[TITLE SLIDE]

From Cyber Skills to Resilient Cyberspace Talent: Advance Australia!

Prepared Text: Professor Greg Austin, ACSC 2018, 12 April 2018

[Slide Two] In 2014, China announced its intention to become a cyber power. In 2016, it announced plans to elevate cyber security as a level one discipline in universities (same level as engineering, medicine, physics, chemistry or law). In 2017, it announced plans to set up a national cyber security vocational college, with a planned throughput of 10,000 new students per year in short courses. China's current shortfall in cyber security positions was estimated at 700,000 in 2016 and is estimated to reach 1.4 million by 2020. On a per capita basis, that shortfall is three time worse than Australia's.

[Slide Three] In the two years since the Australian government announced its Cyber Security Strategy in April 2016, key stakeholders have not agreed a framework for advancing cyber security skills development in a fashion that takes such a daring and ambitious path as China. In Australian universities, cyber security centres are still controlled by engineering or IT departments (with one or two exceptions). And they suffer for it. National policy on cyber education still fails to address many key needs. Surveys have been undertaken, working groups have met, Ministerial roundtables with industry have been held, and reports have been drafted. Some important new measures are underway, not least the agreement to develop a national standardized curriculum for vocational education that was announced in December 2017. Yet the need for a published national audit of cyber needs and capabilities remains unmet after two years.

One critique made in April 2016 of the government's cyber security strategy is that it had no baselines and no evidence base for its ambitions to get more people into cyber security work roles, especially more women. Collectively, in the two years since, the country has produced elements of this evidence base, but it remains fragmented and much of it is not available in the public domain. Moreover, work done to date is not comprehensive across the full range of cyber security skills, especially those that are not narrowly technical. But even at the technical level, there are significant gaps in the results to date.

[SLIDE FOUR] In November 2017, the Department of Prime Minister and Cabinet partnered with the University of New South Wales Canberra to carry forward this cause of developing the evidence base and understanding strategic needs more deeply. Under the rubric of "Realigning Cyber Security Education", we convened a one-day academic conference and a one-day policy workshop. This presentation today is the first public reflection on the contributions and findings of those two days. It is on the basis of this joint undertaking and the positioning of UNSW Canberra on these research-related issues that the presentation today was invited by the organisers. Elements of this presentation will form part of the published proceedings of that two-day investigation, on cyber security education which include research papers from a number of leading scholars, including from Oxford University and the U.S. Army Cyber Institute. The present author, and none of the other participants, are responsible for the conclusions offered today.

The conference revealed a depth of knowledge and commitment among scholars and policy makers (including from industry) that will help resolve the challenges we are addressing today. At the same time, none of the people in the room on either day had a comprehensive picture, and none had specifically addressed in completed research the question for today's session:

how do we measure cyber security skills gaps and how do we fill them based on that evidence base.

Of special note, the former Minister for Cyber Security, Dan Tehan, observed in December 2017 that a number of organisations "have exciting initiatives underway in this space but what we need to do is coordinate our approach and bring it up to a national scale." Tehan is right. We are not there yet.

A Senate Committee Report in 2014 on Australia's innovation system remarked as follows: "Government science, research and innovation measures have … tended to be short term, inadequately funded, and prematurely terminated. Some interventions have lacked a strong evidence base whilst others have operated with limited reporting of outputs and outcomes, and minimal evaluation." A report of the Productivity Commission that was requested by the Treasurer and finalised in December 2016 found that Australia lacked a credible evidence base for evaluating the quality of its school level education across the board. Moreover, it found very little evaluation of programs to between inform the link between school education outcomes and workforce development.

[Slide 5]: Putting this all together in respect of cyber security education, we could make a case that Australia is still operating in the land of the blind in terms of baselines and strategies for national level cyber security education and workforce development. Evaluation and accreditation of curricula is a necessary step, as is certification of skilled immigrants and visa holders. That sort of work is in hand to some degree, but these are just the beginning. They are not only baby steps but they may become meaningless without an evidence base. In preparing the UNSW 2017 conference with PM&C on Realigning Cyber Security Education and in delivering it, we confirmed our initial premise. In Australia, there is not a single university-based scholar devoted primarily to the study of cyber security education methods and policy, beyond basic level issues of cyber security awareness. One of the most important recommendations of the December 2016 Productivity Commission report was to set up a new institution who would take on this evaluation mission for studying Australian school education outcomes, including those related to work force development. This presentation will address what that might mean in the area of cyber security.

