leg of the "cyber security formation" triad: education, cyber security literacy, and work force development.
2. Australian policy makers in government and industry would benefit from a critical evaluation of their cyber security education strategies against each of the ten dilemmas flagged briefly in this note.
3. The massive constraints suggested by the ten dilemmas outlined above suggest that scarce government resources might be best directed to very narrow and high priority needs at an advanced level, such as countering cyber crime or critical infrastructure protection, rather than to the ambition of providing general education for entry level cyber-security operations since these can be met in a variety of ways (migration or remote working) that do not depend on substantial new investment in domestic cyber security education programs. An investment on clear high priority needs will create good trickle down effect but these cannot be planned.
4. Government and public sector investments in expanded cyber security education will be wasted and will continue to lack credibility without the establishment of a university-based centre of excellence in "research and evaluation of cyber security education and training in Australia". Such a centre might usefully be seated in an Education faculty, not an engineering or IT school, or cyber security centre. This could be achieved at a relatively low cost, not exceeding $1.5 million per year if supplemented by industry investments and research grants. This is a very different exercise from a system of recognising centres of excellence in different aspects of cyber security. It would need to be funded outside the system of grants administered by the Australian Research Council. It might ideally be a standing allocation from the Department of Defence or the Attorney General's Department, or a joint program supported by both, to reflect the high priority national security focus of this effort.

5. The complexity of the ten dilemmas outlined above speak to the need for a highly focused special program of cyber security education aimed at supporting the creation and sustainment of a Cyber Civil Reserve Corps of some kind rather than spreading new investments too thinly.

PART 2: STRATEGIC MILITARY EDUCATION PRIORITIES FOR CYBERSPACE

This short note[3] recommends that the ADF move to position ADFA better to maximize its education and training outcomes to reflect the revolution in military affairs that has occurred in the past two decades. There are related areas for improvement in the technologies of education delivery. Key military allies, partners or countries of military interest to Australia have made or are beginning to make massive transformations in the curricula and delivery technologies at peer institutions overseas.

Cyber security for national military defence is a very different phenomenon from cyber security for the defence of enterprises and individual citizens (the civil sector).[4] The Australian government has staked much on development of civil sector cyber security capabilities, through industry promotion and development of a much needed national skills base. In stark contrast, the needs for military defence and national security in cyber space can only be met by a sovereign", non-globalised knowledge economy open to the outside only through our closest intelligence allies in the "five eyes" community (the United States, United Kingdom, Canada, New Zealand, and Australia). Australia can and should compete in niche areas in the globalised civil sector economy of cyber security, but it will be the developments in areas of sovereign capability that will provide a quantum leap to our capability in the civil sector. This is a key lesson from the political economy of cyber security in Israel and, to a lesser extent, in Taiwan.

The government and its military leaders might consider articulating a comprehensive set of policies around the following benchmarks that will have important beneficial flow-on effects for the national economy:

- A national innovation strategy that keeps the country at the forefront of international best practice in cyber technologies that can be applied in war
- A military strategy for cyber-enabled warfare that takes account of the proven and estimated character of such an armed conflict, including public intelligence assessments of likely cyber war threats, forecasts of future technologies and a top-end (but credible) scenario for complex cyber-enabled warfare
- A strategy for sovereign cyber war capability and cyber survivability in a time of direct military confrontation with a major power
- A capital procurement program centred on advanced cyber-enabled war capabilities, including space-based assets and new technologies of decision-making
- A renovation of military institutions, training and education for cyber warfare
- Necessary investments in niche technologies and research capabilities
- A strategy for managing civilian-military divides and critical infrastructure protection in times of military conflict

---

[3] Some of this material has been previously published in Greg Austin, "Australia Rearmed", ACCS Discussion Paper #1, January 2016.

[4] This paragraph and following ones were previously published by the author in Austin, "Are Australia's responses to cyber security adequate?", and is reproduced here with the permission of the publishers.