Strategic View

In order to set priorities and allocate resources, we have to know what we are measuring for. Is it to fill the gaps that we see most easily or is it to fill the gaps that are the most important? To find what skills gaps are the most important, we need to know what sort of cyber space we want. For a business leader, this might seem easy. Private sector firms usually address skills for my business today and the next two or three years, maybe five to ten, and this is more or less a strategic HR decision. The leaders of large businesses might work outside the business to lobby education providers to develop the right pool of trained people, at least with basic skills that meet the strategic HR needs.

There is another consideration however. The leaders of big business need to make their judgement and commitment based not only on today's perceived HR needs for the future of their own business sectors, but also in terms of the future trends in the entire business ecosystem of cyber space.

[Slide Six] The single most important finding of the joint PM&C/UNSW Canberra conference in November last year was one just mentioned, as was argued by Tom Sear. If we want to secure cyber space in Australia, we have to decide what sort of cyber space we want. That idea may sound overly academic and philosophical, not to mention wildly impractical because we operate in a global infosphere–borderless, ubiquitous, and delivering near instantaneous threat. Australia did not construct this infosphere and that we can only control a small number of behaviors and activities in it.

To its credit, the Australian government went a good part of the way to meeting this foundational requirement in its April 2016 Cyber Security Strategy. It set out, in the words of Prime Minister Malcolm Turnbull, his "Government's philosophy and program". It was designed to meet the "dual challenges of the digital age—advancing and protecting our interests online". The Australian government was very wise to set down its philosophy of cyberspace and professionals engaged in the field of securing cyberspace have an obligation to engage with the philosophical and ethical characteristics of this domain. He went to say that "The maintenance of our security online and the protection of freedom online are not only compatible but reinforce each other. A secure cyberspace provides trust and confidence for individuals, business and the public sector to share ideas, collaborate and innovate".

It should be clear therefore at the outset that a national conversation about cyber security skill sets has to be about skill sets for the security impacts of cyberspace. The latter is a far broader framing than the former.

One of the first challenges in setting national policy in this domain is drawing the boundary between sovereign capability and the global realities, both in specific activities we feel we need to protect or promote for security and those that we are prepared to leave to global market forces or global realities to address. Strangely, this essential organizing concept is absent from the 2016 Cyber Security Strategy, even though it is an issue that preoccupies key officials who were involved in it on an almost daily basis. Australia has not yet formed a clear, explicit view of where it wants to draw the boundaries of its influence in the global infosphere. It has been highly reactive, with new legislation or government arrangements that affect security in cyber space being proposed very six to eight weeks on average in the last several years.

As an aside, one example of this reactive, fragmented and tardy approach to the cyber world writ large was the announcement in early April of an investigation by the Privacy Commissioner into whether Facebook breached the Australian Privacy Act in handling the data of Australians that was harvested and supplied to Cambridge Analytica. But did the Australian Privacy Commissioner really need to wait for the Cambridge Analytica scandal to break between 2014 and 2018 to understand that the Company, presided over a privacy catastrophe waiting to happen. This highly topical cyber security controversy, which first surfaced in 2014, is one that concerns all Australians but which has found only the tiniest of places in national conversations about cyber security skill sets. And this in a situation where Australian law of revealing data privacy breaches has just come into force.

The Australian Financial Review reported on 5 February 2018 on a report form CyberArk that 44 per cent of businesses were not prepared to deal with implementation of this law on its entry onto force. Data breaches are one of the most common forms of cyber insecurity globally and for Australians. It was CyberArk which reported in March 2018 that inertia had set in amongst Australian firms in the face of escalating threats. In 2016, AISA reported survey results that suggest that over 60 per cent of cyber sec teams were not growing or falling. These are

indicators of several dimensions of the cyber security skills gap, that seem to bear out the claim of inertia among employers.

Returning to the main argument, sovereign capability and where to draw the line with a global pools of cyber security talents, the country has not decided. In a briefing paper on Human Capital for Cyber Security which I wrote for the November 2017 Cyber Sec education conference, I observed that there is no evidence base about the balance to be struck between immigration of cyber sec professionals at a variety of levels and the pace at which the country needs to produce home-grown professionals. This situation is complicated by the proposition that cyber sec services can be provided offshore, supported by temporary work visits by key staff. Some of Australia's corporations already rely mainly on offshore companies to provide the highest levels of cyber security.

[SLIDE SEVEN] In a free market society, the guiding principle for managing the labour force has to be that of respecting market forces. But this market is distorted by two regulatory regimes. The first influential regulatory regime is Australia's immigration policy for skilled labour. The 2016 Strategy committed the government to "enhancing the visa system to attract the best and brightest entrepreneurial talent and skills to Australia", but this was only for entrepreneurs under the innovation stream of industry policy and not front line cyber security professionals. There are provisions in immigration policy that open up the specific named opportunity for cyber sec talents, but immigration policy in this field is failing the country badly. In Q3 of 2017, according to government data, Australia granted 40 per cent more visas under the old 457 visa category to cooks, chefs and restaurant/café workers than to electrical engineers and ICT professionals. The absolute numbers for the latter group were of the order of 8,000, meaning that only a fraction of this number were dedicated information security professional. The occupation ceiling for ICT Security Specialist under 189 and 489 category visas was set for FY2017/18 at 2,139. By the end of February 2018, according to a private firm, only 8.9 of the available opportunities were filled.

The second influential regulatory regime is that for universities. These are institutions which structure their formal teaching and staffing in fairly rigid frameworks that have not changed much in half a century (except perhaps for distance learning and new one-year master's degrees by course work). Much has been made of the need for collaboration between the university sector and business in research and development. But even this has developed poorly. Less attention has been paid to industry collaboration in teaching in universities and how this might affect teaching and staffing, including for cyber security. Optus and the Commonwealth Bank have made big investments in teaching at several universities (Macquarie, Latrobe, UNSW) but these efforts have yet to bear significant fruit. When they do, the problem identified by Minister Tehan will still be on the table: how to take these education breakthroughs to a national scale in cyber security.

A reasonably basic picture of the cyber sec skills situation in Australia was provided in April 2017 by AUSTCYBER, in its Cyber Security Sector Competitiveness Plan, and I commend it to you. But in its analysis of the work force and education providers, it has little strategic vision and is superficial in its analysis. It draws largely on survey results and does not appear to have taken account of the complexity of the problem.

[Slide Eight] The main challenge in analyzing work force issues in Australia, as in other countries, has been the departure point: the national cyber security work force. On the one hand, this is such a diverse body of skills and activities that it defies easy generalization and

easy measurement beyond fairly superficial analysis. On the other hand, in terms of the private sector, it is ultimately the market (i.e. the firms themselves) that must decide on and deliver the skill sets they want, through on-the-job training to Australian residents, through reliance on offshore services and workers, or through sponsored immigration of specialists. Universities are not only constrained by antiquated learning structure, but they are essentially laissez faire institutions. When it comes to market forces, their primary considerations are student demand and academic rigour, ahead of any consideration of industry needs.

Most countries are destined to face skills shortages in cyber security for decades to come. China estimates that by 2020, its unmet need for cyber security professionals will be 1.4 million. The only thing that can seriously alter this trajectory is technological change in favour of highly secure computing, as discussed in a paper on this subject by the EastWest Institute in 2014 (Gaycken and Austin).

All of this is to say that the Australian government needs to make strategic choices about its highest priorities in this skills gap. Industry groups and individual firms will remain free to measure what they want and act on it. I wish our business leaders luck in getting educational institutions in the country, among its most conservative, to change their practices in the field of cyber security education (while noting that several universities, mine included, have certainly started down that path). Still, the country has no degree specialising in cyber crime, a challenge estimated in 2016 by the government to cost the country between $1 billion and $17 billion.

Even within the Australian government there will be divergent needs (or mission sets) and some of these require high levels of technical and policy coordination either with state governments or with private sector actors:

- Critical infrastructure protection
- Countering cyber crime
- Combating cyber subversion (information warfare)
- Countering cyber espionage
- Preparing for cyber-enabled war.

But all of these speak directly to the need for sovereign capability, even if some of them can be achieved in part through cooperation with close allies. So Australia's most important cyber skill sets are those available to us through sovereign pathways and those available to us through our close cyber space allies. Have we measured those and how should we measure them? Who should measure them? How should we fix gaps that are identified?

Measuring what counts most and what market forces can't fix

[Slide Nine] The acme of cyber skills is the advanced level or super-expert! Australia has not undertaken any public audit of its high end cyber talents that will be needed for success in the five priority mission sets just listed. There have been a number of tallies of cyber security professionals (aggregated across all expertise levels) in some agencies, but only a handful are visible. At the risk of being tendentious, we can note that in 2016 Australia had only two people qualified as a Cyber Guardian, of which there are now only 42 in the world. While that qualification/certification may seem like a less-than-reliable indicator of a country's top end cyber skills, it does provide anecdotal confirmation that we as a country have not focused

adequately on workforce development of our top end talents for the five top national security mission sets.

While ASD, the Commonwealth Bank, Telstra or the Singapore-owned Optus may rightly point out their satisfaction levels with top-end skills of their workforce, none of those organisations represent more than a fraction of the capabilities needed for the top five mission sets.