- A strategy for mobilizing cyber-capable reservists or civilians in times of military crisis
- A sharp distinction between the national needs for cyber security as largely a civil domain set of issues and the needs for cyber-enabled war fighting capability.

Above all else, Australia needs to build a community of interest around the concept of cyber-enabled warfare with a recognised authoritative hub that can unite political, military, diplomatic, business, scientific and technical interests and expertise.

Such changes, long delayed, are becoming more urgent. We are now seeing an intensifying frequency of cyber attacks that sit somewhere on a blurred boundary between peacetime sabotage and political subversion on the one hand and, on the other, acts of war. We need only cite Russian political hacking in the United States, that Senator John McCain and other members of Congress described as an "act of war", and authoritative press reports that the United States has sabotaged North Korean ballistic missile tests by cyber attacks. The claims follow public U.S. admissions that its military capabilities include cyber sabotage of ballistic missiles in pre-launch and post-launch phase.

UNSW Canberra is moving in this direction, most visibly through the establishment of centres for research and teaching in cyber and outer space, with corresponding initial adjustments in formal curricula. ADFA will include new cyber training options in its military training programs, including courses on cyber leadership and cyber warfare and strategy. Yet there appear to be a set of challenges in play in the education and training policy of the armed forces of other countries that require more systemic responses. Australia as a whole in the civil sector (including education policy) is lagging in its response to the information and communications revolution. The leaders of Australia's main political parties, including the Prime Minister, have identified this area of policy as high priority for action by them. This short paper focusses on military education about--and in--the cyber domain, both in civil and military affairs. It recommends several short-term and medium-term actions for the ADF.

Need for Review and Response

A revolution in military affairs has occurred over the past three decades. It would seem to follow that institutions of military education and training should have reflected that change in terms of curriculum content. This is particularly evident in the cyber domain. It is both a man-made field of warfare that cuts across traditional domains of air, land, sea and outer space; as well as the critical foundation of all of our civil prosperity, especially the financial services sector, medical services, civil aviation, and internal security.

As over-arching as the cyber domain may be, there are other areas of military education affected by rapid technological advance. On the one hand, military uses of outer space (including for army and navy operations) are absolutely essential for modern combat. On the other hand, albeit in a very different way, new delivery modes built on the most advanced information and communications technologies can deliver new economies and richer outcomes. Simulation has been revolutionized beyond platform control (such as cockpit training) to battle space management in multi-theatre environments at the strategic level of warfare.

Several submissions to the Defence White Paper have argued in particular for closer attention to the revolutionary impact of information warfare on our military planning, which must include our military education and training. One of these submissions prepared by a researcher at UNSW Canberra, argued that Australia is not only lagging in the cyber domain but has actually slipped in international comparisons on the past 15 years. Subsequently, the leaders of Australia's two main political parties have identified this area of policy in the civil sector as a high priority for action.

It would appear to be timely to reflect on and redress if necessary any mismatch between existing military education priorities in ADFA, including delivery modes, and the future operational needs of the ADF.

While military education is part of a career-long process, complemented with professional and specialist training well after the undergraduate experience, the question for ADFA's future direction is whether the current approach toward undergraduate curricula (and delivery modes) equips graduating officer cadets with the knowledge and learning environment that corresponds closely to the likely future needs of junior officers in the ADF. This is especially important given the average gap of ten-years between commissioning and junior staff college.

At the same time, the ADF has moved to decisively position ADFA and UNSW Canberra with a role in education and training for other target groups (postgraduate education for ADF personnel and training for Canberra-based staff). UNSW now provides:

- A compulsory undergraduate course in cyber security for all cadets and midshipmen (new in 2015)
- Five Master's degrees in cyber security, its management and strategic considerations
- Ph D options in cyber security, including a Professional Doctorate
- Short, non-credit courses for professional development and military education options in cyber security, including training in red/blue exercises (new in 2015).

It should be noted that the Australian Centre for Cyber Security, established at UNSW in 2014, adopts the international standard approach to cyber security which includes a range of human, political, ethical and legal issues as well as narrow technical issues. It also undertakes study of information warfare, as well as the impacts on strategies and planning of the cyber age.

The potential to accelerate this shift in UNSW and ADFA through their provision of online education and training, including for forces deployed overseas in peacekeeping roles, is as large as the need is urgent.

In brief, there are at least five converging factors which dictate a re-think:

- Slow rate of change in Australian university curricula over two decades in response to the profound impacts in the civil sector of the ICT revolution
- Slow rate of change in university curricula in response to the equally deep impacts of the accompanying revolution in military affairs
- A general decline in military education opportunities under pressure of repeat combat deployments

- A high-growth defence budget which now provides for the high transformation costs in military force structure (including personnel and military education) in adapting to the revolution in military affairs
- A likely explosion of advanced information capability in peer organizations (military academies) and officer cadet education in three countries that are central to Australia's future security: United States, Japan and China.

Centrality of Information War and Outer Space as Cross-Domain Environments

In 1998, our major ally, the United States, issued its first Joint Force doctrine on information operations (primarily cyber effect operations). Unclassified sources suggest that the first use of cyber effect operations in war occurred in 1999 in the United States air campaign against the former Yugoslavia, with cyber attacks on the control systems for the Belgrade electric grid to suppress ground lighting that might complicate air targeting.

In 2015, China signalled its intention to adopt a new military strategy premised largely on the combination of cyber effect operations and kinetic (physical) attack. The United Nations, in the July 2015 report of a Group of Governmental Experts, has recognized the growing tendency of a number of countries toward the militarization of cyber space.

The emergence of cyber effect operations and network warfare is however only one feature of the revolution in military affairs that has continued unabated since at least 1990. The idea of cyber-enabled war has evolved on the basis of two other pre-existing technological trends, notably the application of advanced computing technologies to create precision strike weapons (and their delivery platforms) and the development of computer-dependent, space-based systems of command and control, intelligence and reconnaissance.

In May 2015, the Chinese armed forces recognized this in their new military strategy document observing that "Outer space and cyber space have become new commanding heights in strategic competition among all parties". Further deepening the challenges of war-fighting in the future, we see breakthroughs in the development of advanced artificial intelligence, robotic weapons and high performance computing.

The military planning of major powers is now premised on a concept of future war as dependent largely on the combined application of space-based communications and intelligence assets on the one hand, and on the other hand, information dominance in the application of kinetic and non-kinetic forces on land, at sea and in the air. This includes both military and military-related civil domains of the enemy, to undermine that enemy's will to fight.

Consequential Requirements for Military Education at Officer Cadet Level

To quote publicity material on the ADFA website, the current approach to the undergraduate education of ADF officer cadets rests on a marriage between cutting edge leadership training to groom officers of the future for the military environment and "a liberal tertiary undergraduate education" in one of Australia's leading universities. The end result of this approach is that the majority of graduates of ADFA are not exposed in a deep learning environment to the

transformational impacts of emerging new technologies that will shape their career, their families' daily lives, their post-ADF employment, or their success in combat.

The choice to isolate undergraduate officer cadets from military studies has been a deliberate one, but it was premised on several assumptions which might be questioned:

1. That the university curricula in Australia (not just UNSW but other feeder universities) would keep pace with the main knowledge demands of society
2. That university teaching methods would be nimble enough to take up advanced teaching modes, such as computer assisted simulation or globally networked teaching, in many disciplines
3. That we had the luxury of time and money to defer military studies until after graduation
4. That a "liberal" education would somehow be tainted or degraded if it touched closely on military and security affairs.

In contrast with ADFA, Canada's Royal Military College requires all degree programs "to provide a sound, balanced, liberal, scientific and military education". Its Military and Strategic Studies (MSS) degree program "offers students an opportunity to acquire a sound grounding in military history, strategic thought, and international relations, as well as in Canadian government, Politics and Economics, English or French Studies, and Military Psychology and Leadership". Even Engineering degrees require students to take courses in military psychology, military history, military concepts and Canadian politics.