For example, in the ACT electricity grid, the absolute foundation of national security decisions-making, can we be confident that the cyber talents are as top end as they need to be for the mission set they face in an extreme emergency. The ACT electricity grid, alongside that of Sydney, would be the highest priority targets for a wide-ranging cyber attack on Australia, in the unlikely event one were to happen. We might note that, at least in 2016, the ACT energy provider was 50 per cent foreign-owned, and of that foreign ownership, the bulk (60 per cent was owned by China, the state). We also need to note that we are buying 12 $5 billion submarines for that unlikely event, so how many teams of cyber guardians should we be buying?

[Slide Ten] The paper published by Adam Henry with UNSW Canberra on Mastering the Cyber Security Skills Crisis, is a globally significant contribution to the analysis of work force needs. He advocates an approach that disaggregates need accosting to five different elements, each with different levels: education type (e.g, school, tertiary, workplace), purpose (mission sets, like the five national security missions mentioned), skill advancement (basic to advanced expert), applictaion/roles (operator, team leader, manager), field of ecuation (technologies, tools, risk planning, business management).

What is particularly noteworthy about this matrix of needs is they only align with Australia's current education and training opportunities quite modestly. Current offerings align best for basic and intermediate skill levels and most poorly for advanced and expert skill levels.

Cyber War College

[Slide Eleven] There is no time today to debate arguments for and against the above analysis. I will need to simply assert that Australia needs a national level "Cyber War College" to remedy its deficit in top-end cyber talents for national security agencies, including the Australian Defence Force, and in state police forces, not to mention other investigatory arms of government. **[REPEAT]**

There is a second compelling need that the country could satisfy in setting up such a college. It would provide a home for the necessary standard setting and evaluations of such training of high end talents. These would be the baselines for evidence-based policy that do not yet exist.

There is a third compelling need that could be satisfied by the proposal. The Cyber War College would provide a home for a nationally networked cyber range that could conduct national level simulations, including state agencies and police, as well as private sector critical infrastructure operators.

[Slide Twelve] Some questions

Why cyber war and not a cyber security college? Classic disciplines of cyber security and professional qualifications only address a fraction of the challenges of cyber space security at an advanced level. Other important disciplinary perspectives and skill sets include psychology, law, economics, politics and even military strategy. Cyber war evokes the highest level requirements, not the lowest common denominator approach implicit in standardized national curricula that have become the main vehicle for policy advance in this field (quite appropriately to meet civil sector private sector needs). Perhaps the middle ground in naming might be "College for National Cyberspace Security".

Subject matter focus? (a) Complex cyber operations involving multi-vector, multi-theatre, multi-wave sustained cyber attacks of the sort likely to be seen in major war or in a major political crisis. Both offensive preparation and defensive preparation. (b) information warfare, in its cyber and non-cyber manifestations.

Course duration and scheduling? Part-time and full time, modular short courses, remote learning, high level pre-requisites.

Cost? One tenth of one Baracuda submarine. $500 million over first five years, $100 million recurrent after that. The sending governments would contribute by quota. For example, New Zealand (10 percent), each Australian state government (5 per cent), Australian government (30 per cent); private sector (30 per cent).

Where would we get the staff from? USA, UK, Canada, New Zealand, France, Germany, Spain, Netherlands, Singapore, Israel, Italy, India, and Taiwan. Mix of core full-time staff and adjuncts. Variegated clearance levels for different parts of the campus.

Where would we get students from? Australia, New Zealand, UK, Canada, New Zealand; possibly others in separate learning spaces (i.e. different city)

Curriculum and standards board? Representatives from key agencies and leading civil infrastructure providers; to be chaired by a professor with significant experience in public policy for education in advanced cyber operations, most likely from overseas and participating in Board meetings 2-3 times per year.

Location? Headquarters in or near Canberra; remote learning centres in state capitals or military bases. HQ to be in HMAS Harman?

Reprise [Slide Thirteen]

I have given three broad reasons for the proposal for a National Cyber War College. The first was to satisfy education and training needs for top-end talents. This is a compelling enough reason to consider such a proposal. But when we combine that reason with other two, I think the argument is unassailable. The first additional reason was that we need such a college to be the focal point of strategic goal setting for education and training of high end talents. As well as research on baselines and evidence base for forward development. The second additional reason was the need to create a home for national simulation capability for advanced cyber warfare and crisis management. Australia can copy bits and pieces of what other countries do or it can fashion a response that meets our needs most directly. The National Cyber War College can become part of our deterrent posture for a secure cyber space for Australia. That deterrence can operate in peace time, in low intensity conflict, or in the event of a threat of high intensity conflict.

Prof Greg Austin
Coordinator, Research Group on Cyber Security Education
Coordinator, Research Group on Cyber War and Peace
12 April 2018