This Canadian example is useful for its willingness to offer an overarching degree in military affairs as one option for its undergraduates. Its technical degrees appear more cognisant of the broad impacts of advanced technologies than most in Australian universities. Yet it does not venture into comprehensive study of the revolution in social, economic, political, and military affairs brought on by advanced computing, including artificial intelligence, and advanced communications, especially those dependent on space-based assets. Few military academies actually do, but the emerging trend is very clear.

The pace is being set by the United States academies. They are already operating quite impressively in the advanced technologies field. Its military academies are deeply engaged in education on the information revolution and its impacts, including on the military cyber domain. Peer institutions in China intend to do more of it, and Japan will almost certainly follow suit. It should be noted that Japan will make this shift more quickly than most because it is a technology-leading country in outer space, cyber security, computer-based simulation, artificial intelligence and high performance computing.

In the field of cyber related studies, the U.S. Military Academy at West Point is the most advanced:

- In 2001, it became the first undergraduate institution the National Security Agency certified as a "Center of Excellence" in Information Assurance Education
- In 2014, it ranked 9th among more than 5,000 tertiary education providers in the United States in terms of quality of education in cyber security

- It regularly wins in the cadet-level inter-service cyber defence competition (in place since 2001)
- Cadet Cyber Enrichment Program offering internships in industry for cadets
- Cyber Leaders Development Program providing up to 800 hours non-academic training for each cadet
- A community outreach program where cadets teach local students cyber security
- Army Cyber Institute (cyber warfare research and teaching, set up in 2014; planned for 75 staff by 2017, funded in excess of $20 million) which involves cadets in its work
- Co-publisher of the journal *Cyber Defense Review* (launched February 2015)
- Cyber Research Centre (in the Electrical Engineering and Computer Science Faculty)
- Host of the first Joint Service Academy Cyber Security Summit in May 2015.

The United States Air Force Academy (USAFA) has extensive cadet-based programs in cyber security, outer space operations and broader challenges of technological and management innovation. Its Center of Innovation offers a possible model for where ADFA might head, in that it combines a range of disciplines pertinent to the broader information revolution in civil affairs or the revolution in military affairs. The U.S. Naval Academy has an undergraduate major in Cyber Operations.

New ADF moves can be benchmarked against the current and prospective situation in the U.S. armed forces, while acknowledging that we must discount for their size, general levels of technology and the country's superior wealth. At the same time, since the United States is our major ally and we place a high priority on interoperability at many levels, in diverse theatres and in high-intensity scenarios, it could be argued that we need to be much closer to their military education priorities than such discounting might suggest. Arguably, ADF officer education and training needs to be as close to the U.S. benchmarks in cyber military affairs as the capability of the Australian Signals Directorate is to the U.S. National Security Agency (which is also its operational Cyber Command).

Recommendations

Short-term

1. The ADF should continue to review with UNSW and ADFA options for early take up of professional development and training through short courses in cyber military operations
2. ADFA should continue to expand its non-formal training and development activities in the cyber military field
3. The ADF should set in train a number of review and planning measures through an omnibus and general agreement at two-star level, backed if necessary by a VCDF directive, that the forces move as quickly as possible to a much higher standard of training and education at the officer cadet level in cyber military affairs benchmarked in large part by standards set by the United States armed forces, especially in the period after commissioning and before junior staff college
4. The ADF could set up promotional mechanisms, such as a CDF prize or special study scholarships, to elevate the importance of cyber military education and training at ADFA.

Medium-term

1. That the ADF work with UNSW towards establishment within a reasonable time period of cross-disciplinary and cross-faculty "Innovation Centre" whose main mission is to enrich the educational offerings of officer cadets through:

    - The provision of undergraduate education options for officer cadets in advanced information and communications technology and military applications on a par, in terms of content and teaching, approach with world's best practice
    - The linking up (and colocation) of existing research capabilities and centres in UNSW Canberra that are involved in cyber security, outer space, artificial intelligence and capability development; and the provision of world-leading, secure capabilities for computer-assisted simulation across a range of disciplines to be based in the Innovation Centre
    - The vigorous development on non-formal education and leadership activities in these areas of study and activity
    - Establishing direct links with peer innovation centres in military academies in the United States and Allied countries
    - The establishment of a steering committee for the Innovation Centre comprising innovation leaders from UNSW, ADF, the U.S. armed forces, and the broader Australian and Allied communities.

APPENDIX A: PROPOSAL FOR A NATIONAL CYBER SECURITY COLLEGE

Mission: to develop and execute professional training for advanced cyber security operations and policy beyond a single business entity where multiple national level stakeholders are involved, with a special emphasis on five mission sets:

- Securing national and regional networks
- Resilience of critical national infrastructure
- Combatting cyber crime
- Defeating cyber espionage
- Supporting military education and training.

Concept: a partnership between academic, business and government focused in the national capital

Proposed Founding Partners:

- Australian Centre for Cyber Security (ACCS) at UNSW Canberra
- [TBC] ACT Business Council
- [TBC] 2-3 leading Australian cyber security service providers
- [TBC] 2-3 selected government agencies

Legal Status: To enable maximum nimbleness in establishment and execution, the College may be constituted as a non-profit entity which delivers its mission (and quality control) through the harmonized channelling of training and education talents in academic, business and government, for courses delivered by (and under the academic leadership of) ACCS at UNSW Canberra.

Business case:

- Very large unmet national needs
- ACCS is the country's leading academic provider of relevant education, training and research for cyber security at the national level "beyond the enterprise"
- ACCS has shown a substantial growth trajectory since being established in 2014, including grants from the U.S. government
- Canberra, as the national capital, provides a concentration of market share and stakeholder interest
- UNSW Canberra has an impressive record of engagement with national security agencies
- UNSW Canberra has high credibility for delivery of public education and training and management of associated processes (including course development and evaluation)
- ACCS is leading a new three-year international research initiative on cyber security education
- ACCS is supervised by an Advisory Committee comprising leading stakeholder representatives or expertise from government and business.

ABOUT ACCS

The Australian Centre for Cyber Security (ACCS) at the University of New South Wales Canberra is two things. First, it is a focal point for 60 scholars from various faculties across UNSW who conduct research work on different aspects of cyber security. Second, it is a unit based in Canberra at the Defence Force Academy that provides both advanced research as well as undergraduate and graduate education on cyber security. ACCS serves as hub for the biggest concentration of research and tertiary education for the study of cyber security in any single university in the Southern hemisphere. A number of ACCS scholars, in areas ranging from information technology and engineering to law and politics, have significant international reputations for their work.

https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/

ACCS Briefing Papers are a short-form and informal publishing vehicle to stimulate new thinking about research directions, specific research questions and or public policy.

Dr Greg Austin is a Professor in the Australian Centre for Cyber Security, where he leads the Research Group on Cyber War and Peace. He also serves as a Professorial Fellow at the East West Institute, where as Vice President from 2006-2011 working from London and Brussels he helped set up and lead its Worldwide Cyber Security Initiative. Greg is a co-chair of the EastWest Institute working group on Measures of Restraint in Cyber Armaments. He has held senior posts in the International Crisis Group and the Foreign Policy Centre (London). Other assignments include service in government, defence intelligence, academia and journalism. Greg is the author of several books on China's strategic policy, including *China's Ocean Frontier* (1998) and his most recent book, *Cyber Policy in China* (Wiley 2014). This book offers the first comprehensive analysis (military, economic and political) of China's leadership responses to the information society. It explores the dilemmas facing Chinese politicians as they try to marry the development of an information economy with old ways of governing their people and conducting international relations. The book concludes that unless China's ruling party adapts more aggressively to the defining realities of power and social organization in the information age, the 'China cyber dream' is unlikely to become a reality. Greg has a Ph D in International Relations and a Master's degree in international law.